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

EXPUNERE DE MOTIVE
la proiectul de decizie a 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

1. Introducere/Contextul european

În ultimii ani, utilizarea reţelelor publice de comunicaţii electronice s-a extins rapid pentru a cuprinde o gamă mult mai largă de servicii şi aplicaţii oferite utilizatorilor, aceştia devenind din ce în ce mai dependenţi de utilizarea acestor reţele şi servicii. Aceste reţele au devenit infrastructuri critice pentru statele membre ale Uniunii Europene, pentru instituţii publice, pentru întreaga economie şi în general pentru societate.

Deoarece reţelele şi serviciile de comunicaţii electronice au rolul de infrastructură/platformă pentru multe aplicaţii, incidentele care afectează securitatea şi integritatea reţelelor şi serviciilor pot avea un impact semnificativ pentru furnizori, pentru utilizatori, dar şi pentru economia naţională.

Serviciile de comunicaţii electronice joacă un rol foarte important în viaţa de zi cu zi a cetăţenilor. Activităţile utilizatorilor rezidenţiali, cât şi ale celor din mediul de afaceri se bazează pe reţelele şi serviciile de comunicaţii electronice a căror importanţă este conştientizată doar în momentul în care acestea devin indisponibile. Totodată şi alte sectoare ale economiei naţionale (energie, transport etc.) se bazează pe infrastructura de comunicaţii, iar breşele de securitate şi pierderea integrităţii reţelelor de comunicaţii pot afecta aceste sectoare într-un mod semnificativ.

Incidentele care afectează reţelele şi serviciile de comunicaţii electronice au următoarele caracteristici principale:

- serviciile de comunicaţii electronice sunt dependente de diverse echipamente interconectate (routere, switch-uri, servere, nume de domeniu, sisteme de transport etc.). Prin urmare, incidentele pot afecta o multitudine de echipamente şi se pot propaga rapid în alte echipamente prin intermediul reţelei;
- vulnerabilităţile în protocoale sau în topologia reţelei pot duce la incidente grave; în special, convergenţa dintre diferite tipuri de reţele poate implica provocări semnificative pentru securitatea reţelelor şi serviciilor de comunicaţii electronice;
- reţelele de comunicaţii şi sistemele de management ale reţelelor şi serviciilor de comunicaţii electronice sunt predispuse la atacuri de tip hacking;
- în plus faţă de atacuri externe, serviciile de comunicaţii electronice pot fi afectate şi de compromiterea securităţii din surse interne (ex: modificări invalide la bazele de date de gestionare a reţelei de către persoanele neautorizate) în mod accidental sau deliberat.

Instituţiile Uniunii Europene au recunoscut importanţa comunicaţiilor electronice, precum şi necesitatea de a extinde eforturile pentru a asigura rezilienţa acestora. În 2006, Comisia Europeană a emis comunicarea privind „O strategie pentru o societate informaţională sigură - Dialog, parteneriat şi responsabilizare" (COM (2006) 251). Una dintre principalele acţiuni anunţate

în această strategie a fost un dialog între părţile interesate cu privire la securitatea şi rezilienţa reţelelor de comunicaţii electronice în cadrul programului european pentru protecţia infrastructurilor critice adoptat de către Comisia Europeană la sfârşitul anului 2006.

În martie 2009, Comisia Europeană a adoptat o comunicare şi un plan de acţiune privind protecţia infrastructurilor critice de informaţii numit „Protejarea Europei de atacuri cibernetice şi perturbaţii de amploare: ameliorarea gradului de pregătire, a securităţii şi a rezilienţei" (COM(2009)149). Această comunicare se concentrează pe „prevenire, pregătire şi conştientizare" şi defineşte un plan de acţiuni imediate pentru consolidarea securităţii şi a rezilienţei infrastructurilor critice de informaţii.

Importanţa colectării datelor privind incidentele care afectează securitatea şi integritatea reţelelor şi serviciilor a fost evidenţiată de Comisia Europeană în mai multe rânduri. În comunicarea „O strategie pentru o societate informaţională sigură - Dialog, parteneriat şi responsabilizare", Comisia Europeană a subliniat faptul că accesul la informaţii complete, corecte, comparabile şi actualizate referitoare la incidente constituie un element necesar pentru a obţine o mai bună înţelegere a nevoii de acţiuni în scopul asigurării securităţii, precum şi pentru a evalua rezultatele măsurilor puse în aplicare anterior (legale, de reglementare, organizatorice şi tehnice).

În Strategia din 2006, Comisia Europeană a propus un parteneriat cu statele membre şi alte părţi interesate pentru a dezvolta un cadru adecvat de colectare a datelor, inclusiv proceduri şi mecanisme pentru colectarea şi analizarea datelor la nivelul UE în ceea ce priveşte incidentele de securitate şi încrederea consumatorilor. În comunicarea privind protecţia infrastructurilor critice de informaţii, Comisia Europeană remarcă faptul că „*Mecanismele de guvernanţă vor fi cu adevărat eficace numai în cazul în care toţi participanţii dispun de informaţii fiabile pentru a acţiona*" şi apoi ia act de faptul că „*procesele şi practicile de monitorizare şi de raportare a incidentelor de securitate a reţelelor diferă de la un stat membru la altul. Unele dintre acestea nu dispun de o organizaţie de referinţă ca punct de monitorizare. Un aspect şi mai important este faptul că schimbul de date concrete privind incidentele de securitate şi cooperarea dintre statele membre par insuficient dezvoltate, desfăşurându-se pe baze informale sau limitându-se la schimburi bilaterale sau, în cazul schimburilor multilaterale, implicând un număr redus de state membre*."

Comisia Europeană a subliniat în comunicarea sa privind protecţia infrastructurilor critice de informaţii că există o incoerenţă în punerea în aplicare a sistemelor de avertizare timpurie, schimbul de informaţii cu privire la incidente şi coordonarea răspunsului la aceste incidente. Sunt necesare sisteme de raportare a incidentelor pentru a permite un răspuns rapid la aceste incidente. Aceste sisteme de raportare ajută, de asemenea, la prevenirea apariţiei unor incidente similare. Comisia a menţionat, de asemenea, nevoia pentru o mai bună coordonare şi cooperare între statele membre. Gradul de interconectare a reţelelor de comunicaţii electronice devine din ce în ce mai mare, iar ameninţările la adresa acestora devin din ce în ce mai complexe şi pot avea un caracter global. În plus, expertiza în ceea ce priveşte ameninţările, precum şi nevoia de a preveni şi a răspunde la incidente devin o necesitate internaţională. Există o mare oportunitate pentru experţii din toate Statele Membre pentru a-şi uni eforturile pentru a îmbunătăţi rezilienţa reţelelor şi serviciilor de comunicaţii electronice.

În primul rând, autorităţile naţionale ar trebui să fie în măsură să implementeze sisteme eficiente de raportare a incidentelor. Ca urmare, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice naţionale va creşte. În al doilea rând, comunicarea între autorităţile naţionale are un rol important în creşterea rezilienţei infrastructurilor de comunicaţii europene.

Cadrul de reglementare, la nivel european, pentru reţelele şi serviciile de comunicaţii electronice adoptat în noiembrie 2009 introduce un nou capitol în vederea îndeplinirii obiectivului de asigurare a unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Astfel, conform pct. 44 din preambulul Directivei 2009/140/CE a Parlamentului European și a Consiliului de modificare a Directivelor 2002/21/CE privind un cadru 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, „*Comunicarea fiabilă și sigură a informațiilor prin rețelele de comunicații electronice este tot mai importantă pentru întreaga economie și în general pentru societate. Complexitatea sistemului, defecțiunile tehnice sau greșelile umane, accidentele sau atacurile, toate acestea pot avea consecințe asupra funcționării și disponibilității infrastructurii fizice care asigură furnizarea de servicii importante cetățenilor UE, inclusiv servicii de e-guvernare. Prin urmare, autoritățile naționale de reglementare*

ar trebui să asigure menţinerea integrităţii și securităţii reţelelor publice de comunicaţii. Agenţia Europeană pentru Securitatea Reţelelor Informatice și a Datelor (ENISA) ar trebui să contribuie la nivelul sporit de securitate a comunicaţiilor electronice, printre altele, prin furnizarea de consultanţă de specialitate și promovarea schimbului de cele mai bune practici. Atât ENISA, cât și 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 sau serviciilor, precum și de a obţine date complete și certe referitoare la incidentele reale privind securitatea care au avut un impact semnificativ asupra funcţionării reţelelor sau serviciilor. (...)"

Conform prevederilor alin. (1) – (3) ale art. 13a din Directiva 2002/21/CE a Parlamentului European și a Consiliului privind un cadru de reglementare comun pentru reţelele și serviciile de comunicaţii electronice (Directiva cadru), astfel cum a fost modificată de Directiva 2009/140/CE a Parlamentului European și a Consiliului:

„(1) Statele membre se asigură că întreprinderile care furnizează reţele publice de comunicaţii sau servicii de comunicaţii electronice accesibile publicului iau măsurile tehnice și organizatorice corespunzătoare pentru a gestiona în mod corespunzător riscurile privind securitatea reţelelor și serviciilor. Ţinând seama de progresele ştiinţifice de la momentul respectiv din domeniu, aceste măsuri trebuie să garanteze un nivel de securitate adecvat riscului existent. În special, trebuie luate măsuri pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor interconectate.

(2) Statele membre se asigură că întreprinderile care furnizează reţele publice de comunicaţii iau toate măsurile necesare pentru a garanta integritatea reţelelor proprii, astfel încât să asigure continuitatea furnizării serviciilor prin intermediul acestor reţele.

(3) Statele membre se asigură că întreprinderile care furnizează reţele publice de comunicaţii sau servicii de comunicaţii electronice accesibile publicului notifică autorităţii naţionale de reglementare competente orice încălcare a normelor de securitate sau pierdere a integrităţii care au avut un impact semnificativ asupra funcţionării reţelelor sau a serviciilor.

După caz, autoritatea naţională de reglementare în cauză informează autorităţile naţionale de reglementare din celelalte state şi Agenţia Europeană pentru Securitatea Reţelelor Informatice şi a Datelor(ENISA). Autoritatea naţională de reglementare respectivă poate informa publicul sau poate solicita întreprinderilor să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării serveşte interesului public.

O dată pe an, autoritatea naţională de reglementare în cauză prezintă Comisiei şi ENISA un raport de sinteză privind notificările primite şi măsurile luate în conformitate cu prezentul alineat."

În cadrul acestui articol este prevăzută obligaţia furnizorilor de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului de a asigura un nivel adecvat al securităţii reţelelor sau serviciilor de comunicaţii electronice. De asemenea, furnizorii de reţele publice de comunicaţii electronice au obligaţia de a lua toate măsurile necesare pentru a garanta integritatea reţelelor proprii, în scopul garantării continuităţii furnizării serviciilor de comunicaţii electronice prin intermediul acestor reţele. În ceea ce priveşte raportarea încălcării normelor de securitate sau a pierderii integrităţii, textul distinge între notificarea transmisă de furnizorii de reţele publice de comunicaţii electronice şi servicii de comunicaţii electronice destinate publicului către autoritatea naţională de reglementare, raportul de sinteză anual către Comisia Europeană şi ENISA, elaborat de autoritatea naţională de reglementare, pe baza notificărilor transmise de furnizori şi notificarea „ad-hoc" a încălcărilor de securitate între autorităţile de reglementare, precum şi între acestea din urmă şi ENISA.

În plus, potrivit art. 13a alin. (4) din Directiva cadru revizuită, Comisia Europeană, ţinând seama în cea mai mare măsură de avizul ENISA, poate adopta măsuri tehnice de punere în aplicare a acestui articol, cu scopul de a armoniza dispoziţiile privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor.

ENISA a fost creată în 2004 şi are rol în asigurarea unui nivel ridicat de securitate a reţelelor informatice şi a datelor în UE, precum şi în armonizarea măsurilor de securitate tehnice şi organizaţionale corespunzătoare, prin următoarele acţiuni: îndrumarea autorităţilor naţionale şi a altor instituţii ale UE în calitate de expert în materie de securitate a reţelelor informatice şi a datelor, îndeplinirea rolului de forum pentru schimbul de bune practici, facilitarea contactelor între instituţiile UE, autorităţile naţionale şi furnizori.

În contextul implementării art. 13a din Directiva cadru revizuită, statele membre se confruntă cu provocarea de a introduce, în reglementările şi practicile lor naţionale, măsuri de

securitate coerente şi armonizate la nivelul Uniunii Europene. Pe de altă parte, există o mare diversitate între statele membre datorită faptului că o parte dintre acestea au stabilit deja un sistem pentru raportarea incidentelor de către furnizorii de comunicaţii electronice (în unele cazuri chiar de ani de zile), însă cele mai multe sunt în stadiu incipient sau sunt încă în faza de planificare a unui astfel de sistem.

În scopul creării acestei baze comune, întemeiată pe numitori comuni în statele membre, ENISA şi statele membre s-au angajat într-o discuţie permanentă (printr-o serie de seminarii, reuniuni, conferinţe telefonice, schimburi de mesaje prin intermediul poştei electronice) în care opiniile, perspectiva şi experienţele din diferite state membre au fost împărtăşite şi evaluate. Scopul colaborării dintre ENISA şi statele membre a fost acela de a găsi o bază care ar putea fi adoptată de către toate statele şi de a crea un cadru prin care diferitele state membre vor comunica într-un „limbaj comun" atât între ele, cât şi cu ENISA şi Comisia Europeană. Colaborarea între Statele Membre şi ENISA a avut ca rezultat elaborarea a două ghiduri *„Technical Guideline on Minimum Security Measures*[1]*"* şi *„Technical Guidelines for Reporting Incidents*[2]*".*

Ghidul *„Technical Guideline on Minimum Security Measures"* îşi propune să sprijine statele membre în implementarea art. 13a, alin. (1) şi (2) din Directiva cadru revizuită, prin stabilirea măsurilor minime de securitate pe care o autoritate de reglementare în comunicaţii ar trebui să le ia în considerare când evaluează gradul de îndeplinire de către furnizorii de reţele şi servicii a obligaţiei de asigurare a securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Acest document îşi propune să ofere o bază pentru o implementare unitară şi armonizată a prevederilor art.13a în ţările membre ale Uniunii Europene.

