ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

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

EXPUNERE DE MOTIVE

la proiectul Deciziei Autorității Naționale pentru Administrare și Reglementare în Comunicații privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului

1. Introducere

În prezent, măsurile de securitate care trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului sunt stabilite, la nivel de legislație secundară, prin Decizia președintelui ANCOM nr. 512/2013 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. Cadrul legal primar care a stat la baza acestei decizii a fost reprezentat de art. 46-48 din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, cu modificările și completările ulterioare.

Începând cu anul 2013, ANCOM a colectat datele referitoare la incidentele de securitate cu impact semnificativ raportate de către furnizorii de rețele publice de comunicații electronice și de servicii de comunicații electronice destinate publicului, a monitorizat constant evoluția lor, îndeplinind totodată obligația de raportare către Comisia Europeană şi Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), așa cum prevede art. 5 din Decizia președintelui ANCOM nr. 512/2013. De asemenea, ANCOM a analizat constant incidentele de securitate cu impact semnificativ notificate și a publicat anual un raport cu privire la acestea în cadrul secțiunii dedicate de pe pagina proprie de internet[1]. În aprilie 2016, a fost publicat și un *Ghid de implementare a măsurilor de securitate în domeniul managementului incidentelor conform deciziei nr. 512/2013*, prin care[2] ANCOM și-a propus să ofere sprijin furnizorilor în implementarea măsurilor de securitate în domeniul managementului incidentelor.

De la intrarea în vigoare a Deciziei președintelui ANCOM nr. 512/2013, atât ecosistemul tehnologic, cât și cel al vulnerabilităților și al amenințărilor la adresa securității rețelelor și serviciilor de comunicații electronice s-au aflat într-un dinamism continuu. În societatea modernă, nevoia de conectivitate a cunoscut o creștere explozivă în decursul ultimilor ani, atât în ceea ce privește serviciile clasice, de voce, cât mai ales în domeniul serviciilor inovative cu valoare adăugată – de conectivitate IoT, comandă și operare de echipamente la distanță în timp real sau transferuri de volume mari de date la viteze de lucru ridicate. Această realitate a generat o creștere fără precedent a complexității rețelelor de comunicații electronice, cu precădere a celor mobile, complexitate ce a determinat înmulțirea numărului de factori de risc la adresa securității rețelelor, concomitent cu o necesitate

[1] Disponibil la următoarea adresă: https://www.ancom.ro/rapoarte-si-studii-privind-securitatea-si-integritatea-retelelor-si-serviciilor-de-comunicatii-electronice_4958.
[2] Disponibil la următoarea adresă: www.ancom.ro/uploads/links_files/Ghid_de_implementare_a_masurilor_de_securitate.pdf.

evidentă de creștere a securității și rezilienței unor astfel de sisteme de comunicații. De asemenea, nu este de neglijat nici faptul că, odată cu dezvoltarea și punerea în funcțiune a rețelelor 5G, potențialul și aplicabilitatea serviciilor de comunicații electronice 5G au devenit nenumărate. Tehnologia este menită să răspundă nevoilor utilizatorilor de rate foarte mari de transfer al datelor, latențe scăzute, precum și QoS îmbunătățite, necesare pentru serviciile emergente, dispozitive IoT, servicii "over-the-top", platforme de colaborare online, streaming audio/video etc. Tocmai cu această diversitate de echipamente conectate, dispozitive și aplicații, cresc importanța și provocările privind securitatea rețelelor de comunicații electronice, fiind necesar ca și cadrul legal să țină pasul cu această evoluție prin crearea mecanismelor necesare pentru prevenirea și/sau minimizarea amenințărilor, vulnerabilităților, impactului incidentelor de securitate. În acest context, și pe plan european au fost întreprinse o serie de acțiuni concrete, despre care vom aminti în capitolul următor.

2. Cadrul legal relevant

În ceea ce privește cadrul legislativ relevant, în cele ce urmează vom aminti principalele directive, regulamente, recomandări, legi, ghiduri europene și naționale care sunt aplicabile în domeniul securității rețelelor și serviciilor de comunicații electronice, care au stat la baza proiectului de decizie privind securitatea rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice destinate publicului.

Astfel, la nivel european, în decembrie 2018, a fost publicată ***Directiva (UE) 2018/1972 de instituire a Codului european al comunicațiilor electronice*** (denumită în continuare *Codul european al comunicațiilor electronice* sau *Codul*). Aceasta are rolul de a actualiza cadrul de reglementare în domeniul comunicațiilor electronice, pregătind totodată terenul legislativ pentru noile tehnologii (cum sunt rețelele de comunicații electronice de bandă largă bazate pe fibră optică, dar și cele 5G, IoT). Articolul 40 din Cod înlocuiește articolul 13a din Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, în timp ce articolul 41 din Cod înlocuiește articolul 13b din Directiva 2002/21/CE.

Strategia UE privind uniunea securității[3] vizează perioada 2020-2025 și își propune să consolideze capacitățile pentru a se asigura un mediu de securitate adaptat exigențelor vremurilor. Scopul enunțat este de a răspunde în mod eficient și coordonat la amenințările aflate în rapidă evoluție. În accepțiunea acesteia, există o legătură directă între riscul de apariție a amenințărilor la adresa securității și gradul de vulnerabilitate al modului de viață și al mijloacelor de subzistență. Potrivit Strategiei, cu cât gradul de vulnerabilitate este mai mare, cu atât este mai mare riscul ca această vulnerabilitate să fie exploatată.

În data de 26 martie 2019, Comisia Europeană a emis ***Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 privind Securitatea cibernetică a rețelelor 5G***[4], document ce abordează riscurile la adresa securității cibernetice a rețelelor 5G, prin formularea unor orientări privind analiza de risc și măsurile adecvate de gestionare a acestora la nivel național, prin pregătirea unei evaluări coordonate a riscurilor la nivel european și prin stabilirea unui proces de elaborare a unui set comun de instrumente care să cuprindă cele mai bune măsuri de gestionare a riscurilor.

Pentru a avea o abordare comună care să răspundă riscurilor la adresa securității cibernetice a rețelelor 5G, *Grupul de cooperare NIS* (*NISCG*) a emis în data de 9 octombrie 2019 un raport cuprinzător intitulat ***EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks***[5]. Acesta identifică principalele amenințări și actori ai acestora, resursele cele mai sensibile, principalele vulnerabilități (inclusiv cele tehnice, precum și alte tipuri de vulnerabilități, cum ar fi cadrul legal și

[3] Comunicarea Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind uniunea securității nr. 605/2020, disponibilă la adresa: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605.

[4] Disponibil la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019H0534.

[5] Disponibil la adresa: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

politici care pot fi aplicabile furnizorilor de echipamente, inclusiv în țări terțe) și principalele riscuri asociate în cazul rețelelor 5G. Conform raportului, principalii actori ar putea fi: actor ce produce o amenințare accidentală (cum ar fi un impact nedorit sau un efect secundar dintr-o operațiune care nu vizează funcționarea unei rețele de comunicații mobile), un hacker individual, un grup de hackeri, un grup de crimă organizată, un om din interior, un actor susținut de stat. Principalele amenințări ar putea fi: compromiterea confidențialității (inclusiv spionaj), compromiterea disponibilității, compromiterea integrității.

Ulterior, în data de 29 ianuarie 2020, NISCG a publicat[6] documentul ***Cybersecurity of 5G networks EU Toolbox of Risk Mitigating Measures***, (denumit în continuare *Setul de Instrumente* sau *5G Toolbox*). Acesta conține măsuri de atenuare a riscurilor identificate în raportul *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*. Se identifică două categorii de măsuri care, combinate, sunt necesare pentru a atenua în mod eficient riscurile la adresa securității rețelelor și serviciilor de comunicații electronice: măsuri strategice (notate cu SM) și măsuri tehnice (notate cu TM). Acestea pot fi adoptate de către Statele Membre și/sau de către Comisia Europeană. Totodată, o serie de acțiuni de sprijin (notate cu SA) în vederea susținerii implementării măsurilor (ex. acțiuni în domeniul standardelor 5G, consolidarea capacităților de testare și audit, îmbunătățirea eforturilor de coordonare în caz de incidente etc.) sunt enumerate în cuprinsul 5G Toolbox. Scopul este de a reduce riscurile identificate și asigurarea securității rețelelor 5G.

Măsurile strategice acoperă măsuri privind creșterea competențelor de reglementare, măsuri specifice pentru a aborda riscurile legate de vulnerabilitățile non-tehnice (de exemplu, riscul de interferențe ale unei țări terțe sau riscurile de dependență de un singur producător de echipamente), precum și posibile inițiative pentru promovarea unui lanț de aprovizionare sigur, durabil și divers. Măsurile tehnice și operaționale includ măsuri pentru consolidarea securității rețelelor și echipamentelor 5G prin suplimentarea măsurilor de securitate ce vizează tehnologiile, procesele, resursele umane sau fizice, asigurarea unui control strict al accesului și managementul, operarea și monitorizarea sigură a rețelei, inclusiv aspecte ce vizează utilizarea certificării pentru componentele și/sau procesele din cadrul rețelei 5G. Implementarea măsurilor tehnice și operaționale, în ceea ce privește atenuarea riscurilor, va varia în funcție de sfera măsurilor și de tipurile de riscuri care trebuie abordate.

Sursa: European Commission, Directorate-General for Communication, *Setul de instrumente al UE pentru securitatea rețelelor 5G: un set de măsuri solide și cuprinzătoare pentru o abordare coordonată la nivelul UE menită să asigure securitatea rețelelor 5G*, Publications Office, 2020, https://data.europa.eu/doi/10.2775/400067

Comisia Europeană urmărește modul în care Statele Membre pun în aplicare măsurile strategice și măsurile tehnice din Setul de Instrumente. Securitatea rețelelor 5G este o prioritate majoră pentru Comisie și o componentă esențială a strategiei sale privind securitatea Uniunii, întrucât

[6] Disponibil la adresa: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

aceste rețele sunt o infrastructură centrală, ce constituie baza unei game largi de servicii esențiale pentru funcționarea pieței interne și pentru întreținerea și exploatarea unor funcții vitale în societate și economie. În comunicarea sa din 15 iunie 2023[7], Comisia ia act de adoptarea celui de-al doilea raport intermediar cu privire la punerea în aplicare a Setului de Instrumente de către Grupul de cooperare NIS. Comisia a îndemnat Statele Membre care nu au pus încă în aplicare setul de instrumente să adopte de urgență măsuri relevante, astfel cum se recomandă în setul de instrumente al UE, pentru a aborda în mod rapid și eficace riscurile. Raportul include și recomandări pentru statele membre în vederea asigurării unui nivel de securitate adecvat.

Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (denumit în continuare *Regulamentul privind securitatea cibernetică*) trasează două direcții majore: pe de o parte, confirmă mandatul ENISA în domeniul securității cibernetice, iar, pe de altă parte, creează cadrul de certificare a securității cibernetice. Urmare a solicitării din 18.01.2021 a Comisiei Europene, în conformitate cu prevederile art. 48 alin. (1) din Regulamentul privind securitatea cibernetică, ENISA va elabora propunerea de sistem European de certificare a securității cibernetice pentru rețelele 5G[8]. Solicitarea este în acord cu mandatul ENISA conform art. 8 alin. (1) lit. b) din Regulament, cu Setul de Instrumente al UE pentru Securitatea Rețelelor 5G, dar și cu Strategia de securitate cibernetică a UE pentru deceniul digital.

Pentru a se asigura o abordare eficientă și armonizată în cadrul Uniunii Europene, ENISA sprijină Statele Membre în implementarea art. 40 din Codul european al comunicațiilor electronice. Prin grupul de experti ECASEC[9] (constituit din reprezentanți ai autorităților competente), ENISA a publicat ghidul ***Technical Guideline on Security Measures Under the EECC, 4th Edition, July 2021***[10]. Acest document abordează măsurile generale de securitate, ce țin de implementarea prevederilor art. 40 – 41 din Codul european al comunicațiilor electronice, în mod independent de serviciile furnizate sau de tipul rețelelor de comunicații electronice. În ghid sunt stabilite 29 de obiective generale de securitate, grupate pe 8 domenii, bazate preponderent pe standarde din seria ISO/IEC 27xxx. Fiecare obiectiv include mai multe măsuri de securitate pe care furnizorii le pot adopta în vederea îndeplinirii obiectivelor de securitate. Suplimentar, grupul de experți ECASEC a elaborat ghidul ***5G Supplement to the Guideline on Security Measures under the EECC, 2nd Edition, July***[11] care vine în completarea celui menționat anterior, elaborând măsuri specifice rețelelor 5G (conține profilul de securitate 5G).

În data de 24 mai 2023, ENISA a publicat[12] ***5G Security Controls Matrix***, un instrument cuprinzător care conține atât măsuri generale de securitate, cât și măsuri de securitate specifice, provenite din standardele 3GPP referitoare la rețelele 5G, astfel încât amenințările la adresa rețelelor 5G sa fie tratate în mod corespunzător. Acesta își propune să fie o centralizare a unor măsuri tehnice de securitate pentru rețelele 5G, pentru a sprijini implementarea măsurilor tehnice din Setul de instrumente, bazându-se pe măsurile din documentele tehnice ale ENISA și, după caz, alte standarde și specificații.

