

## **EXPUNERE DE MOTIVE**

### **la proiectul de decizie a președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice**

#### **1. Introducere/Contextul european**

În ultimii ani, utilizarea rețelelor publice de comunicații electronice s-a extins rapid pentru a cuprinde o gamă mult mai largă de servicii și aplicații oferite utilizatorilor, aceștia devenind din ce în ce mai dependenți de utilizarea acestor rețele și servicii. Aceste rețele au devenit infrastructuri critice pentru statele membre ale Uniunii Europene, pentru instituții publice, pentru întreaga economie și în general pentru societate.

Deoarece rețelele și serviciile de comunicații electronice au rolul de infrastructură/platformă pentru multe aplicații, incidentele care afectează securitatea și integritatea rețelelor și serviciilor pot avea un impact semnificativ pentru furnizori, pentru utilizatori, dar și pentru economia națională.

Serviciile de comunicații electronice joacă un rol foarte important în viața de zi cu zi a cetățenilor. Activitățile utilizatorilor rezidențiali, cât și ale celor din mediul de afaceri se bazează pe rețelele și serviciile de comunicații electronice a căror importanță este conștientizată doar în momentul în care acestea devin indisponibile. Totodată și alte sectoare ale economiei naționale (energie, transport etc.) se bazează pe infrastructura de comunicații, iar breșele de securitate și pierderea integrității rețelelor de comunicații pot afecta aceste sectoare într-un mod semnificativ.

Incidentele care afectează rețelele și serviciile de comunicații electronice au următoarele caracteristici principale:

- serviciile de comunicații 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 și se pot propaga rapid în alte echipamente prin intermediul rețelei;

- vulnerabilitățile în protocoale sau în topologia rețelei pot duce la incidente grave; în special, convergența dintre diferite tipuri de rețele poate implica provocări semnificative pentru securitatea rețelelor și serviciilor de comunicații electronice;

- rețelele de comunicații și sistemele de management ale rețelelor și serviciilor de comunicații electronice sunt predispuși la atacuri de tip hacking;

- în plus față de atacuri externe, serviciile de comunicații electronice pot fi afectate și de compromiterea securității din surse interne (ex: modificări invalide la bazele de date de gestionare a rețelei de către persoanele neautorizate) în mod accidental sau deliberat.

Instituțiile Uniunii Europene au recunoscut importanța comunicațiilor electronice, precum și necesitatea de a extinde eforturile pentru a asigura reziliența acestora. În 2006, Comisia Europeană a emis comunicarea privind „O strategie pentru o societate informațională sigură - Dialog, parteneriat și responsabilizare” (COM (2006) 251). Una dintre principalele acțiuni anunțate

În această strategie a fost un dialog între părțile interesate cu privire la securitatea și reziliența rețelelor de comunicații electronice în cadrul programului european pentru protecția infrastructurilor critice adoptat de către Comisia Europeană la sfârșitul anului 2006.

În martie 2009, Comisia Europeană a adoptat o comunicare și un plan de acțiune privind protecția infrastructurilor critice de informații numit „Protejarea Europei de atacuri cibernetice și perturbații de amploare: ameliorarea gradului de pregătire, a securității și a rezilienței” (COM(2009)149). Această comunicare se concentrează pe „prevenire, pregătire și conștientizare” și definește un plan de acțiuni imediate pentru consolidarea securității și a rezilienței infrastructurilor critice de informații.

Importanța colectării datelor privind incidentele care afectează securitatea și integritatea rețelelor și serviciilor a fost evidențiată de Comisia Europeană în mai multe rânduri. În comunicarea „O strategie pentru o societate informațională sigură - Dialog, parteneriat și responsabilizare”, Comisia Europeană a subliniat faptul că accesul la informații complete, corecte, comparabile și actualizate referitoare la incidente constituie un element necesar pentru a obține o mai bună înțelegere a nevoii de acțiuni în scopul asigurării securității, precum și pentru a evalua rezultatele măsurilor puse în aplicare anterior (legale, de reglementare, organizatorice și tehnice).

În Strategia din 2006, Comisia Europeană a propus un parteneriat cu statele membre și alte părți interesate pentru a dezvolta un cadru adecvat de colectare a datelor, inclusiv proceduri și mecanisme pentru colectarea și analizarea datelor la nivelul UE în ceea ce privește incidentele de securitate și încrederea consumatorilor. În comunicarea privind protecția infrastructurilor critice de informații, Comisia Europeană remarcă faptul că „*Mecanismele de guvernare vor fi cu adevărat eficiente numai în cazul în care toți participanții dispun de informații fiabile pentru a acționa*” și apoi ia act de faptul că „*procesele și practicile de monitorizare și de raportare a incidentelor de securitate a rețelelor diferă de la un stat membru la altul. Unele dintre acestea nu dispun de o organizație de referință ca punct de monitorizare. Un aspect și mai important este faptul că schimbul de date concrete privind incidentele de securitate și cooperarea dintre statele membre par insuficient dezvoltate, desfășurându-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 protecția infrastructurilor critice de informații că există o incoerență în punerea în aplicare a sistemelor de avertizare timpurie, schimbul de informații cu privire la incidente și 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 apariției unor incidente similare. Comisia a menționat, de asemenea, nevoia pentru o mai bună coordonare și cooperare între statele membre. Gradul de interconectare a rețelelor de comunicații electronice devine din ce în ce mai mare, iar amenințările la adresa acestora devin din ce în ce mai complexe și pot avea un caracter global. În plus, expertiza în ceea ce privește amenințările, precum și nevoia de a preveni și a răspunde la incidente devin o necesitate internațională. Există o mare oportunitate pentru experții din toate Statele Membre pentru a-și uni eforturile pentru a îmbunătăți reziliența rețelelor și serviciilor de comunicații electronice.

În primul rând, autoritățile naționale ar trebui să fie în măsură să implementeze sisteme eficiente de raportare a incidentelor. Ca urmare, securitatea și integritatea rețelelor și serviciilor de comunicații electronice naționale va crește. În al doilea rând, comunicarea între autoritățile naționale are un rol important în creșterea rezilienței infrastructurilor de comunicații europene.

Cadrul de reglementare, la nivel european, pentru rețelele și serviciile de comunicații electronice adoptat în noiembrie 2009 introduce un nou capitol în vederea îndeplinirii obiectivului de asigurare a unui nivel adecvat al securității și integrității rețelelor și serviciilor de comunicații 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 rețelele și serviciile de comunicații electronice, 2002/19/CE privind accesul la rețelele de comunicații electronice și la infrastructura asociată, precum și interconectarea acestora și 2002/20/CE privind autorizarea rețelelor și serviciilor de comunicații 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 menținerea integrității și securității rețelelor publice de comunicații. Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) ar trebui să contribuie la nivelul sporit de securitate a comunicațiilor electronice, printre altele, prin furnizarea de consultanță de specialitate și promovarea schimbului de cele mai bune practici. Atât ENISA, cât și autoritățile naționale de reglementare ar trebui să dispună de mijloacele necesare îndeplinirii atribuțiilor lor, inclusiv de competențele de a obține informații suficiente pentru a fi în măsură să evalueze nivelul de securitate a rețelelor sau serviciilor, precum și de a obține date complete și certe referitoare la incidentele reale privind securitatea care au avut un impact semnificativ asupra funcționării rețelelor 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 rețelele și serviciile de comunicații 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 rețele publice de comunicații sau servicii de comunicații electronice accesibile publicului iau măsurile tehnice și organizatorice corespunzătoare pentru a gestiona în mod corespunzător riscurile privind securitatea rețelelor și serviciilor. Ținând seama de progresele științifice 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 și limita impactul incidentelor de securitate asupra utilizatorilor și asupra rețelelor interconectate.*

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

*(3) Statele membre se asigură că întreprinderile care furnizează rețele publice de comunicații sau servicii de comunicații electronice accesibile publicului notifică autoritățile naționale de reglementare competente orice încălcare a normelor de securitate sau pierdere a integrității care au avut un impact semnificativ asupra funcționării rețelelor sau a serviciilor.*

*După caz, autoritatea națională de reglementare în cauză informează autoritățile naționale de reglementare din celelalte state și Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA). Autoritatea națională de reglementare respectivă poate informa publicul sau poate solicita întreprinderilor să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării servește interesului public.*

*O dată pe an, autoritatea națională de reglementare în cauză prezintă Comisiei și ENISA un raport de sinteză privind notificările primite și măsurile luate în conformitate cu prezentul alineat.”*

În cadrul acestui articol este prevăzută obligația furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului de a asigura un nivel adecvat al securității rețelelor sau serviciilor de comunicații electronice. De asemenea, furnizorii de rețele publice de comunicații electronice au obligația de a lua toate măsurile necesare pentru a garanta integritatea rețelelor proprii, în scopul garantării continuității furnizării serviciilor de comunicații electronice prin intermediul acestor rețele. În ceea ce privește raportarea încălcării normelor de securitate sau a pierderii integrității, textul distinge între notificarea transmisă de furnizorii de rețele publice de comunicații electronice și servicii de comunicații electronice destinate publicului către autoritatea națională de reglementare, raportul de sinteză anual către Comisia Europeană și ENISA, elaborat de autoritatea națională de reglementare, pe baza notificărilor transmise de furnizori și notificarea „ad-hoc” a încălcărilor de securitate între autoritățile de reglementare, precum și între acestea din urmă și ENISA.

În plus, potrivit art. 13a alin. (4) din Directiva cadru revizuită, Comisia Europeană, ținând 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 dispozițiile privind asigurarea securității și integrității rețelelor și serviciilor.

ENISA a fost creată în 2004 și are rol în asigurarea unui nivel ridicat de securitate a rețelelor informatice și a datelor în UE, precum și în armonizarea măsurilor de securitate tehnice și organizaționale corespunzătoare, prin următoarele acțiuni: îndrumarea autorităților naționale și a altor instituții ale UE în calitate de expert în materie de securitate a rețelelor informatice și a datelor, îndeplinirea rolului de forum pentru schimbul de bune practici, facilitarea contactelor între instituțiile UE, autoritățile naționale și furnizori.

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

securitate coerente și 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 comunicații 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 și statele membre s-au angajat într-o discuție permanentă (printr-o serie de seminarii, reuniuni, conferințe telefonice, schimburi de mesaje prin intermediul poștei electronice) în care opiniile, perspectiva și experiențele din diferite state membre au fost împărtășite și evaluate. Scopul colaborării dintre ENISA și statele membre a fost acela de a găsi o bază care ar putea fi adoptată de către toate statele și de a crea un cadru prin care diferitele state membre vor comunica într-un „limbaj comun” atât între ele, cât și cu ENISA și Comisia Europeană. Colaborarea între Statele Membre și ENISA a avut ca rezultat elaborarea a două ghiduri „*Technical Guideline on Minimum Security Measures*<sup>1</sup>” și „*Technical Guidelines for Reporting Incidents*<sup>2</sup>”.

Ghidul „*Technical Guideline on Minimum Security Measures*” își propune să sprijine statele membre în implementarea art. 13a, alin. (1) și (2) din Directiva cadru revizuită, prin stabilirea măsurilor minime de securitate pe care o autoritate de reglementare în comunicații ar trebui să le ia în considerare când evaluează gradul de îndeplinire de către furnizorii de rețele și servicii a obligației de asigurare a securității și integrității rețelelor și serviciilor de comunicații electronice. Acest document își propune să ofere o bază pentru o implementare unitară și armonizată a prevederilor art.13a în țările membre ale Uniunii Europene.