Ghidul *„Tehnical Guidelines for Reporting Incidents"* îşi propune să sprijine statele membre în implementarea art. 13a, alin. (3) din Directiva cadru revizuită, prin stabilirea condiţiilor în care se realizează notificarea Comisiei Europene şi a ENISA de către autorităţile de reglementare în cazul încălcării normelor de securitate sau al pierderii integrităţii reţelelor, care au avut un impact semnificativ asupra funcţionării reţelelor sau a serviciilor. Totodată, acest ghid constituie o bază de plecare în vederea emiterii de către autorităţile din statele membre a unor reglementări privind circumstanţele, formatul şi procedurile aplicabile în cazul notificărilor pe care trebuie să le transmită furnizorii de reţele publice de comunicaţii electronice şi servicii de comunicaţii electronice destinate publicului acestor autorităţi.

2. Cadrul legal naţional

Ordonanţa de Urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată, cu modificări şi completări, prin Legea nr. 140/2012, include un capitol special dedicat securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice care transpune în legislaţia naţională prevederile Capitolului IIIA din Directiva cadru revizuită, şi are ca scop stabilirea unui cadru general pentru asigurarea utilizării în siguranţă a reţelelor şi serviciilor de comunicaţii electronice, în special prin informarea utilizatorilor în legătură cu incidentele care afectează în mod semnificativ securitatea şi integritatea reţelelor şi serviciilor, precum şi prin stabilirea responsabilităţilor furnizorilor şi a atribuţiilor autorităţii de reglementare în acest domeniu.

Conform art. 46 şi 47 din Ordonanţa de Urgenţă a Guvernului nr. 111/2011:

„Art. 46 - (1) Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a lua toate măsurile tehnice şi organizatorice adecvate pentru a administra riscurile care pot afecta securitatea reţelelor şi serviciilor.

(2) Măsurile luate potrivit alin. (1) trebuie 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.

[1] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/minimum-security-requirements/copy_of_minimum-security-requirements/technical-guideline-on-minimum-security-measures

[2] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/Technical%20Guidelines%20on%20Incident%20Reporting/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting

(3) Furnizorii de reţele publice de comunicaţii electronice au obligaţia de a lua măsurile necesare pentru a garanta integritatea reţelelor şi pentru a asigura continuitatea furnizării serviciilor prin intermediul acestor reţele.

(4) Acolo unde este cazul, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului colaborează pentru implementarea măsurilor prevăzute de prezentul articol.

Art. 47 - (1) Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a notifica ANCOM, în cel mai scurt timp, cu privire la orice încălcare a securităţii sau pierdere a integrităţii care are un impact semnificativ asupra furnizării reţelelor sau serviciilor.

(2) ANCOM poate informa publicul cu privire la existenţa cazului prevăzut la alin. (1) sau poate solicita furnizorului să informeze publicul cu privire la existenţa acestui caz, atunci când consideră că este în interesul public.

(3) Acolo unde consideră necesar, ANCOM informează autorităţile naţionale de reglementare în comunicaţii din alte state membre ale Uniunii Europene şi Agenţia Europeană pentru Securitatea Reţelelor Informatice şi a Datelor cu privire la încălcarea securităţii reţelelor şi serviciilor sau pierderea integrităţii reţelelor.

(4) ANCOM transmite anual un raport succint Comisiei Europene şi Agenţiei Europene pentru Securitatea Reţelelor Informatice şi a Datelor cu privire la notificările primite potrivit alin. (1) şi măsurile adoptate în aceste cazuri."

Astfel, furnizorii de reţele publice de comunicaţii electronice şi servicii de comunicaţii electronice destinate publicului trebuie să ia măsurile tehnice şi organizatorice adecvate pentru a gestiona în mod corespunzător riscurile privind securitatea reţelelor şi serviciilor de comunicaţii electronice, în special pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor interconectate. De asemenea, furnizorii de reţele publice de comunicaţii electronice au obligaţia de a lua toate măsurile necesare pentru a garanta integritatea reţelelor proprii, astfel încât să asigure continuitatea furnizării serviciilor prin intermediul acestor reţele.

Textul legal introduce trei tipuri de raportări privind incidentele care afectează securitatea şi integritatea reţelelor şi serviciilor. În primul rând, furnizorii au obligaţia de a transmite ANCOM, în cel mai scurt timp, informaţii cu privire la încălcarea securităţii sau pierderea integrităţii care are un impact semnificativ asupra furnizării reţelelor sau serviciilor de comunicaţii electronice. Pe baza acestor informaţii, ANCOM poate informa ENISA şi autorităţile de reglementare în comunicaţii din alte state membre ale Uniunii Europene în cazul în care incidentul respectiv este de interes pentru aceste organizaţii. ANCOM va transmite anual Comisiei Europene şi ENISA un raport privind notificările primite de la furnizori şi măsurile adoptate. În plus, atunci când consideră că este în interesul public, ANCOM poate informa publicul sau poate solicita furnizorilor să informeze publicul în cazul producerii incidentelor cu impact semnificativ.

Totodată, art. 48 din Ordonanţa de Urgenţă a Guvernului nr. 111/2011 împuterniceşte ANCOM să stabilească modalitatea de implementare a dispoziţiilor art. 46 şi 47, inclusiv măsurile care definesc circumstanţele, formatul şi procedurile aplicabile în cazul cerinţelor de notificare.

3. Securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

Un produs, sistem sau serviciu este considerat a fi protejat în măsura în care utilizatorii săi se pot baza pe faptul că acesta funcţionează (sau va funcţiona) conform scopului urmărit.

Securitatea reprezintă totalitatea aspectelor care se referă la definirea, realizarea şi menţinerea controlului accesului, autentificării, nerepudierii, confidenţialităţii, integrităţii şi disponibilităţii. Aceste dimensiuni de securitate sunt seturi de măsuri prin care se urmăreşte asigurarea protecţiei în cazul ameninţărilor la adresa securităţii şi nu se limitează doar la modalităţile de administrare a reţelei şi serviciului de comunicaţii electronice, ci se extind la aplicaţii şi la informaţii disponibile prin intermediul serviciilor de comunicaţii electronice şi care sunt accesate de către utilizatorul final. Măsurile de securitate vizează elementele reţelei, serviciile şi aplicaţiile cu scopul de a detecta, anticipa şi corecta vulnerabilităţile de securitate.

Controlul accesului protejează împotriva utilizării neautorizate a resurselor. Această dimensiune asigură faptul că numai personalul autorizat poate accesa elementele reţelei, informaţia stocată, fluxurile de informaţii, serviciile şi aplicaţiile. Autentificarea serveşte confirmării identităţilor celor implicaţi în comunicaţie, asigură validitatea identităţilor pretinse ale entităţilor participante în procesul comunicaţiei (persoană, dispozitiv, serviciu sau aplicaţie).

Nerepudierea asigură mijloace pentru prevenirea unor situaţii în care o entitate ar putea nega realizarea unei anumite acţiuni, reprezentând astfel o modalitate de a dovedi producerea unui eveniment sau a unei acţiuni, precum şi a originii sale. În cadrul securităţii informaţiei, nerepudierea implică faptul că un participant al unui schimb de informaţie nu poate nega trimiterea sau primirea unui mesaj.

Confidenţialitatea este proprietatea informaţiei de a nu fi disponibilă sau dezvăluită unor persoane, entităţi sau procese neautorizate. Confidenţialitatea datelor protejează datele de dezvăluiri neautorizate astfel încât conţinutul nu poate fi înţeles de către entităţi neautorizate. Confidenţialitatea datelor înseamnă protecţia comunicaţiilor sau a datelor stocate împotriva interceptării şi citirii de către persoane neautorizate.

Integritatea reprezintă acea proprietate prin care se protejează acurateţea (exactitatea) şi caracterul complet al resurselor. Integritatea datelor asigură corectitudinea sau acurateţea datelor, fiind proprietatea care demonstrează caracterul nemodificat al acestora, confirmând faptul că datele trimise, primite sau stocate nu sunt modificate sau distruse într-o manieră neautorizată. Pe de altă parte, integritatea este capacitatea sistemului de a-şi păstra atributele specifice din punct de vedere al performanţei şi funcţionalităţii. Integritatea reţelei presupune îndeplinirea funcţiei dorite a reţelei într-o manieră corespunzătoare. Prin urmare, integritatea reţelei poate fi înţeleasă ca fiind capacitatea unei reţele de a menţine şi/sau restabili un nivel acceptabil de performanţă şi funcţionalitate în cazul unor condiţii nefavorabile (defecţiuni, atacuri externe etc.)

Disponibilitatea asigură faptul că nu există refuzul accesului autorizat la elemente ale reţelei, informaţii stocate, fluxuri de informaţii, servicii şi aplicaţii, refuz care poate apărea datorită evenimentelor cu impact asupra reţelei. Disponibilitatea este proprietatea unei resurse de a fi accesibilă la momentul oportun şi uşor de utilizat la cererea unei entităţi autorizate. Protecţia disponibilităţii reţelei înseamnă protecţia capacităţii reţelei de a asigura continuitatea furnizării serviciilor oferite.

Conform Regulamentului (CE) nr. 460/2004 privind instituirea Agenţiei Europene pentru Securitatea Reţelelor Informatice şi a Datelor (ENISA), cu modificările şi completările ulterioare, prin „securitatea reţelelor şi a informaţiilor" se înţelege capacitatea reţelelor sau a sistemelor informatice de a rezista, la un anumit nivel de încredere, la evenimente accidentale sau la acţiuni ilegale sau răuvoitoare care compromit disponibilitatea, autenticitatea, integritatea şi confidenţialitatea datelor stocate sau transmise şi a serviciilor asociate, oferite sau accesibile prin aceste reţele şi sisteme.

Totodată, conform *ETSI EG 202 009-1: „User Group; Quality of telecom services; Part 1: Methodology for identification of parameters relevant to the users"*, securitatea comunicaţiilor electronice este unul dintre criteriile importante după care se evaluează calitatea serviciului (QoS) pentru utilizatorii serviciului respectiv, alături de alte criterii precum disponibilitatea, fidelitatea/acurateţea, viteza, capacitatea, rezistenţa, flexibilitatea, uşurinţa utilizării serviciului.

Conform recomandării *ITU-T X. 805: "Security architecture for systems providing end-to-end communications"*, în scopul de a oferi o soluţie de securitate cap-la-cap, dimensiunile de securitate trebuie aplicate unei ierarhii de echipamente de reţea şi grupări de utilităţi, adică nivelurilor ierarhice de securitate ale unui sistem de comunicaţii.

După funcţionalitatea lor, sunt identificate 3 niveluri de securitate:

- nivelul de securitate a infrastructurii;
- nivelul de securitate a serviciilor;
- nivelul de securitate a aplicaţiilor.

Nivelul de securitate a infrastructurii constă în mijloace de transmisie în cadrul reţelei, precum şi elemente specifice de reţea care sunt protejate de dimensiunile securităţii. Nivelul infrastructură stă la baza construirii reţelelor, serviciilor şi aplicaţiilor.

Nivelul de securitate a serviciilor se referă la securitatea serviciilor de comunicaţii electronice oferite utilizatorilor finali de către furnizori. Acest nivel este utilizat pentru protecţia atât a furnizorilor de servicii, cât şi a utilizatorilor săi împotriva ameninţărilor la adresa securităţii. De exemplu, atacatorii pot încerca să blocheze capacitatea furnizorului de a oferi servicii sau pot încerca să întrerupă un anumit serviciu disponibil utilizatorului.

Nivelul de securitate a aplicaţiilor se referă la securitatea aplicaţiilor disponibile prin intermediul serviciilor de comunicaţii electronice şi care sunt accesate de către utilizatori. Există 4 ţinte pentru atacurile în cadrul acestui nivel: utilizatorii aplicaţiei respective, furnizorii aplicaţiei, furnizorii de servicii de conţinut şi furnizorii de servicii de comunicaţii electronice.

Asigurarea securităţii infrastructurii contribuie într-o bună măsură la asigurarea securităţii serviciilor şi, la rândul ei, asigurarea securităţii serviciilor contribuie la securitatea aplicaţiilor folosite de utilizatorii finali. Fiecare nivel de securitate are vulnerabilităţi diferite şi oferă flexibilitatea combaterii potenţialelor ameninţări în cel mai potrivit mod pentru un anumit nivel de securitate. Dimensiunile de securitate sunt aplicate nivelurilor de securitate pentru a diminua vulnerabilităţile existente la fiecare nivel.

Termenul de „securitate" este utilizat în sensul minimizării vulnerabilităţii resurselor. „Resursele" înseamnă orice prezintă valoare pentru organizaţie, pentru operaţiunile sale de afaceri şi continuitatea acestora. Resursele unei organizaţii care furnizează reţele şi servicii de comunicaţii electronice includ:

a) informaţii: de rutare, de configurare a echipamentelor, referitoare la utilizatorii de servicii, referitoare la serviciile furnizate, la traficul efectuat, taxare, baze de date, documentaţie de sistem, manuale de utilizare, contracte şi acorduri, proceduri operaţionale, materiale pentru instruire, planuri pentru continuitatea afacerii, acorduri privind alternativele disponibile în cazuri de urgenţă, dovezi de audit, înregistrări etc.

b) software: de control al comunicaţiilor, management al operaţiunilor, de management al informaţiilor privind utilizatorii, de taxare, de aplicaţii, de sistem, de dezvoltare şi utilităţi etc.

c) fizice: clădiri, echipamente de comutare sau rutare, sisteme de transmisie, echipamente terminale, mediile utilizate pentru transmiterea semnalelor, servere şi staţii de lucru, medii mobile etc.

d) servicii: de procesare a informaţiilor, de reţea, utilităţi suport (alimentare cu energie electrică, iluminat, control al temperaturii şi umidităţii, stingere a incendiilor) etc.

e) oameni: ingineri de comunicaţii, specialişti IT etc.

f) intangibile: controlul organizaţiei, „know-how" etc.