Ghidul ENISA ***Technical Guideline on Incident Reporting under the EECC[13], March 2021*** tratează raportarea incidentelor de securitate de către Statele Membre către ENISA și Comisie

[7] Disponibil la adresa: https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

[8] Pagina dedicată certificării securutății cibernetice: https://certification.enisa.europa.eu/.

[9] European Competent Authorities for Secure Electronic Communications. Obiectivele grupului se află pe pagina de internet a grupului de la adresa: https://resilience.enisa.europa.eu/article-13.

[10] Disponibil la adresa: https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc.

[11] Disponibil la adresa: https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc.

[12] Disponibil la adresa: https://www.enisa.europa.eu/publications/5g-security-controls-matrix.

[13] Disponibil la adresa: https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc.

și a fost de asemenea revizuit prin grupul de experți ECASEC, ținând cont de prevederile Codului european al comunicațiilor electronice.

În cadrul unui sondaj ad-hoc și cu caracter informativ realizat între membrii grupului ECASEC (posibilitate de răspuns și din partea țărilor candidate EEA/EFTA/EU) a reieșit că majoritatea statelor utilizează sau se raportează în vreun fel la ghidul ENISA (versiunile anterioare ale *Technical Guideline on Security Measures Under the EECC*) în reglementările naționale (56% dintre respondenți au integrat complet în legislație sau în mare parte, cu mici deviații sau referențiază ghidul, 40% au o abordare diferită, însă ghidul a reprezentat o referință importantă, și doar o mică parte au o abordare complet diferită, independentă). Se confirmă astfel importanța ghidurilor ENISA la elaborarea reglementărilor naționale, pentru a se asigura o abordare eficientă și armonizată de-a lungul Uniunii Europene a securității rețelelor și serviciilor de comunicații electronice.

Pe plan național, Codul european al comunicațiilor electronice este transpus de **Legea nr. 198/2022 pentru modificarea şi completarea unor acte normative în domeniul comunicațiilor electronice şi pentru stabilirea unor măsuri de facilitare a dezvoltării rețelelor de comunicații electronice**. Prin acest act normativ au fost modificate, printre altele, dispozițiile Ordonanței de urgență a Guvernului nr. 111/2011, relevante în contextul prezentului proiect de decizie fiind **prevederile Capitolului IV: Securitatea rețelelor și serviciilor de comunicații electronice** din acest ultim act normativ.

Revizuirea și actualizarea cadrului legal secundar în domeniul securității rețelelor și serviciilor de comunicații electronice pe plan național având în vedere modificările apărute la nivelul legislației primare, al evoluției tehnologice și al contextului național și european este o prioritate pentru ANCOM, așa cum se confirmă și în planul de acțiuni al Autorității. ANCOM, în calitatea sa de autoritate de reglementare în domeniul comunicațiilor din România, este direct și nemijlocit interesată de asigurarea continuității serviciilor de comunicații oferite utilizatorilor finali de către furnizorii de rețele și servicii de comunicații electronice, promovarea intereselor utilizatorilor finali constituind un obiectiv statutar. Monitorizarea incidentelor raportate de furnizori, în virtutea exercitării prerogativelor legale, reprezintă o preocupare constantă a Autorității, iar datele obținute, centralizate și prelucrate în ultimii ani de către ANCOM indică existența în continuare a unor vulnerabilități importante la nivelul rețelelor ce ar putea fi adresate în contextul modificării legislației secundare actuale.

Prin urmare, prezentul proiect își propune să coreleze prevederile Deciziei președintelui ANCOM nr. 512/2013 cu actualul cadru legal primar (național, european), menționat mai sus. S-au avut în vedere, totodată, evoluția tehnologică din ultimii ani (rețelele de comunicații electronice de bandă largă - rețele 5G, serviciile de comunicații interpersonale care nu se bazează pe numere etc.), noile amenințări la adresa securității comunicațiilor electronice, fiind de asemenea vizate și aspectele referitoare la raportarea incidentelor de securitate cu impact semnificativ.

3. Sinteza elementelor de noutate aduse de transpunerea Codului european al comunicațiilor electronice

Securitatea rețelelor și serviciilor capătă o definiție nouă, mult mai extinsă față de precedenta, astfel cum rezultă din dispozițiile art. 4 alin. (1) pct. 54^1 din Ordonanţa de urgenţă a Guvernului nr. 111/2011, aspect tratat în capitolul următor dedicat acestui subiect.

Prevederile relevante în domeniul securității comunicațiilor electronice sunt tratate în cadrul Capitolului IV - Securitatea rețelelor și serviciilor de comunicații electronice. Potrivit dispozițiilor art. 46 alin. (1)-(3):

„(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, obiective și proporționale pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice.

(2) Măsurile luate potrivit alin. (1), inclusiv criptarea, după caz, trebuie să asigure un nivel de securitate corespunzător riscului identificat ținând seama de stadiul actual al tehnologiei și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și asupra altor rețele și servicii.

(3) Măsurile luate potrivit alin. (1) trebuie să vizeze următoarele domenii: politica de securitate şi managementul riscului, securitatea resurselor umane, securitatea reţelelor şi serviciilor, a facilităţilor asociate şi a informaţiilor, managementul operaţiunilor, managementul incidentelor, managementul continuităţii activităţii, monitorizarea, testarea şi auditarea, conştientizarea ameninţărilor."

Aceste dispoziții aduc o serie de precizări suplimentare față de textul anterior al aceluiași articol, cum ar fi mențiunile referitoare la **criptare sau precizarea domeniilor pe care trebuie să le vizeze măsurile tehnice și organizatorice** pe care furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului sunt obligați să le ia pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice.

În ceea ce privește criptarea prevăzută de dispozițiile art. 46 alin. (2) din Ordonanța de urgență a Guvernului nr. 111/2011, menționăm că standardul ISO/IEC 27002:2022 conține prevederi generale aplicabile și relevante în materia politicilor organizației în domeniul criptării.

Ordonanța de urgență a Guvernului nr. 111/2011 introduce, de asemenea, noi prevederi legate de informarea gratuită a utilizatorilor, în sensul că aceste informări nu se vor face doar în cazul incidentelor cu impact semnificativ ca până acum, ci şi în cazul amenințărilor de securitate specifice și semnificative și cu privire la măsurile pe care utilizatorii le pot lua pentru a-și proteja securitatea comunicațiilor (de exemplu, prin folosirea unor anumite tipuri de software sau tehnologii de criptare). Astfel, prevederile art. 47 alin. (3) din Ordonanța de urgență a Guvernului nr. 111/2011 menționează că *„(3) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a informa, în mod gratuit, utilizatorii potențial afectați de o amenințare specifică și semnificativă de securitate, cu privire la orice măsură de protecție sau măsură corectivă care poate fi luată de utilizatori. Acolo unde este cazul, furnizorii informează utilizatorii și cu privire la amenințarea în sine*.".

Noile prevederi ale Ordonanței de urgență a Guvernului nr. 111/2011 referitoare la securitatea rețelelor și serviciilor de comunicații electronice sunt aplicabile în cazul a trei categorii de servicii: **servicii de acces la internet, servicii de comunicații interpersonale bazate sau nu pe numere și servicii care constau în transmiterea de semnale**.

Serviciile de **comunicații interpersonale care nu se bazează pe numere (NI-ICS[14])** sunt definite de pct. 9^3 de la art. 4 alin. (1) din Ordonanța de urgență a Guvernului nr. 111/2011 și reprezintă „*un serviciu de comunicații interpersonale care nu utilizează resurse publice de numerotație, respectiv un număr sau mai multe numere din planurile naționale sau internaționale de numerotație, sau nu permite comunicarea cu un număr sau mai multe numere din planurile naționale sau internaționale de numerotație*". Acestea pot consta, de exemplu, în apeluri video, webmail, aplicații pentru conferințe, servicii de mesagerie etc.

Un serviciu de **comunicații interpersonale bazat pe numere (NB-ICS[15])** se conectează la rețeaua publică comutată de telefonie și utilizează resurse de numerotație alocate. Conform clarificării aduse de considerentul nr. 18 din Codul european al comunicațiilor electronice, aceste servicii de comunicații interpersonale includ atât serviciile în care numerele utilizatorilor finali se atribuie în scopul asigurării conectivității cap-la-cap (*end-to-end*), cât și serviciile care le permit utilizatorilor finali să intre în contact cu persoanele cărora li s-au atribuit numerele respective. Aceste servicii sunt, spre exemplu: servicii de telefonie destinate publicului la puncte fixe, servicii de telefonie destinate publicului la puncte mobile, SMS, VoIP etc. Spre deosebire de aceste servicii, un serviciu de

[14] Number-independent interpersonal communication services.
[15] Number-based interpersonal communication services.

comunicații interpersonale care nu se bazează pe numere nu se conectează la rețeaua publică comutată de telefonie și nu utilizează resurse de numerotație alocate.

Serviciile privind **transmiterea de semnale** constau, de exemplu, în servicii de transmisiuni folosite pentru furnizarea serviciilor M2M (telemedicină, controlul traficului etc.), linii închiriate etc.

Tot ca un element de noutate, **criteriile folosite pentru a stabili amploarea impactului unui incident** sunt specificate clar de dispozițiile art. 47 alin. (2) din Ordonanța de urgență a Guvernului nr. 111/2011, acestea incluzând și impactul economic și societal și întinderea geografică a zonei afectate de incidentul de securitate, precum și alte criterii enumerate de textul amintit (a se vedea cap. 7 din prezentul document).

Având în vedere faptul că definiția securității a fost extinsă, cuprinzând și informația transmisă, prelucrată sau stocată prin rețele și servicii, Codul precizează că autoritatea competentă trebuie să primească sprijin din partea CSIRT-urilor naționale, fapt ce se regăsește transpus în legislația primară prin dispozițiile art. 49^2 din Ordonanța de urgență a Guvernului nr. 111/2011: „Art. 49^2 - *(1) În vederea punerii în aplicare a prezentului capitol, ANCOM beneficiază de asistență din partea echipelor de intervenție în caz de incidente de securitate informatică și a echipei de răspuns la incidente de securitate informatică la nivel național, desemnate în temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, în ceea ce privește aspectele care intră în atribuțiile acestora. (2) În vederea punerii în aplicare a prevederilor prezentului capitol, ANCOM se poate consulta și poate solicita cooperarea cu Directoratul Național de Securitate Cibernetică, cu Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și cu alte autorități naționale, după caz*.".

Toate aceste elemente, împreună cu noile provocări din domeniul securității rețelelor și serviciilor de comunicații electronice, implică, astfel, și actualizarea legislației secundare elaborate de ANCOM în temeiul Ordonanței de urgență a Guvernului nr. 111/2011.

4. Securitatea rețelelor și serviciilor de comunicații electronice

Astfel cum menționam în capitolul precedent, dispozițiile art. 4 alin. (1) pct. 54^1 din Ordonanța de urgență a Guvernului nr. 111/2011 introduc o definiție mai largă a securității rețelelor și serviciilor, specificând clar dimensiunile securității: **disponibilitatea**, **autenticitatea**, **integritatea** și **confidențialitatea** rețelelor și serviciilor, a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de rețelele ori serviciile de comunicații electronice respective sau accesibile prin intermediul acestora. Este extrem de important ca definiția securității rețelelor și serviciilor să fie suficient de cuprinzătoare, iar cele patru elemente amintite (disponibilitatea, autenticitatea, integritatea, confidențialitatea) să aibă o înțelegere unitară și corectă, impactul asupra acestora în cazul unui incident de securitate să fie evaluat corect. Definiția generală a dimensiunilor securității menționate, acceptată și de ENISA și preluată în ghidul *Technical Guideline on Security Measures Under the EECC, 4th Edition, July 2021*, este cea dată de standardul ISO/IEC 27000:2018, dar și de glosarul de termeni al National Institute of Standards and Technology (NIST). De asemenea, termenii se găsesc în mai multe publicații ale NIST, în funcție de contextul în care se utilizează și domeniul în care se aplică. Prin urmare, definițiile generale date de ISO/IEC menționate în ghidul ENISA se regăsesc și în proiectul de decizie.

ISO/IEC 27000:2018 definește **disponibilitatea** ca fiind proprietatea de a fi accesibil și utilizabil la cerere, de o entitate autorizată[16]. Disponibilitatea asigură că informația sau sistemele sunt gata să răspundă (să fie „disponibile") nevoilor utilizatorilor legitimi, în momentul în care aceștia solicită. Aceasta implică și continuitatea serviciilor și se poate asocia cu fiabilitatea sistemului (având în vedere că poate fi impactată de elemente care nu sunt neapărat rău-intenționate, cum ar fi lucrări

[16] *property of being accessible and usable on demand by an authorized entity*.

programate, actualizări de sistem, defecțiuni hardware, erori umane, calamități naturale, incendii, cutremure, după cum pot exista și cauze rău-intenționate cum sunt atacuri cibernetice, DDoS etc.). Disponibilitatea asigură faptul că nu există refuzul accesului autorizat la elemente ale rețelei, informații stocate, fluxuri de informații, servicii şi aplicații, refuz care poate apărea datorită evenimentelor cu impact asupra rețelei. Măsurile de securitate pot include elemente cum ar fi redundanța, back-up, recuperare în caz de dezastru, virtualizare etc. Disponibilitatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate, a serviciilor aferente oferite de respectivele rețele, sau accesibile prin intermediul acestora, de a fi accesibile și utilizabile la cerere de persoane, procese, sisteme care sunt autorizate în acest sens.