Ghidul „*Technical Guidelines for Reporting Incidents*” își propune să sprijine statele membre în implementarea art. 13a, alin. (3) din Directiva cadru revizuită, prin stabilirea condițiilor în care se realizează notificarea Comisiei Europene și a ENISA de către autoritățile de reglementare în cazul încălcării normelor de securitate sau al pierderii integrității rețelelor, care au avut un impact semnificativ asupra funcționării rețelelor sau a serviciilor. Totodată, acest ghid constituie o bază de plecare în vederea emiterii de către autoritățile din statele membre a unor reglementări privind circumstanțele, formatul și procedurile aplicabile în cazul notificărilor pe care trebuie să le transmită furnizorii de rețele publice de comunicații electronice și servicii de comunicații electronice destinate publicului acestor autorități.

## **2. Cadrul legal național**

Ordonanța de Urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, include un capitol special dedicat securității și integrității rețelelor și serviciilor de comunicații electronice care transpune în legislația națională prevederile Capitolului IIIA din Directiva cadru revizuită, și are ca scop stabilirea unui cadru general pentru asigurarea utilizării în siguranță a rețelelor și serviciilor de comunicații electronice, în special prin informarea utilizatorilor în legătură cu incidentele care afectează în mod semnificativ securitatea și integritatea rețelelor și serviciilor, precum și prin stabilirea responsabilităților furnizorilor și a atribuțiilor autorității de reglementare în acest domeniu.

Conform art. 46 și 47 din Ordonanța de Urgență a Guvernului nr. 111/2011:

*„Art. 46 - (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua toate măsurile tehnice și organizatorice adecvate pentru a administra riscurile care pot afecta securitatea rețelelor și serviciilor.*

*(2) Măsurile luate potrivit alin. (1) trebuie să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, având în vedere cele mai noi tehnologii.*

---

<sup>1</sup> [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](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)

<sup>2</sup> <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 rețele publice de comunicații electronice au obligația de a lua măsurile necesare pentru a garanta integritatea rețelelor și pentru a asigura continuitatea furnizării serviciilor prin intermediul acestor rețele.

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

Art. 47 - (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a notifica ANCOM, în cel mai scurt timp, cu privire la orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor sau serviciilor.

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

(3) Acolo unde consideră necesar, ANCOM informează autoritățile naționale de reglementare în comunicații din alte state membre ale Uniunii Europene și Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor cu privire la încălcarea securității rețelelor și serviciilor sau pierderea integrității rețelelor.

(4) ANCOM transmite anual un raport succint Comisiei Europene și Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor cu privire la notificările primite potrivit alin. (1) și măsurile adoptate în aceste cazuri.”

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

Textul legal introduce trei tipuri de raportări privind incidentele care afectează securitatea și integritatea rețelelor și serviciilor. În primul rând, furnizorii au obligația de a transmite ANCOM, în cel mai scurt timp, informații cu privire la încălcarea securității sau pierderea integrității care are un impact semnificativ asupra furnizării rețelelor sau serviciilor de comunicații electronice. Pe baza acestor informații, ANCOM poate informa ENISA și autoritățile de reglementare în comunicații din alte state membre ale Uniunii Europene în cazul în care incidentul respectiv este de interes pentru aceste organizații. ANCOM va transmite anual Comisiei Europene și ENISA un raport privind notificările primite de la furnizori și 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 Ordonanța de Urgență a Guvernului nr. 111/2011 împuternicește ANCOM să stabilească modalitatea de implementare a dispozițiilor art. 46 și 47, inclusiv măsurile care definesc circumstanțele, formatul și procedurile aplicabile în cazul cerințelor de notificare.

### **3. Securitatea și integritatea rețelelor și serviciilor de comunicații electronice**

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

Securitatea reprezintă totalitatea aspectelor care se referă la definirea, realizarea și menținerea controlului accesului, autentificării, nerepudierii, confidențialității, integrității și disponibilității. Aceste dimensiuni de securitate sunt seturi de măsuri prin care se urmărește asigurarea protecției în cazul amenințărilor la adresa securității și nu se limitează doar la modalitățile de administrare a rețelei și serviciului de comunicații electronice, ci se extind la aplicații și la informații disponibile prin intermediul serviciilor de comunicații electronice și care sunt accesate de către utilizatorul final. Măsurile de securitate vizează elementele rețelei, serviciile și aplicațiile cu scopul de a detecta, anticipa și corecta vulnerabilitățile de securitate.

Controlul accesului protejează împotriva utilizării neautorizate a resurselor. Această dimensiune asigură faptul că numai personalul autorizat poate accesa elementele rețelei, informația stocată, fluxurile de informații, serviciile și aplicațiile. Autentificarea servește confirmării identităților celor implicați în comunicație, asigură validitatea identităților pretinse ale entităților participante în procesul comunicației (persoană, dispozitiv, serviciu sau aplicație).

Nerepudierea asigură mijloace pentru prevenirea unor situații în care o entitate ar putea nega realizarea unei anumite acțiuni, reprezentând astfel o modalitate de a dovedi producerea unui eveniment sau a unei acțiuni, precum și a originii sale. În cadrul securității informației, nerepudierea implică faptul că un participant al unui schimb de informație nu poate nega trimiterea sau primirea unui mesaj.

Confidențialitatea este proprietatea informației de a nu fi disponibilă sau dezvăluită unor persoane, entități sau procese neautorizate. Confidențialitatea datelor protejează datele de dezvăluiri neautorizate astfel încât conținutul nu poate fi înțeles de către entități neautorizate. Confidențialitatea datelor înseamnă protecția comunicațiilor sau a datelor stocate împotriva interceptării și citirii de către persoane neautorizate.

Integritatea reprezintă acea proprietate prin care se protejează acuratețea (exactitatea) și caracterul complet al resurselor. Integritatea datelor asigură corectitudinea sau acuratețea 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-și păstra atributele specifice din punct de vedere al performanței și funcționalității. Integritatea rețelei presupune îndeplinirea funcției dorite a rețelei într-o manieră corespunzătoare. Prin urmare, integritatea rețelei poate fi înțeleasă ca fiind capacitatea unei rețele de a menține și/sau restabili un nivel acceptabil de performanță și funcționalitate în cazul unor condiții nefavorabile (defecțiuni, atacuri externe etc.)

Disponibilitatea asigură faptul că nu există refuzul accesului autorizat la elemente ale rețelei, informații stocate, fluxuri de informații, servicii și aplicații, refuz care poate apărea datorită evenimentelor cu impact asupra rețelei. Disponibilitatea este proprietatea unei resurse de a fi accesibilă la momentul oportun și ușor de utilizat la cererea unei entități autorizate. Protecția disponibilității rețelei înseamnă protecția capacității rețelei de a asigura continuitatea furnizării serviciilor oferite.

Conform Regulamentului (CE) nr. 460/2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA), cu modificările și completările ulterioare, prin „securitatea rețelelor și a informațiilor” se înțelege capacitatea rețelelor sau a sistemelor informatice de a rezista, la un anumit nivel de încredere, la evenimente accidentale sau la acțiuni ilegale sau răuvoitoare care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor stocate sau transmise și a serviciilor asociate, oferite sau accesibile prin aceste rețele și 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 comunicațiilor electronice este unul dintre criteriile importante după care se evaluează calitatea serviciului (QoS) pentru utilizatorii serviciului respectiv, alături de alte criterii precum disponibilitatea, fidelitatea/acuratețea, viteza, capacitatea, rezistența, flexibilitatea, ușurința utilizării serviciului.

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

După funcționalitatea lor, sunt identificate 3 niveluri de securitate:

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

Nivelul de securitate a infrastructurii constă în mijloace de transmisie în cadrul rețelei, precum și elemente specifice de rețea care sunt protejate de dimensiunile securității. Nivelul infrastructură stă la baza construirii rețelelor, serviciilor și aplicațiilor.

Nivelul de securitate a serviciilor se referă la securitatea serviciilor de comunicații electronice oferite utilizatorilor finali de către furnizori. Acest nivel este utilizat pentru protecția atât a furnizorilor de servicii, cât și a utilizatorilor săi împotriva amenințărilor la adresa securității. 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 aplicațiilor se referă la securitatea aplicațiilor disponibile prin intermediul serviciilor de comunicații electronice și care sunt accesate de către utilizatori. Există 4 ținte pentru atacurile în cadrul acestui nivel: utilizatorii aplicației respective, furnizorii aplicației, furnizorii de servicii de conținut și furnizorii de servicii de comunicații electronice.

Asigurarea securității infrastructurii contribuie într-o bună măsură la asigurarea securității serviciilor și, la rândul ei, asigurarea securității serviciilor contribuie la securitatea aplicațiilor folosite de utilizatorii finali. Fiecare nivel de securitate are vulnerabilități diferite și oferă flexibilitatea combaterii potențialelor amenințări în cel mai potrivit mod pentru un anumit nivel de securitate. Dimensiunile de securitate sunt aplicate nivelurilor de securitate pentru a diminua vulnerabilitățile existente la fiecare nivel.

Termenul de „securitate” este utilizat în sensul minimizării vulnerabilității resurselor. „Resursele” înseamnă orice prezintă valoare pentru organizație, pentru operațiunile sale de afaceri și continuitatea acestora. Resursele unei organizații care furnizează rețele și servicii de comunicații electronice includ:

- a) informații: de rutare, de configurare a echipamentelor, referitoare la utilizatorii de servicii, referitoare la serviciile furnizate, la traficul efectuat, taxare, baze de date, documentație de sistem, manuale de utilizare, contracte și acorduri, proceduri operaționale, materiale pentru instruire, planuri pentru continuitatea afacerii, acorduri privind alternativele disponibile în cazuri de urgență, dovezi de audit, înregistrări etc.
- b) software: de control al comunicațiilor, management al operațiunilor, de management al informațiilor privind utilizatorii, de taxare, de aplicații, de sistem, de dezvoltare și utilități etc.
- c) fizice: clădiri, echipamente de comutare sau rutare, sisteme de transmisie, echipamente terminale, mediile utilizate pentru transmiterea semnalelor, servere și stații de lucru, medii mobile etc.
- d) servicii: de procesare a informațiilor, de rețea, utilități suport (alimentare cu energie electrică, iluminat, control al temperaturii și umidității, stingere a incendiilor) etc.
- e) oameni: ingineri de comunicații, specialiști IT etc.
- f) intangibile: controlul organizației, „know-how” etc.

În dezvoltarea oricărui cadru de lucru privind securitatea, este importantă cunoașterea resurselor ce trebuie protejate, a amenințărilor asupra acestor resurse, a vulnerabilităților asociate, precum și a riscului global asupra resurselor, risc provenit din amenințări și vulnerabilități. Amenințările, vulnerabilitățile și riscurile sunt elementele fundamentale care trebuie luate în considerare în vederea asigurării securității.

Amenințarea reprezintă o posibilă încălcare a securității. Exemple de amenințări pot fi:

- dezvăluirea neautorizată a informațiilor;
- 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.

Amenințările pot fi accidentale sau intenționate, active sau pasive. O amenințare accidentală este aceea fără intenție premeditată, de exemplu o defecțiune software sau o eroare fizică. O amenințare intenționată este realizată de către o persoană ce comite un act deliberat (atunci când o amenințare intenționată are ca rezultat o acțiune, acea acțiune se numește atac). O amenințare activă este, de exemplu, alterarea datelor sau distrugerea unui echipament fizic. O astfel de amenințare 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 amenințări. Vulnerabilitatea este acea slăbiciune în proiectarea, implementarea, operarea sau controlul intern al unui proces care ar putea expune sistemul la amenințări.

Riscul reprezintă probabilitatea ca o vulnerabilitate din sistem să afecteze securitatea, precum și severitatea efectului determinat de utilizarea intenționată sau neintenționată a unei astfel de vulnerabilități. Riscul este o mărime a efectelor contrare care pot rezulta dacă o vulnerabilitate este exploatată de către o amenințare. Riscul nu poate fi total eliminat, de aceea unul dintre obiectivele securității este de a reduce riscul la un nivel acceptabil. Pentru realizarea acestui obiectiv, este necesară înțelegerea amenințărilor și vulnerabilităților și aplicarea măsurilor de contracarare potrivite (servicii și mecanisme de securitate). Determinarea riscului trebuie să identifice, să cuantifice și să stabilească prioritatea tratării riscului prin prisma criteriilor de risc acceptabil și a obiectivelor relevante pentru organizație.