În dezvoltarea oricărui cadru de lucru privind securitatea, este importantă cunoaşterea resurselor ce trebuie protejate, a ameninţărilor asupra acestor resurse, a vulnerabilităţilor asociate, precum şi a riscului global asupra resurselor, risc provenit din ameninţări şi vulnerabilităţi. Ameninţările, vulnerabilităţile şi riscurile sunt elementele fundamentale care trebuie luate în considerare în vederea asigurării securităţii.

Ameninţarea reprezintă o posibilă încălcare a securităţii. Exemple de ameninţări pot fi:

- dezvăluirea neautorizată a informaţiilor;
- distrugerea neautorizată sau modificarea datelor, echipamentelor sau altor resurse;
- furtul, îndepărtarea sau pierderea resurselor;
- întreruperea sau refuzul serviciilor;
- identificarea în mod fraudulos cu o entitate autorizată.

Ameninţările pot fi accidentale sau intenţionate, active sau pasive. O ameninţare accidentală este aceea fără intenţie premeditată, de exemplu o defecţiune software sau o eroare fizică. O ameninţare intenţionată este realizată de către o persoană ce comite un act deliberat (atunci când o ameninţare intenţionată are ca rezultat o acţiune, acea acţiune se numeşte atac). O ameninţare activă este, de exemplu, alterarea datelor sau distrugerea unui echipament fizic. O astfel de ameninţare implică schimbarea stării resurselor implicate.

O vulnerabilitate este un defect sau o slăbiciune a unei resurse sau grup de resurse care poate fi exploatată de una sau mai multe ameninţări. Vulnerabilitatea este acea slăbiciune în proiectarea, implementarea, operarea sau controlul intern al unui proces care ar putea expune sistemul la ameninţări.

Riscul reprezintă probabilitatea ca o vulnerabilitate din sistem să afecteze securitatea, precum şi severitatea efectului determinat de utilizarea intenţionată sau neintenţionată a unei astfel de vulnerabilităţi. Riscul este o mărime a efectelor contrare care pot rezulta dacă o vulnerabilitate este exploatată de către o ameninţare. Riscul nu poate fi total eliminat, de aceea unul dintre obiectivele securităţii este de a reduce riscul la un nivel acceptabil. Pentru realizarea acestui obiectiv, este necesară înţelegerea ameninţărilor şi vulnerabilităţilor şi aplicarea măsurilor de contracarare potrivite (servicii si mecanisme de securitate). Determinarea riscului trebuie să identifice, să cuantifice şi să stabilească prioritatea tratării riscului prin prisma criteriilor de risc acceptabil şi a obiectivelor relevante pentru organizaţie.

În înţelesul acestei decizii, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice se defineşte astfel: 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.

4. Măsuri de securitate

4.1 Definire şi scop

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

Astfel de măsuri pot fi preventive, corective sau de detectare. Măsurile preventive reduc vulnerabilităţile şi probabilitatea de apariţie a unui incident, implementarea lor conducând de exemplu la insuccesul unui potenţial atac. Măsurile corective reduc impactul/efectele unui incident şi restabilesc funcţionarea/operarea în condiţii normale. Măsurile de detectare descoperă incidente/atacuri şi activează măsuri preventive sau corective.

O securitate adecvată a reţelelor şi serviciilor de comunicaţii electronice se poate realiza prin punerea în aplicare a unui set adecvat de măsuri de securitate. Aceste măsuri trebuie stabilite şi implementate în funcţie de profilul organizaţiei şi condiţiile operaţionale şi trebuie monitorizate şi îmbunătăţite în mod continuu. Furnizorii de reţele şi servicii de comunicaţii electronice trebuie să adopte măsuri de securitate conform riscurilor evaluate, aceste măsuri tehnice şi organizatorice fiind menite să prevină şi să limiteze impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor interconectate, asigurând continuitatea furnizării serviciilor prin intermediul reţelelor. Reţelele de comunicaţii electronice trebuie planificate, construite, operate şi întreţinute astfel încât să funcţioneze în siguranţă, fiabilitatea şi rezilienţa acestora putând fi obţinută în urma implementării măsurilor adecvate de securitate.

Măsurile de securitate se aplică tuturor resurselor identificate în cadrul procesului de identificare a riscurilor (informaţii, resurse software, hardware, servicii, utilităţi, resurse umane etc.), resurse care, în cazul în care sunt afectate, pot compromite securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. Identificarea resurselor, evidenţierea caracteristicilor acestora, clasificarea acestora, precum şi conştientizarea importanţei lor fac posibilă o implementare corespunzătoare a măsurilor de securitate.

Măsurile de securitate sunt selectate luând în considerare riscurile existente în cadrul organizaţiei. Cerinţele 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. Măsurile de securitate pot preveni posibile incidente, pot limita consecinţele incidentelor atunci când acestea au loc sau pot asigura rectificarea rapidă şi eficientă a întreruperilor serviciilor de comunicaţii electronice, restabilind furnizarea la condiţii normale şi trebuie să acopere orice condiţii de operare (operare normală, cu întreruperi), diverse tipuri de incidente şi evenimente de securitate, precum şi situaţii de urgenţă, cazuri de dezastru sau crize majore.

Asigurarea unui nivel adecvat de securitate este un proces continuu de punere în aplicare, revizuire, actualizare a măsurilor de securitate. Efectele măsurilor de securitate trebuie monitorizate. Este posibil ca setul măsurilor de securitate selectate să nu poată realiza o securitate „totală”, fiind astfel necesare acţiuni suplimentare pentru monitorizarea, evaluarea şi îmbunătăţirea eficienţei măsurilor de securitate în sprijinul atingerii obiectivelor de securitate.

Pentru a fi eficiente, măsurile de securitate trebuie avute în vedere în faza de stabilire a cerinţelor sistemelor, proiectelor etc. În caz contrar, se pot înregistra costuri suplimentare şi pot fi adoptate soluţii ineficiente, putându-se ajunge la imposibilitatea realizării unei securităţi adecvate.

Măsurile de securitate au ca obiective principale reducerea semnificativă a numărului de incidente şi întreruperi operaţionale, a fraudelor, prevenirea pierderii, distrugerii, furtului sau compromiterii resurselor, îmbunătăţirea calităţii serviciilor oferite utilizatorilor, creşterea încrederii utilizatorilor în serviciile furnizate de organizaţii.

Ca rezultat al implementării măsurilor de securitate adecvate, furnizorii de reţele şi servicii de comunicaţii electronice vor fi capabili să asigure o securitate şi integritate adecvată a reţelelor şi serviciilor de comunicaţii electronice, vor avea o abordare clară şi completă asupra tuturor

activităţilor aferente acestui domeniu, vor deţine capacităţile restabilirii serviciilor la condiţii normale de funcţionare în cazul apariţiei incidentelor, vor reuşi să conştientizeze personalul organizaţiilor şi utilizatorii asupra importanţei securităţii şi vor spori încrederea acestora în serviciile oferite, ansamblul măsurilor de securitate contribuind semnificativ la îmbunătăţirea calităţii serviciilor şi la asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice.

4.2 Nivelul actual al securităţii şi integrităţii reţelelor şi serviciilor

ANCOM şi-a propus stabilirea măsurilor minime de securitate ce trebuie implementate de către furnizorii de reţele şi servicii de comunicaţii electronice. Astfel, în vederea analizării/estimării nivelului de securitate şi integritate al reţelelor şi serviciilor de comunicaţii electronice existent la momentul actual şi identificării măsurilor ce sunt deja implementate, în luna iulie 2012, ANCOM a transmis către cei mai importanţi 20 de furnizori de reţele şi servicii de comunicaţii electronice, din punct de vedere al numărului de utilizatori şi al acoperirii reţelei, un chestionar privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. Chestionarul a cuprins 43 de întrebări structurate în 7 mari teme: aspecte generale privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, managementul riscului, măsuri privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, monitorizarea incidentelor, informarea utilizatorilor cu privire la incidentele semnificative, testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, costul şi beneficiile măsurilor de securitate.

În urma analizării răspunsurilor[3] primite de la cei 20 de furnizori de reţele şi servicii de comunicaţii electronice la chestionarul transmis de ANCOM, a rezultat că majoritatea dintre aceştia au o preocupare activă în asigurarea securităţii şi integrităţii reţelelor şi serviciilor. Cu toate acestea, doar o parte dintre furnizori au 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, 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. Prin urmare, domeniul securităţii şi integrităţii nu este abordat unitar de către furnizorii chestionaţi. Acest fapt se datorează şi inexistenţei unui standard internaţional pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor, standardul utilizat preponderent de respondenţi fiind ISO/CEI 27001, standard ce se referă în principal la securitatea informaţiei.

Majoritatea furnizorilor au indicat că deţin o politică privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, însă din celelalte răspunsuri nu a reieşit o direcţie clară de acţiune pe care o politică adecvată ar trebui să o impună.

Managementul riscului este un proces continuu şi trebuie să fie parte integrantă a tuturor activităţilor desfăşurate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor. Cu toate că managementul riscurilor constituie un domeniu fundamental pe baza căruia ar trebui luată decizia stabilirii măsurilor de securitate, din răspunsurile multor furnizori a rezultat că acestui domeniu i se acordă un interes scăzut, analiza de risc nefiind completă în multe cazuri sau chiar lipsind cu desăvârşire. Astfel, rezultă că un număr relativ redus de furnizori au proceduri documentate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice (proceduri ce includ analiza corectă, completă a riscurilor), măsurile privind securitatea şi integritatea fiind luate de unii furnizori ad-hoc, în urma detecţiei unor probleme/apariţiei unor incidente.

Majoritatea furnizorilor chestionaţi monitorizează incidentele petrecute în reţea, însă nu toţi au proceduri în vederea tratării incidentelor, în cazul acestora acţiunile şi deciziile fiind luate în momentul apariţiei incidentului.

În ceea ce priveşte testarea securităţii şi integrităţii reţelelor şi serviciilor, o mare parte a furnizorilor nu efectuează o astfel de activitate, nefiind astfel la curent cu vulnerabilităţile existente/actuale. Din răspunsurile primite, a reieşit că doar 7 furnizori efectuează audituri de securitate pentru a se asigura că securitatea şi integritatea reţelelor este una adecvată.

În ceea ce priveşte informarea utilizatorilor cu privire la incidentele semnificative, din răspunsurile furnizorilor a reieşit că majoritatea dintre aceştia îşi informează utilizatorii doar în măsura existenţei unor solicitări ale acestora şi a reclamaţiilor primite, noţiunea de „incident

[3] Raportul privind aspectele constatate în urma analizării răspunsurilor furnizorilor se găseşte la adresa: http://www.ancom.org.ro/uploads/links_files/Raport_masuri_securitate_implementate_fz.pdf

semnificativ" fiind totodată percepută în mod diferit în rândul respondenţilor. Niciun furnizor nu şi-a informat utilizatorii din proprie iniţiativă cu privire la un incident semnificativ, principala motivaţie fiind inexistenţa vreunui incident semnificativ în ultimele 12 luni şi doar 2 furnizori au adus detalii privind desfăşurarea (în ultimele 12 luni) a unor campanii pentru conştientizarea de către clienţi a existenţei fraudelor sau a altor aspecte ce pot afecta securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Majoritatea furnizorilor chestionaţi au recunoscut necesitatea/beneficiile stabilirii unor măsuri minime de securitate şi integritate ce ar trebui respectate de către furnizorii de reţele şi servicii de comunicaţii electronice, printre cele mai importante beneficii regăsindu-se asigurarea continuităţii serviciilor oferite către clienţi, protejarea datelor personale ale clienţilor şi angajaţilor, păstrarea confidenţialităţii, integrităţii şi disponibilităţii resurselor organizaţiei, reducerea numărului incidentelor de securitate şi a reclamaţiilor la adresa securităţii, îmbunătăţirea controlului sistemelor şi proceselor interne ale organizaţiilor, îmbunătăţirea calităţii serviciului, reducerea riscurilor în privinţa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

Ca urmare a analizării răspunsurilor la chestionar, ANCOM consideră că este necesară stabilirea unor linii directoare în scopul asigurării unei securităţi şi integrităţi adecvate a reţelelor şi serviciilor. Astfel, ANCOM îşi propune - prin proiectul de decizie privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de reţele publice sau de servicii de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice - stabilirea domeniilor pe care trebuie să le vizeze măsurile de securitate adoptate de furnizori.

4.3 Obligaţiile ce incumbă furnizorilor de reţele şi servicii de comunicaţii electronice

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a lua toate măsurile tehnice şi organizatorice adecvate pentru a administra riscurile care pot afecta securitatea reţelelor şi serviciilor de comunicaţii electronice, în scopul prevenirii sau minimizării impactului incidentelor de securitate asupra utilizatorilor şi reţelelor interconectate, având în vedere cele mai noi tehnologii. De asemenea, furnizorii de reţele publice de comunicaţii electronice au obligaţia de a lua toate măsurile necesare pentru a garanta integritatea reţelelor proprii, astfel încât să asigure continuitatea furnizării serviciilor prin intermediul acestor reţele. Măsurile minime pe care trebuie să le stabilească şi să le implementeze furnizorii astfel încât să îndeplinească această obligaţie vor viza cel puţin următoarele domenii:

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;

Obiectivul urmărit prin stabilirea acestui domeniu îl constituie angajarea conducerii organizaţiei şi sprijinirea demersurilor legate de asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Conducerea organizaţiei trebuie să stabilească o direcţie clară a politicii de securitate şi să demonstreze susţinerea şi angajamentul său pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor. Politica de securitate trebuie aprobată de către conducerea organizaţiei şi comunicată angajaţilor şi părţilor terţe relevante într-o formă accesibilă şi inteligibilă.

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.

Managementul riscului trebuie să fie parte integrantă a tuturor activităţilor desfăşurate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor. Managementul riscului trebuie să fie un proces continuu care să stabilească contextul (domeniul de aplicare şi limitele acestuia, precum şi criteriile de bază necesare procesului de management al riscului), să identifice, să estimeze, să evalueze şi să trateze riscurile. Riscurile sunt identificate, cuantificate, prioritizate prin prisma criteriilor de risc acceptate şi a obiectivelor relevante pentru organizaţie. Rezultatele acestor procese determină acţiunile organizaţiei şi priorităţile pentru managementul riscurilor de securitate şi pentru implementarea măsurilor de securitate selecţionate în vederea protecţiei împotriva riscurilor.