În ceea ce privește **autenticitatea**, ISO/IEC 27000:2018 definește conceptul ca fiind proprietatea ca o entitate să fie ceea ce pretinde că este[17], definiția fiind preluată de ENISA în ghidul *Technical Guideline on Security Measures Under the EECC, 4th Edition, July 2021*. Autenticitatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de respectivele rețele, sau accesibile prin intermediul acestora, de a fi veritabile, verificabile, de încredere, existând certitudinea în validitatea transmisiei datelor, a conținutului sau a entităților ce comunică.

Conform ISO/IEC 27000:2018, **integritatea** este proprietatea acurateței și deplinătății[18]. Recomandarea ITU X.800 (03/91) definește integritatea (integritatea datelor) ca fiind proprietatea ca datele să nu fie alterate, modificate sau distruse într-un mod neautorizat. Obiectivul în acest caz este de a se preveni ca datele să fie alterate, modificate, utilizate în mod ilicit de entități neautorizate, adică să fie asigurată integritatea lor. Trebuie acordată atenție astfel încât datele să nu fie modificate nici în cazul tranzitului[19] (având în vedere interconectarea rețelelor). 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-şi păstra atributele specifice din punct de vedere al performanței și funcționalității. Măsurile de securitate pot include elemente cum ar fi proceduri de backup și restaurare, criptare, controlul versiunii, controlul accesului utilizatorilor, software privind detecția erorilor etc. Astfel, integritatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice destinate publicului, inclusiv a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de respectivele rețelele, sau accesibile prin intermediul acestora, de a nu fi alterate, modificate, distruse într-un mod neautorizat, ilicit, existând certitudinea acurateței și deplinătății.

ISO/IEC 27000:2018 definește **confidențialitatea** ca fiind proprietatea ca informația să nu fie făcută disponibilă sau dezvăluită către persoane, entități sau procese[20] neautorizate[21]. Confidențialitatea informației înseamnă ca aceasta să fie protejată pentru a nu fi expusă accesului unor părți neautorizate, astfel încât entitățile neautorizate să nu aibă acces la informații la care nu au acest drept de acces. Confidențialitatea datelor protejează datele de accesări neautorizate. Dintre măsurile privind protecția confidențialității putem aminti criptarea, verificarea biometrică, utilizarea parolelor, autentificarea prin mai multe etape etc. Prin urmare, confidențialitatea reprezintă proprietatea rețelelor publice de comunicații electronice, a serviciilor de comunicații electronice

[17] *property that an entity is what it claims to be*.
[18] *property of accuracy and completeness.*
[19] Bibliografia de specialitate din domeniul securității cibernetice deosebește trei stări în care datele se pot afla*: data at rest* (adică datele stocate pe sistemele de stocare cum sunt HDD, benzi magnetice, cloud, etc.), *data in motion* (acele date care se află în tranzit prin intermediul rețelei), *data in processing* (acele date care sunt utilizate activ de sistemele informatice, include si datele din RAM).
[20] Conform ISO/IEC 27000:2018, procesele reprezintă un set de activități interdependente sau care interacționează, care transformă intrările (eng. *input*) în ieșiri (eng. *output*).
[21] (eng. *property that information is not made available or disclosed to unauthorized individuals, entities, or processes*).

destinate publicului, prin care asigură ca datele stocate, transmise ori prelucrate sau a serviciilor aferente oferite de respectivele rețelele, sau accesibile prin intermediul acestora, să fie făcute disponibile sau dezvăluite doar către persoane, entități sau procese autorizate.

Completările aduse prin prezentul proiect de decizie (inclusiv anexele) au scopul de a spori măsurile de securitate implementate de furnizori pentru a corespunde noilor tehnologii, precum și pentru a răspunde mai bine noilor amenințări aflate într-un dinamism continuu, având în vedere și ghidurile și documentele relevante indicate în cap. 2.

Totodată, art. 49 alin. (1) lit. a) din Ordonanța de urgență a Guvernului nr. 111/2011 prevede explicit că ANCOM poate solicita furnizorilor toate informațiile necesare evaluării securității rețelelor şi serviciilor, inclusiv măsurile de securitate implementate și documentația ce a stat la baza acestora. Prin urmare, ca element de noutate față de dispozițiile Deciziei președintelui ANCOM nr. 512/2013, dispozițiile art. 3 alin. (4) din proiectul de decizie prevăd că *„(4) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului care au un număr de cel puțin 100.000 de conexiuni vor transmite anual către ANCOM, până la data de 10 februarie a fiecărui an, măsurile de securitate existente la data de 31 decembrie a anului anterior raportării, pe structura domeniilor și obiectivelor de securitate identificate în anexa nr. 1, evidențiind totodată evoluțiile față de raportarea anterioară.*". Obiectivul urmărit prin această prevedere este de a se asigura supravegherea și monitorizarea constantă a modalității de îndeplinire a obligațiilor în materia securității la nivelul pieței de comunicații electronice, prin acoperirea unui procent semnificativ al acesteia, de a verifica măsurile implementate de furnizori, dar și de a garanta un cadru de reglementare predictibil și clar.

Această obligație a fost impusă doar furnizorilor ce au peste 100.000 de conexiuni, pentru a asigura un echilibru corect între cerințele și obligațiile bazate pe riscuri, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte. De asemenea, potrivit proiectului de decizie, atunci când consideră necesar, ANCOM solicită furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului transmiterea, într-un termen stabilit de aceasta, dar care nu poate depăși 30 de zile de la primirea solicitării, a tuturor informațiilor necesare evaluării securității rețelelor și serviciilor, inclusiv a documentației ce a stat la baza implementării măsurilor de securitate, precum și a deciziei de excludere a anumitor obiective de securitate, în cazul furnizorilor de servicii de comunicații interpersonale care nu se bazează pe numere, precum și furnizorilor de servicii de comunicații interpersonale bazate pe numere care nu exercită un control efectiv asupra transmiterii semnalului.

5. Grupul consultativ pentru securitatea comunicațiilor electronice

Prin art. 8 din prezentul proiect de decizie, ANCOM propune crearea Grupului Consultativ pentru Securitatea Comunicațiilor Electronice ce va fi constituit din reprezentanții Autorității cu atribuții în securitatea rețelelor și serviciilor și experți tehnici ai furnizorilor de rețele publice de comunicații electronice sau servicii de comunicații electronice destinate publicului care au un număr de cel puțin 100.000 de conexiuni.

Acest grup va avea drept scop promovarea armonizării măsurilor de securitate, îmbunătățirea și promovarea continuă a securității rețelelor și serviciilor de comunicații electronice, diseminarea diverselor aspecte de securitate, inclusiv cele referitoare la incidente, promovarea cooperării, evaluarea riscurilor emergente, schimbul de informații și cunoștințe sau analiza provocărilor pentru securitatea rețelelor și serviciilor, identificarea unor soluții la probleme punctuale ce pot apărea etc.

Pentru atingerea scopurilor mai sus amintite, membrii grupului vor conlucra şi colabora cu privire la aspecte precum identificarea celor mai bune practici în domeniul securității rețelelor și serviciilor de comunicații electronice, vor oferi clarificări privind raportarea incidentelor de securitate sau vor dezbate realizarea unei metode de uniformizare a raportării incidentelor şi vor colabora la implementarea măsurilor de securitate. Este esențial să se convină asupra detaliilor tehnice necesare pentru a permite o implementare eficace și eficientă a măsurilor de securitate.

Tot în cadrul acestui grup, ANCOM va putea oferi furnizorilor o serie de informări privind diverse subiecte ce țin de securitate, despre incidente de securitate, vulnerabilități și amenințări sau informări despre evoluția lucrărilor altor grupuri din domeniul securității rețelelor și serviciilor de comunicații electronice. În paralel, şi furnizorii vor putea oferi informări cu privire la subiecte discutate la diverse forumuri la care participă, despre diverse probleme pe care le întâmpină în activitățile lor etc. Totodată, reprezentanții furnizorilor vor fi invitați/încurajați să inițieze teme noi de discuții sau activități ce țin de securitatea comunicațiilor electronice.

Având în vedere importanța asigurării securității rețelelor și serviciilor de comunicații electronice, precum și amploarea pe care o pot avea anumite incidente, unele subiecte pot fi discutate cu precădere de către membrii grupului, în funcție de necesitățile sau de constrângerile identificate la momentul respectiv. Prin urmare, o restrângere a numărului de participanți poate fi necesară.

În cazul în care se vor dezbate subiecte care țin de aspecte generale referitoare la securitatea rețelelor și serviciilor de comunicații electronice, ANCOM poate invita să participe la discuții și reprezentanți ai altor entități - autorități, instituții publice, persoane juridice de drept public sau privat și asociații de profil care reprezintă interesele furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, care nu îndeplinesc criteriile de la alin. (3).

Suplimentar, reprezentanții grupului ar putea colabora la adoptarea de standarde din domeniul securității la nivel național (ex. Asociația de Standardizare din România - ASRO) sau ar putea participa la grupuri de lucru ASRO.

Membrii se alătură grupului în calitatea lor profesională de angajați ai furnizorilor, pe de o parte, şi de angajați ai Autorității, pe de altă parte. Experții vor fi desemnați de organizația lor să participe și să reprezinte organizația în grupul consultativ.

6. Domeniile și obiectivele de securitate aferente acestora

Conform art. 46 alin. (1) și (2) din Ordonanța de urgență a Guvernului nr. 111/2011, 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, obiective și proporționale pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor de comunicații electronice. Măsurile luate, inclusiv criptarea, după caz, trebuie să asigure un nivel de securitate corespunzător riscului identificat ținând seama de stadiul actual al tehnologiei și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și asupra altor rețele și servicii. Așadar, într-o primă etapă, furnizorii trebuie să efectueze analize specifice pentru situația lor particulară, pentru a determina ce resurse se află în domeniul de aplicare, iar, ulterior, să efectueze o evaluare a riscurilor pentru a determina măsurile de securitate adecvate. Evaluările riscurilor se vor actualiza pentru a adresa și eventualele modificări efectuate în trecut asupra rețelei și incidentele din trecut. În ceea ce privește măsurile de securitate pe care furnizorii trebuie să le implementeze, în Anexa nr. 1 se regăsesc domeniile vizate de acestea, grupate în opt categorii.

Standardele fac distincție între resurse primare și secundare. În conformitate cu ISO/IEC 27005, resursele primare sunt cele care reprezintă de fapt domeniul de activitate al organizației, iar cele secundare sunt acelea pe care se bazează cele primare, care practic susțin furnizarea rețelelor și serviciilor de comunicații electronice. Resursele primare sunt de fapt rețelele și serviciile de comunicații electronice furnizate, iar cele secundare sunt sistemele și procesele care susțin furnizarea acestor rețele și servicii (cum sunt de exemplu stații de bază, routere, surse de alimentare cu energie electrică etc.). Suplimentar, mai pot exista și anumite resurse critice (care pot fi sisteme informatice, rețele, procese, datele etc). Resursele critice sunt acele resurse care, dacă sunt compromise sau se defectează, produc un impact sever asupra securității rețelelor și serviciilor. Prin urmare, acestea trebuie protejate cu prioritate. Resursele unei organizații care furnizează rețele și servicii de comunicații electronice pot include mai multe categorii de resurse (care, în funcție de rolul pe care îl îndeplinesc, pot fi resurse primare, secundare, critice):

a) **informații**, **procese de afaceri și diverse activități**: de rutare, de configurare a echipamentelor, referitoare la utilizatorii de servicii, referitoare la serviciile furnizate, la traficul efectuat, facturare, baze de date, documentație de sistem, manuale de utilizare, contracte şi 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 şi utilități etc.

c) **fizice, hardware (este formată din toate elementele fizice care susțin procesele)**: echipamente de comutare sau rutare, sisteme de transmisie, echipamente terminale, mediile utilizate pentru transmiterea semnalelor, servere, stații de lucru și dispozitive de rețea utilizate pentru a asigura serviciile interne, dar și externe, medii mobile etc. Aceste echipamente pot fi numeroase, de exemplu în aceste categorii mai pot intra: servere DNS, server DHCP, server de jurnal, server de autentificare etc., echipamente de rețea și comunicații (backbone router, CMTS, NAS, AP, modem, switch etc.), echipamente de securitate (firewall, IPS, IDS, VPN etc.) etc.

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

e) **resurse umane:** ingineri de comunicații, specialiști IT etc.

f) **clădiri și diverse incinte:** în care sisteme sunt instalate și operate, includ instalațiile de cablare, locurile de management și monitorizare a rețelei, săli cu echipamente de telecomunicații, centre de date etc.

g) **intangibile**: controlul organizaţiei, „know-how” etc.