În înțelesul acestei decizii, securitatea și integritatea rețelelor și serviciilor de comunicații electronice se definește astfel: capacitatea unei rețele sau a unui serviciu de comunicații electronice de a rezista evenimentelor, accidentale sau rău intenționate, care pot compromite sau

afecta continuitatea furnizării rețelelor și serviciilor la un nivel de performanță echivalent cu cel anterior producerii evenimentului.

#### **4. Măsurile de securitate**

##### **4.1 Definiție și scop**

Măsurile de securitate reprezintă mijloace (de natură administrativă, tehnică, managerială sau juridică) de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, tehnici etc. menite să elimine sau să reducă riscurile privind securitatea și integritatea rețelelor sau a serviciilor de comunicații electronice. Măsurile de securitate sunt dedicate protecției resurselor (hardware, software, informații etc.), constituind practici/metode prin care vulnerabilitățile și amenințările se elimină sau se previn, se descoperă și se raportează în scopul acțiunilor corective, minimizându-se efectele negative pe care le pot produce.

Astfel de măsuri pot fi preventive, corective sau de detectare. Măsurile preventive reduc vulnerabilitățile și probabilitatea de apariție a unui incident, implementarea lor conducând de exemplu la insuccesul unui potențial atac. Măsurile corective reduc impactul/efectele unui incident și restabilesc funcționarea/operarea în condiții normale. Măsurile de detectare descoperă incidente/atacuri și activează măsuri preventive sau corective.

O securitate adecvată a rețelelor și serviciilor de comunicații electronice se poate realiza prin punerea în aplicare a unui set adecvat de măsuri de securitate. Aceste măsuri trebuie stabilite și implementate în funcție de profilul organizației și condițiile operaționale și trebuie monitorizate și îmbunătățite în mod continuu. Furnizorii de rețele și servicii de comunicații electronice trebuie să adopte măsuri de securitate conform riscurilor evaluate, aceste măsuri tehnice și organizatorice fiind menite să prevină și să limiteze impactul incidentelor de securitate asupra utilizatorilor și asupra rețelelor interconectate, asigurând continuitatea furnizării serviciilor prin intermediul rețelelor. Rețelele de comunicații electronice trebuie planificate, construite, operate și întreținute astfel încât să funcționeze în siguranță, fiabilitatea și reziliența acestora putând fi obținută în urma implementării măsurilor adecvate de securitate.

Măsurile de securitate se aplică tuturor resurselor identificate în cadrul procesului de identificare a riscurilor (informații, resurse software, hardware, servicii, utilități, resurse umane etc.), resurse care, în cazul în care sunt afectate, pot compromite securitatea și integritatea rețelelor și serviciilor de comunicații electronice. Identificarea resurselor, evidențierea caracteristicilor acestora, clasificarea acestora, precum și conștientizarea importanței lor fac posibilă o implementare corespunzătoare a măsurilor de securitate.

Măsurile de securitate sunt selectate luând în considerare riscurile existente în cadrul organizației. Cerințele de securitate pot fi identificate doar printr-o evaluare sistematică a riscurilor la adresa securității. Rezultatele evaluării riscurilor vor ajuta la determinarea acțiunilor corespunzătoare și a priorităților implementării măsurilor de securitate în scopul protejării împotriva acestor riscuri. Măsurile de securitate pot preveni posibile incidente, pot limita consecințele incidentelor atunci când acestea au loc sau pot asigura rectificarea rapidă și eficientă a întreruperilor serviciilor de comunicații electronice, restabilind furnizarea la condiții normale și trebuie să acopere orice condiții de operare (operare normală, cu întreruperi), diverse tipuri de incidente și evenimente de securitate, precum și situații de urgență, 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 acțiuni suplimentare pentru monitorizarea, evaluarea și îmbunătățirea eficienței 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 cerințelor sistemelor, proiectelor etc. În caz contrar, se pot înregistra costuri suplimentare și pot fi adoptate soluții ineficiente, putându-se ajunge la imposibilitatea realizării unei securități adecvate.

Măsurile de securitate au ca obiective principale reducerea semnificativă a numărului de incidente și întreruperi operaționale, a fraudelor, prevenirea pierderii, distrugerii, furtului sau compromiterii resurselor, îmbunătățirea calității serviciilor oferite utilizatorilor, creșterea încrederii utilizatorilor în serviciile furnizate de organizații.

Ca rezultat al implementării măsurilor de securitate adecvate, furnizorii de rețele și servicii de comunicații electronice vor fi capabili să asigure o securitate și integritate adecvată a rețelelor și serviciilor de comunicații electronice, vor avea o abordare clară și completă asupra tuturor



activităților aferente acestui domeniu, vor deține capacitățile restabilirii serviciilor la condiții normale de funcționare în cazul apariției incidentelor, vor reuși să conștientizeze personalul organizațiilor și utilizatorii asupra importanței securității și vor spori încrederea acestora în serviciile oferite, ansamblul măsurilor de securitate contribuind semnificativ la îmbunătățirea calității serviciilor și la asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice.

#### **4.2 Nivelul actual al securității și integrității rețelelor și serviciilor**

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

În urma analizării răspunsurilor<sup>3</sup> primite de la cei 20 de furnizori de rețele și servicii de comunicații electronice la chestionarul transmis de ANCOM, a rezultat că majoritatea dintre aceștia au o preocupare activă în asigurarea securității și integrității rețelelor și serviciilor. Cu toate acestea, doar o parte dintre furnizori au proceduri clare și documentate pentru asigurarea continuității rețelelor și serviciilor, în majoritatea cazurilor stabilirea unor măsuri de securitate efectuându-se reactiv, în momentul apariției unui incident. În plus, puțini dintre furnizori au o abordare completă a domeniului securității și integrității rețelelor și serviciilor de comunicații electronice, majoritatea axându-se doar pe anumite domenii de interes. Prin urmare, domeniul securității și integrității nu este abordat unitar de către furnizorii chestionați. Acest fapt se datorează și inexistenței unui standard internațional pentru asigurarea securității și integrității rețelelor și serviciilor, standardul utilizat preponderent de respondenți fiind ISO/CEI 27001, standard ce se referă în principal la securitatea informației.

Majoritatea furnizorilor au indicat că dețin o politică privind asigurarea securității și integrității rețelelor și serviciilor de comunicații electronice, însă din celelalte răspunsuri nu a reieșit o direcție clară de acțiune pe care o politică adecvată ar trebui să o impună.

Managementul riscului este un proces continuu și trebuie să fie parte integrantă a tuturor activităților desfășurate în vederea asigurării securității și integrității rețelelor și 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 desăvârșire. Astfel, rezultă că un număr relativ redus de furnizori au proceduri documentate în vederea asigurării securității și integrității rețelelor și serviciilor de comunicații electronice (proceduri ce includ analiza corectă, completă a riscurilor), măsurile privind securitatea și integritatea fiind luate de unii furnizori ad-hoc, în urma detecției unor probleme/apariției unor incidente.

Majoritatea furnizorilor chestionați monitorizează incidentele petrecute în rețea, însă nu toți au proceduri în vederea tratării incidentelor, în cazul acestora acțiunile și deciziile fiind luate în momentul apariției incidentului.

În ceea ce privește testarea securității și integrității rețelelor și serviciilor, o mare parte a furnizorilor nu efectuează o astfel de activitate, nefiind astfel la curent cu vulnerabilitățile existente/actuale. Din răspunsurile primite, a reieșit că doar 7 furnizori efectuează audituri de securitate pentru a se asigura că securitatea și integritatea rețelelor este una adecvată.

În ceea ce privește informarea utilizatorilor cu privire la incidentele semnificative, din răspunsurile furnizorilor a reieșit că majoritatea dintre aceștia își informează utilizatorii doar în măsura existenței unor solicitări ale acestora și a reclamațiilor primite, noțiunea de „incident

---

<sup>3</sup> Raportul privind aspectele constatate în urma analizării răspunsurilor furnizorilor se găsește la adresa: [http://www.ancom.org.ro/uploads/links\\_files/Raport\\_masuri\\_securitate\\_implementate\\_fz.pdf](http://www.ancom.org.ro/uploads/links_files/Raport_masuri_securitate_implementate_fz.pdf)

semnificativ” fiind totodată percepută în mod diferit în rândul respondenților. Niciun furnizor nu și-a informat utilizatorii din proprie inițiativă cu privire la un incident semnificativ, principala motivație fiind inexistența vreunui incident semnificativ în ultimele 12 luni și doar 2 furnizori au adus detalii privind desfășurarea (în ultimele 12 luni) a unor campanii pentru conștientizarea de către clienți a existenței fraudelor sau a altor aspecte ce pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Majoritatea furnizorilor chestionați au recunoscut necesitatea/beneficiile stabilirii unor măsuri minime de securitate și integritate ce ar trebui respectate de către furnizorii de rețele și servicii de comunicații electronice, printre cele mai importante beneficii regăsindu-se asigurarea continuității serviciilor oferite către clienți, protejarea datelor personale ale clienților și angajaților, păstrarea confidențialității, integrității și disponibilității resurselor organizației, reducerea numărului incidentelor de securitate și a reclamațiilor la adresa securității, îmbunătățirea controlului sistemelor și proceselor interne ale organizațiilor, îmbunătățirea calității serviciului, reducerea riscurilor în privința securității și integrității rețelelor și serviciilor de comunicații electronice.

Ca urmare a analizării răspunsurilor la chestionar, ANCOM consideră că este necesară stabilirea unor linii directe în scopul asigurării unei securități și integrități adecvate a rețelelor și serviciilor. Astfel, ANCOM își propune - prin proiectul de decizie privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice sau de servicii de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice - stabilirea domeniilor pe care trebuie să le vizeze măsurile de securitate adoptate de furnizori.

#### **4.3 Obligațiile ce incumbă furnizorilor de rețele și servicii de comunicații electronice**

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

##### I. Politica de securitate și managementul riscului

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

##### **1) să stabilească o politică de securitate adecvată;**

Obiectivul urmărit prin stabilirea acestui domeniu îl constituie angajarea conducerii organizației și sprijinirea demersurilor legate de asigurarea securității și integrității rețelelor și serviciilor de comunicații electronice. Conducerea organizației trebuie să stabilească o direcție clară a politicii de securitate și să demonstreze susținerea și angajamentul său pentru asigurarea securității și integrității rețelelor și serviciilor. Politica de securitate trebuie aprobată de către conducerea organizației și comunicată angajaților și părților terțe relevante într-o formă accesibilă și inteligibilă.

##### **2) să stabilească un management al riscului care:**

**a) să stabilească domeniul de aplicare, precum și 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, amenințărilor, vulnerabilităților, măsurilor existente și a consecințelor pe care pierderea/încălcarea securității le-ar putea avea asupra resurselor;**

**c) să estimeze riscurile prin evaluarea impactului pe care îl poate avea concretizarea unei amenințări care exploatează o vulnerabilitate a unei resurse și prin evaluarea probabilității de apariție a incidentelor;**

**d) să evalueze riscul;**

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

Managementul riscului trebuie să fie parte integrantă a tuturor activităților desfășurate în vederea asigurării securității și integrității rețelelor și serviciilor. Managementul riscului trebuie să fie un proces continuu care să stabilească contextul (domeniul de aplicare și limitele acestuia, precum și criteriile de bază necesare procesului de management al riscului), să identifice, să estimeze, să evalueze și să trateze riscurile. Riscurile sunt identificate, cuantificate, prioritizate prin prisma criteriilor de risc acceptate și a obiectivelor relevante pentru organizație. Rezultatele acestor procese determină acțiunile organizației și prioritățile pentru managementul riscurilor de securitate și pentru implementarea măsurilor de securitate selecționate în vederea protecției împotriva riscurilor.