Organizaţia trebuie să definească domeniul de aplicare şi limitele managementului riscului. Domeniul de aplicare al procesului de management al riscului trebuie definit astfel încât să asigure că toate resursele relevante sunt luate în considerare în cadrul evaluării riscului. Managementul riscului trebuie să vizeze criterii de bază precum: criterii de evaluare a riscului, criterii pentru stabilirea impactului, criterii de acceptare a riscului.

Scopul identificării riscurilor este determinarea a ceea ce ar putea cauza o întrerupere în asigurarea continuităţii furnizării reţelelor şi serviciilor (breşă de securitate sau o pierdere a integrităţii), precum şi obţinerea informaţiilor privind modul şi locul producerii acestei întreruperi. Procesul de elaborare a unui inventar al resurselor este o premisă importantă de gestionare a riscurilor. O organizaţie trebuie să identifice toate resursele şi să documenteze importanţa acestora în furnizarea reţelelor şi serviciilor de comunicaţii electronice. Ameninţările şi sursele acestora trebuie identificate. Ameninţările pot fi naturale sau de origine umană, pot fi accidentale sau intenţionate. Trebuie identificate vulnerabilităţile care pot fi exploatate de către ameninţări şi astfel pot aduce prejudicii resurselor organizaţiei. Trebuie identificate consecinţele pe care un incident le poate avea asupra resurselor. Această activitate identifică prejudiciile sau consecinţele ce pot fi cauzate de un scenariu al unui incident. Impactul unui incident se determină pe baza criteriului de stabilire a impactului.

Pe baza listei cu scenariile incidentelor relevante identificate, incluzând identificarea ameninţărilor, a vulnerabilităţilor, a resurselor ce pot fi afectate, a consecinţelor asupra resurselor şi a listelor cu măsurile existente şi planificate, trebuie evaluat impactul pe care incidentele le-ar putea avea asupra securităţii şi integrităţii reţelelor şi serviciilor, precum şi probabilitatea de apariţie a incidentelor. Riscul estimat reprezintă combinaţia dintre probabilitatea apariţiei/producerii unui incident şi consecinţele sale.

Nivelurile de risc trebuie comparate în funcţie de criteriile de evaluare şi cele de acceptare a riscului. Pentru a evalua riscurile, organizaţiile trebuie să compare riscurile estimate cu criteriul de evaluare a riscurilor definit în timpul stabilirii contextului. În urma evaluării riscului, rezultă priorităţi pentru tratarea riscului considerând nivelurile estimate de risc şi necesitatea luării unor măsuri/desfăşurării unor activităţi.

Pentru tratarea riscului, sunt valabile 3 opţiuni: reducerea, evitarea şi acceptarea riscului. Opţiunile pentru tratarea riscului trebuie selectate pe baza rezultatului determinării (identificării, estimării şi evaluării) riscului, precum şi a beneficiilor şi a costurilor preconizate pentru implementarea acestor opţiuni. După ce a fost realizată tratarea riscului, trebuie determinate riscurile reziduale, ceea ce implică o nouă iteraţie a determinării riscului ţinând cont de efectele preconizate ale opţiunii de tratare a riscului propusă. În anumite circumstanţe, atunci când revizuirea criteriului de acceptare a riscului nu se poate realiza în timp util, apare necesitatea acceptării anumitor riscuri reziduale care nu îndeplinesc acest criteriu. Astfel de situaţii pot fi motivate de unele constrângeri (temporare sau permanente) de ordin tehnic, financiar sau operaţional (de exemplu atunci când costurile aferente reducerii riscului sunt foarte ridicate, în situaţia în care reducerea sau evitarea unor riscuri implică apariţia altor riscuri).

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

Pentru a reduce riscurile la adresa securităţii şi integrităţii reţelelor şi serviciilor, conducerea organizaţiei, angajaţii, contractorii şi alte părţi terţe trebuie să înţeleagă responsabilităţile ce le revin şi să deţină cunoştinţe corespunzătoare rolurilor alocate.

Conducerea organizaţiei trebuie să susţină în mod activ asigurarea securităţii şi integrităţii reţelelor şi serviciilor şi trebuie să ceară angajaţilor şi părţilor terţe să aplice măsuri de securitate în conformitate cu politicile stabilite şi cu procedurile organizaţiei.

Trebuie definite clar responsabilităţile pentru protecţia resurselor şi pentru desfăşurarea proceselor de securitate. Dacă angajaţii nu sunt conştienţi de responsabilităţile lor legate de asigurarea securităţii, aceştia pot produce pagube considerabile organizaţiei. Organizaţiile ar trebui să numească ingineri de telecomunicaţii şi alte categorii de personal care au acreditările, cunoştinţele şi competenţele potrivite pentru a fi responsabili de supravegherea aspectelor legate de instalarea, întreţinerea, operarea şi controlul reţelelor de comunicaţii electronice.

Condiţiile contractului de angajare sau fişele de post pot fi utilizate pentru susţinerea cu documente a rolurilor şi responsabilităţilor privind 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 asigurarea întreţinerii sau gestiunii de către terţe părţi a produselor şi serviciilor (servicii IT, software, interconectare, baze de date, facilităţi asociate etc).

Obiectivul acestui domeniu îl constituie asigurarea securităţii produselor şi serviciilor achiziţionate de la părţi externe, accesate sau administrate de către părţi externe. Securitatea şi integritatea reţelelor şi serviciilor nu ar trebui să fie redusă prin introducerea de produse şi servicii provenite de la terţi. În cazul externalizării unor activităţi, responsabilitatea privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor revine în întregime organizaţiei.

Riscurile la adresa securităţii şi integrităţii reţelelor şi serviciilor provenite de la procese care implică părţi externe trebuie să fie identificate şi trebuie luate măsuri de securitate corespunzătoare. În general, toate cerinţele de securitate presupuse de lucrul cu părţi externe trebuie să se regăsească într-un acord încheiat cu partea externă care să asigure o securitate adecvată. Partea externă trebuie să fie conştientă de obligaţiile ce îi revin şi trebuie să accepte responsabilităţile şi obligaţiile implicate de asigurarea unei securităţi corespunzătoare. În plus, organizaţia trebuie să se asigure printr-o monitorizare şi evaluare continuă a faptului că serviciile şi produsele furnizate de partea externă respectă cerinţele de securitate stabilite şi că incidentele şi problemele de securitate sunt tratate în mod corespunzător.

În ceea ce priveşte relaţia cu utilizatorii serviciilor şi reţelelor de comunicaţii electronice, organizaţia trebuie să se asigure că există o delimitare clară a responsabilităţilor în ceea ce priveşte infrastructura proprie şi cea a utilizatorilor de servicii de comunicaţii electronice. Atunci când furnizorul instalează echipamente la sediul utilizatorilor în scopul furnizării serviciului, acestea ar trebui să fie protejate în scopul de a reduce riscul ameninţărilor de mediu, precum şi riscul de acces neautorizat. În plus, este recomandat ca starea şi disponibilitatea echipamentelor să fie monitorizate de la distanţă. În ceea ce priveşte contractul încheiat între furnizorul de reţele şi servicii de comunicaţii electronice şi utilizatori, acesta trebuie să cuprindă, conform art.51 alin.(1) lit.h) din Ordonanţa de Urgenţă a Guvernului nr.111/2011 „*categoriile de măsuri ce pot fi luate de furnizori în cazul apariţiei unor incidente, ameninţări şi vulnerabilităţi privind securitatea sau integritatea reţelei sau serviciilor*". Astfel, în caz de incidente, ameninţări şi vulnerabilităţi privind securitatea sau integritatea reţelelor sau serviciilor, furnizorii trebuie să prevadă în contracte tipul de acţiune pe care ar putea să o întreprindă şi impactul acesteia asupra continuităţii furnizării reţelelor şi serviciilor la un nivel normal (limitare, restricţionare, întrerupere sau suspendare a serviciului), impactul asupra utilizatorului şi condiţiile în care se pot produce aceste acţiuni.

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;

Angajaţii, contractorii şi alte părţi terţe trebuie să corespundă rolurilor alocate în organizaţie sau în relaţia cu aceasta. Verificările vor avea în vedere normele legale privind protejarea datelor cu caracter personal, a vieţii private şi din domeniul legislaţiei muncii. Procedurile organizaţiei vor defini criteriile şi limitele verificărilor (cine poate efectua verificarea, cum, când şi de ce se

efectuează verificările). Organizaţiile ar trebui să ia în considerare, de asemenea, verificări mai detaliate pentru posturi care dau accesul personalului la sistemele critice pentru furnizarea de reţele şi servicii, la informaţii referitoare la interceptarea legală, precum şi accesul la informaţiile despre clienţi (ex: informaţii personale, date de trafic).

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

Angajaţii şi, acolo unde este relevant, alte părţi terţe, trebuie să primească o instruire corespunzătoare şi actualizări periodice în ceea ce priveşte politicile şi procedurile organizaţionale, ţinând cont de atribuţiile specifice funcţiei lor, în vederea asigurării unui nivel adecvat de conştientizare şi educaţie în ceea ce priveşte securitatea şi integritatea reţelelor şi serviciilor şi pentru utilizarea corectă a resurselor organizaţiei.

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

Obiectivul acestui domeniu este ca organizaţia să se asigure că responsabilităţile legate de încetarea contractului de muncă sau schimbarea locului de muncă sunt clar definite şi alocate. Angajaţii care părăsesc organizaţia trebuie să returneze organizaţiei resursele pe care le deţin sau le utilizează în numele său pentru respectiva organizaţie, iar drepturile de acces trebuie revocate. Dacă angajatul deţine cunoştinţe importante pentru operaţiile în curs de derulare, aceste informaţii trebuie documentate şi transferate organizaţiei. În cazul schimbării locului de muncă în cadrul aceleiaşi organizaţii, drepturile de acces trebuie ajustate astfel încât să reflecte noua poziţie in organizaţie.

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

Scopul procesului disciplinar este de a preveni şi descuraja încălcarea de către angajaţi a politicilor şi procedurilor organizaţiei referitoare la asigurarea securităţii şi integrităţii reţelelor şi serviciilor.

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);

În vederea prevenirii accesului fizic neautorizat, a distrugerilor, a pătrunderii în interiorul organizaţiei, a deteriorării echipamentelor şi a accesului neautorizat la informaţii, centrele de comunicaţii (centrele de comutaţie, centrele de control şi operare etc.) trebuie amplasate în zone sigure (teren rigid, mediu care nu este afectat de deteriorări produse de vânt şi apă, mediu care nu este afectat de deteriorări produse de perturbaţii/interferenţe electromagnetice etc.), trebuie să fie rezistente la cutremure şi la foc şi trebuie protejate de un perimetru de securitate definit (existenţa barierelor fizice, a unor sisteme adecvate de detectare a intruziunilor etc.). Zonele de securitate trebuie protejate prin măsuri adecvate de control al accesului pentru a se asigura că accesul este permis doar personalului autorizat. Organizaţia trebuie să proiecteze şi să aplice măsuri de protecţie fizică împotriva incendiilor, inundaţiilor, cutremurelor, exploziilor, tulburărilor publice şi a oricăror alte forme de dezastre naturale sau produse de oameni.

Protejarea echipamentelor este necesară pentru reducerea riscului de acces neautorizat şi pentru protejare împotriva distrugerilor şi a pierderilor. Trebuie adoptate măsuri de securitate pentru minimizarea riscurilor privind potenţialele ameninţări fizice (furt, foc, apă, praf, vibraţii, substanţe chimice, radiaţii electromagnetice, vandalism etc.). Echipamentele care necesită o protecţie specială trebuie izolate pentru a reduce nivelul general de protecţie necesar. Condiţiile de mediu care ar putea afecta negativ funcţionarea sistemelor de comunicaţii (temperatură, umiditate etc.) ar trebui monitorizate.

În ceea ce priveşte securitatea cablurilor folosite în transportul semnalelor, acestea trebuie protejate împotriva deteriorării şi interceptării (ex: amplasarea subterană, folosirea fibrei optice, protecţia electromagnetică corespunzătoare etc.) şi trebuie identificate clar pentru a minimiza erorile de manipulare.

Pentru zonele izolate unde sunt instalate echipamente de comunicaţii (ex: staţii de bază în reţele mobile), trebuie proiectate, dezvoltate şi puse în aplicare măsuri de securitate speciale pentru a asigura securitatea fizică. Echipamentele trebuie monitorizate de la distanţă pentru a verifica disponibilitatea, alimentarea cu energie, condiţiile de mediu etc. şi pentru a detecta incidentele.

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

Furnizarea reţelelor şi serviciilor de comunicaţii electronice depinde într-o mare măsură de utilităţile suport, în special de furnizarea de energie electrică. Astfel, echipamentele ar trebui protejate împotriva penelor de curent sau a altor întreruperi cauzate de probleme ale utilităţilor suport. Pentru a asigura continuitatea alimentării cu energie electrică, pot fi utilizate mai multe căi de alimentare, astfel încât căderea uneia să nu împiedice furnizarea reţelelor şi serviciilor sau/şi pot fi folosite baterii sau generatoare de curent. În plus, trebuie luate măsuri şi pentru asigurarea funcţionării adecvate a celorlalte utilităţi suport (alimentare cu apă, aer condiţionat etc.).

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

Organizaţia trebuie să asigure accesul autorizat al angajaţilor şi să prevină accesul neautorizat la resursele organizaţiei. Pentru controlul alocării drepturilor de acces la sisteme şi servicii, trebuie instituite proceduri care să acopere toate etapele din perioada în care utilizatorului i se permite accesul, pornind de la înregistrarea de noi utilizatori până la anularea înregistrării utilizatorilor care nu mai necesită acces la resursele organizaţiei. Utilizatorii trebuie să fie informaţi despre responsabilităţile lor în menţinerea unui sistem eficient de control al accesului, în special în privinţa folosirii parolelor şi a securităţii echipamentelor. Sistemele critice în furnizarea reţelelor şi serviciilor de comunicaţii electronice trebuie să aibă alocat un spaţiu dedicat (izolat).