Este responsabilitatea furnizorului de a analiza resursele pe care le deține, de a efectua propria evaluare de risc, de a identifica resursele critice etc., iar, ulterior, în funcție de evaluarea riscului și în funcție de serviciile/rețelele furnizate să adopte măsurile de securitate. În acest sens, pot fi luate ca referințe standardele relevante din domeniu. Spre exemplu, *ISO/IEC 27005 Tehnologia informaţiei. Tehnici de securitate. Managementul riscului de securitate a informaţiei* furnizează linii directoare pentru managementul riscului de securitate. Suplimentar, acest demers al furnizorului poate fi sprijinit si de documentele emise de ENISA, precum *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*, care identifică principalele amenințări și actori ai acestora, resursele cele mai sensibile, principalele vulnerabilități (inclusiv cele tehnice, precum și alte tipuri de vulnerabilități, cum ar fi cadrul legal și politici care pot fi aplicabile furnizorilor de echipamente, în țări terțe) și principalele riscuri asociate în cazul rețelelor 5G, sau cum este *ENISA Threat Landscape for 5G Networks Report,* care oferă informații detaliate despre expunerea resurselor rețelelor 5G la diverse amenințări.

Părțile terțe și externalizarea (engl. *outsourcing*) pot de asemenea prezenta relevanță din punctul de vedere al securității. Prin „terți” se înțeleg acele persoane cu care furnizorul colaborează pentru a furniza serviciile, ca de exemplu cei de la care sunt achiziționate echipamente/servicii, furnizorii proprii (eng. *suppliers*), auditori, consultanți, subcontractanți etc. Chiar dacă anumite procese sunt subcontractate, externalizate, furnizorul rămâne responsabil pentru implementarea măsurilor de securitate adecvate pentru a proteja securitatea rețelelor și serviciilor pe care le furnizează. Menționăm că terții nu includ autorități sau utilizatorii finali.

Cadrul legal prevede explicit că furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua măsuri de securitate ce trebuie să prevină sau să reducă la minimum impactul incidentelor de securitate asupra utilizatorilor și asupra altor rețele sau servicii. Ținând cont de stadiul actual al tehnologiei, aceste măsuri trebuie să asigure un nivel de securitate adecvat riscului existent. În special, trebuie luate măsuri, inclusiv

criptarea, după caz, pentru a preveni și a reduce la minimum impactul incidentelor de securitate asupra utilizatorilor și asupra altor rețele și servicii. Totodată, art. 46 alin. (3) din Ordonanța de urgență a Guvernului nr. 111/2011 prevede că măsurile luate trebuie să vizeze următoarele domenii:

(a) politica de securitate și managementul riscului;
(b) securitatea resurselor umane;
(c) securitatea rețelelor și serviciilor, a facilităților asociate și a informațiilor;
(d) managementul operațiunilor;
(e) managementul incidentelor;
(f) managementul continuității activității;
(g) monitorizarea, testarea și auditarea;
(h) conștientizarea amenințărilor.

Având în vedere toate aceste considerente de până acum, se impune analiza și, acolo unde este cazul, punerea în concordanță a prevederilor din reglementările secundare, inclusiv în ceea ce privește obiectivele de securitate, raportarea incidentelor de securitate. De asemenea, prevederile proiectului de decizie stabilesc că, având în vedere situația lor particulară dată de faptul că anumiți furnizori nu exercită în mod normal un control efectiv asupra transmiterii semnalelor în rețea, gradul de risc aferent unor astfel de servicii putând fi astfel considerat în unele privințe mai redus decât în cazul serviciilor tradiționale de comunicații electronice, furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere, precum și furnizorii servicii de comunicații interpersonale bazate pe numere care nu exercită un control efectiv asupra transmiterii semnalului pot exclude anumite obiective de securitate aferente domeniilor identificate în anexa nr. 1 la proiectul de decizie.

De asemenea, furnizorii vor avea în continuare obligația de a actualiza măsurile prevăzute la art. 3 alin. (2) din proiectul de decizie ori de câte ori este necesar, însă cel puțin o dată la 12 luni, având în vedere dinamica amenințărilor care pot interveni la adresa securității rețelelor și serviciilor de comunicații electronice.

Astfel, domeniile și obiectivele de securitate aferente, prevăzute de prezentul proiect de decizie, reprezintă un minimum pe care furnizorii vizați au obligația de a îl implementa, sub rezerva mențiunilor exprimate anterior pentru cazul furnizorilor de comunicații interpersonale care nu se bazează pe numere și al celor de comunicații interpersonale care se bazează pe numere, dar care nu exercită un control efectiv asupra transmiterii semnalului, aceste domenii si obiective fiind următoarele:

I. Politica de securitate şi managementul riscului

Obiective de securitate

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

1) să stabilească o politică de securitate adecvată;

2) să stabilească un management al riscului care:

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

b) să identifice riscurile, prin identificarea resurselor, amenințărilor, vulnerabilităților, măsurilor existente şi a consecințelor pe care incidentele de securitate le-ar putea avea asupra resurselor și să se asigure că personalul de conducere este informat în mod corespunzător despre aceste

riscuri, dar și despre măsurile de reducere a lor; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, se vor avea în vedere, totodată, potențiale riscuri cauzate de expunerea la terțe părți considerate a prezenta un grad de risc ridicat, ori dependența de un singur producător;

c) să analizeze riscurile prin estimarea impactului pe care îl poate avea concretizarea unei amenințări care exploatează o vulnerabilitate a unei resurse şi prin estimarea 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 şi să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului;

f) să se asigure că riscurile reziduale sunt acceptate de personalul de conducere.

3) să stabilească o structură adecvată a rolurilor şi responsabilităţilor în asigurarea securităţii reţelelor şi serviciilor, să informeze personalul despre rolurile și responsabilitățile în asigurarea securităţii reţelelor şi serviciilor, precum și despre cazurile și modalitățile în care se pot contacta persoanele responsabile;

4) să stabilească o politică cu privire la cerinţele de securitate atât pentru achiziţionarea de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate (echipamente, servicii IT, software, interconectare, baze de date, facilităţi asociate etc.), cât şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii;

5) să includă cerințe de securitate în contractele pentru achiziţionarea de la terţe părţi de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii, inclusiv în ceea ce privește confidențialitatea și transferul securizat al informației, să țină evidența incidentelor de securitate cauzate de terțe părți, să ia măsuri pentru a reduce riscurile reziduale care nu au fost adresate de terțele părți sau sunt rezultate din interacțiunea cu acestea;

6) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să includă în politica privind cerinţele de securitate pentru achiziţionarea de la terţe părţi de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a acestor produse şi servicii, cel puțin următoarele elemente:

a) referitor la echipamentele identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, obligația achiziționării unor echipamente puse la dispoziție de terțele părți, precum și a proceselor și serviciilor acestora (procese TIC, servicii TIC, produse TIC, echipamente din componența rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, servicii cloud etc.) certificate în conformitate cu sistemele europene de certificare aplicabile, în cazul în care astfel de sisteme de certificare prevăzute de Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) sunt obligatorii în temeiul dreptului național sau european;

b) obligația de a depune diligențele necesare pentru a se asigura că terții respectă standardele relevante în proiectarea și fabricarea echipamentelor, precum și în gestionarea ciclului de viață al acestora;

c) prezentarea documentelor justificative de către terți care să ateste că aceștia au depus diligențele necesare în vederea asigurării nivelului de calitate al proceselor interne de securitate aplicabile, inclusiv asigurarea *securității prin proiectare* („*security by design*"), integrată în procesul de dezvoltare a produsului;

d) furnizarea de către terți a garanțiilor și documentelor justificative care să ateste că aceștia au depus diligențele necesare în ceea ce privește: implementarea tuturor funcționalităților de securitate conform standardelor relevante, că în produsele pe care le pun la dispoziție nu există vulnerabilități introduse și/sau omise voit; aceștia vor informa imediat despre vulnerabilități de îndată ce acestea devin cunoscute;

e) obligația de a depune diligențele necesare pentru a se asigura că terții asigură protecția adecvată și nedivulgarea oricăror informații confidențiale despre beneficiarii echipamentelor, serviciilor, lucrărilor, sau a altor informații confidențiale către alte entități;

f) obligația de a depune diligențele necesare pentru a se asigura că terții vor oferi asistență în investigarea și remedierea incidentelor de securitate și posibilitatea de a colabora în vederea efectuării unor eventuale teste periodice de securitate și de penetrare ale produselor pe care le pun la dispoziție.

Acest domeniu de securitate presupune stabilirea unor măsuri constând în existența unei politici de securitate adecvate la nivelul organizației, stabilirea unui management al riscului (având în vedere că măsurile de securitate adecvate sunt bazate pe evaluarea de risc), stabilirea unei structuri adecvate a rolurilor şi a responsabilităților în asigurarea securității, stabilirea unei politici cu privire la cerințele de securitate atât pentru achiziționarea de la terțe părți de produse şi servicii identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, cât şi pentru asigurarea întreținerii sau gestiunii de către terțe părți a acestor produse şi servicii.

Completările aduse au în vedere consolidarea prevederilor pentru a răspunde adecvat riscurilor aferente rețelelor 5G identificate în *EU coordinated risk assessment of 5G networks security* (potențiale riscuri cauzate de expunerea la furnizori considerați a prezenta un risc ridicat, dependența de un furnizor unic de echipamente 5G sau prestatori de servicii aflate sub controlul altor state).

Setul de Instrumente introduce nevoia solicitării, în cadrul procedurilor de achiziții derulate de către furnizor, a standardelor de securitate de la producătorii de echipamente. Totodată, se prevede utilizarea sistemelor europene de certificare pentru elementele de rețea 5G, echipamentele utilizatorilor și/sau proceselor furnizorilor, fiind adresate riscurile provenite din calitatea scăzută a produselor, din exploatarea rețelelor 5G de organizații rău intenționate, perturbarea semnificativă a infrastructurilor și serviciilor critice. Având în vedere continua lor dezvoltare și prezență în rândul utilizatorilor finali, trebuie avute în vedere și riscurile provenite din exploatarea dispozitivelor conectate, IoT etc. În acest context, apare necesitatea utilizării sistemelor europene de certificare pentru alte produse și servicii TIC cum sunt serviciile cloud, IoT etc. Furnizorii rețelelor 5G vor trebui să aibă implementate măsuri și procese care să administreze constant și adecvat riscurile la adresa securității rețelelor și serviciilor. Furnizorii de rețele 5G trebuie să aibă o politică ce conține cerințe pentru achiziţionarea de la terţe părţi de produse şi servicii, aceștia având posibilitatea transferului diligențelor în sarcina terților (de exemplu, prin clauze contractuale, solicitare de declarații pe proprie răspundere, certificate de conformitate, auditarea terților, prezentarea unor secțiuni relevante extrase din propriile lor proceduri interne, prin compensații financiare în cazul în care sistemele livrate nu sunt sigure, stabilirea unor indicatori de performanță care se monitorizează și se raportează periodic - SLA etc). ISO/IEC 27002:2022 conține informații relevante în ceea ce privește securitatea lanțului de

aprovizionare, rolul furnizorului în relația cu terții lui, la următoarele secțiuni: *5.14 Transferul informațiilor, 5.19 Securitatea informației în relațiile cu furnizorii, 5.20 Abordarea securității informației în cadrul acordurilor cu furnizorii, 5.21 Managementul securității informației în lanțul de aprovizionare TIC, 5.22 Monitorizarea, revizuirea și managementul schimbării serviciilor furnizorilor, 5.23 Securitatea informației pentru utilizarea serviciilor cloud, 6.6 Acorduri de confidențialitate și nedezvăluire, 8.8 Managementul vulnerabilităților tehnice, 8.30 Dezvoltare externalizată*. De menționat este că și în prezent practica din piață referitoare la achizițiile desfășurate de organizații mari prin propriile departamente de achiziții prevede precalificarea furnizorilor/producătorilor prin prezentarea unui set de documente și completarea unor chestionare. Prin intermediul obiectivelor de securitate de la pct. 6) se creează un cadru legal care încurajează comunicarea și colaborarea pentru a minimiza/elimina efectele incidentelor de securitate. Riscurile vor trebui luate în evidență, revizuite și actualizate. Actualizarea va trebui realizată astfel încât să țină cont de riscurile specifice rețelelor 5G.

II. Securitatea resurselor umane

Obiective de securitate

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

1) să stabilească un proces privind verificarea de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor în conformitate cu legile aplicabile, reglementări şi etică, proporţionale cu riscurile percepute și să efectueze, în baza procesului menționat, controale de verificare de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor;

2) să se asigure că personalul are cunoştinţe suficiente de securitate şi este instruit permanent cu privire la securitatea reţelelor şi serviciilor, inclusiv prin implementarea unor programe de instruire regulată în domeniul securității rețelelor și serviciilor de comunicații electronice, precum și să pună la dispoziția personalului materiale și documentații suport actualizate;

3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilităţi, care să cuprindă inclusiv aspecte privind revocarea drepturilor de acces, predarea echipamentelor dacă nu mai sunt necesare, precum și instruirea personalului în cazul schimbărilor responsabilităților în cadrul organizației;

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

Domeniul de securitate cuprinde măsuri ce țin de verificarea de fond a candidaților pentru angajare, cunoștințe suficiente din domeniul securității, instruirea personalului, stabilirea unui proces de gestionare a schimbării de personal, precum și stabilirea unui proces disciplinar pentru angajații care produc o încălcare a securităţii reţelelor sau serviciilor de comunicaţii electronice. În ceea ce privește standardele din materie, menționăm că relevante sunt prevederile generale din ISO/IEC 27002 și ISO/IEC 27001. Completările aduse de proiectul de decizie vizează în principal consolidarea și clarificarea formulării anterioare.