Organizația trebuie să definească domeniul de aplicare și 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 continuității furnizării rețelelor și serviciilor (breșă de securitate sau o pierdere a integrității), precum și obținerea informațiilor privind modul și locul producerii acestei întreruperi. Procesul de elaborare a unui inventar al resurselor este o premisă importantă de gestionare a riscurilor. O organizație trebuie să identifice toate resursele și să documenteze importanța acestora în furnizarea rețelelor și serviciilor de comunicații electronice. Amenințările și sursele acestora trebuie identificate. Amenințările pot fi naturale sau de origine umană, pot fi accidentale sau intenționate. Trebuie identificate vulnerabilitățile care pot fi exploatate de către amenințări și astfel pot aduce prejudicii resurselor organizației. Trebuie identificate consecințele pe care un incident le poate avea asupra resurselor. Această activitate identifică prejudiciile sau consecințele 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 amenințărilor, a vulnerabilităților, a resurselor ce pot fi afectate, a consecințelor asupra resurselor și a listelor cu măsurile existente și planificate, trebuie evaluat impactul pe care incidentele le-ar putea avea asupra securității și integrității rețelelor și serviciilor, precum și probabilitatea de apariție a incidentelor. Riscul estimat reprezintă combinația dintre probabilitatea apariției/producerii unui incident și consecințele sale.

Nivelurile de risc trebuie comparate în funcție de criteriile de evaluare și cele de acceptare a riscului. Pentru a evalua riscurile, organizațiile trebuie să compare riscurile estimate cu criteriul de evaluare a riscurilor definit în timpul stabilirii contextului. În urma evaluării riscului, rezultă priorități pentru tratarea riscului considerând nivelurile estimate de risc și necesitatea luării unor măsuri/desfășurării unor activități.

Pentru tratarea riscului, sunt valabile 3 opțiuni: reducerea, evitarea și acceptarea riscului. Opțiunile pentru tratarea riscului trebuie selectate pe baza rezultatului determinării (identificării, estimării și evaluării) riscului, precum și a beneficiilor și a costurilor preconizate pentru implementarea acestor opțiuni. După ce a fost realizată tratarea riscului, trebuie determinate riscurile reziduale, ceea ce implică o nouă iterație a determinării riscului ținând cont de efectele preconizate ale opțiunii de tratare a riscului propusă. În anumite circumstanțe, 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 situații pot fi motivate de unele constrângeri (temporare sau permanente) de ordin tehnic, financiar sau operațional (de exemplu atunci când costurile aferente reducerii riscului sunt foarte ridicate, în situația în care reducerea sau evitarea unor riscuri implică apariția altor riscuri).

**3) să stabilească o structură adecvată a rolurilor și responsabilităților în asigurarea securității și integrității rețelelor și serviciilor;**

Pentru a reduce riscurile la adresa securității și integrității rețelelor și serviciilor, conducerea organizației, angajații, contractorii și alte părți terțe trebuie să înțeleagă responsabilitățile ce le revin și să dețină cunoștințe corespunzătoare rolurilor alocate.

Conducerea organizației trebuie să susțină în mod activ asigurarea securității și integrității rețelelor și serviciilor și trebuie să ceară angajaților și părților terțe să aplice măsuri de securitate în conformitate cu politicile stabilite și cu procedurile organizației.

Trebuie definite clar responsabilitățile pentru protecția resurselor și pentru desfășurarea proceselor de securitate. Dacă angajații nu sunt conștienți de responsabilitățile lor legate de asigurarea securității, aceștia pot produce pagube considerabile organizației. Organizațiile ar trebui să numească ingineri de telecomunicații și alte categorii de personal care au acreditările, cunoștințele și competențele potrivite pentru a fi responsabili de supravegherea aspectelor legate de instalarea, întreținerea, operarea și controlul rețelelor de comunicații electronice.

Condițiile contractului de angajare sau fișele de post pot fi utilizate pentru susținerea cu documente a rolurilor și responsabilităților privind asigurarea securității și integrității rețelelor și serviciilor.

**4) să stabilească o politică cu privire la cerințele de securitate pentru achiziționarea de produse și servicii de la terțe părți și asigurarea întreținerii sau gestiunii de către terțe părți a produselor și serviciilor (servicii IT, software, interconectare, baze de date, facilități asociate etc).**

Obiectivul acestui domeniu îl constituie asigurarea securității produselor și serviciilor achiziționate de la părți externe, accesate sau administrate de către părți externe. Securitatea și integritatea rețelelor și serviciilor nu ar trebui să fie redusă prin introducerea de produse și servicii provenite de la terți. În cazul externalizării unor activități, responsabilitatea privind asigurarea securității și integrității rețelelor și serviciilor revine în întregime organizației.

Riscurile la adresa securității și integrității rețelelor și serviciilor provenite de la procese care implică părți externe trebuie să fie identificate și trebuie luate măsuri de securitate corespunzătoare. În general, toate cerințele de securitate presupuse de lucrul cu părți externe trebuie să se regăsească într-un acord încheiat cu partea externă care să asigure o securitate adecvată. Partea externă trebuie să fie conștientă de obligațiile ce îi revin și trebuie să accepte responsabilitățile și obligațiile implicate de asigurarea unei securități corespunzătoare. În plus, organizația trebuie să se asigure printr-o monitorizare și evaluare continuă a faptului că serviciile și produsele furnizate de partea externă respectă cerințele de securitate stabilite și că incidentele și problemele de securitate sunt tratate în mod corespunzător.

În ceea ce privește relația cu utilizatorii serviciilor și rețelelor de comunicații electronice, organizația trebuie să se asigure că există o delimitare clară a responsabilităților în ceea ce privește infrastructura proprie și cea a utilizatorilor de servicii de comunicații 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 amenințărilor de mediu, precum și riscul de acces neautorizat. În plus, este recomandat ca starea și disponibilitatea echipamentelor să fie monitorizate de la distanță. În ceea ce privește contractul încheiat între furnizorul de rețele și servicii de comunicații electronice și utilizatori, acesta trebuie să cuprindă, conform art.51 alin.(1) lit.h) din Ordonanța de Urgență a Guvernului nr.111/2011 „*categoriile de măsuri ce pot fi luate de furnizori în cazul apariției unor incidente, amenințări și vulnerabilități privind securitatea sau integritatea rețelei sau serviciilor*”. Astfel, în caz de incidente, amenințări și vulnerabilități privind securitatea sau integritatea rețelelor sau serviciilor, furnizorii trebuie să prevadă în contracte tipul de acțiune pe care ar putea să o întreprindă și impactul acesteia asupra continuității furnizării rețelelor și serviciilor la un nivel normal (limitare, restricționare, întrerupere sau suspendare a serviciului), impactul asupra utilizatorului și condițiile în care se pot produce aceste acțiuni.

## II. Securitatea resurselor umane

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

**1) să efectueze controale de verificare de fond a candidaților pentru angajare, a contractorilor și a terților în conformitate cu legile aplicabile, reglementări și etică, proporționale cu riscurile percepute;**

Angajații, contractorii și alte părți terțe trebuie să corespundă rolurilor alocate în organizație sau în relația cu aceasta. Verificările vor avea în vedere normele legale privind protejarea datelor cu caracter personal, a vieții private și din domeniul legislației muncii. Procedurile organizației vor defini criteriile și limitele verificărilor (cine poate efectua verificarea, cum, când și de ce se

efectuează verificările). Organizațiile ar trebui să ia în considerare, de asemenea, verificări mai detaliate pentru posturi care dau accesul personalului la sistemele critice pentru furnizarea de rețele și servicii, la informații referitoare la interceptarea legală, precum și accesul la informațiile despre clienți (ex: informații personale, date de trafic).

**2) să se asigure că personalul său are cunoștințe suficiente de securitate și este instruit permanent cu privire la securitatea și integritatea rețelelor și serviciilor;**

Angajații și, acolo unde este relevant, alte părți terțe, trebuie să primească o instruire corespunzătoare și actualizări periodice în ceea ce privește politicile și procedurile organizaționale, ținând cont de atribuțiile specifice funcției lor, în vederea asigurării unui nivel adecvat de conștientizare și educație în ceea ce privește securitatea și integritatea rețelelor și serviciilor și pentru utilizarea corectă a resurselor organizației.

**3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri și responsabilități;**

Obiectivul acestui domeniu este ca organizația să se asigure că responsabilitățile legate de încetarea contractului de muncă sau schimbarea locului de muncă sunt clar definite și alocate. Angajații care părăsesc organizația trebuie să returneze organizației resursele pe care le dețin sau le utilizează în numele său pentru respectiva organizație, iar drepturile de acces trebuie revocate. Dacă angajatul deține cunoștințe importante pentru operațiile în curs de derulare, aceste informații trebuie documentate și transferate organizației. În cazul schimbării locului de muncă în cadrul aceleiași organizații, drepturile de acces trebuie ajustate astfel încât să reflecte noua poziție în organizație.

**4) să stabilească un proces disciplinar pentru angajații care produc o încălcare a securității și integrității rețelelor sau serviciilor de comunicații electronice.**

Scopul procesului disciplinar este de a preveni și descuraja încălcarea de către angajați a politicilor și procedurilor organizației referitoare la asigurarea securității și integrității rețelelor și serviciilor.

III. Securitatea și integritatea rețelelor, a facilităților asociate și a informațiilor

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

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

În vederea prevenirii accesului fizic neautorizat, a distrugerilor, a pătrunderii în interiorul organizației, a deteriorării echipamentelor și a accesului neautorizat la informații, centrele de comunicații (centrele de comutație, centrele de control și operare etc.) trebuie amplasate în zone sigure (teren rigid, mediu care nu este afectat de deteriorări produse de vânt și apă, mediu care nu este afectat de deteriorări produse de perturbații/interferențe electromagnetice etc.), trebuie să fie rezistente la cutremure și la foc și trebuie protejate de un perimetru de securitate definit (existența 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. Organizația trebuie să proiecteze și să aplice măsuri de protecție fizică împotriva incendiilor, inundațiilor, cutremurelor, exploziilor, tulburărilor publice și a oricăror alte forme de dezastre naturale sau produse de oameni.

Protejarea echipamentelor este necesară pentru reducerea riscului de acces neautorizat și pentru protejare împotriva distrugerilor și a pierderilor. Trebuie adoptate măsuri de securitate pentru minimizarea riscurilor privind potențialele amenințări fizice (furt, foc, apă, praf, vibrații, substanțe chimice, radiații electromagnetice, vandalism etc.). Echipamentele care necesită o protecție specială trebuie izolate pentru a reduce nivelul general de protecție necesar. Condițiile de mediu care ar putea afecta negativ funcționarea sistemelor de comunicații (temperatură, umiditate etc.) ar trebui monitorizate.

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

Pentru zonele izolate unde sunt instalate echipamente de comunicații (ex: stații de bază în rețele mobile), trebuie proiectate, dezvoltate și puse în aplicare măsuri de securitate speciale pentru a asigura securitatea fizică. Echipamentele trebuie monitorizate de la distanță pentru a verifica disponibilitatea, alimentarea cu energie, condițiile de mediu etc. și pentru a detecta incidentele.

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

Furnizarea rețelelor și serviciilor de comunicații electronice depinde într-o mare măsură de utilitățile 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 utilităților 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 rețelelor și serviciilor sau/și pot fi folosite baterii sau generatoare de curent. În plus, trebuie luate măsuri și pentru asigurarea funcționării adecvate a celorlalte utilități suport (alimentare cu apă, aer condiționat etc.).