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.

Reţelele de comunicaţii trebuie să fie protejate corespunzător în scopul de a preveni şi detecta atacurile realizate cu ajutorul programelor maliţioase, precum şi tentativele de a indisponibiliza sau bloca resurse/servicii, acţiuni ce pot afecta furnizarea reţelelor şi serviciilor. Protecţia împotriva codurilor cu potenţial dăunător trebuie să se bazeze pe programe de detectare şi reparare/recuperare, pe conştientizarea nevoii de securitate şi pe gestionarea corespunzătoare a accesului la sistemele de comunicaţii.

În scopul de a proteja echipamentele care utilizează protocolul IP (servere, routere etc.) de atacuri informatice (ex. DoS/DDoS), organizaţia trebuie să stabilească şi să implementeze măsuri de contracarare a unor astfel de atacuri în scopul de a asigura continuitatea furnizării reţelelor şi serviciilor (ex: mecanisme de filtrare a pachetelor de date, restricţii ale porturilor de comunicaţii folosite pentru atacurile informatice, reducerea sau suspendarea activităţii unor echipamente).

Dat fiind faptul că atacurile informatice pot fi generate din foarte multe reţele localizate în spaţii geografice diferite, este recomandabil ca furnizorii să lucreze în strânsă colaborare cu ceilalţi furnizori, precum şi cu organizaţiile interne şi internaţionale cu atribuţii şi competenţe în răspunsul la atacurile informatice.

În scopul împiedicării atacurilor informatice iniţiate de la computerele infectate ale utilizatorilor de servicii de comunicaţii electronice, furnizorii trebuie să precizeze în contractele încheiate cu aceştia măsurile ce pot fi luate în cazul apariţiei unor incidente, ameninţări (restricţionarea, suspendarea serviciului etc.). În acelaşi timp, furnizorii ar trebui să atragă atenţia utilizatorilor cu privire la ameninţările existente în mediul electronic (viruşi, botnet etc.) şi să îi încurajeze să ia măsurile de protecţie necesare.

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;

Pentru a se asigura instalarea, operarea, controlul şi întreţinerea în mod corect şi în condiţii de securitate a reţelei prin care se furnizează serviciile de comunicaţii electronice, trebuie stabilite responsabilităţi şi proceduri privind managementul, instalarea, utilizarea/operarea adecvată a resurselor hardware şi software. Procedurile operaţionale trebuie să fie documentate, păstrate şi puse la dispoziţia tuturor celor avizaţi. Procedurile trebuie să specifice instrucţiunile detaliate pentru execuţia fiecăreia dintre activităţile prevăzute mai sus.

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

Controlul neadecvat al schimbărilor în reţelele de comunicaţii electronice şi în software-ul de aplicaţii constituie o cauză frecventă a defecţiunilor şi a breşelor de securitate. Schimbările suferite de mediul operaţional, în special atunci când se transferă un sistem din faza de dezvoltare în cea operaţională, pot afecta securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. Schimbările în sistemele operaţionale trebuie realizate numai atunci când există motive întemeiate.

În vederea asigurării unui nivel de performanţă corespunzător şi pentru a reduce riscurile şi disfuncţionalităţile sistemelor, este necesară o planificare şi o pregătire prealabilă. Utilizarea resurselor trebuie să fie monitorizată şi optimizată, iar modificările sistemelor şi software-urilor trebuie prevăzute din timp. Trebuie instituite măsuri de detectare, pentru identificarea din timp a posibilelor probleme (ex: creşterea riscului la care este supus un anumit sistem) şi trebuie planificate acţiuni corective adecvate.

Trebuie menţinut un control strict asupra schimbărilor efectuate în sistemele operaţionale şi în software-ul de aplicaţii având în vedere, în principal, următoarele aspecte: identificarea şi înregistrarea schimbărilor semnificative, planificarea şi testarea schimbărilor, evaluarea impactului potenţial, inclusiv asupra securităţii şi integrităţii reţelelor şi serviciilor, proceduri de rezervă pentru recuperare în caz de schimbări nereuşite sau evenimente neprevăzute.

Introducerea unor sisteme noi şi schimbările majore aduse celor existente trebuie să urmeze un proces de documentare, specificare, testare, control al calităţii şi implementare controlată. Acest proces trebuie să cuprindă o determinare a riscului, o analiză a impactului modificărilor şi o specificare a măsurilor de securitate necesare. Totodată, acest proces trebuie să asigure necompromiterea securităţii şi a procedurilor existente.

Atunci când se efectuează schimbări, trebuie păstrat un jurnal care să conţină toate informaţiile relevante referitoare la aceste schimbări.

Trebuie realizate estimări şi planificări privind cerinţele necesare în vederea atingerii performanţelor/capacităţilor adecvate.

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

În vederea asigurării unei protecţii corespunzătoare a resurselor organizaţiei, toate resursele trebuie înregistrate şi trebuie să aibă un deţinător autorizat. Resursele organizaţiei au un grad diferit de sensibilitate şi importanţă în activitatea de furnizare a reţelelor şi serviciilor, astfel încât, pentru asigurarea unui grad de protecţie adecvat şi pentru stabilirea unor măsuri de utilizare corespunzătoare, acestea trebuie clasificate în mod corespunzător.

Resursele unui furnizor de reţele şi servicii de comunicaţii electronice includ:

a) informaţii: de rutare, de configurare a echipamentelor, referitoare la utilizatorii de servicii, referitoare la serviciile furnizate, la traficul efectuat, taxare, baze de date, documentaţie de sistem, manuale de utilizare, contracte şi acorduri, proceduri operaţionale, materiale pentru instruire, planuri pentru continuitatea afacerii, acorduri privind alternativele disponibile în cazuri de urgenţă, dovezi de audit, înregistrări etc.

b) software: de control al comunicaţiilor, management al operaţiunilor, de management al informaţiilor privind utilizatorii, de taxare, de aplicaţii, de sistem, de dezvoltare şi utilităţi etc.

c) fizice: clădiri, echipamente de comutare sau rutare, sisteme de transmisie, echipamente terminale, mediile utilizate pentru transmiterea semnalelor, servere şi staţii de lucru, medii mobile etc.

d) servicii: de procesare a informaţiilor, de reţea, utilităţi suport (alimentare cu energie electrică, iluminat, control al temperaturii şi umidităţii, stingere a incendiilor) etc.
e) oameni: ingineri de comunicaţii, specialişti IT etc.
f) intangibile: controlul organizaţiei, „know-how" etc.

În vederea stabilirii gradului de sensibilitate şi importanţă a resurselor organizaţiei în activitatea de furnizare a reţelelor şi serviciilor, furnizorii trebuie să ia în considerare cerinţele legale privind asigurarea în mod neîntrerupt a posibilităţii efectuării apelurilor de urgenţă. De asemenea, furnizorii trebuie să ţină seama de prevederile legale privind securitatea prelucrării datelor cu caracter personal şi cele referitoare la confidenţialitatea comunicărilor, precum şi a datelor de trafic aferente.

Toate resursele identificate trebuie să fie în responsabilitatea unei anumite părţi a organizaţiei astfel desemnate, iar regulile privind utilizarea acestora în mod acceptabil trebuie să fie identificate, documentate şi implementate.

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;

Procedurile pentru managementul incidentelor, precum şi definirea responsabilităţilor sunt necesare pentru a asigura un răspuns rapid, eficace şi sistematic la incidentele care afectează securitatea şi integritatea reţelelor şi serviciilor. Procedurile trebuie să stabilească modul de abordare a diverselor tipuri de incidente, identificarea impactului unui incident (asupra serviciilor, utilizatorilor, resurselor, în funcţie de localizare/arie geografică etc.), analiza şi identificarea cauzei incidentului, măsurile care pot fi luate pentru a minimiza efectele incidentului şi pentru a remedia defecţiunile care au cauzat incidentul, planificarea şi implementarea acţiunilor corective pentru împiedicarea reapariţiei sale, comunicarea cu cei afectaţi de incident, colectarea probelor etc. Prin intermediul acestor proceduri, cei răspunzători de managementul incidentelor înţeleg prioritatea organizaţiei în ceea ce priveşte tratarea acestor incidente.

Procesele pentru managementul incidentelor trebuie să asigure că ameninţările, vulnerabilităţile şi incidentele care pot afecta securitatea şi integritatea reţelelor şi serviciilor sunt comunicate şi tratate în mod corespunzător, permiţându-se aplicarea unor măsuri corective în timp util.

În plus faţă de monitorizarea sistemelor şi a alertelor, incidentele care pot afecta continuitatea furnizării reţelelor şi serviciilor pot fi detectate şi prin raportarea evenimentelor, ameninţărilor şi a vulnerabilităţilor. Astfel, în vederea prevenirii apariţiei incidentelor, trebuie să existe proceduri de raportare a evenimentelor, a vulnerabilităţilor şi a ameninţărilor care să stabilească modul de raportare, precum şi acţiunile ce trebuie întreprinse.

Evaluarea/triajul reprezintă procesul de sortare, clasificare, corelare, prioritizare a evenimentelor, a rapoartelor despre incidente şi a vulnerabilităţilor. Prin evaluarea incidentelor, se identifică potenţialele probleme de securitate şi se prioritizează activităţile. Astfel, informaţiile primite sunt revizuite pentru a stabili validitatea acestora şi pentru a determina tipul de eveniment raportat, precum şi pentru a stabili măsurile iniţiale care trebuie luate. Evaluarea permite ca toate informaţiile despre posibilele incidente să treacă printr-un singur punct de contact pentru corelarea tuturor datelor raportate. Clasificarea unui eveniment implică nu doar identificarea tipului acestuia, ci şi corelarea cu alte evenimente şi incidente. În funcţie de tipul incidentului şi de impactul acestuia, organizaţia trebuie să aibă un proces de escaladare (transmiterea informaţiilor către şefi ierarhici superiori – escaladare ierarhică sau către alte compartimente competente, cu solicitarea unei acţiuni din partea acestora – escaladare funcţională) prin care să se stabilească acţiunile ce trebuie întreprinse, precum şi responsabilităţile corespunzătoare. Astfel, organizaţia trebuie să specifice în ce condiţii diferitele moduri de răspuns/reacţie la un incident sunt invocate/apelate (şi părţile interesate notificate), inclusiv condiţiile pentru activarea planurilor pentru situaţiile deosebite.

Răspunsul la incidente include măsurile luate pentru a studia un incident, pentru a atenua efectele acestuia şi pentru a-l rezolva. Răspunsul la incidente poate include activităţi tehnice,

manageriale, legale etc. Astfel, sunt analizate informaţiile referitoare la un incident, sunt investigate diferite opţiuni de atenuare şi recuperare, sunt aplicate măsuri privind limitarea efectelor unui incident (ex: izolarea unui sistem afectat, schimbarea configuraţiilor), sunt identificate şi eliminate/diminuate vulnerabilităţile, se produce recuperarea în urma incidentului cu o confirmare a faptului că sistemele afectate funcţionează normal, sunt implementate metode de monitorizare suplimentare etc.

Informaţiile strânse în urma evaluării incidentelor trebuie folosite pentru identificarea incidentelor care se repetă sau au un impact semnificativ. Organizaţiile trebuie să stabilească mecanisme şi procese prin care lecţiile învăţate în urma unui incident sunt împărtăşite în interiorul organizaţiei. Astfel, pot fi identificate metode de a îmbunătăţi atât nivelul de securitate, cât şi mecanismul de tratare a incidentelor (managementul incidentelor).

2) să stabilească un sistem de detectare a incidentelor;

Procesul de detectare a incidentelor implică/presupune orice observaţie a unei activităţi rău intenţionate, suspecte sau accidentale, precum şi colectarea de informaţii care pot oferi o perspectivă asupra ameninţărilor curente sau a riscurilor la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. În procesul de detectare, informaţiile despre incidente, vulnerabilităţi şi ameninţări sunt colectate reactiv (de la surse interne sau externe, sub formă de rapoarte sau notificări) sau proactiv (monitorizarea indicatorilor care pot anunţa iminenţa unui incident sau exploatarea unei vulnerabilităţi, prin mecanisme cum ar fi sisteme de monitorizare a reţelei sau prin sisteme de detecţie a intruziunilor - IDS). Odată detectate, activităţile sau informaţiile privind incidente, vulnerabilităţi şi ameninţări sunt trimise pentru triaj/evaluare sub formă de raport, alertă sau notificare.

3) să stabilească o procedură adecvată de raportare a incidentelor către ANCOM, precum şi către alte autorităţi responsabile, precum 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.).

Conform prezentului proiect de decizie, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite ANCOM o notificare iniţială privind existenţa/apariţia unui incident cu impact semnificativ asupra furnizării reţelelor şi serviciilor în 6 ore de la detectarea acestuia şi o notificare finală privind incidentul în două săptămâni de la detectarea acestuia, în condiţiile şi formatul prevăzute în proiectul de decizie. Astfel, prin procedurile interne, furnizorul trebuie să creeze mecanisme care să asigure că informaţiile pe care trebuie să le prezinte ANCOM sunt disponibile şi complete, iar raportarea se va face în condiţiile şi formatul stabilite de autoritate.

Pentru a asigura transparenţa informaţiilor cu privire la incidentele care afectează semnificativ securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, furnizorii trebuie să stabilească planuri de comunicare a incidentelor către utilizatori, astfel încât furnizorii să poată răspunde solicitării ANCOM, atunci când interesul public reclamă necesitatea raportării incidentelor către public. Conform proiectului de decizie, ANCOM poate stabili în sarcina unui furnizor de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului obligaţia de a informa publicul cu privire la existenţa unui incident cu impact semnificativ, stabilind şi modalităţile alternative pentru realizarea acestei informări. Aceste modalităţi prevăzute în cuprinsul proiectului de decizie nu exclud însă posibilitatea informării utilizatorilor, la cerere, prin intermediul serviciului de relaţii cu clienţii.