În cazul rețelelor 5G, Setul de Instrumente prevede o serie de cerințe care vizează monitorizarea, operarea și managementul rețelei sigure, precum și securitate fizică robustă. Acest deziderat se poate îndeplini printr-o abordare bazată pe evaluarea riscului în cazul elementelor specifice tehnologiei 5G având în vedere mediul în care aceste elemente sunt puse în funcțiune și utilizate. Având în vedere aceste prevederi din Setul de Instrumente, în ceea ce privește domeniul securității resurselor umane, se dorește consolidarea controlului accesului fizic, precum limitarea numărului de persoane care au acces, verificarea personalului în prealabil din punct de vedere securitate (verificări de fond), asigurarea că persoanele respective au fost instruite și sunt calificate,

toate entitățile care au acces, în special la componente critice sau sensibile ale rețelei 5G, sunt într-un număr cât mai limitat și monitorizate.

Măsurile de securitate se aplică și contractorilor, personalului terților etc. Operarea rețelelor de comunicații electronice se bazează în mare măsură pe terți (de exemplu, personalul terților care gestionează părți critice ale rețelei, servicii de suport tehnic localizate în alte state etc.). Raportul *NIS CG EU coordinated risk assessment of the cybersecurity of 5G networks* amintește printre vulnerabilități lipsa personalului specializat și instruit care să securizeze, monitorizeze și să întrețină rețelele 5G. Prin urmare, trebuie efectuată verificarea de fond temeinică a personalului, înainte de a primi acces la informații sau la sisteme confidențiale. Verificarea de fond se aplică inclusiv subcontractanților și personalului terților, însă ar trebui extins să țină cont de personalul din alte țări care gestionează funcționalități critice ale rețelei.

Referitor la pct. 3 privind stabilirea și menținerea unui proces adecvat pentru gestionarea schimbărilor de personal sau modificărilor responsabilităților și rolurilor, obiectivele de securitate au fost consolidate ținând cont de faptul că schimbările de personal sau modificările de roluri şi responsabilități poartă riscuri de securitate. Context în care vor exista proceduri prin care va fi stabilit un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilități, fiind prevăzute inclusiv aspecte ce vizează personalul terților sau contractanților. Se vor avea în vedere măsuri ce țin de revocarea timpurie a drepturilor de acces, legitimațiilor de acces (ex. cartele magnetice), sau orice fel de echipamente care nu mai sunt necesare sau nu se mai justifică deținerea lor. Procesul schimbărilor de personal ar trebui să prevadă existența unei evidențe cu personalul care va avea acces fizic la componente critice și/sau sensibile ale rețelei, să prevadă și faptul că respectivele persoane au fost verificate din punct de vedere al securității, au fost instruite în mod corespunzător.

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

Obiective de securitate

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

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

2) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, să stabilească măsuri de securitate suplimentare pentru accesul fizic la rețea și la facilitățile asociate, în conformitate cu importanța obiectivului protejat; măsurile de securitate vor ține cont de riscurile specifice acestor rețele, inclusiv cele generate de accesul părților terțe;

3) să stabilească o securitate adecvată a utilităţilor suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor, cel puțin prin: implementarea unor măsuri prin care să se asigure securitatea adecvată a utilităţilor suport, dar și a facilităților conexe, proiectarea și dimensionarea acestora astfel încât să fie în acord cu cerințele și specificațiile producătorilor de echipamente;

4) să stabilească măsuri de securitate adecvate pentru accesul logic la reţea şi la sistemele informatice, care să prevadă cel puțin:

a) implementarea unor mecanisme de control al accesului logic pe baza unor identificatori unici;

b) managementul drepturilor de acces, definirea rolurilor, a drepturilor de acces și a responsabilităților, mecanismele de autentificare adecvate tipului de acces solicitat, precum și monitorizarea accesului, procese privind aprobarea excepțiilor și înregistrarea fraudelor;

c) măsuri de securitate privind accesul logic al terților, de la distanță, la resurse, aplicarea principiului „*privilegiilor minime*", a principiului „*separării sarcinilor*", monitorizarea continuă a accesului, aplicarea autentificării bazate pe tehnologii de ultimă generație.

5) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, se vor implementa măsuri de securitate suplimentare pentru accesul logic care vor ține cont de riscurile specifice ale acestor rețele. Controlul strict al accesului și/sau restricționarea accesului vor fi avute în vedere în cazul terților sau furnizorilor de servicii gestionate (entitățile care furnizează servicii legate de instalarea, gestionarea, funcționarea sau întreținerea produselor, rețelelor, infrastructurii, aplicațiilor TIC sau a oricăror alte rețele și sisteme informatice, prin intermediul asistenței sau al administrării active efectuate fie la sediul clienților, fie la distanță) care sunt considerați de risc ridicat sau care accesează din țări din afara Uniunii Europene rețelele și sistemele informatice;

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

7) să aplice măsuri de securitate adecvate în cazul managementului actualizărilor, corecțiilor software, dar și în cazul traficului de management și de semnalizare, în vederea prevenirii intervențiilor neautorizate în cadrul rețelei sau componentelor acesteia;

8) să asigure utilizarea adecvată a criptării datelor în timpul stocării sau a transmiterii lor prin rețea pentru a preveni incidentele de securitate și/sau minimiza impactul acestora asupra utilizatorilor finali sau a altor rețele sau servicii de comunicații electronice;

9) să asigure protecția adecvată a cheilor criptografice și a oricăror altor informații de autentificare pentru a nu fi divulgate sau alterate, iar accesul la cheile private să fie monitorizat și controlat.

Domeniul de securitate presupune măsuri ce țin de obiectivele furnizorilor în materia securității fizice a rețelei şi a infrastructurii asociate, securitatea utilităților-suport, securitatea pentru accesul (logic) la rețea şi la sistemele informatice, securitatea pentru a asigura protecția rețelelor şi serviciilor de comunicații electronice împotriva codurilor cu potențial dăunător. Completările aduse au în vedere elementele de noutate introduse de Ordonanța de urgență a Guvernului nr. 111/2011, precum și anumite măsuri specifice securității rețelelor 5G, ținând cont de riscurile asociate și măsurile tehnice stabilite în Setul de Instrumente, precum și de amenințările la securitatea fizică și logică aflate în continuă evoluție.

În cazul rețelelor 5G, Setul de Instrumente prevede măsuri tehnice ce implică implementarea unor măsuri tehnice adecvate, flexibile și verificabile pentru asigurarea controlului strict al accesului la rețeaua de comunicații electronice, aplicarea *principiului privilegiului minim* și aplicarea *principiului separării sarcinilor*. Trebuie să existe implementate proceduri prin care se asigură că măsurile produc efecte constant și evoluează cu tehnologia. Aceste măsuri constau în aplicarea efectivă a unor principii referitoare la privilegii și drepturi, autentificare, accesul de la distanță, având în vedere și accesul terțelor părți, în special terții considerați de risc înalt. De asemenea, trebuie avută în vedere consolidarea securității fizice a componentelor critice și sensibile ale rețelelor 5G. Măsurile tehnice includ consolidarea controlului accesului fizic, controale de acces în vigoare pentru persoanele care accesează perimetrele, limitarea numărului de persoane care primesc acces, verificarea personalului în prealabil din punctul de vedere al securității (eng. *security-vetted*), asigurări că persoanele respective (se aplică inclusiv terților) au fost instruite și sunt calificate, toate entitățile care au acces în special la componente critice sau sensibile ale rețelei 5G sunt limitate și monitorizate. Setul de

Instrumente conține prevederi referitoare inclusiv la protecția integrității software, securitatea actualizărilor și managementului corecțiilor (eng. *patch*), prin existența unor mecanisme și procese adecvate care identifică și țin evidența modificărilor și actualizărilor (atunci când sunt efectuate actualizări de software și se implementează corecții de securitate în rețelele 5G).

În ceea ce privește politica privind controlul accesului, aceasta va include prevederi referitoare la controlul strict și/sau restricționarea accesului părților terțe (în special în cazul terților sau prestatorilor „*managed services*" care sunt considerate de risc crescut sau cei care accesează rețeaua și sistemele informatice din țări din afara UE). Controlul accesului (inclusiv cel de la distanță) va asigura accesul temporar părților terțe.

Totodată, în ceea ce privește securitatea fizică adecvată a rețelei şi a infrastructurii asociate, furnizorul de servicii sau rețele 5G nu va trebui să neglijeze nici aspecte ce țin de măsuri de securitate în domeniul managementului pieselor de schimb (strategii de tip „*multi-vendor*", pentru a evita dependența de producător unic), cel puțin în cazul resurselor critice.

Reamintim că Anexa nr. 1 conține obiective de securitate, ceea ce inseamnă că măsurile de securitate efective se vor stabili în conformitate cu importanța obiectivului protejat și vor ține cont de riscurile specifice. Pentru exemplificare, în cazul în care stațiile de bază conțin componente *multi-access edge computing* sau în cazul hub-uri de transmisiuni, securitatea acestora ar trebui sporită cu măsuri suplimentare. Măsurile de securitate efective sunt stabilite de furnizori, în urma propriei evaluări a riscurilor, respectând principiul proporționalității.

Furnizarea rețelelor şi serviciilor de comunicații electronice depinde într-o mare măsură de utilitățile suport, în special de furnizarea de energie electrică, dar și a altor perturbații ce pot fi cauzate de avarii sau deranjamente în cadrul utilităților suport. Prin urmare, aceste aspecte impun o consolidare a prevederilor din decizie. Așadar, pentru asigurarea securității utilităților suport trebuie implementate măsuri bazate pe standarde relevante și bune practici prin care să se asigure securitatea adecvată a acestora, dar și a facilităților conexe (sisteme de răcire pasivă, alimentare cu energie electrică prin intermediul bateriilor de rezervă, generatoare electrice, combustibil de rezervă etc.). Utilitățile suport trebuie astfel proiectate și dimensionate încât să fie în acord cu cerințele și specificațiile producătorilor de echipamente, precum și prevederile legale aplicabile. Echipamentele trebuie protejate împotriva perturbațiilor sau întreruperii alimentării cu energie electrică sau a altor întreruperi cauzate de probleme ale utilităților suport.

Reţelele de comunicaţii și sistemele informatice trebuie să fie protejate corespunzător în scopul de a menține integritatea lor, de a preveni şi detecta atacurile realizate cu ajutorul programelor maliţioase, precum şi tentativele de a indisponibiliza sau bloca resurse, acţiuni ce pot afecta furnizarea reţelelor şi serviciilor. Furnizorul de rețele sau de servicii de comunicații electronice trebuie să se asigure și să ia măsuri astfel încât programele software/aplicațiile să nu fie alterate sau manipulate, prin măsuri de securitate adecvate.

Așadar, pentru a proteja echipamentele care utilizează protocolul IP (servere, routere etc.), precum și pentru a menține securitatea rețelelor și sistemelor informatice și de a le proteja de atacuri informatice (ex. DoS/DdoS, virusuri, *malware*, atacuri tip *code injections*), organizaţia trebuie să stabilească şi să implementeze măsuri de contracarare a unor astfel de atacuri. Măsurile de securitate implementate pot viza: protecție de tip *defence-in-depth* (pe mai multe niveluri privind securitatea sistemelor informatice/aplicațiilor: antivirus, securitatea parolelor, criptarea, autentificare multi-factor, hashing de parole, scanari de vulnerabilități, sisteme de detecție intruziune etc.; securitatea rețelei: VPN; sisteme *firewall* etc.; securitatea fizică). Se vor mai avea în vedere măsuri cum ar fi: măsuri care asigură că software-ul și sistemele informatice utilizate sau implicate în activitatea furnizorului nu pot fi manipulate sau modificate fără autorizație, sistemele primesc actualizări de securitate la zi, se folosesc sisteme de detecție accesare pagini de internet potențial dăunătoare, datele critice în materia securității (parole, chei private etc.) nu sunt divulgate, se folosește autentificarea cu parole, angajații sunt instruiți pentru a putea identifica posibile probleme de securitate etc.