## **3) să stabilească măsuri de securitate adecvate pentru accesul (logic) la rețea și la sistemele informatice;**

Organizația trebuie să asigure accesul autorizat al angajaților și să prevină accesul neautorizat la resursele organizației. Pentru controlul alocării drepturilor de acces la sisteme și 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 organizației. Utilizatorii trebuie să fie informați despre responsabilitățile lor în menținerea unui sistem eficient de control al accesului, în special în privința folosirii parolelor și a securității echipamentelor. Sistemele critice în furnizarea rețelelor și serviciilor de comunicații electronice trebuie să aibă alocat un spațiu dedicat (izolat).

## **4) să stabilească măsuri de securitate adecvate pentru a asigura protecția rețelelor și serviciilor de comunicații electronice împotriva codurilor cu potențial dăunător, codurilor mobile neautorizate și a atacurilor informatice, inclusiv DoS/DDoS.**

Rețelele de comunicații trebuie să fie protejate corespunzător în scopul de a preveni și detecta atacurile realizate cu ajutorul programelor malițioase, precum și tentativele de a indisponibiliza sau bloca resurse/servicii, acțiuni ce pot afecta furnizarea rețelelor și serviciilor. Protecția împotriva codurilor cu potențial dăunător trebuie să se bazeze pe programe de detectare și reparare/recuperare, pe conștientizarea nevoii de securitate și pe gestionarea corespunzătoare a accesului la sistemele de comunicații.

În scopul de a proteja echipamentele care utilizează protocolul IP (serve, routere etc.) de atacuri informatice (ex. DoS/DDoS), organizația trebuie să stabilească și să implementeze măsuri de contracarare a unor astfel de atacuri în scopul de a asigura continuitatea furnizării rețelelor și serviciilor (ex: mecanisme de filtrare a pachetelor de date, restricții ale porturilor de comunicații folosite pentru atacurile informatice, reducerea sau suspendarea activității unor echipamente).

Dat fiind faptul că atacurile informatice pot fi generate din foarte multe rețele localizate în spații geografice diferite, este recomandabil ca furnizorii să lucreze în strânsă colaborare cu ceilalți furnizori, precum și cu organizațiile interne și internaționale cu atribuții și competențe în răspunsul la atacurile informatice.

În scopul împiedicării atacurilor informatice inițiate de la computerele infectate ale utilizatorilor de servicii de comunicații electronice, furnizorii trebuie să precizeze în contractele încheiate cu aceștia măsurile ce pot fi luate în cazul apariției unor incidente, amenințări (restricționarea, suspendarea serviciului etc.). În același timp, furnizorii ar trebui să atragă atenția utilizatorilor cu privire la amenințările existente în mediul electronic (virusi, botnet etc.) și să îi încurajeze să ia măsurile de protecție necesare.

#### IV. Managementul operațiunilor

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

##### **1) să stabilească proceduri operaționale și responsabilități adecvate;**

Pentru a se asigura instalarea, operarea, controlul și întreținerea în mod corect și în condiții de securitate a rețelei prin care se furnizează serviciile de comunicații electronice, trebuie stabilite responsabilități și proceduri privind managementul, instalarea, utilizarea/operarea adecvată a resurselor hardware și software. Procedurile operaționale trebuie să fie documentate, păstrate și puse la dispoziția tuturor celor avizați. Procedurile trebuie să specifice instrucțiunile detaliate pentru execuția fiecăreia dintre activitățile prevăzute mai sus.

##### **2) să stabilească proceduri privind managementul schimbărilor efectuate în rețeaua de comunicații electronice și în software-urile de aplicații;**

Controlul neadecvat al schimbărilor în rețelele de comunicații electronice și în software-ul de aplicații constituie o cauză frecventă a defecțiunilor și a breșelor de securitate. Schimbările suferite de mediul operațional, în special atunci când se transferă un sistem din faza de dezvoltare în cea operațională, pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice. Schimbările în sistemele operaționale trebuie realizate numai atunci când există motive întemeiate.

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

Trebuie menținut un control strict asupra schimbărilor efectuate în sistemele operaționale și în software-ul de aplicații având în vedere, în principal, următoarele aspecte: identificarea și înregistrarea schimbărilor semnificative, planificarea și testarea schimbărilor, evaluarea impactului potențial, inclusiv asupra securității și integrității rețelelor și serviciilor, proceduri de rezervă pentru recuperare în caz de schimbări nereușite sau evenimente neprevăzute.

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

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

Trebuie realizate estimări și planificări privind cerințele necesare în vederea atingerii performanțelor/capacităților adecvate.

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

În vederea asigurării unei protecții corespunzătoare a resurselor organizației, toate resursele trebuie înregistrate și trebuie să aibă un deținător autorizat. Resursele organizației au un grad diferit de sensibilitate și importanță în activitatea de furnizare a rețelelor și serviciilor, astfel încât, pentru asigurarea unui grad de protecție adecvat și pentru stabilirea unor măsuri de utilizare corespunzătoare, acestea trebuie clasificate în mod corespunzător.

Resursele unui furnizor de rețele și servicii de comunicații electronice includ:

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

b) software: de control al comunicațiilor, management al operațiunilor, de management al informațiilor privind utilizatorii, de taxare, de aplicații, de sistem, de dezvoltare și utilități etc.

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

d) servicii: de procesare a informațiilor, de rețea, utilități suport (alimentare cu energie electrică, iluminat, control al temperaturii și umidității, stingere a incendiilor) etc.

e) oameni: ingineri de comunicații, specialiști IT etc.

f) intangibile: controlul organizației, „know-how” etc.

În vederea stabilirii gradului de sensibilitate și importanță a resurselor organizației în activitatea de furnizare a rețelelor și serviciilor, furnizorii trebuie să ia în considerare cerințele legale privind asigurarea în mod neîntrerupt a posibilității efectuării apelurilor de urgență. De asemenea, furnizorii trebuie să țină seama de prevederile legale privind securitatea prelucrării datelor cu caracter personal și cele referitoare la confidențialitatea comunicărilor, precum și a datelor de trafic aferente.

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

#### V. Managementul incidentelor

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

**1) să stabilească procese și proceduri pentru managementul incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente și escaladarea acestuia), inclusiv prin definirea rolurilor și responsabilităților;**

Procedurile pentru managementul incidentelor, precum și definirea responsabilităților sunt necesare pentru a asigura un răspuns rapid, eficace și sistematic la incidentele care afectează securitatea și integritatea rețelelor și serviciilor. Procedurile trebuie să stabilească modul de abordare a diverselor tipuri de incidente, identificarea impactului unui incident (asupra serviciilor, utilizatorilor, resurselor, în funcție de localizare/arie geografică etc.), analiza și identificarea cauzei incidentului, măsurile care pot fi luate pentru a minimiza efectele incidentului și pentru a remedia defecțiunile care au cauzat incidentul, planificarea și implementarea acțiunilor corective pentru împiedicarea reapariției sale, comunicarea cu cei afectați de incident, colectarea probelor etc. Prin intermediul acestor proceduri, cei răspunzători de managementul incidentelor înțeleg prioritatea organizației în ceea ce privește tratarea acestor incidente.

Procesele pentru managementul incidentelor trebuie să asigure că amenințările, vulnerabilitățile și incidentele care pot afecta securitatea și integritatea rețelelor și serviciilor sunt comunicate și tratate în mod corespunzător, permițându-se aplicarea unor măsuri corective în timp util.

În plus față de monitorizarea sistemelor și a alertelor, incidentele care pot afecta continuitatea furnizării rețelelor și serviciilor pot fi detectate și prin raportarea evenimentelor, amenințărilor și a vulnerabilităților. Astfel, în vederea prevenirii apariției incidentelor, trebuie să existe proceduri de raportare a evenimentelor, a vulnerabilităților și a amenințărilor care să stabilească modul de raportare, precum și acțiunile ce trebuie întreprinse.

Evaluarea/triajul reprezintă procesul de sortare, clasificare, corelare, priorizare a evenimentelor, a rapoartelor despre incidente și a vulnerabilităților. Prin evaluarea incidentelor, se identifică potențialele probleme de securitate și se prioritizează activitățile. Astfel, informațiile primite sunt revizuite pentru a stabili validitatea acestora și pentru a determina tipul de eveniment raportat, precum și pentru a stabili măsurile inițiale care trebuie luate. Evaluarea permite ca toate informațiile 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 și corelarea cu alte evenimente și incidente. În funcție de tipul incidentului și de impactul acestuia, organizația trebuie să aibă un proces de escaladare (transmiterea informațiilor către șefi ierarhici superiori – escaladare ierarhică sau către alte compartimente competente, cu solicitarea unei acțiuni din partea acestora – escaladare funcțională) prin care să se stabilească acțiunile ce trebuie întreprinse, precum și responsabilitățile corespunzătoare. Astfel, organizația trebuie să specifice în ce condiții diferitele moduri de răspuns/reacție la un incident sunt invocate/apelate (și părțile interesate notificate), inclusiv condițiile pentru activarea planurilor pentru situațiile deosebite.

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



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

Informațiile strânse în urma evaluării incidentelor trebuie folosite pentru identificarea incidentelor care se repetă sau au un impact semnificativ. Organizațiile trebuie să stabilească mecanisme și procese prin care lecțiile învățate în urma unui incident sunt împărtășite în interiorul organizației. Astfel, pot fi identificate metode de a îmbunătăți atât nivelul de securitate, cât și mecanismul de tratare a incidentelor (managementul incidentelor).

## **2) să stabilească un sistem de detectare a incidentelor;**

Procesul de detectare a incidentelor implică/presupune orice observație a unei activități rău intenționate, suspecte sau accidentale, precum și colectarea de informații care pot oferi o perspectivă asupra amenințărilor curente sau a riscurilor la adresa securității și integrității rețelelor și serviciilor de comunicații electronice. În procesul de detectare, informațiile despre incidente, vulnerabilități și amenințări sunt colectate reactiv (de la surse interne sau externe, sub formă de rapoarte sau notificări) sau proactiv (monitorizarea indicatorilor care pot anunța iminența unui incident sau exploatarea unei vulnerabilități, prin mecanisme cum ar fi sisteme de monitorizare a rețelei sau prin sisteme de detecție a intruziunilor - IDS). Odată detectate, activitățile sau informațiile privind incidente, vulnerabilități și amenințări 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 și către alte autorități responsabile, precum și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori de rețele și servicii de comunicații electronice afectați, media, clienți, parteneri de afaceri etc.).**

Conform prezentului proiect de decizie, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a transmite ANCOM o notificare inițială privind existența/apariția unui incident cu impact semnificativ asupra furnizării rețelelor și serviciilor în 6 ore de la detectarea acestuia și o notificare finală privind incidentul în două săptămâni de la detectarea acestuia, în condițiile și formatul prevăzute în proiectul de decizie. Astfel, prin procedurile interne, furnizorul trebuie să creeze mecanisme care să asigure că informațiile pe care trebuie să le prezinte ANCOM sunt disponibile și complete, iar raportarea se va face în condițiile și formatul stabilite de autoritate.

Pentru a asigura transparența informațiilor cu privire la incidentele care afectează semnificativ securitatea și integritatea rețelelor și serviciilor de comunicații 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 rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului obligația de a informa publicul cu privire la existența unui incident cu impact semnificativ, stabilind și modalitățile alternative pentru realizarea acestei informări. Aceste modalități prevăzute în cuprinsul proiectului de decizie nu exclud însă posibilitatea informării utilizatorilor, la cerere, prin intermediul serviciului de relații cu clienții.

Independent de solicitările exprese venite din partea Autorității, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pot stabili modalități alternative și facultative de informare a publicului cu privire la existența unui incident cu impact semnificativ, acestea fiind, de altfel, și o cale de a îmbunătăți comunicarea cu utilizatorii, fiind o indicație a angajamentului și a capacității furnizorului de a restabili rapid serviciile.

Contactele cu grupurile specializate de interes sau cu alte forumuri de specialiști în securitate trebuie menținute în vederea accesului la informații privind securitatea și integritatea rețelelor și serviciilor (ex: informații privind amenințările și vulnerabilitățile actuale, recomandări și rapoarte privind atacuri și vulnerabilități, bune practici în asigurarea securității și integrității și răspuns la incidente). Pot fi create acorduri de schimb de informații pentru îmbunătățirea cooperării și a coordonării problemelor de securitate.