Independent de solicitările exprese venite din partea Autorităţii, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului pot stabili modalităţi alternative şi facultative de informare a publicului cu privire la existenţa unui incident cu impact semnificativ, acestea fiind, de altfel, şi o cale de a îmbunătăţi comunicarea cu utilizatorii, fiind o indicaţie a angajamentului şi a capacităţii furnizorului de a restabili rapid serviciile.

Contactele cu grupurile specializate de interes sau cu alte forumuri de specialişti în securitate trebuie menţinute în vederea accesului la informaţii privind securitatea şi integritatea reţelelor şi serviciilor (ex: informaţii privind ameninţările şi vulnerabilităţile actuale, recomandări şi rapoarte privind atacuri şi vulnerabilităţi, bune practici în asigurarea securităţii şi integrităţii şi răspuns la incidente). Pot fi create acorduri de schimb de informaţii pentru îmbunătăţirea cooperării şi a coordonării problemelor de securitate.

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 ale serviciului;

Pentru a contracara discontinuitatea furnizării reţelelor şi serviciilor în cazuri de perturbare gravă a funcţionării reţelei sau a serviciului (de ex. în urma producerii unui dezastru sau a unei situaţii de forţă majoră), organizaţia trebuie să stabilească o strategie de acţiune în astfel de cazuri.

Evenimentele (sau succesiunea de evenimente) care pot determina întreruperi ale proceselor afacerii organizaţiei, precum şi resursele implicate în procesele critice ale organizaţiei trebuie identificate împreună cu probabilitatea şi impactul unor asemenea discontinuităţi din punct de vedere al duratei, nivelului pagubelor şi perioadei de redresare. În funcţie de rezultatele determinării riscurilor, trebuie elaborată o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice în situaţii deosebite.

În procesele de stabilire şi elaborare a strategiei pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice în situaţii deosebite, furnizorii trebuie să aibă în vedere implementarea de măsuri adecvate pentru a reduce probabilitatea apariţiei perturbărilor grave ale funcţionării reţelei sau serviciului sau de reducere a eventualelor efecte, precum şi obligaţiile stabilite în sarcina acestora prin cadrul legal în vigoare din domeniul comunicaţiilor electronice, în funcţie de specificul activităţii sale.

Strategia de continuitate vizează alegerea unor metode alternative de operare şi pot fi folosite ulterior producerii unei situaţii deosebite, în scopul de a menţine operaţiunile la un nivel acceptabil sau de a le relua într-un interval de timp cât mai scurt. Strategia de continuitate implică acţiuni precum: salvarea datelor relevante în mod regulat, utilizarea site-urilor alternative (exemplu: *cold site, hot site, mobile site, mirrored site*), evitarea resurselor unice (single points of failure), elaborarea unei metodologii de înlocuire a echipamentelor (exemplu: acorduri încheiate cu furnizorii de echipamente şi/sau achiziţionarea unor echipamente de rezervă) şi stabilirea de mecanisme de prioritizare, suspendare sau restricţionare a anumitor servicii.

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

În vederea implementării strategiei de continuitate, organizaţia trebuie să identifice şi să asigure suficiente resurse financiare, organizaţionale, tehnice şi de mediu.

În scopul implementării unei strategii de continuitate eficiente, organizaţia poate folosi mijloace de colectare în avans a informaţiilor cu privire la dezastre naturale sau alte evenimente (ex: atac DDoS) care ar putea afecta continuitatea furnizării serviciilor şi reţelelor (ex: colectarea informaţiilor despre evoluţia vremii, colectarea anomaliilor de trafic şi recepţionarea avertizărilor timpurii), iar personalul relevant ar trebui informat în timp util. În scopul unui răspuns cât mai prompt şi eficient în cazul producerii unei situaţii deosebite, organizaţia trebuie să stabilească acţiunile premergătoare unei eventuale intervenţii ale instituţiilor cărora le revine responsabilitatea privind organizarea apărării împotriva dezastrelor, în condiţiile legislaţiei aplicabile în domeniu.

Personalul reprezintă una din resursele principale angrenate în procesul de recuperare în caz de dezastru. Astfel, personalul organizaţiei, inclusiv managementul, trebuie să cunoască responsabilităţile şi rolurile specifice în cazul apariţiei unei perturbări grave a funcţionării reţelei sau serviciului şi să fie instruit corespunzător.

Strategiile de continuitate alese trebuie susţinute de planuri de continuitate şi recuperare.

Planurile de continuitate şi recuperare reprezintă o colecţie documentată de proceduri şi informaţii, care sunt dezvoltate, compilate şi disponibile pentru a fi utilizate în cazul producerii unei perturbări grave a funcţionării reţelei sau serviciului, în scopul de a permite continuarea furnizării serviciilor de comunicaţii electronice la un nivel acceptabil şi restabilirea furnizării serviciilor la nivelul anterior producerii incidentului.

Strategia de continuitate presupune parcurgerea a două etape care angrenează resurse şi acţiuni distincte şi care constau în asigurarea continuităţii furnizării serviciilor de comunicaţii, precum şi în restabilirea furnizării serviciilor la nivelul anterior producerii incidentului.

Fiecare plan trebuie să specifice condiţiile de activare, procedura de escaladare, resursele implicate cât şi persoanele responsabile de executarea fiecărei acţiuni din plan.

În procesul de implementare a planurilor de continuitate şi recuperare, se vor avea în vedere şi acţiuni de urgenţă pentru a asigura securitatea personalului.

Pentru ca procedurile convenite în cadrul procesului de continuitate să fie în concordanţă cu obiectivele stabilite, planurile de continuitate şi recuperare trebuie testate în mod regulat. Se asigură, astfel, că acestea sunt eficiente şi adecvate.

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;

Sistemele trebuie monitorizate şi evenimentele care pot afecta securitatea şi integritatea reţelelor şi serviciilor trebuie înregistrate. Trebuie ţinute jurnale/înregistrări de operator, iar defecţiunile trebuie înregistrate pentru a se asigura identificarea problemelor. Monitorizarea alarmelor, precum şi a altor aspecte legate de performanţa reţelei este necesară pentru a evita afectarea/alterarea funcţionării reţelelor de comunicaţii electronice sau pentru a lua măsuri de remediere a problemelor apărute. O monitorizare efectivă şi eficientă oferă acces la informaţii critice pentru a identifica utilizatorii afectaţi, pentru a verifica starea echipamentelor şi circuitelor şi pentru a asigura o recuperare eficientă şi rapidă a furnizării reţelelor şi serviciilor de comunicaţii electronice. Nivelul de monitorizare necesar pentru fiecare sistem depinde de nivelul determinat de risc, ţinând cont de factori precum criticitatea şi sensibilitatea proceselor şi sistemelor, experienţa acumulată în privinţa infiltrărilor, a vulnerabilităţilor şi a utilizării neconforme a sistemelor, interconectarea sistemelor etc. Jurnalele, înregistrările ajută la analiza problemelor, identificarea cauzelor şi a vulnerabilităţilor şi pot oferi suport pentru rezolvarea incidentelor. Totodată, monitorizarea va fi utilizată şi pentru verificarea eficacităţii măsurilor de securitate adoptate.

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;

Planurile de recuperare şi backup în cazul situaţiilor deosebite trebuie testate şi actualizate în mod regulat pentru a se asigura că sunt eficiente şi adecvate. Testarea acestor planuri va asigura cunoaşterea de către toţi membrii echipei a planurilor, a atribuţiilor şi a responsabilităţilor pentru asigurarea continuităţii afacerii. Planificarea testelor trebuie să indice cum şi când trebuie testat fiecare element. Trebuie folosite mai multe tehnici pentru ca organizaţia să se asigure că planurile vor opera şi în realitate: testarea diverselor scenarii, simulări, testări tehnice, testări prin utilizarea unui alt amplasament (diferit de amplasamentul principal), teste privind serviciile furnizate de terţi, repetiţii complete.

În ceea ce priveşte planurile de recuperare pentru sistemele individuale, acestea trebuie testate pentru a avea siguranţa că răspund cerinţelor organizaţiei. În cazul sistemelor importante, procedurile de recuperare trebuie să cuprindă toate elementele (echipamente, date, aplicaţii) necesare recuperării întregului sistem în caz de dezastru sau alte situaţii deosebite.

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

Implementarea modificărilor în reţeaua de comunicaţii electronice, precum şi în sistemele folosite pentru operarea şi monitorizarea furnizării reţelelor şi serviciilor, trebuie controlată prin utilizarea unor proceduri formale pentru controlul schimbărilor în vederea minimizării posibilităţii de deteriorare a sistemelor sau de introducere de noi vulnerabilităţi. Introducerea unor echipamente, sisteme şi software-uri noi, precum şi schimbările majore aduse celor existente trebuie să urmeze un proces formal de documentare, specificare, testare, control al calităţii şi implementare.

Este bine ca testarea să se facă într-un mediu separat atât de cel de producţie, cât şi de cel de dezvoltare pentru a asigura o protecţie suplimentară. În plus, informaţiile şi echipamentele folosite trebuie să permită testarea în mod adecvat a funcţionării în condiţii cât mai aproape de cele existente în realitate în procesul de furnizare a reţelelor şi serviciilor de comunicaţii electronice.

4) să stabilească o politică adecvată pentru evaluarea şi testarea securităţii tuturor resurselor;

Securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice trebuie analizată în mod periodic pentru verificarea gradului de eficienţă a măsurilor implementate. Verificarea securităţii implică examinarea echipamentelor, sistemelor şi software-ului pentru asigurarea implementării corecte a măsurilor de securitate. Această verificare poate presupune şi efectuarea de teste de penetrare şi determinare a vulnerabilităţilor. Testele de penetrare şi de determinare a vulnerabilităţilor oferă o imagine a securităţii şi integrităţii reţelei şi serviciului la un moment dat şi nu pot înlocui determinarea riscului.

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.

Pentru a asigura conformitatea cu standardele şi politicile de securitate, organizaţia trebuie să se asigure că toate procedurile de securitate sunt respectate. Dacă în urma analizei sunt constatate neconformităţi, organizaţia trebuie să stabilească motivele, să evalueze necesitatea de a acţiona astfel încât neconformitatea să nu se mai repete, să stabilească şi să implementeze acţiuni corective adecvate, în timp util şi să analizeze consecinţele acestora. Rezultatele analizelor şi acţiunilor corective trebuie înregistrate, iar înregistrările păstrate.

Cerinţele de audit şi activităţile care implică verificări asupra sistemelor operaţionale trebuie planificate astfel încât să minimizeze riscul întreruperii proceselor de afaceri. Dacă în procesul de audit sunt implicaţi terţi, organizaţia trebuie să ia măsuri de securitate astfel încât riscurile adiţionale presupuse de această activitate să fie eliminate/minimizate. Este de preferat ca sistemele/instrumentele de auditare folosite să fie separate de cele de producţie şi de dezvoltare.

ANCOM subliniază că lista domeniilor de securitate nu este exhaustivă, furnizorii având posibilitatea de a include şi alte măsuri de securitate adecvate nevoilor specifice ale organizaţiei şi care îndeplinesc obiectivul de asigurare a unui înalt nivel de securitate şi integritate a reţelelor şi serviciilor de comunicaţii electronice.

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a evalua şi, dacă este cazul, de a actualiza măsurile de securitate specificate în proiectul de decizie ori de câte ori este necesar, însă cel puţin o dată la 12 luni. 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. Analiza trebuie să cuprindă determinarea oportunităţilor de îmbunătăţire şi a nevoii de modificare a modului de abordare a securităţii (politici, măsuri de securitate şi obiective, procese şi proceduri).

O atenţie deosebită trebuie acordată procesului de management al riscului care trebuie monitorizat, revizuit şi îmbunătăţit continuu. Monitorizarea şi revizuirea permanentă sunt necesare pentru a asigura că rezultatul determinării şi tratării riscului, contextul şi planurile de management rămân relevante şi corespund circumstanţelor de la un moment dat. Riscurile nu sunt statice, ameninţările, vulnerabilităţile, probabilităţile de apariţie a unui incident sau consecinţele acestuia modificându-se în timp (uneori chiar într-un interval de timp foarte scurt şi în mod imprevizibil).

Măsurile de securitate, precum şi obiectivele acestor măsuri pot fi îmbunătăţite şi în urma rezultatelor analizelor de management anterioare, 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 raportate, precum şi a sugestiilor/feedback-ului diferitelor părţi interesate.

De asemenea, conform art. 49 alin. (2) din Ordonanţa de Urgenţă a Guvernului nr. 111/2011, *„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”*. Măsurile impuse de ANCOM trebuie să asigure un nivel adecvat al securităţii reţelelor şi serviciilor de comunicaţii electronice şi vor trebui implementate de către furnizorii de reţele şi servicii de comunicaţii electronice. În plus, ANCOM poate elabora ghiduri de bune practici în vederea asigurării unui nivel adecvat al securităţii reţelelor şi serviciilor de comunicaţii

electronice, ghiduri care trebuie avute în vedere la stabilirea măsurilor de securitate de către furnizori.

5. Raportarea către ANCOM a incidentelor care afectează în mod semnificativ securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

5.1. Definire şi scop

În înţelesul acestui proiect de decizie, un incident reprezintă un eveniment care poate afecta sau ameninţa, direct sau indirect, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. Un eveniment reprezintă un fenomen observabil, care nu poate fi anticipat sau controlat în totalitate.

O procedură naţională eficace de raportare oferă numeroase beneficii. Un astfel de sistem facilitează informarea, în timp util, a părţilor interesate în legătură cu producerea unui incident. În acelaşi timp, ANCOM poate urmări eficienţa măsurilor de securitate adoptate de furnizori, precum şi a răspunsului acestora în momentul producerii incidentelor, poate colecta date referitoare la tipurile de ameninţări şi vulnerabilităţi ce vor fi utilizate în cadrul unei analize aprofundate a securităţii reţelelor şi serviciilor, constituind o bază pentru emiterea de recomandări şi ghiduri de bune practici.

Deoarece gradul de interconectare a reţelelor de comunicaţii electronice devine din ce în ce mai mare, nevoia de a partaja informaţiile referitoare la ameninţările la adresa securităţii acestora creşte în mod constant. Astfel, informaţiile puse la dispoziţia Autorităţii prin intermediul sistemului de raportare pot fi valorificate prin intermediul oferirii de ghiduri şi bune practici de către ANCOM.