Referitor la pct. 5 și 6 ale pct. III din Anexa nr. 1 la proiectul de decizie, în conformitate cu art. 46 alin. (2) din Ordonanța de urgență a Guvernului nr. 111/2011, pentru a preveni și/sau reduce impactul incidentelor de securitate asupra utilizatorilor sau asupra altor rețele și servicii, măsurile de securitate prevăd inclusiv utilizarea criptării. ENISA acordă atenție majoră acestei prevederi și abordează subiectul în ghidul *Guideline on Security Measures Under the EECC, 4th Edition, July 2021* prin două obiective de securitate: *SO 13: Use of encryption* și *SO 14: Protection of security-critical data*. În concluzie, aceste obiective sunt reflectate la pct. 5 – 6 menționate mai sus. Se va asigura utilizarea adecvată a criptării datelor în timpul stocării sau transmiterii prin rețea. Datele ce urmează a fi criptate se stabilesc pe baza analizei de risc. Posibilitatea de a implementa criptarea poate fi influențată de limitările tehnologice (tehnologii, echipamente și protocoale mai vechi). Datele care se criptează pot include, spre exemplu, conținutul comunicațiilor, date critice despre utilizatori (cum ar fi identificatori unici), trafic de semnalizare și management, metadate etc. Algoritmii de criptare, precum și lungimile recomandate ale cheilor criptografice vor fi conform standardelor internaționale. Totodată, trebuie asigurată protecția adecvată a cheilor criptografice, sau a altor date critice din punctul de vedere al securității. Materialul cheilor criptografice, parolele, *shared-secrets*, sau orice materiale critice din punctul de vedere al securității trebuie protejate în mod adecvat, trebuie asigurată confidențialitatea și integritatea acestor informații. Va exista un control strict al accesului la cheile private și o monitorizare a acestuia. Sistemul de management al cheilor, parolelor sau materialelor critice din punct de vedere al securității va include utilizarea, valabilitatea și protecția lor, pe întreaga lor durată de viață. Toate cheile criptografice trebuie protejate împotriva modificării sau pierderii lor, iar cele private sau secrete vor fi protejate împotriva utilizării neautorizate sau dezvăluirii lor, iar acele echipamente care le vor genera, stoca, arhiva, trebuie de asemenea protejate fizic și logic. Datele critice din punct de vedere al securității se vor proteja utilizând mecanisme (bazate pe standarde, bune practici) cum ar fi control dual, funcții de *hashing* etc.

IV. Managementul operațiunilor

Obiective de securitate

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

1) să stabilească proceduri operaţionale şi responsabilităţi adecvate și să se asigure că toate sistemele necesare furnizării rețelelor și serviciilor de comunicații electronice sunt gestionate conform acestor proceduri operaționale;

2) să stabilească proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice, inclusiv schimbările software și să se asigure că acestea sunt realizate conform procedurilor adoptate;

3) să întocmească și să păstreze cel puțin un an jurnale care să conţină informaţiile relevante referitoare la schimbările de la pct. 2, inclusiv în cazul schimbărilor software (evidența schimbărilor, a corecțiilor, a actualizărilor etc.);

4) să efectueze evaluări prealabile ale impactului potențial al unei schimbări de sistem;

5) să stabilească proceduri de gestionare a resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate și controlul configurării astfel încât disponibilitatea şi starea acestora să fie verificată, care să includă:

a) identificarea și inventarierea resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, inclusiv cele ale unor terțe

părți, întocmirea de registre actualizate care să conțină detalii despre tehnologiile și componentele puse în funcțiune, dependența între aceste resurse, precum și identificarea configurărilor sistemelor;

b) stabilirea proprietarilor resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, definirea rolurilor, responsabilităților;

c) evaluarea de criticitate a resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate bazată pe evaluarea de risc.

Acest domeniu acoperă aspecte ce țin în principal de procedurile operaționale ale organizației, managementul schimbărilor și managementul resurselor. Furnizorii trebuie să stabilească și să mențină proceduri privind managementul schimbărilor efectuate în rețeaua de comunicații electronice precum și în sistemele informatice (software) pentru a minimiza probabilitatea apariției incidentelor rezultate în timpul sau în urma schimbărilor respective. Introducerea unor sisteme noi, schimbările majore aduse celor existente sau schimbări aduse unor elemente importante, trebuie să urmeze un proces de documentare, definire a cerințelor tehnice, testare, control al calității și implementare controlată. Acest proces trebuie să cuprindă o determinare a riscului, o analiză a impactului modificărilor și stabilirea măsurilor de securitate necesare. La evaluarea impactului trebuie avut în vedere, în mod evident, și impactul asupra comunicațiilor de urgență.

În ceea ce privește standardele relevante, prevederile generale aplicabile acestui domeniu sunt cele din ISO/IEC 27002 și ISO/IEC 27001.

Pe de altă parte, este necesară consolidarea și completarea măsurilor aferente acestui domeniu, care răspunde și nevoii de a avea măsuri care asigură integritatea software, managementul corecțiilor și actualizărilor software (eng. *patch*), prin existența în cadrul furnizorului a mecanismelor adecvate și a proceselor care identifică și țin evidența modificărilor, actualizărilor. În cazul rețelelor 5G, Setul de Instrumente prevede că furnizorii trebuie să respecte cerințele de bază în domeniul securității (cum ar fi, de exemplu, implementarea bunelor practici în domeniul securității în ceea ce privește configurarea echipamentelor, managementul rețelei, actualizări de securitate, politici privind securitatea etc.).

Completările aduse prin proiectul de decizie au scopul de a consolida prevederile existente, iar la stabilirea lor s-a plecat de la ghidurile ENISA menționate în cuprinsul cap. 2, precum și de la Setul de Instrumente.

Având în vedere că au existat incidente de securitate importante care au afectat mulți utilizatori care au avut drept cauză un management al schimbărilor defectuos, este important ca la stabilirea procedurilor privind managementul schimbărilor să fie avute în vedere aspecte cum ar fi: identificarea, înregistrarea, planificarea și verificarea schimbărilor, evaluarea impactului potențial direct sau indirect (inclusiv asupra securității), aprobarea formală a schimbării, informarea celor implicați în schimbare, dar și mecanisme pentru recuperare în caz de schimbare nereușită sau evenimente neprevăzute. Procedurile vor fi documentate și vor include sistemele care fac obiectul acestora, obiectivele, procedurile de revenire (*roll-back*), descrierea metodologiei sau proceselor care se urmează în vederea efectuării schimbărilor etc. În ceea ce privește gestionarea resurselor, conform pct. 2-4 de la Domeniul IV din Anexa nr. 1 la proiectul de decizie, măsurile de securitate implică identificarea resurselor, precum și identificarea configurărilor sistemelor.

V. Managementul incidentelor

Obiective de securitate

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

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

2) să se asigure de pregătirea adecvată, existența și disponibilitatea personalului pentru managementul incidentelor care afectează securitatea reţelelor şi serviciilor de comunicaţii electronice;

3) să stabilească și să implementeze procese și sisteme de detectare a incidentelor de securitate și a evenimentelor care pot conduce la incidente;

4) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, centrele de operațiuni de rețea și/sau centrele de operațiuni de securitate vor funcționa pe teritoriul național și/sau pe teritoriul Uniunii Europene; acestea ar trebui să asigure vizibilitatea și monitorizarea componentelor rețelei respective pentru a detecta evenimente de securitate și pentru a identifica și preveni amenințări;

5) să stabilească o procedură adecvată de raportare a incidentelor către ANCOM, precum şi către alte autorităţi responsabile, precum şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori de reţele şi servicii de comunicaţii electronice afectaţi, media, clienţi, parteneri de afaceri etc.);

6) să stabilească procese și proceduri pentru restabilirea prioritară a serviciilor ce contribuie la realizarea comunicațiilor de urgență.

Domeniul presupune măsuri ce țin de procese şi proceduri pentru managementul incidentelor de securitate, procese și sisteme de detectare a incidentelor de securitate și a evenimentelor care pot conduce la incidente, raportarea incidentelor către ANCOM și către alte autorități responsabile, precum şi stabilirea planurilor de comunicare a incidentelor către alte părți externe. Managementul incidentelor de securitate este de importanță majoră în contextul noilor reglementări. 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.), identificarea și analizarea cauzei incidentului, măsurile care pot fi luate pentru a minimiza efectele incidentului şi 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, dar și restabilirea funcționării serviciilor în cel mai scurt timp posibil, cu prioritizarea restabilirii serviciilor ce contribuie la realizarea comunicațiilor de urgență etc.

Completările prevederilor de bază au caracter de consolidare, în timp ce raportarea incidentelor de securitate cu impact semnificativ este tratată în cap. 8 din prezentul document.

În ceea ce privește măsurile de securitate suplimentare specifice rețelelor 5G, completarea își găsește justificarea în măsurile din Setul de Instrumente. Menționăm totodată că în cazul rețelelor 5G se ține cont de gradul ridicat de complexitate și potențiala dependență de părți terțe, de prestatori de servicii de tip „*managed services*", furnizori de echipamente, accesul de la distanță din alte țări etc. Aceste aspecte implică capabilități adecvate, mature, de management al incidentelor, capabilități de ultimă generație de detecție a incidentelor, precum și raportarea completă și de încredere a incidentelor de securitate cu impact semnificativ. Pentru toate aceste considerente sunt necesare completările aduse.

Furnizorii trebuie să asigure, totodată, operarea, monitorizarea și managementul sigur al rețelei prin existența centrelor de operațiuni de rețea[22] și/sau centrelor de operațiuni de securitate[23] pe teritoriul național, sau dacă acest deziderat nu se poate îndeplini, aceste centre vor fi operate cel

[22] Network Operation Center (NOC).
[23] Security Operation Center (SOC).

puțin pe teritoriul Uniunii Europene. Aceste centre trebuie să asigure cel puțin vizibilitate la toate componentele critice și sensibile, să detecteze anomalii, să identifice și evite amenințări. Măsura tehnică implică, totodată, obligația ca furnizorul să asigure o protecție adecvată a traficului de management, să evite modificările neautorizate din cadrul rețelei sau componentelor acesteia. ENISA de asemenea acordă atenție acestui aspect în cadrul obiectivului de securitate SO 19 din ghidul *Technical Guideline on Security Measures Under the EECC, 4th Edition, July 2021*. În concluzie, acest deziderat se reflectă la pct. 4.

VI. Managementul continuității afacerii

Obiective de securitate

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

1) să stabilească o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice în situaţiile generate de perturbări grave ale funcţionării reţelei sau serviciului; aceasta va include și măsuri privind asigurarea rezilienței lanțului de aprovizionare cu echipamente și software necesare furnizării rețelelor și serviciilor de comunicații;

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

3) în ceea ce privește rețelele definite la art. 2 lit. f) din Legea nr. 163/2021, planurile de continuitate şi de recuperare să aibă în vedere suplimentar:

- dependența de alte sectoare și servicii critice a căror afectare poate impacta direct sau indirect securitatea rețelelor și serviciilor;

- afectarea altor sectoare și servicii critice dependente de continuitatea furnizării rețelelor și serviciilor de comunicații electronice;

4) să stabilească o strategie pentru asigurarea accesului neîntrerupt la comunicațiile de urgență.

Domeniul tratează aspecte relevante ce țin de managementul continuității afacerii (strategii de continuitate și planuri de intervenție și continuitate pentru a reduce impactul avariilor majore, precum și efectele dezastrelor cauzate de natură sau factori umani), pentru a se asigura astfel continuitatea furnizării rețelelor și serviciilor de comunicații electronice. Acesta implică obligația furnizorilor de a stabili o strategie pentru asigurarea continuității furnizării rețelelor şi serviciilor, să dețină capabilități de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare. În acest sens, pe lângă stabilirea măsurilor și politicilor adecvate pentru restabilirea cât mai repede posibil a serviciilor de rețea și de comunicații importante, se vor avea în vedere măsuri pentru restabilirea cu prioritate a celor mai importante procese sau servicii, precum cele ce susțin comunicațiile de urgență. Caracterul important al comunicațiilor de urgență este evidențiat și de art. 62 alin. (2) din Ordonanța de urgență a Guvernului nr. 111/2011 care prevede explicit că „*Furnizorii de servicii de comunicații de voce au obligația de a lua toate măsurile necesare pentru a asigura acces neîntrerupt la serviciile de urgență, precum și transmiterea neîntreruptă a avertizărilor publice*".

Cu privire la implementarea ~~în practică a~~ măsurilor, părțile interesate se pot raporta atât la ghidurile ENISA amintite, cât și la îndrumări suplimentare ce se regăsesc și în standardele ISO/IEC 22301, ISO/IEC 27002 și ISO/IEC 27001.

În ceea ce privește măsurile de la pct. 1 din Domeniul VI din Anexa nr. 1 la proiectul de decizie referitor la asigurarea continuității furnizării rețelelor şi serviciilor de comunicații electronice în situațiile generate de perturbări grave, prevederile existente în Decizia președintelui ANCOM nr. 512/2013 au

fost completate astfel încât măsurile conținute de acest punct să includă și măsuri privind asigurarea rezilienței lanțului de aprovizionare, având in vedere importanța securizării acestuia (măsurile implementate pot include, de exemplu, posibilitatea înlăturării unor terți în cazul indisponibilității momentane sau permanente a acestora de a furniza componente).

Referitor la măsurile de securitate specifice rețelelor 5G, relevante sunt măsurile tehnice din Setul de Instrumente care se referă la consolidarea planurilor de reziliență și continuitate la nivelul furnizorilor. Furnizorii vor trebui să aibă planuri adecvate în cazul unui dezastru care afectează operarea rețelelor și să se asigure că orice dependență critică este identificată (cartografiată) și redusă. Totodată, furnizorii la rândul lor ar trebui să solicite acorduri similare de la părțile terțe și să colaboreze numai cu terți care demonstrează stabilitate pe termen lung. Sunt astfel abordate riscurile specifice cum ar fi perturbarea semnificativă a infrastructurilor și serviciilor critice, avarii majore datorate întreruperii alimentării cu energie electrică etc.