## VI. Managementul continuității afacerii

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

### **1) să stabilească o strategie pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în situațiile generate de perturbări grave ale funcționării rețelei sau ale serviciului;**

Pentru a contracara discontinuitatea furnizării rețelelor și serviciilor în cazuri de perturbare gravă a funcționării rețelei sau a serviciului (de ex. în urma producerii unui dezastru sau a unei situații de forță majoră), organizația trebuie să stabilească o strategie de acțiune în astfel de cazuri.

Evenimentele (sau succesiunea de evenimente) care pot determina întreruperi ale proceselor afacerii organizației, precum și resursele implicate în procesele critice ale organizației trebuie identificate împreună cu probabilitatea și impactul unor asemenea discontinuități din punct de vedere al duratei, nivelului pagubelor și perioadei de redresare. În funcție de rezultatele determinării riscurilor, trebuie elaborată o strategie pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în situații deosebite.

În procesele de stabilire și elaborare a strategiei pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în situații deosebite, furnizorii trebuie să aibă în vedere implementarea de măsuri adecvate pentru a reduce probabilitatea apariției perturbărilor grave ale funcționării rețelei sau serviciului sau de reducere a eventualelor efecte, precum și obligațiile stabilite în sarcina acestora prin cadrul legal în vigoare din domeniul comunicațiilor electronice, în funcție de specificul activității sale.

Strategia de continuitate vizează alegerea unor metode alternative de operare și pot fi folosite ulterior producerii unei situații deosebite, în scopul de a menține operațiunile la un nivel acceptabil sau de a le relua într-un interval de timp cât mai scurt. Strategia de continuitate implică acțiuni 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 și/sau achiziționarea unor echipamente de rezervă) și stabilirea de mecanisme de priorizare, suspendare sau restricționare a anumitor servicii.

### **2) să dețină capacități de implementare a strategiei de continuitate și să stabilească planuri de continuitate și de recuperare;**

În vederea implementării strategiei de continuitate, organizația trebuie să identifice și să asigure suficiente resurse financiare, organizaționale, tehnice și de mediu.

În scopul implementării unei strategii de continuitate eficiente, organizația poate folosi mijloace de colectare în avans a informațiilor cu privire la dezastru naturale sau alte evenimente (ex: atac DDoS) care ar putea afecta continuitatea furnizării serviciilor și rețelelor (ex: colectarea informațiilor despre evoluția vremii, colectarea anomaliilor de trafic și recepționarea avertizărilor timpurii), iar personalul relevant ar trebui informat în timp util. În scopul unui răspuns cât mai prompt și eficient în cazul producerii unei situații deosebite, organizația trebuie să stabilească acțiunile premergătoare unei eventuale intervenții ale instituțiilor cărora le revine responsabilitatea privind organizarea apărării împotriva dezastrului, în condițiile legislației aplicabile în domeniu.

Personalul reprezintă una din resursele principale angrenate în procesul de recuperare în caz de dezastru. Astfel, personalul organizației, inclusiv managementul, trebuie să cunoască responsabilitățile și rolurile specifice în cazul apariției unei perturbări grave a funcționării rețelei sau serviciului și să fie instruit corespunzător.

Strategiile de continuitate alese trebuie susținute de planuri de continuitate și recuperare.

Planurile de continuitate și recuperare reprezintă o colecție documentată de proceduri și informații, care sunt dezvoltate, compilate și disponibile pentru a fi utilizate în cazul producerii unei perturbări grave a funcționării rețelei sau serviciului, în scopul de a permite continuarea furnizării serviciilor de comunicații electronice la un nivel acceptabil și restabilirea furnizării serviciilor la nivelul anterior producerii incidentului.

Strategia de continuitate presupune parcurgerea a două etape care angrenează resurse și acțiuni distincte și care constau în asigurarea continuității furnizării serviciilor de comunicații, precum și în restabilirea furnizării serviciilor la nivelul anterior producerii incidentului.

Fiecare plan trebuie să specifice condițiile de activare, procedura de escaladare, resursele implicate cât și persoanele responsabile de executarea fiecărei acțiuni din plan.

În procesul de implementare a planurilor de continuitate și recuperare, se vor avea în vedere și acțiuni de urgență pentru a asigura securitatea personalului.

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

#### VII. Monitorizare, testare și audit

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația:

#### **1) să stabilească politici de monitorizare a sistemelor, precum și politici privind jurnalele de sistem;**

Sistemele trebuie monitorizate și evenimentele care pot afecta securitatea și integritatea rețelilor și serviciilor trebuie înregistrate. Trebuie ținute jurnale/înregistrări de operator, iar defecțiunile trebuie înregistrate pentru a se asigura identificarea problemelor. Monitorizarea alarmelor, precum și a altor aspecte legate de performanța rețelei este necesară pentru a evita afectarea/alterarea funcționării rețelilor de comunicații electronice sau pentru a lua măsuri de remediere a problemelor apărute. O monitorizare efectivă și eficientă oferă acces la informații critice pentru a identifica utilizatorii afectați, pentru a verifica starea echipamentelor și circuitelor și pentru a asigura o recuperare eficientă și rapidă a furnizării rețelilor și serviciilor de comunicații electronice. Nivelul de monitorizare necesar pentru fiecare sistem depinde de nivelul determinat de risc, ținând cont de factori precum criticitatea și sensibilitatea proceselor și sistemelor, experiența acumulată în privința infiltrărilor, a vulnerabilităților și a utilizării neconforme a sistemelor, interconectarea sistemelor etc. Jurnalele, înregistrările ajută la analiza problemelor, identificarea cauzelor și a vulnerabilităților și pot oferi suport pentru rezolvarea incidentelor. Totodată, monitorizarea va fi utilizată și pentru verificarea eficacității măsurilor de securitate adoptate.

#### **2) să stabilească politici pentru testarea, inclusiv prin exerciții, a planurilor de continuitate și de recuperare în cazul perturbărilor grave ale funcționării rețelei sau serviciului;**

Planurile de recuperare și backup în cazul situațiilor deosebite trebuie testate și actualizate în mod regulat pentru a se asigura că sunt eficiente și adecvate. Testarea acestor planuri va asigura cunoașterea de către toți membrii echipei a planurilor, a atribuțiilor și a responsabilităților pentru asigurarea continuității afacerii. Planificarea testelor trebuie să indice cum și când trebuie testat fiecare element. Trebuie folosite mai multe tehnici pentru ca organizația să se asigure că planurile vor opera și în realitate: testarea diverselor scenarii, simulări, testări tehnice, testări prin utilizarea unui alt amplasament (diferit de amplasamentul principal), teste privind serviciile furnizate de terți, repetiții complete.

În ceea ce privește planurile de recuperare pentru sistemele individuale, acestea trebuie testate pentru a avea siguranța că răspund cerințelor organizației. În cazul sistemelor importante, procedurile de recuperare trebuie să cuprindă toate elementele (echipamente, date, aplicații) necesare recuperării întregului sistem în caz de dezastru sau alte situații deosebite.

#### **3) să stabilească politici pentru testarea echipamentelor, sistemelor și software-lor, în special înainte de conectarea/punerea lor în funcțiune;**

Implementarea modificărilor în rețeaua de comunicații electronice, precum și în sistemele folosite pentru operarea și monitorizarea furnizării rețelilor și serviciilor, trebuie controlată prin utilizarea unor proceduri formale pentru controlul schimbărilor în vederea minimizării posibilității de deteriorare a sistemelor sau de introducere de noi vulnerabilități. Introducerea unor echipamente, sisteme și software-uri noi, precum și schimbările majore aduse celor existente trebuie să urmeze un proces formal de documentare, specificare, testare, control al calității și implementare.

Este bine ca testarea să se facă într-un mediu separat atât de cel de producție, cât și de cel de dezvoltare pentru a asigura o protecție suplimentară. În plus, informațiile și echipamentele folosite trebuie să permită testarea în mod adecvat a funcționării în condiții cât mai aproape de cele existente în realitate în procesul de furnizare a rețelilor și serviciilor de comunicații electronice.

**4) să stabilească o politică adecvată pentru evaluarea și testarea securității tuturor resurselor;**

Securitatea și integritatea rețelelor și serviciilor de comunicații electronice trebuie analizată în mod periodic pentru verificarea gradului de eficiență a măsurilor implementate. Verificarea securității implică examinarea echipamentelor, sistemelor și software-ului pentru asigurarea implementării corecte a măsurilor de securitate. Această verificare poate presupune și efectuarea de teste de penetrare și determinare a vulnerabilităților. Testele de penetrare și de determinare a vulnerabilităților oferă o imagine a securității și integrității rețelei și serviciului la un moment dat și nu pot înlocui determinarea riscului.

**5) să stabilească o politică pentru monitorizarea conformității și pentru audit, cu un proces de raportare a conformității și de rezolvare a deficiențelor constatate în timpul auditului.**

Pentru a asigura conformitatea cu standardele și politicile de securitate, organizația trebuie să se asigure că toate procedurile de securitate sunt respectate. Dacă în urma analizei sunt constatate neconformități, organizația trebuie să stabilească motivele, să evalueze necesitatea de a acționa astfel încât neconformitatea să nu se mai repete, să stabilească și să implementeze acțiuni corective adecvate, în timp util și să analizeze consecințele acestora. Rezultatele analizelor și acțiunilor corective trebuie înregistrate, iar înregistrările păstrate.

Cerințele de audit și activitățile care implică verificări asupra sistemelor operaționale trebuie planificate astfel încât să minimizeze riscul întreruperii proceselor de afaceri. Dacă în procesul de audit sunt implicați terți, organizația trebuie să ia măsuri de securitate astfel încât riscurile adiționale presupuse de această activitate să fie eliminate/minimizate. Este de preferat ca sistemele/instrumentele de auditare folosite să fie separate de cele de producție și de dezvoltare.

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

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a evalua și, dacă este cazul, de a actualiza măsurile de securitate specificate în proiectul de decizie ori de câte ori este necesar, însă cel puțin o dată la 12 luni. Măsurile de securitate trebuie să fie analizate și evaluate cel puțin o dată la 12 luni sau ori de câte ori apar schimbări semnificative în mediul organizațional, în condițiile de desfășurare a afacerii, în cadrul legal sau în condițiile tehnice, pentru a asigura o securitate și integritate a rețelelor și serviciilor adecvată și eficace. Analiza trebuie să cuprindă determinarea oportunităților de îmbunătățire și a nevoii de modificare a modului de abordare a securității (politici, măsuri de securitate și obiective, procese și proceduri).

O atenție deosebită trebuie acordată procesului de management al riscului care trebuie monitorizat, revizuit și îmbunătățit continuu. Monitorizarea și revizuirea permanentă sunt necesare pentru a asigura că rezultatul determinării și tratării riscului, contextul și planurile de management rămân relevante și corespund circumstanțelor de la un moment dat. Riscurile nu sunt statice, amenințările, vulnerabilitățile, probabilitățile de apariție a unui incident sau consecințele acestuia modificându-se în timp (uneori chiar într-un interval de timp foarte scurt și în mod imprevizibil).

Măsurile de securitate, precum și obiectivele acestor măsuri pot fi îmbunătățite și în urma rezultatelor analizelor de management anterioare, a acțiunilor preventive și corective, a analizelor privind conformitatea cu politicile și procedurile organizației, a evaluării periodice a eficienței măsurilor de securitate, luând în considerare rezultatele auditurilor de securitate, a incidentelor raportate, precum și a sugestiilor/feedback-ului diferitelor părți interesate.