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

În acest context, raportarea incidentelor joacă un rol important în consolidarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, deoarece contribuie la asigurarea:

- unei diseminări rapide a informaţiilor între părţile interesate;
- accesului la o arie largă de expertiză cu privire la astfel de incidente;
- unei analize a ameninţărilor şi vulnerabilităţilor la adresa securităţii şi integrităţii reţelelor şi serviciilor;
- identificării de bune practici bazate pe lecţiile învăţate în procesul de management al incidentelor;

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

În plus, sunt urmărite şi următoarele obiective:

- identificarea cauzelor incidentelor, inclusiv ameninţările şi vulnerabilităţile cele mai frecvente;
- urmărirea lecţiilor învăţate în urma aplicării măsurilor de detecţie, răspuns şi de recuperare luate în timpul, precum şi după incident;
- elaborarea de bune practici pentru asigurarea securităţii reţelelor şi serviciilor şi modificarea acestora, dacă este necesar;
- înţelegerea tendinţelor viitoare;
- creşterea transparenţei pieţei faţă de utilizatori.

Prin analizarea incidentelor cu impact semnificativ, ANCOM poate evalua nivelul de securitate a reţelelor şi serviciilor de comunicaţii electronice şi a măsurilor de reglementare anterioare. În cazul incidentelor cu impact semnificativ, ANCOM poate analiza în detaliu cauzele incidentului, acţiunile furnizorului de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice şi alte aspecte legate de acest incident. ANCOM poate cere furnizorilor să ia măsuri corespunzătoare astfel încât acest tip de incident să nu se mai producă/repete. Analizele statistice ale incidentelor pot constitui, de asemenea, un instrument eficient de a monitoriza/urmări tendinţele.

ANCOM va colecta informaţii cu privire la incidentele cu impact semnificativ pentru:

- elaborarea unui raport anual cu privire la securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice;
- informarea în mod corespunzător, acolo unde consideră necesar, a celorlalte autorităţi naţionale de reglementare din celelalte state şi ENISA cu privire la incidentele de încălcare a securităţii reţelelor şi serviciilor sau de pierdere a integrităţii reţelelor;

- emiterea de recomandări şi bune practici privind managementul/gestionarea incidentelor pentru a maximiza valoarea lecţiilor învăţate la nivel naţional;

- crearea de statistici referitoare la cauzele incidentelor, a tipurilor de atacuri, ameninţări şi vulnerabilităţi, la serviciile şi reţelele cele mai afectate de incidente etc.

Astfel, conform art. 47 alin. (3) şi (4) din Ordonanţa de urgenţă a Guvernului nr. 111/2011, ANCOM trebuie:

- să prezinte anual Comisiei Europene şi ENISA un raport de sinteză privind notificările primite de la furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului şi măsurile luate pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor;

- să informeze autorităţile naţionale de reglementare din celelalte state şi ENISA în cazurile în care un incident poate afecta furnizorii de comunicaţii electronice din alt stat membru.

Schema de raportare poate fi revizuită astfel încât să reflecte feedback-ul primit de la părţile interesate şi experienţa câştigată prin implementarea acestor noi cerinţe. De asemenea, vor fi luate în considerare şi ghidurile elaborate de ENISA pentru a aborda într-o manieră comună cu celelalte State Membre ale Uniunii Europene implementarea art.13a din Directiva cadru.

5.2. Managementul/administrarea incidentelor

Pentru un management eficient al incidentelor este necesară o înţelegere a modului în care incidentele sunt detectate, tratate şi rezolvate. Prin stabilirea unei structuri şi clasificări generale a incidentelor, este posibilă obţinerea unei imagini generale a fluxului unui incident.

Un incident poate fi detectat extern de către un utilizator prin raportarea unor evenimente sau erori la serviciul de relaţii cu clienţii al furnizorului sau de o terţă parte (mass-media, autorităţi publice sau alte organizaţii) sau poate fi detectat de personalul furnizorului (prin intermediul alarmelor din centrul operaţional de control, prin diverse sisteme de detectare, prin urmărirea unui mesaj de eroare, audit etc.).

Atunci când un eveniment/incident este detectat, trebuie efectuată o evaluare iniţială a situaţiei pentru a confirma categoria incidentului şi gravitatea acestuia. Acest lucru se face prin clasificarea tipului evenimentului, precum şi prin evaluarea consecinţelor acestuia. În funcţie de caracteristicile evenimentului, acesta poate fi clasificat în mai multe clase de gravitate şi este tratat în mod diferit de organizaţie. Analizarea unui incident permite furnizorului să înţeleagă:

- domeniul afectat de incident: numărul de sisteme afectate;
- impactul: gradul în care fiecare sistem este afectat;
- cât de critic este impactul: influenţa incidentului asupra funcţionării reţelei şi a serviciului;
- prioritatea cu care trebuie răspuns la acest incident.

Tratarea unui incident presupune mai multe etape: identificarea tipului de incident şi a consecinţelor acestuia, limitarea consecinţelor incidentului, eliminarea cauzei şi prevenirea reapariţiei acesteia, revenirea la un mod normal de furnizare a serviciilor, evaluarea modului de acţiune al organizaţiei şi eficienţei în procesul de eliminare a consecinţelor acestui incident şi nu în ultimul rând lecţiile învăţate cu această ocazie astfel încât greşelile descoperite să nu se mai repete.

Este esenţial ca furnizorul să implementeze un sistem de evidenţă a incidentelor. Prin studierea acestor incidente, se pot detecta tipurile de evenimente care sunt mai frecvente, de ce apar acestea, modul în care acestea sunt detectate, consecinţele şi costurile pe care le implică pentru organizaţie. Un aspect foarte important este înregistrarea tuturor incidentelor. Deşi multe dintre incidente nu prezintă un pericol major pentru organizaţie atunci când sunt văzute ca evenimente izolate, analizate împreună pot dezvălui modul în care apar incidentele şi cauzele acestora.

Managementul unui incident trebuie să fie proactiv, controlat şi coerent. De obicei, acţiunile multor organizaţii sunt de tip reactiv, acestea concentrându-se asupra tratării/răspunsului la incident prin acţiuni întreprinse pentru a rezolva sau pentru a atenua consecinţele unui incident atunci când acesta a avut loc. Acestea trebuie să îşi extindă mijloacele de acţiune şi prin măsuri proactive de analizare a potenţialelor ameninţări şi riscuri, astfel încât să prevină apariţia incidentelor.

Furnizorii de reţele şi servicii de comunicaţii electronice trebuie să dezvolte procese care să trateze/răspundă la incidente, dar şi procese care să prevină apariţia sau reapariţia incidentelor. Acestea includ procese pentru planificarea şi implementarea unui management al incidentelor,

îmbunătăţirea securităţii infrastructurii organizaţiei pentru a preveni incidentele sau pentru a atenua efectele unui incident, detectarea, trierea şi răspunsul la incidente atunci când acestea apar.

5.3. Sistemul de raportare a incidentelor

Un sistem de raportare a incidentelor reprezintă un set complex de reguli, proceduri stabilite şi acţiuni întreprinse pentru a crea un mecanism de raportare a incidentelor.

În funcţie de scopul unui sistem de raportare, pot fi identificate trei tipuri de astfel de sisteme:

a) Răspunsul imediat la incidente

Sistemul de raportare are scopul de a permite schimbul de informaţii în timp real şi coordonarea în timpul situaţiilor de urgenţă sau în timpul desfăşurării incidentelor.

b) Prevenirea incidentelor (întreruperilor)

Acest tip de raportare se axează pe reducerea întreruperilor în furnizarea reţelelor şi serviciilor de comunicaţii electronice ca un mijloc de a garanta utilizatorilor un anumit nivel al calităţii serviciului. Scheme de acest tip au ca obiectiv colectarea la nivelul sectorului de comunicaţii electronice a informaţiilor privind ameninţările şi folosirea acestor informaţii astfel încât întreruperile în furnizarea serviciilor să fie prevenite. Pe baza acestor raportări, se pot efectua analize şi audituri în scopul descoperirii ameninţărilor potenţiale şi aplicării unor măsuri de contracarare a acestora.

c) Rectificarea deficienţelor/incidentelor

Acest tip de raportare se axează pe obligaţiile furnizorilor de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului de a lua toate măsurile adecvate pentru a administra riscurile care pot afecta securitatea reţelelor şi serviciilor astfel încât, printre altele, să prevină sau să minimizeze impactul acestor incidente asupra utilizatorilor, precum şi pe obligaţia furnizorilor de reţele publice de comunicaţii electronice de a asigura continuitatea furnizării serviciilor prin intermediul acestor reţele. Prin respectarea acestor obligaţii, se pot atinge obiectivele de rezilienţă/securitate a comunicaţiilor electronice, precum şi de protecţie a utilizatorilor. Astfel, incidentele, precum şi acţiunile întreprinse de furnizori sunt urmărite/monitorizate pentru ca autoritatea să se asigure ca aceleaşi tipuri de incidente să nu se mai repete sau că furnizorii de servicii restabilesc serviciile pentru utilizatorii finali cât mai repede. În acest caz, este esenţial să existe proceduri prin care să fie colectate informaţii complete care să servească drept punct de plecare pentru ca autoritatea să impună corectarea deficienţelor constatate şi implementarea modificărilor necesare. Autoritatea are dreptul de a cere informaţii referitoare la incidente şi explicaţii privind măsurile adoptate de furnizori astfel încât incidentele să nu se mai repete. În cazul schemelor de tip prevenirea incidentelor şi rectificarea deficienţelor/incidentelor, acestea tind să se axeze pe impactul incidentelor asupra utilizatorilor serviciului (numărul utilizatorilor afectaţi, suprafaţa geografică afectată şi durata unui incident).

Prin impunerea obligaţiei de raportare a incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, ANCOM urmăreşte şi rectificarea deficienţelor/incidentelor de către furnizori şi prevenirea apariţiei incidentelor.

Pe lângă o definire clară a domeniului de aplicare şi a obiectivelor de raportare, în spatele fiecărui sistem de raportare ar trebui să existe o reprezentare clară a incidentelor ce ar trebui să fie raportate. Există patru elemente cheie pentru un sistem de raportare eficient:

- definirea clară a categoriilor cauzelor incidentului (motivul pentru care incidentul a avut loc);
- formatul de raportare, ale cărui câmpuri/domenii trebuie să fie bine definite;
- criteriile/parametrii luaţi în considerate pentru a raporta/defini un incident;
- valorile/pragurile acestor parametri care declanşează mecanismul de raportare.

5.4. Obligaţiile ce incumbă furnizorilor de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului

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

a) de a transmite ANCOM o notificare iniţială privind existenţa/apariţia unui incident cu impact semnificativ asupra furnizării reţelelor şi serviciilor în termen de 6 ore de la detectarea acestuia, la adresa de poştă electronică incidente@ancom.org.ro;

b) de a transmite ANCOM o notificare finală privind existenţa unui incident cu impact semnificativ asupra furnizării reţelelor şi serviciilor în termen de două săptămâni de la detectarea acestuia, fie pe suport fizic, fie ca înscris în formă electronică.

Folosind investigaţiile şi rapoartele trimise de furnizori, autoritatea poate iniţia o investigaţie pentru a verifica măsurile de securitate implementate de către aceştia şi poate solicita îmbunătăţiri ale măsurilor de securitate. De asemenea, în cazul în care un furnizor nu raportează un incident semnificativ conform prevederilor acestei decizii, acesta va fi sancţionat în baza art. 142 pct. 16 din Ordonanţa de urgenţă a Guvernului nr. 111/2011.

5.5. Cauza unui incident care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

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

În categoria eroare umană trebuie încadrate incidentele cauzate de operarea şi configurarea defectuoasă a echipamentelor, sistemelor, utilităţilor, implementarea şi folosirea greşită a instrumentelor software, aplicarea eronată a procedurilor etc.

Categoria eroare de sistem va fi folosită pentru a include incidentele datorate defecţiunilor hardware, erorilor de programare ale software-lui, dimensionării şi/sau implementării greşite a reţelei şi erorilor în elaborarea politicilor, procedurilor sau manualelor.

Categoria fenomen natural va include incidentele cauzate de condiţii meteorologice nefavorabile (ex. furtuni, temperaturi excesive, căderi masive de zăpadă etc.), cutremure, pandemii, inundaţii, incendii, alunecări de teren, fenomene meteorologice spaţiale etc.

Categoria acţiune rău intenţionată va include incidentele cauzate de acţiunile efectuate în mod deliberat, ca de exemplu: accesul neautorizat la echipamente de reţea, platforme, aplicaţii (software), baze de date, atacurile de tip DoS (refuzul serviciilor) sau DDoS (refuzul serviciilor realizat în mod distribuit), efectuare de modificări neautorizate ale sistemelor şi datelor, vandalism, sabotaj, furt etc.

Nu toate acţiunile (sau inacţiunile) care pot provoca un incident se datorează furnizorului de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului şi sunt sub controlul direct al acestuia. Astfel, mai există şi incidente provocate de părţi externe, precum: distrugerea unor echipamente şi cabluri în urma unor lucrări de construcţie, defecţiuni în reţeaua de distribuţie a energiei electrice etc. De obicei, această cauză externă 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. În acest caz, în cuprinsul raportării către ANCOM, furnizorul va indica la tipul cauzei incidentului cauza iniţială, iar câmpul privind „mai multe informaţii despre cauza incidentului" va cuprinde detalii referitoare atât la cauza iniţială, cât şi la cauza subsecventă care a declanşat incidentul (de 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 al unui echipament al furnizorului de utilităţi şi cauză externă/parte terţă, iar cauza subsecventă este eroare de sistem – defecţiune hardware al unui echipament de comunicaţii electronice).

5.6. Parametrii şi valorile acestora, factori declanşatori ai mecanismului de raportare

În spatele fiecărui sistem de raportare trebuie să existe o idee clară în ceea ce priveşte criteriile şi pragurile care ar trebui să declanşeze mecanismul de raportare a incidentelor. Astfel, parametrii care vor fi luaţi în considerare la evaluarea impactului sunt numărul de conexiuni afectate şi durata unui incident.