VII. Monitorizare, testare şi audit

Obiective de securitate

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

1) să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem care să asigure vizibilitate adecvată, să detecteze anomalii, să identifice și să prevină amenințări, inclusiv în ceea ce privește asigurarea comunicațiilor de urgență;

2) să stabilească politici pentru testarea, inclusiv prin exerciţii, a planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcţionării reţelei sau serviciului, având în vedere scenarii realiste care să acopere cât mai multe situații posibile; în urma analizei rezultatelor vor fi luate măsurile corespunzătoare;

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

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

5) să stabilească o politică pentru monitorizarea conformităţii şi pentru audit, cu un proces de raportare a conformităţii şi de rezolvare a deficienţelor constatate în timpul auditului; în cazul rețelelor definite la art. 2 lit. f) din Legea nr. 163/2021, politica pentru monitorizarea conformității va cuprinde aplicarea măsurilor de securitate din standardele relevante. Domeniul tratează aspecte relevante ce țin de monitorizarea, testarea și auditarea rețelelor, sistemelor și facilităților asociate și include măsuri privind politicile de monitorizare a sistemelor și privind jurnalele de sistem, inclusiv în ceea ce privește asigurarea comunicațiilor de urgență, politici pentru testarea planurilor de continuitate și intervenție, politici pentru testarea echipamentelor, sistemelor şi software-lor, politică pentru evaluarea şi testarea securităţii tuturor resurselor identificate ca fiind relevante din punctul de vedere al securității și a căror afectare poate conduce la incidente de securitate, monitorizarea conformităţii şi pentru audit, proces de raportare a conformităţii şi de rezolvare a deficienţelor constatate în timpul auditului.

Completările aduse au scopul de consolidare a măsurilor și adaptare la noile evoluții în domeniu, urmărind liniile directoare ale ghidurilor relevante. În ceea ce privește standardele aplicabile, relevante pot fi prevederile generale din ISO/IEC 27002 și ISO/IEC 27001.

VIII. Conștientizarea amenințărilor

Obiective de securitate

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

1) să stabilească și să implementeze procese de monitorizare, colectare și analiză continuă a informațiilor despre amenințările relevante la adresa securității rețelelor și serviciilor de comunicații electronice;

2) să ia măsuri adecvate de atenuare și prevenire a amenințărilor relevante la adresa securității rețelelor și serviciilor de comunicații electronice.

Conștientizarea amenințărilor este un domeniu prevăzut de dispozițiile art. 46 alin. (3) din Ordonanța de urgență a Guvernului nr. 111/2011. Conform acestor prevederi, măsurile luate de furnizori trebuie să vizeze conștientizarea amenințărilor, ceea ce implică monitorizarea și colectarea informațiilor despre amenințările relevante la securitatea rețelelor și serviciilor de comunicații electronice (ex. sisteme de tip OSINT), actualizarea permanentă a cunoștințelor despre amenințări, înțelegerea mediului în care organizația funcționează, diverse comunicări, detecția și investigarea amenințărilor[24].

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului vor stabili și menține mecanisme adecvate pentru monitorizarea și colectarea informațiilor despre amenințările relevante la securitatea rețelelor și serviciilor de comunicații electronice. Informațiile despre amenințări se vor putea folosi pentru a preveni, detecta sau răspunde la amenințări. Furnizorii la rândul lor pot detecta și investiga amenințările, dar de regulă ei primesc și utilizează informațiile și avertizările produse de alte surse. Acestea pot viza trei niveluri, astfel: strategic (informații generale despre peisajul amenințărilor aflat în continuă schimbare – de exemplu: tipuri de atacatori, tipuri de atacuri), tactic (de exemplu: informații despre metodologiile atacatorilor, tehnologii, mecanisme), operațional (de exemplu: detalii despre atacuri, inclusiv indicatori tehnici). Măsurile de securitate adecvate includ monitorizarea continuă a amenințărilor (pot consta în monitorizarea fluxurilor de informare a unor entități specializate/competente cum sunt cele de tip OSINT[25], a informărilor comerciale din piață, a cercetărilor din domeniul securității[26], în vederea identificării amenințărilor relevante pentru rețelele și serviciile furnizate. Suplimentar, identificarea amenințărilor se poate face prin partajarea bilaterală informală și ad-hoc a informațiilor cu organizații relevante. Aceste măsuri implică apartenența și contactul cu grupuri specializate în securitatea rețelelor și serviciilor de comunicații electronice. Organizația trebuie astfel să îmbunătățească și să actualizeze constant cunoștințele și informațiile pe care le deține despre amenințări, să înțeleagă mediul în care organizația funcționează, să primească informări timpurii cu privire la amenințările la securitatea rețelelor și serviciilor (alerte, sfaturi, remedii referitoare la atacuri și vulnerabilități). În cadrul procedurilor se vor defini rolurile, responsabilitățile, procesele, mecanismele de colectare a informațiilor referitoare la amenințările semnificative, existente sau emergente și măsurile de atenuare corespunzătoare. Scopul este să se asigure că organizația este mereu conștientă de contextul în care își desfășoară activitatea.

Este important de menționat faptul că aceste obiective de securitate sunt complementate și de obligația prevăzută la art. 47 alin. (3) din Ordonanța de urgență nr. 111/2011, potrivit căreia: "*(3) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a informa, în mod gratuit, utilizatorii potențial afectați de o*

[24] În acest sens ghidul ENISA Technical Guideline on Security Measures Under the EECC, 4th Edition, July 2021 conține două obiective de securitate dedicate, denumite SO28: Threat intelligence și SO29: Informing users about threats;
[25] *Open-source intelligence*, care poate include surse de informații publice provenite din media, internet, autorități publice, resurse academice sau profesionale, comerț etc. Conform Glosarului de termeni pentru domeniul securității cibernetice, *Open Source Intelligence (OSINT)* reprezintă procesul de colectare şi analiză a datelor şi informațiilor din surse publice, în contextul realizării unor materiale de intelligence;
[26] Ca de exemplu, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape sau recenta publicație *ENISA 5G Threat Landscape Report to Enhance 5G Security*;

amenințare specifică și semnificativă de securitate, cu privire la orice măsură de protecție sau măsură corectivă care poate fi luată de utilizatori. Acolo unde este cazul, furnizorii informează utilizatorii și cu privire la amenințarea în sine".

Ca urmare, furnizorii vor stabili, menține și implementa procese și proceduri pentru informarea utilizatorilor finali despre amenințările de securitate care îi pot afecta. Aceste procese și proceduri vor fi documentate, actualizate și revizuite periodic și vor include roluri și responsabilități, mecanisme și criterii pentru identificarea amenințărilor semnificative și mecanismele și metodele folosite pentru informarea cât mai repede posibil și adecvată a utilizatorilor finali. Utilizatorii finali vor trebui informați cu privire la recomandările și bunele practici cu privire la măsurile folosite pentru a înlătura amenințările specifice.

Informarea propriu zisă a utilizatorilor finali poate fi realizată prin buletine informative, pagini web dedicate care conțin informații despre amenințări, sau orice alt mijloc/mecanism documentat și testat de informare a utilizatorilor în cazul unor amenințări de securitate semnificative. Exemplele menționate anterior sunt în principal mijloace de informare în masă, dar pot fi folosite și mijloace de informare individuale. În cazul rețelelor 5G, procesele și procedurile de informare a utilizatorilor sunt identice însă ar trebui să includă și măsuri care au în vedere existența unor mecanisme pentru informarea utilizatorilor finali despre dispozitivele utilizatorilor potențial vulnerabile, inclusiv IoT și riscurile aferente.

7. Valorile minime ale duratelor de back-up electric fix

Numărul incidentelor electrice ocupă în continuare o pondere însemnată din totalul incidentelor de securitate care au un impact semnificativ, raportate Autorității de către furnizorii de rețele și servicii de comunicații electronice. Situația a fost analizată de ANCOM în cadrul Rapoartelor privind incidentele care au afectat securitatea rețelelor și serviciilor de comunicații electronice publicate anual detaliindu-se separat impactul pe care îl au incidentele datorate întreruperii furnizării energiei electrice în raport cu totalul celor raportate. Astfel, în ultimii 5 ani, procentajul acestui tip de incidente depășește valoarea de 40% din totalul incidentelor raportate, iar în anul 2022 a ajuns la valoarea de 55% potrivit graficului următor (Figura nr. 1). Totodată, reținem că durata medie a incidentelor cu cauza menționată se situează în jurul valorii de 6 ore, cu un maxim absolut de 6 ore și 28 minute, înregistrat în 2022 (Figura nr. 2).

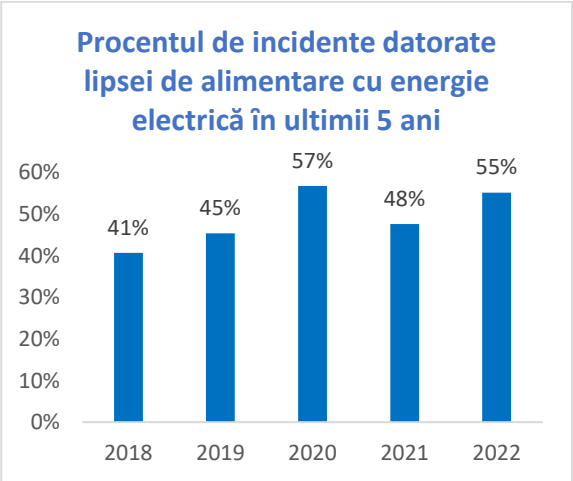

Figura nr. 1

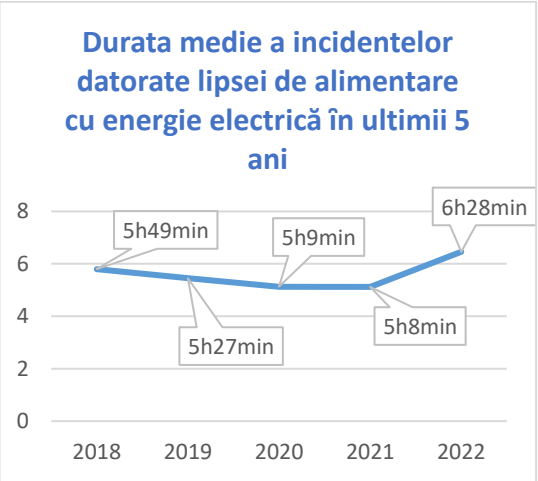

Figura nr. 2

Mai mult, conform datelor unui studiu de profil, finalizat și publicat de către ANCOM la începutul anului 2021[27], incidentele electrice neraportabile, respectiv neîncadrabile în categoria incidentelor cu impact semnificativ, provoacă în egală măsură disfuncționalități notabile ale unor elemente de rețea,

[27] Studiu disponibil la următoarea adresă: https://www.ancom.ro/uploads/links_files/Incidente_energie_studiu_2021.pdf.

cu impact imediat asupra continuității furnizării cel puțin a anumitor tipuri de servicii, fapt evidențiat de anumite categorii de reclamații și sesizări ale utilizatorilor finali, transmise atât furnizorilor, cât și către ANCOM. Potrivit datelor transmise de furnizori, s-a observat un nivel de incidență important în ceea ce privește întreruperea furnizării energiei electrice, operatorii mobili înregistrând un număr total de peste 100.000 de evenimente de acest tip în decurs de 12 luni calendaristice, având asociate cca. 38.000 de situații de depășire a capacităților de back-up electric instalate, cu impact imediat în asigurarea continuității serviciilor.

În Decizia președintelui ANCOM nr. 512/2013 sunt stipulate o serie de măsuri privind securitatea utilităților-suport necesare asigurării funcționării în condiții normale a rețelelor de comunicații electronice, aceste măsuri având însă un caracter larg, calitativ. În contextul dezideratului de întărire a securității și rezilienței rețelelor, aflat în atenția Autorității și în strânsă corelație cu preocupările de la nivel european, este necesară introducerea unor măsuri de securitate specifice pentru adresarea incidentelor electrice.

Implementarea noilor măsuri impuse se va face în termen de 18 luni de la data publicării Deciziei în Monitorul Oficial, iar identificarea și analiza categoriilor de probleme/constrângeri întâmpinate de furnizori în implementarea soluțiilor se va face prin intermediul grupului consultativ constituit potrivit art. 8 din proiectul de decizie.

Este important de precizat faptul că deși nevoile de comunicare ale societății actuale sunt adresate în principal de către rețelele mobile, cu un trend ascendent în această direcție pe termen mediu și lung, rețelele fixe joacă în continuare un rol important în furnizarea diverselor tipuri de servicii de comunicații electronice către utilizatorii finali. Drept urmare, furnizorii ficși mari, care pot influența buna funcționare a unor elemente cheie ale ansamblului național de rețele și servicii de comunicații electronice, intră deopotrivă sub incidența prevederilor referitoare la măsurile de back-up electric din proiectul de decizie.