De asemenea, conform art. 49 alin. (2) din Ordonanța de Urgență a Guvernului nr. 111/2011, „ANCOM poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și serviciilor, precum și respectarea acestora în cazurile de încălcare a securității rețelelor și serviciilor sau pierdere a integrității rețelelor, putând impune măsuri în acest sens”. Măsurile impuse de ANCOM trebuie să asigure un nivel adecvat al securității rețelelor și serviciilor de comunicații electronice și vor trebui implementate de către furnizorii de rețele și servicii de comunicații electronice. În plus, ANCOM poate elabora ghiduri de bune practici în vederea asigurării unui nivel adecvat al securității rețelelor și serviciilor de comunicații

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 și integritatea rețelelor și serviciilor de comunicații electronice**

### **5.1. Definiție și scop**

În înțelesul acestui proiect de decizie, un incident reprezintă un eveniment care poate afecta sau amenința, direct sau indirect, securitatea și integritatea rețelelor și serviciilor de comunicații electronice. Un eveniment reprezintă un fenomen observabil, care nu poate fi anticipat sau controlat în totalitate.

O procedură națională eficientă de raportare oferă numeroase beneficii. Un astfel de sistem facilitează informarea, în timp util, a părților interesate în legătură cu producerea unui incident. În același timp, ANCOM poate urmări eficiența măsurilor de securitate adoptate de furnizori, precum și a răspunsului acestora în momentul producerii incidentelor, poate colecta date referitoare la tipurile de amenințări și vulnerabilități ce vor fi utilizate în cadrul unei analize aprofundate a securității rețelelor și serviciilor, constituind o bază pentru emiterea de recomandări și ghiduri de bune practici.

Deoarece gradul de interconectare a rețelelor de comunicații electronice devine din ce în ce mai mare, nevoia de a partaja informațiile referitoare la amenințările la adresa securității acestora crește în mod constant. Astfel, informațiile puse la dispoziția Autorității prin intermediul sistemului de raportare pot fi valorificate prin intermediul oferirii de ghiduri și bune practici de către ANCOM.

Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înțelegeri clare a naturii și amplitudinii provocărilor existente la adresa securității și integrității rețelelor și serviciilor.

În acest context, raportarea incidentelor joacă un rol important în consolidarea securității și integrității rețelelor și serviciilor de comunicații electronice, deoarece contribuie la asigurarea:

- unei diseminări rapide a informațiilor între părțile interesate;
- accesului la o arie largă de expertiză cu privire la astfel de incidente;
- unei analize a amenințărilor și vulnerabilităților la adresa securității și integrității rețelelor și serviciilor;
- identificării de bune practici bazate pe lecțiile învățate în procesul de management al incidentelor;

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

În plus, sunt urmărite și următoarele obiective:

- identificarea cauzelor incidentelor, inclusiv amenințările și vulnerabilitățile cele mai frecvente;
- urmărirea lecțiilor învățate în urma aplicării măsurilor de detecție, răspuns și de recuperare luate în timpul, precum și după incident;
- elaborarea de bune practici pentru asigurarea securității rețelelor și serviciilor și modificarea acestora, dacă este necesar;
- înțelegerea tendințelor viitoare;
- creșterea transparenței pieței față de utilizatori.

Prin analizarea incidentelor cu impact semnificativ, ANCOM poate evalua nivelul de securitate a rețelelor și serviciilor de comunicații electronice și a măsurilor de reglementare anterioare. În cazul incidentelor cu impact semnificativ, ANCOM poate analiza în detaliu cauzele incidentului, acțiunile furnizorului de rețele publice de comunicații electronice sau de servicii de comunicații electronice și 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 tendințele.

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

- elaborarea unui raport anual cu privire la securitatea și integritatea rețelelor și serviciilor de comunicații electronice;
- informarea în mod corespunzător, acolo unde consideră necesar, a celorlalte autorități naționale de reglementare din celelalte state și ENISA cu privire la incidentele de încălcare a securității rețelelor și serviciilor sau de pierdere a integrității rețelelor;

- emiterea de recomandări și bune practici privind managementul/gestionarea incidentelor pentru a maximiza valoarea lecțiilor învățate la nivel național;
- crearea de statistici referitoare la cauzele incidentelor, a tipurilor de atacuri, amenințări și vulnerabilități, la serviciile și rețelele cele mai afectate de incidente etc.

Astfel, conform art. 47 alin. (3) și (4) din Ordonanța de urgență a Guvernului nr. 111/2011, ANCOM trebuie:

- să prezinte anual Comisiei Europene și ENISA un raport de sinteză privind notificările primite de la furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și măsurile luate pentru asigurarea securității și integrității rețelelor și serviciilor;

- să informeze autoritățile naționale de reglementare din celelalte state și ENISA în cazurile în care un incident poate afecta furnizorii de comunicații electronice din alt stat membru.

Schema de raportare poate fi revizuită astfel încât să reflecte feedback-ul primit de la părțile interesate și experiența câștigată prin implementarea acestor noi cerințe. De asemenea, vor fi luate în considerare și 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 înțelegere a modului în care incidentele sunt detectate, tratate și rezolvate. Prin stabilirea unei structuri și clasificări generale a incidentelor, este posibilă obținerea 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 relații cu clienții al furnizorului sau de o terță parte (mass-media, autorități publice sau alte organizații) sau poate fi detectat de personalul furnizorului (prin intermediul alarmelor din centrul operațional 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 inițială a situației pentru a confirma categoria incidentului și gravitatea acestuia. Acest lucru se face prin clasificarea tipului evenimentului, precum și prin evaluarea consecințelor acestuia. În funcție de caracteristicile evenimentului, acesta poate fi clasificat în mai multe clase de gravitate și este tratat în mod diferit de organizație. Analizarea unui incident permite furnizorului să înțeleagă:

- domeniul afectat de incident: numărul de sisteme afectate;
- impactul: gradul în care fiecare sistem este afectat;
- cât de critic este impactul: influența incidentului asupra funcționării rețelei și a serviciului;
- prioritatea cu care trebuie răspuns la acest incident.

Tratarea unui incident presupune mai multe etape: identificarea tipului de incident și a consecințelor acestuia, limitarea consecințelor incidentului, eliminarea cauzei și prevenirea reapariției acesteia, revenirea la un mod normal de furnizare a serviciilor, evaluarea modului de acțiune al organizației și eficienței în procesul de eliminare a consecințelor acestui incident și nu în ultimul rând lecțiile învățate cu această ocazie astfel încât greșelile descoperite să nu se mai repete.

Este esențial ca furnizorul să implementeze un sistem de evidență 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, consecințele și costurile pe care le implică pentru organizație. Un aspect foarte important este înregistrarea tuturor incidentelor. Deși multe dintre incidente nu prezintă un pericol major pentru organizație atunci când sunt văzute ca evenimente izolate, analizate împreună pot dezvălui modul în care apar incidentele și cauzele acestora.

Managementul unui incident trebuie să fie proactiv, controlat și coerent. De obicei, acțiunile multor organizații sunt de tip reactiv, acestea concentrându-se asupra tratării/răspunsului la incident prin acțiuni întreprinse pentru a rezolva sau pentru a atenua consecințele unui incident atunci când acesta a avut loc. Acestea trebuie să își extindă mijloacele de acțiune și prin măsuri proactive de analizare a potențialelor amenințări și riscuri, astfel încât să prevină apariția incidentelor.

Furnizorii de rețele și servicii de comunicații electronice trebuie să dezvolte procese care să trateze/răspundă la incidente, dar și procese care să prevină apariția sau reapariția incidentelor. Acestea includ procese pentru planificarea și implementarea unui management al incidentelor,

îmbunătățirea securității infrastructurii organizației pentru a preveni incidentele sau pentru a atenua efectele unui incident, detectarea, trierea și 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 și acțiuni întreprinse pentru a crea un mecanism de raportare a incidentelor.

În funcție 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 informații în timp real și coordonarea în timpul situațiilor de urgență sau în timpul desfășurării incidentelor.

b) Prevenirea incidentelor (întreruperilor)

Acest tip de raportare se axează pe reducerea întreruperilor în furnizarea rețelelor și serviciilor de comunicații electronice ca un mijloc de a garanta utilizatorilor un anumit nivel al calității serviciului. Scheme de acest tip au ca obiectiv colectarea la nivelul sectorului de comunicații electronice a informațiilor privind amenințările și folosirea acestor informații astfel încât întreruperile în furnizarea serviciilor să fie prevenite. Pe baza acestor rapoarte, se pot efectua analize și audituri în scopul descoperirii amenințărilor potențiale și aplicării unor măsuri de contracarare a acestora.

c) Rectificarea deficiențelor/incidentelor

Acest tip de raportare se axează pe obligațiile furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului de a lua toate măsurile adecvate pentru a administra riscurile care pot afecta securitatea rețelelor și serviciilor astfel încât, printre altele, să prevină sau să minimizeze impactul acestor incidente asupra utilizatorilor, precum și pe obligația furnizorilor de rețele publice de comunicații electronice de a asigura continuitatea furnizării serviciilor prin intermediul acestor rețele. Prin respectarea acestor obligații, se pot atinge obiectivele de reziliență/securitate a comunicațiilor electronice, precum și de protecție a utilizatorilor. Astfel, incidentele, precum și acțiunile întreprinse de furnizori sunt urmărite/monitorizate pentru ca autoritatea să se asigure ca aceleași 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 esențial să existe proceduri prin care să fie colectate informații complete care să servească drept punct de plecare pentru ca autoritatea să impună corectarea deficiențelor constatate și implementarea modificărilor necesare. Autoritatea are dreptul de a cere informații referitoare la incidente și explicații privind măsurile adoptate de furnizori astfel încât incidentele să nu se mai repete. În cazul schemelor de tip prevenirea incidentelor și rectificarea deficiențelor/incidentelor, acestea tind să se axeze pe impactul incidentelor asupra utilizatorilor serviciului (numărul utilizatorilor afectați, suprafața geografică afectată și durata unui incident).

Prin impunerea obligației de raportare a incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, ANCOM urmărește și rectificarea deficiențelor/incidentelor de către furnizori și prevenirea apariției incidentelor.

Pe lângă o definiție clară a domeniului de aplicare și 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:

- definiția 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 luați în considerare pentru a raporta/defini un incident;
- valorile/pragurile acestor parametri care declanșează mecanismul de raportare.

### **5.4. Obligațiile ce incumbă furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului**

Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au următoarele obligații:

a) de a transmite ANCOM o notificare inițială privind existența/apariția unui incident cu impact semnificativ asupra furnizării rețelelor și serviciilor în termen de 6 ore de la detectarea acestuia, la adresa de poștă electronică [incidente@ancom.org.ro](mailto:incidente@ancom.org.ro);

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

Folosind investigațiile și rapoartele trimise de furnizori, autoritatea poate iniția o investigație pentru a verifica măsurile de securitate implementate de către aceștia și poate solicita îmbunătățiri ale măsurilor de securitate. De asemenea, în cazul în care un furnizor nu raportează un incident semnificativ conform prevederilor acestei decizii, acesta va fi sancționat în baza art. 142 pct. 16 din Ordonanța de urgență a Guvernului nr. 111/2011.

### **5.5. Cauza unui incident care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice**

Cauza unui incident reprezintă evenimentul sau factorul care declanșează incidentul. ANCOM a identificat 5 cauze ale incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice: eroare umană, eroare de sistem, fenomen natural, acțiune rău intenționată și cauză externă/parte terță.

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

Categoria eroare de sistem va fi folosită pentru a include incidentele datorate defecțiunilor hardware, erorilor de programare ale software-ului, dimensionării și/sau implementării greșite a rețelei și erorilor în elaborarea politicilor, procedurilor sau manualelor.

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

Categoria acțiune rău intenționată va include incidentele cauzate de acțiunile efectuate în mod deliberat, ca de exemplu: accesul neautorizat la echipamente de rețea, platforme, aplicații (software), baze de date, atacurile de tip DoS (refuzul serviciilor) sau DDoS (refuzul serviciilor realizat în mod distribuit), efectuare de modificări neautorizate ale sistemelor și datelor, vandalism, sabotaj, furt etc.