Un incident trebuie raportat ANCOM de fiecare dată când impactul incidentului este egal sau mai mare decât un prag predefinit. Astfel, mecanismul de raportare al furnizorilor către ANCOM este declanşat în momentul în care un incident afectează un număr mai mare de 5.000 de conexiuni timp de cel puţin o oră.

În sensul acestui proiect de decizie, 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 celulare: o cartelă SIM activă;

- în cazul serviciilor de retransmisie a programelor media audiovizuale liniare: o conexiune de retransmisie a programelor media audiovizuale.

Acest criteriu este pur cantitativ şi nu ia în considerare tipul utilizatorilor afectaţi. Astfel, fiecare utilizator are aceeaşi importanţă şi nu există nicio distincţie, de exemplu, între un utilizator rezidenţial şi o bancă sau un spital. Nivelul de importanţă al unei infrastructuri deservite de către un furnizor de comunicaţii electronice nu va fi parte din domeniul de aplicare al raportării către ANCOM, deoarece infrastructura critică nu face obiectul Ordonanţei de Urgenţă a Guvernului nr. 111/2011.

Durata incidentului reprezintă intervalul de timp, exprimat în minute, din momentul în care serviciul începe să se degradeze sau s-a întrerupt, până în momentul în care acesta este adus în parametrii normali de funcţionare.

În determinarea impactului unui incident, au fost luate în considerare mai multe cerinţe în ceea ce priveşte definirea parametrilor şi a valorilor acestor parametri. Astfel, procedura care determină impactul unui incident trebuie să fie simplă, să fie orientată pe efectul incidentului asupra utilizatorilor şi reţelelor interconectate şi trebuie să ia în calcul şi aspecte practice, precum numărul de incidente care ar trebui raportate.

În prima parte a anului 2012, ANCOM a transmis către cei mai mari 40 de furnizori de reţele şi servicii de comunicaţii electronice din perspectiva numărului de utilizatori un chestionar[4] privind incidentele care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice către un număr mai mare de 5.000 de utilizatori timp de cel puţin o oră în cursul anului 2011. Acest chestionar a avut scopul de a identifica numărul şi impactul incidentelor, atât asupra utilizatorilor, cât şi asupra furnizorilor. În urma analizării şi centralizării răspunsurilor la chestionare, a fost identificat un număr de 268 de incidente care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în cursul anului 2011.

Cauzele principale identificate ale incidentelor sunt cele din tabel:

Cauza incidentului	**Detalii despre incident**	**Numărul incidentelor raportate**
Atac rău intenţionat	Atac asupra securităţii logice (DDoS, hacking)	3
	Atac asupra securităţii fizice (furt)	35
	Atac asupra securităţii fizice (deteriorare fibră optică)	7
Fenomene şi dezastre naturale	Condiţii meteorologice nefavorabile	31
Eroare umană	Accident	14
Defecţiune hardware/software	Hardware	72
	Software	34
Cauze externe/părţi terţe	Alimentarea cu energie electrică	29
	Defecţiune software	6
	Defecţiune hardware	2
	Fibră optică deteriorată de lucrări efectuate de terţi	35
Numărul total al incidentelor raportate		268

[4] Chestionarul privind incidentele care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în anul 2011 se găseşte la adresa: http://www.ancom.org.ro/chestionare_4950

În urma analizării incidentelor raportate de furnizorii de reţele şi servicii de comunicaţii electronice, s-a observat că cel mai des întâlnite cauze ale incidentelor sunt:

1. Defecţiune hardware/software

Aproape 40% din totalul defecţiunilor au fost cauzate de defecţiuni hardware/software. Sistemele utilizate în comunicaţii, precum şi software-urile aferente sunt din ce în ce mai complexe şi astfel din ce în ce mai predispuse la defectări.

2. Deteriorarea fibrei optice de către terţi

Cablurile sunt adesea deteriorate accidental. În lucrările de construcţii, modul de manipulare a excavatoarelor este o cauză frecventă pentru cablurile tăiate. O altă cauză frecvent întâlnită este deteriorarea cablurilor datorată lucrărilor de întreţinere la sistemul de distribuire a utilităţilor.

4. Furtul cablurilor

Creşterea în valoare a metalului din care sunt constituite cablurile influenţează negativ furnizarea de reţele de comunicaţii. Circuitele telefonice tradiţionale conţin perechi de cablu din cupru, iar hoţii sunt din ce în ce mai atraşi de câştigurile obţinute din vânzarea cuprului la centrele de reciclare. Acest lucru a condus la un număr mare de deficienţe de funcţionare şi întreruperi în furnizarea reţelelor şi serviciilor de comunicaţii electronice. Reţelele bazate pe cupru nu sunt singurele afectate, cablurile cu fibră optică sunt frecvent deteriorate de hoţi în căutarea cablurilor de cupru.

5. Condiţiile meteorologice nefavorabile

Fenomenele naturale, cum ar fi ninsorile şi ploile abundente, provoacă de cele mai multe ori întreruperi ale alimentării cu energie electrică şi blocaje rutiere, ce împiedică accesul echipelor de intervenţie ale furnizorilor afectaţi la locaţiile cu echipamente, pentru efectuarea cât mai rapidă a reparaţiilor.

5.7. Notificarea iniţială

Notificarea iniţială reprezintă un raport cu privire la faptul că un incident cu impact semnificativ a avut loc, raport ce trebuie să fie transmis la scurt timp după ce a fost detectat (6 ore de la detectare). Notificarea conţine caracteristicile de bază ale incidentului şi estimarea consecinţelor acestuia, pe baza informaţiilor disponibile imediat după eveniment.

Este important ca personalul furnizorului să nu fie supraîncărcat cu obligaţiile de raportare în timp ce răspunde la un incident. În cazul incidentelor care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, înlăturarea efectelor acestui incident este responsabilitatea furnizorilor, care ar trebui să aibă toate resursele necesare pentru a face acest lucru. Astfel, în primă fază, furnizorul va trebui să raporteze doar informaţii minime referitoare la un incident:

- ora descoperirii incidentului;
- serviciile şi/sau reţelele care sunt afectate de incident;
- 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;;
- estimarea efectelor în ceea ce priveşte apelarea numărului unic pentru apeluri de urgenţă 112;
- o descriere sumară a cauzei/cauzelor care a/au provocat incidentul;
- estimarea graficului de restabilire a furnizării reţelelor şi serviciilor de comunicaţii electronice în parametrii normali de funcţionare;
- îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;
- informaţiile oferite publicului cu privire la existenţa unui incident, modalitatea de comunicare şi ora la care au fost comunicate informaţiile, dacă este cazul;
- toate aspectele/elementele care pot permite ANCOM să decidă dacă informarea publicului privind incidentul este sau nu în interesul publicului;
- 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.

Intervalul de 6 ore în care furnizorul trebuie să trimită ANCOM notificarea iniţială permite furnizorului să se concentreze în primul rând pe acţiunile de limitare a efectului unui incident.

În cazul în care un astfel de incident poate afecta furnizarea reţelelor şi serviciilor de comunicaţii electronice de către un furnizor din alt stat membru al Uniunii Europene, ANCOM va

avea în vedere informarea autorităţii de reglementare din respectivul stat şi ENISA cu privire la acest incident.

5.8. Notificarea finală

Notificarea finală va trebui să conţină informaţii complete cu privire la incidentul cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, precum şi un rezumat al măsurilor luate pentru a elimina vulnerabilităţile identificate şi pentru a preveni reapariţia incidentului în viitor. Unele dintre aceste informaţii pot fi disponibile numai după încheierea şi analiza incidentului. De asemenea, furnizorii au posibilitatea de a aloca resurse umane pentru rapoarte detaliate după ce un incident a fost rezolvat. Notificarea finală poate servi ca bază de analiză a incidentelor individuale.

Formatul informaţiilor pe care furnizorii vor trebui să le completeze în vederea transmiterii la ANCOM a notificării finale a fost detaliat în cuprinsul prezentului proiect de decizie.

Obiectivul formatului standardizat de raportare a incidentelor este ca ANCOM să se asigure că informaţiile transmise de furnizori sunt comparabile. Utilizarea unui model standard va face procesul de colectare a datelor şi de analiză mai eficace şi mai eficient şi în acelaşi timp va evita incoerenţele.

În anumite cazuri, este posibil ca furnizorii să nu deţină la momentul transmiterii notificării finale toate informaţiile cerute în formularul-tip de raportare a incidentelor care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. În acest caz, furnizorii trebuie să transmită în două săptămâni de la detectarea incidentului formularul-tip cu toate informaţiile disponibile la acel moment, urmând ca, în momentul în care deţin şi celelalte informaţii, să le transmită ANCOM printr-o notificare suplimentară, însă nu mai târziu de 3 săptămâni de la detectarea incidentului cu impact semnificativ.

Informaţiile colectate şi agregate de ANCOM pot fi apoi utilizate de către autoritate pentru a realiza un raport privind starea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

5.9. Informarea publicului cu privire la incidentele care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

În scopul protejării utilizatorilor finali, sunt necesare măsuri pentru a asigura continuitatea furnizării reţelelor şi serviciilor, dar şi pentru asigurarea transparenţei informaţiilor cu privire la incidentele care afectează în mod semnificativ securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Incidentele pot afecta un număr mare de utilizatori, întreprinderi şi servicii şi pot afecta chiar siguranţa publică. Prin urmare, ele pot fi de interes pentru publicul larg şi informarea cu privire la aceste incidente este esenţială. În anumite cazuri, este necesară contracararea în mod activ a zvonurilor sau a panicii în rândul utilizatorilor printr-o informare corespunzătoare a publicului despre un eveniment, o ameninţare sau despre modul de contracarare a incidentului şi de răspuns la un incident sau despre alte informaţii importante.

Utilizatorii pot percepe aceste informaţii ca o dovadă a angajamentului şi a capacităţii furnizorului de a restabili rapid serviciile. Astfel, utilizatorii pot fi educaţi cu privire la posibilele ameninţări la adresa funcţionării serviciului. Utilizatorii înţeleg cauza întreruperii furnizării serviciului şi de ce furnizarea serviciului nu a putut fi reluată mai devreme. Raportarea incidentelor (către public) este astfel o cale de a îmbunătăţi comunicarea cu utilizatorii.

Conform art. 47 alin. (2) din Ordonanţa de Urgenţă a Guvernului nr. 111/2011, ANCOM va putea informa publicul cu privire la existenţa unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice atunci când consideră că este în interesul public. Această informare se va realiza prin intermediul paginii proprii de internet a ANCOM. De asemenea, la solicitarea ANCOM, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului vor informa publicul cu privire la existenţa unui incident cu impact semnificativ, prin utilizarea uneia sau a mai multor modalităţi indicate de proiectul de decizie. De aceea, ANCOM trebuie să primească în cadrul notificării iniţiale toate informaţiile necesare cu privire la incident pentru a lua o decizie în privinţa oportunităţii de publicare. Astfel, ANCOM trebuie să fie informat dacă furnizorul, din proprie iniţiativă, a pus la dispoziţia publicului informaţiile cu privire la incident şi să aibă la dispoziţie toate aspectele/elementele care îi pot permite să decidă dacă informarea privind incidentul este sau nu în interesul public.

De principiu, ANCOM consideră că toate incidentele cu impact semnificativ, aşa cum au fost ele definite în cuprinsul prezentului proiect, sunt în interesul public şi intenţionează să publice informaţii despre acestea pe pagina de internet a autorităţii. Cu toate acestea, ANCOM are posibilitatea de a analiza şi de a decide de la caz la caz cu privire la informarea publicului, pe baza datelor aflate la dispoziţia sa cu privire la anumite aspecte, cum ar fi aria geografică afectată de incident, efectele incidentului în ceea ce priveşte apelarea numărului unic pentru apeluri de urgenţă 112, informaţiile oferite publicului de către furnizor cu privire la existenţa unui incident, modalitatea de comunicare şi ora la care au fost comunicate informaţiile, dacă este cazul, elementele precizate de funizori care pot permite ANCOM să decidă dacă informarea privind incidentul este sau nu în interesul public, numărul conexiunilor afectate, durata incidentului, precum şi pe baza argumentelor temeinice oferite de furnizorii în cauză care ar putea justifica nepublicarea informaţiilor referitoare la incidentul cu impact semnificativ.

Nu în ultimul rând, furnizorii pot raporta ANCOM şi pot informa publicul şi despre alte incidente care nu îndeplinesc pragurile stabilite în decizie pentru a fi considerate incidente cu impact semnificativ, din proprie iniţiativă, pentru a îndeplini responsabilitatea lor socială şi responsabilitatea în faţa utilizatorilor.

6. Dispoziţii finale şi tranzitorii

Deoarece de la intrarea în vigoare a dispoziţiilor Ordonanţei de Urgenţă a Guvernului nr. 111/2011 şi până în momentul elaborării prezentului proiect de decizie niciun furnizor nu a transmis ANCOM vreo notificare cu privire la apariţia unui incident cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice şi datorită faptului că ANCOM trebuie să transmită ENISA şi Comisiei Europene un raport anual privind incidentele cu impact semnificativ care au avut loc în cursul anului 2013 în România, furnizorii de reţele publice de comunicaţii electronice sau servicii de comunicaţii electronice destinate publicului trebuie să transmită ANCOM, în termen de 30 de zile de la data intrării în vigoare a prezentei decizii, 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 deciziei, completând formularul-tip de raportare din Anexa nr. 2 şi respectând instrucţiunile de completare din Anexa nr. 3 la proiectul de decizie.

Pentru a se asigura un grad ridicat de transparenţă, precum şi pentru a crea condiţiile primirii de către ANCOM a unor informaţii exacte, reale, complete, provenind de la persoane ce au capacitatea de a reprezenta respectiva organizaţie, cu privire la incidentele cu impact semnificativ asupra securităţii şi integrităţii reţelelor şi serviciilor, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia de a transmite ANCOM datele de contact ale persoanelor responsabile pentru raportarea acestor incidente, în termen de 5 zile de la intrarea în vigoare a deciziei, precum şi orice modificări ce intervin asupra datelor de contact, în termen de 5 zile de la survenirea acestora.