Nu toate acțiunile (sau inacțiunile) care pot provoca un incident se datorează furnizorului de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și sunt sub controlul direct al acestuia. Astfel, mai există și incidente provocate de părți externe, precum: distrugerea unor echipamente și cabluri în urma unor lucrări de construcție, defecțiuni în rețeaua de distribuție 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 construcție, cauzele incidentului vor fi eroare umană și cauză externă/parte terță).

Unele incidente pot avea o cauză inițială și 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 inițială, iar câmpul privind „mai multe informații despre cauza incidentului” va cuprinde detalii referitoare atât la cauza inițială, cât și la cauza subsecventă care a declanșat 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 inițială este eroare de sistem al unui echipament al furnizorului de utilități și cauză externă/parte terță, iar cauza subsecventă este eroare de sistem – defecțiune hardware al unui echipament de comunicații electronice).

### **5.6. Parametrii și valorile acestora, factori declanșatori ai mecanismului de raportare**

În spatele fiecărui sistem de raportare trebuie să existe o idee clară în ceea ce privește criteriile și pragurile care ar trebui să declanșeze mecanismul de raportare a incidentelor. Astfel, parametrii care vor fi luați în considerare la evaluarea impactului sunt numărul de conexiuni afectate și 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 declanșat în momentul în care un incident afectează un număr mai mare de 5.000 de conexiuni timp de cel puțin 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 rețele publice fixe pe care o operează sau prin rețeaua publică fixă a unui terț; un abonat poate avea alocate una sau mai multe linii de acces;
- în cazul serviciilor de telefonie, acces la internet și transmisiuni de date furnizate prin intermediul rețelelor 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 și nu ia în considerare tipul utilizatorilor afectați. Astfel, fiecare utilizator are aceeași importanță și nu există nicio distincție, de exemplu, între un utilizator rezidențial și o bancă sau un spital. Nivelul de importanță al unei infrastructuri deservite de către un furnizor de comunicații electronice nu va fi parte din domeniul de aplicare al raportării către ANCOM, deoarece infrastructura critică nu face obiectul Ordonanței de Urgență 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 funcționare.

În determinarea impactului unui incident, au fost luate în considerare mai multe cerințe în ceea ce privește definirea parametrilor și a valorilor acestor parametri. Astfel, procedura care determină impactul unui incident trebuie să fie simplă, să fie orientată pe efectul incidentului asupra utilizatorilor și rețelelor interconectate și trebuie să ia în calcul și 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 rețele și servicii de comunicații electronice din perspectiva numărului de utilizatori un chestionar<sup>4</sup> privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice către un număr mai mare de 5.000 de utilizatori timp de cel puțin o oră în cursul anului 2011. Acest chestionar a avut scopul de a identifica numărul și impactul incidentelor, atât asupra utilizatorilor, cât și asupra furnizorilor. În urma analizării și centralizării răspunsurilor la chestionare, a fost identificat un număr de 268 de incidente care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în cursul anului 2011.

Cauzele principale identificate ale incidentelor sunt cele din tabel:

<b>Cauza incidentului</b>	<b>Detalii despre incident</b>	<b>Numărul incidentelor raportate</b>
Atac rău intenționat	Atac asupra securității logice (DDoS, hacking)	3
	Atac asupra securității fizice (furt)	35
	Atac asupra securității fizice (deteriorare fibră optică)	7
Fenomene și dezastre naturale	Condiții meteorologice nefavorabile	31
Eroare umană	Accident	14
Defecțiuni hardware/software	Hardware	72
	Software	34
Cauze externe/părți terțe	Alimentarea cu energie electrică	29
	Defecțiuni software	6
	Defecțiuni hardware	2
	Fibră optică deteriorată de lucrări efectuate de terți	35
Numărul total al incidentelor raportate		268

<sup>4</sup> Chestionarul privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2011 se găsește la adresa: [http://www.ancom.org.ro/chestionare\\_4950](http://www.ancom.org.ro/chestionare_4950)

În urma analizării incidentelor raportate de furnizorii de rețele și servicii de comunicații electronice, s-a observat că cel mai des întâlnite cauze ale incidentelor sunt:

1. Defecțiuni hardware/software

Aproape 40% din totalul defecțiunilor au fost cauzate de defecțiuni hardware/software. Sistemele utilizate în comunicații, precum și software-urile aferente sunt din ce în ce mai complexe și astfel din ce în ce mai predispuse la defectări.

2. Deteriorarea fibrei optice de către terți

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

4. Furtul cablurilor

Creșterea în valoare a metalului din care sunt constituite cablurile influențează negativ furnizarea de rețele de comunicații. Circuitele telefonice tradiționale conțin perechi de cablu din cupru, iar hoții sunt din ce în ce mai atrași de câștigurile obținute din vânzarea cuprului la centrele de reciclare. Acest lucru a condus la un număr mare de deficiențe de funcționare și întreruperi în furnizarea rețelilor și serviciilor de comunicații electronice. Rețelele bazate pe cupru nu sunt singurele afectate, cablurile cu fibră optică sunt frecvent deteriorate de hoți în căutarea cablurilor de cupru.

5. Condițiile meteorologice nefavorabile

Fenomenele naturale, cum ar fi ninsorile și ploile abundente, provoacă de cele mai multe ori întreruperi ale alimentării cu energie electrică și blocaje rutiere, ce împiedică accesul echipelor de intervenție ale furnizorilor afectați la locațiile cu echipamente, pentru efectuarea cât mai rapidă a reparațiilor.

### **5.7. Notificarea inițială**

Notificarea inițială 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 conține caracteristicile de bază ale incidentului și estimarea consecințelor acestuia, pe baza informațiilor disponibile imediat după eveniment.

Este important ca personalul furnizorului să nu fie supraîncărcat cu obligațiile de raportare în timp ce răspunde la un incident. În cazul incidentelor care afectează securitatea și integritatea rețelilor și serviciilor de comunicații 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 informații minime referitoare la un incident:

- ora descoperirii incidentului;
- serviciile și/sau rețelele care sunt afectate de incident;
- estimarea ariei geografice afectate, a numărului de conexiuni afectate, precum și a efectelor incidentului asupra furnizării rețelilor și serviciilor de către alți furnizori, pe piața națională de comunicații electronice sau pe cea din alt stat membru al Uniunii Europene;;
- estimarea efectelor în ceea ce privește apelarea numărului unic pentru apeluri de urgență 112;
- o descriere sumară a cauzei/cauzelor care a/au provocat incidentul;
- estimarea graficului de restabilire a furnizării rețelilor și serviciilor de comunicații electronice în parametrii normali de funcționare;
- îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;
- informațiile oferite publicului cu privire la existența unui incident, modalitatea de comunicare și ora la care au fost comunicate informațiile, 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 poștă electronică) ale persoanei/persoanelor care poate/pot da mai multe informații privind incidentul.

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

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

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

### **5.8. Notificarea finală**

Notificarea finală va trebui să conțină informații complete cu privire la incidentul cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, precum și un rezumat al măsurilor luate pentru a elimina vulnerabilitățile identificate și pentru a preveni reapariția incidentului în viitor. Unele dintre aceste informații pot fi disponibile numai după încheierea și analiza incidentului. De asemenea, furnizorii au posibilitatea de a alocă resurse umane pentru rapoarte detaliate după ce un incident a fost rezolvat. Notificarea finală poate servi ca bază de analiză a incidentelor individuale.

Formatul informațiilor 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 informațiile transmise de furnizori sunt comparabile. Utilizarea unui model standard va face procesul de colectare a datelor și de analiză mai eficace și mai eficient și în același timp va evita incoerențele.

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

Informațiile colectate și agregate de ANCOM pot fi apoi utilizate de către autoritate pentru a realiza un raport privind starea securității și integrității rețelelor și serviciilor de comunicații electronice.

### **5.9. Informarea publicului cu privire la incidentele care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice**

În scopul protejării utilizatorilor finali, sunt necesare măsuri pentru a asigura continuitatea furnizării rețelelor și serviciilor, dar și pentru asigurarea transparenței informațiilor cu privire la incidentele care afectează în mod semnificativ securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Incidentele pot afecta un număr mare de utilizatori, întreprinderi și servicii și pot afecta chiar siguranța publică. Prin urmare, ele pot fi de interes pentru publicul larg și informarea cu privire la aceste incidente este esențială. 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 amenințare sau despre modul de contracarare a incidentului și de răspuns la un incident sau despre alte informații importante.

Utilizatorii pot percepe aceste informații ca o dovadă a angajamentului și a capacității furnizorului de a restabili rapid serviciile. Astfel, utilizatorii pot fi educați cu privire la posibilele amenințări la adresa funcționării serviciului. Utilizatorii înțeleg cauza întreruperii furnizării serviciului și de ce furnizarea serviciului nu a putut fi reluată mai devreme. Raportarea incidentelor (către public) este astfel o cale de a îmbunătăți comunicarea cu utilizatorii.

Conform art. 47 alin. (2) din Ordonanța de Urgență a Guvernului nr. 111/2011, ANCOM va putea informa publicul cu privire la existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații 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 rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului vor informa publicul cu privire la existența unui incident cu impact semnificativ, prin utilizarea uneia sau a mai multor modalități indicate de proiectul de decizie. De aceea, ANCOM trebuie să primească în cadrul notificării inițiale toate informațiile necesare cu privire la incident pentru a lua o decizie în privința oportunității de publicare. Astfel, ANCOM trebuie să fie informat dacă furnizorul, din proprie inițiativă, a pus la dispoziția publicului informațiile cu privire la incident și să aibă la dispoziție 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, așa cum au fost ele definite în cuprinsul prezentului proiect, sunt în interesul public și intenționează să publice informații despre acestea pe pagina de internet a autorității. Cu toate acestea, ANCOM are posibilitatea de a analiza și de a decide de la caz la caz cu privire la informarea publicului, pe baza datelor aflate la dispoziția sa cu privire la anumite aspecte, cum ar fi aria geografică afectată de incident, efectele incidentului în ceea ce privește apelarea numărului unic pentru apeluri de urgență 112, informațiile oferite publicului de către furnizor cu privire la existența unui incident, modalitatea de comunicare și ora la care au fost comunicate informațiile, dacă este cazul, elementele precizate de furnizori care pot permite ANCOM să decidă dacă informarea privind incidentul este sau nu în interesul public, numărul conexiunilor afectate, durata incidentului, precum și pe baza argumentelor temeinice oferite de furnizorii în cauză care ar putea justifica nepublicarea informațiilor referitoare la incidentul cu impact semnificativ.

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

## **6. Dispoziții finale și tranzitorii**

Deoarece de la intrarea în vigoare a dispozițiilor Ordonanței de Urgență a Guvernului nr. 111/2011 și până în momentul elaborării prezentului proiect de decizie niciun furnizor nu a transmis ANCOM vreo notificare cu privire la apariția unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice și datorită faptului că ANCOM trebuie să transmită ENISA și Comisiei Europene un raport anual privind incidentele cu impact semnificativ care au avut loc în cursul anului 2013 în România, furnizorii de rețele publice de comunicații electronice sau servicii de comunicații 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 securității și integrității rețelelor și serviciilor de comunicații 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 și respectând instrucțiunile de completare din Anexa nr. 3 la proiectul de decizie.

Pentru a se asigura un grad ridicat de transparență, precum și pentru a crea condițiile primirii de către ANCOM a unor informații exacte, reale, complete, provenind de la persoane ce au capacitatea de a reprezenta respectiva organizație, cu privire la incidentele cu impact semnificativ asupra securității și integrității rețelelor și serviciilor, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația 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 și orice modificări ce intervin asupra datelor de contact, în termen de 5 zile de la survenirea acestora.