În scopul stabilirii unor durate minime de back-up electric necesar a fi asigurate pentru elementele de rețea de comunicații electronice, ANCOM a avut în vedere și a analizat, în mod agregat, o serie de date, principalii factori contributivi în stabilirea valorilor stipulate în proiectul de decizie supus consultării publice fiind:

a) Rezultatele studiului extins asupra incidenței evenimentelor/avariilor electrice și implicațiilor acestora asupra rețelelor de comunicații, publicat de către ANCOM în primăvara anului 2021, disponibil pe site-ul Autorității la adresa:
https://www.ancom.ro/uploads/links_files/Incidente_energie_studiu_2021.pdf;

b) Valorile individuale ale duratelor de back-up uzitate, respectiv prevăzute în legislațiile secundare aplicabile în unele State Membre ale Uniunii Europene, temă a cărei sinteză se poate consulta la adresa:
https://www.enisa.europa.eu/publications/power-supply-dependencies/at_download/fullReport;

c) Valorile duratelor de back-up raportate ca fiind deja implementate în rețelele naționale, obținute ca urmare a intervievării furnizorilor, realizate la finele anului 2020 de către ANCOM prin intermediul unui chestionar specializat – valori care se regăsesc în studiul menționat la punctul a);

d) Dezideratul de implementare în mod concret a activităților de întărire generală a securității rețelelor, în contextul apariției și dezvoltării rapide a rețelelor de comunicații electronice bazate pe tehnologia 5G, în sensul „5G Toolbox" (prin intermediul măsurilor tehnice specificate în secțiunea TM11, având asociat grupul de acțiuni-suport SA08). Documentul la care se face referire poate fi accesat la adresa:
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468;

e) Frecvența, localizarea și duratele avariilor apărute în rețeaua electrică de distribuție națională, potrivit raportărilor ANRE. Mai multe detalii se găsesc la adresa:
https://www.anre.ro/ro/energie-electrica/rapoarte/rapoarte-indicatori-performanta;

f) Particularitățile de exploatare a rețelelor de comunicații electronice din România, prin prisma unor caracteristici-cheie, cum ar fi morfologia terenului (clutter), cu impact asupra timpilor de acces

fizic (în locațiile care găzduiesc echipamente de rețea) sau a arealului geografic deservit de echipamentele instalate într-o anumită locație.

În cele ce urmează facem unele precizări, menite să conducă la o mai bună înțelegere a prevederilor proiectului de decizie, precum și unele recomandări, cu titlu de bune practici în securizarea în mod corect și responsabil a rețelelor de comunicații electronice, din punct de vedere al asigurării continuității în alimentarea cu energie electrică a echipamentelor de rețea.

a) Precizări și clarificări

În ceea ce privește stabilirea duratelor de back-up electric de o oră – durată aplicabilă oricărui element de rețea situat în municipiile reședință de județ și de 3 ore – durată aplicabilă oricărui element de rețea situat în afara municipiilor reședință de județ, respectiv 6 ore timp de back-up electric fix extins, considerăm important de menționat faptul că aceste valori sunt în general egale cu valorile limită inferioară de back-up declarate a fi deja aplicate la nivelul rețelelor furnizorilor naționali, potrivit datelor colectate de la aceștia în cadrul studiului ANCOM menționat anterior. Din acest punct de vedere, în măsura în care raportările au fost făcute cu un nivel adecvat de corectitudine, impunerea introdusă nu ar trebui să ridice probleme majore din punct de vedere al costurilor sau al timpilor de conformare.

În municipiile reședință de județ, potrivit art. 4 alin. (1) lit. a) din proiect, se stabilește o durată de back-up electric de o oră, inferioară celei aplicabile restului localităților, întrucât s-au luat în calcul atât densitatea elementelor de rețea/overlapping, termenele mai mici de restabilire a alimentării cu energie electrică în caz de incident energetic, la nivelul furnizorilor de energie electrică, precum și accesul mai facil al echipelor de teren care să suplinească, după caz, necesarul energetic prin soluții de back-up mobil.

În egală măsură, este necesar a menționa faptul că duratele impuse nu sunt mai restrictive decât măsurile similare aplicabile la nivelul Uniunii Europene, deși indicele de frecvență (SAIFI) a întreruperilor neplanificate în furnizarea energiei electrice depășește sistematic plaja de valori înregistrate la nivel european, iar indicele de durată a întreruperilor (SAIDI) este superior mediei europene, indiferent de tipul întreruperilor (planificate sau neplanificate) – așa cum rezultă din statisticile anuale publicate de ANRE pentru anul 2019. Prin aceasta se urmărește în mod direct ca duratele de back-up impuse să nu transfere problemele existente în rețelele de furnizare a energiei electrice în sarcina furnizorilor. Pentru acest aspect, sunt necesare măsuri suplimentare implementate în conjuncție cu instituțiile și furnizorii din domeniu.

În ceea ce privește prevederile art. 4 alin. (2) din proiectul de decizie, potrivit cărora *„Capacitatea de back-up electric necesară se va calcula avându-se în vedere puterea maximă absorbită de echipamentul de securizat [...]”*, s-a avut în vedere faptul că, deși încărcarea diferitelor resurse de rețea/trafic este variabilă și are un caracter dinamic, o eventuală calculație făcută pe baza mediei de utilizare a resurselor de rețea aferente unei locații nu este acceptabilă, aceasta neasigurând atingerea deziderатului de garantare a resurselor de alimentare pe o durată clar definită, bine stabilită, cuantificabilă. În egală măsură, în cazul unei avarii electrice, este de așteptat ca necesarul de comunicații aferent zonei geografice afectate de incident, îndeosebi al comunicațiilor mobile, să crească pe durata desfășurării incidentului. Pe de altă parte, ca efect colateral, măsura stabilită va avea impact asupra unei planificări mai judicioase a resurselor și configurațiilor de rețea, cu consecințe directe asupra consumului de energie în sens global.

Prevederile alin. (3) ale aceluiași articol vin să completeze metoda de calcul a necesarului de energie electrică aferent unei locații, prin includerea valorilor de *„[...] putere maximă absorbită de sistemele de climatizare, sistemele de supraveghere alarme externe și sistemele de control-acces.”*, întrucât în perioadele cu temperaturi ambiante excesive (pozitive sau negative) consumul de energie al sistemelor-suport are valori semnificative raportat la necesarul total de energie electrică al unei locații, iar practica operatorilor arată că de multe ori sunt necesare fie limitarea capacității de trafic, fie oprirea temporară a unora dintre tehnologiile instalate, pentru asigurarea continuității în mod minimal a unor servicii de bază în locațiile respective. Pentru păstrarea unei proporționalități între dimensiunea impactului incidentului electric și efortul investițional necesar din partea operatorilor,

alin. (4) al aceluiași articol stabilește exceptarea din calculul totalului energetic de asigurat pentru categoriile reglementate de art. 4 alin. (1) lit. a) și lit. b) din Proiect a consumului sistemelor de climatizare, furnizorii având însă obligația să asigure regimul termic/condițiile tehnice adecvate de funcționare a echipamentelor pe toată durata alimentării din sursa de back-up.

Astfel, măsurile propuse au în vedere favorizarea continuității furnizării serviciilor de comunicații electronice către utilizatori în toate zonele țării, mai cu seamă în contextul sporirii din ultimii doi ani și preconizate și în viitor a gradului de utilizare a serviciilor de comunicații electronice și dependența tot mai mare a populației de buna funcționare a acestora pentru activități importante, cu impact semnificativ asupra societății și care nu pot fi amânate (ex. telemuncă, telește coală, servicii publice digitale).

În sensul excepției stipulate de art. 4 alin. (5), s-au avut în vedere cazurile de echipamente de rețea mobilă care deservesc în mod normal clienți punctuali pentru acoperire *deep-indoor* (de ex., repetoare radio) sau echipamentele destinate asigurării unei capacități extinse la nivel *outdoor* (de ex., microcelule, picocelule) și care nu sunt prevăzute în mod curent cu resurse de back-up, întrucât nu se consideră a reprezenta o amenințare directă asupra continuității furnizării serviciilor, atât timp cât este asigurată acoperirea în zonele respective la nivel *outdoor*. Pe de altă parte, în cazul echipamentelor din aceste categorii care vor furniza servicii specifice 5G și care vor deveni dominante în etape ulterioare de dezvoltare a rețelelor, se va respecta obligația de asigurare a back-up-ului electric, în sensul prevăzut de art. 4 alin. (1) din proiectul de decizie, întrucât aceste echipamente vor constitui baza funcționării unor servicii critice sau pot avea un impact semnificativ din punct de vedere economic și societal.

În ceea ce privește rețelele fixe, în sensul prevederilor art. 4 alin. (5), s-a stabilit excluderea echipamentelor instalate în locațiile utilizatorilor care nu sunt prevăzute în mod curent cu resurse de back-up electric, avându-se în vedere tipologia uzitată de alimentare a acestora (respectiv, din sursa de energie electrică a abonatului/utilizatorului) precum și restricțiile de ordin fizic (în sensul disponibilității spațiului de instalare a unor soluții de back-up electric la abonat/utilizator). Totodată, au fost excluse și echipamentele de rețea fixă aflate în proximitatea locațiilor utilizatorilor finali, precum acele cabinete stradale sau camerele tehnice telecom ale clădirilor, care găzduiesc echipamente de comunicații ce preced echipamentele terminale (CPE[28]), întrucât CPE ale abonatului ar fi oricum nefuncționale în eventualitatea apariției unui incident electric în zonă, cu excepția cazului în care utilizatorul și-ar fi asigurat singur o soluție de back-up electric pentru aceste echipamente.

Termenul de aliniere a rețelelor la condițiile impuse prin prezentul proiect, de 18 luni de la intrarea în vigoare a acestui act normativ, stabilit la art. 11 alin. (1) teza finală, este considerat necesar pentru derularea aspectelor operaționale (realizarea unei analize, identificarea soluțiilor tehnice necesare pentru implementarea noilor prevederi, în condiții de înaltă calitate tehnică) și investiționale (realizarea procedurilor de achiziție a soluțiilor de back-up electric) necesare, păstrând în același timp un orizont rezonabil de vizibilitate a efectelor implementării măsurilor prevăzute în prezenta decizie.

b) Recomandări

Pe baza interpretării datelor primite de la furnizorii de comunicații electronice mobile, în cadrul studiului realizat de ANCOM în primul trimestru al anului 2021, notăm că, deși durata de back-up raportată este de cel puțin 3 ore, s-au înregistrat totuși cazuri de depășire a disponibilității soluțiilor de back-up electric de ordinul miilor. Depășirile de durată disponibilă de back-up indică fie un calcul neadecvat al capacităților necesare, fie probleme majore în continuitatea asigurării furnizării de energie electrică de către distribuitor. Deși timpii raportați de back-up – fie ei teoretici sau presupus-măsurați – induc ideea de nivel ridicat de reziliență, numărul situațiilor de depășire a capacităților instalate este în discrepanță cu acești timpi. În scopul îndeplinirii noilor cerințe privind asigurarea back-up-ului electric, recomandăm evaluarea cu atenție ridicată a necesarului energetic pentru fiecare

[28] CPE semnifică Customer Premises Equipment

locație care intră sub incidența prezentei decizii și efectuarea de exerciții/teste periodice în rețea pentru a se asigura/verifica funcționalitatea soluțiilor, respectiv nivelul de corelație între rezultatele calculelor și realitatea din teren.

Avându-se în vedere curba de creștere a traficului în rețelele mobile, cu predilecție a traficului de date, precum și dinamica de dezvoltare a rețelei fiecărui furnizor determinată de către acesta pe baze statistice sau prin predicționare, în sensul probabilității și frecvenței de adăugare a unor echipamente fizice active de rețea (hardware) în anumite locații, furnizorii pot alege *a priori* soluții de back-up electric care să asigure durate superioare celor minime obligatorii prevăzute în prezenta decizie, pentru o mai rapidă realiniere a capacității electrice de back-up în cazurile de extindere de rețea.

În scopul stabilirii locațiilor cu potențial de încadrare în categoria prevăzută la alin. (1) lit. c), respectiv cu necesar de back-up fix extins, de minimum 6 ore, recomandăm o analiză atentă asupra factorului contributor constituit de nivelul de corelație între frecvența de apariție și durata incidentelor electrice – în sensul în care, în anumite situații, timpul scurs între două avarii consecutive ar putea să fie insuficient restabilirii capacității nominale instalate de back-up (de ex., timpul necesar reîncărcării acumulatorilor, timpul necesar realimentării cu combustibil a generatoarelor fixe etc.).

Cel puțin în ceea ce privește incidentele electrice cu impact semnificativ, conform datelor transmise de către operatorii de rețele și servicii de comunicații electronice către ANCOM, observăm că durata medie a acestora are o valoare diferită, superioară față de durata medie a întreruperilor văzute din perspectiva furnizorilor de electricitate, respectiv prezentate în raportul ANRE pe anul 2019. Această stare de fapt poate indica eventuale dificultăți în gestionarea de către operatori a episoadelor de indisponibilitate a energiei electrice la nivel de management operațional: logistică inadecvată a soluțiilor de back-up electric mobil (de ex., timpi mari de transport, branșare/debranșare a generatoarelor mobile) sau lipsa completă a autonomiei de back-up electric, cu impact negativ asupra timpului de repunere în serviciu a rețelei după revenirea alimentării cu energie electrică din rețeaua publică (de ex., întreruperea generează probleme software/hardware conexe, cu impact semnificativ în timpul de restabilire a serviciilor). Pentru o bună evidență a situației de fapt și în scopul respectării prevederilor art. 4 din prezenta decizie, încurajăm furnizorii să documenteze și să aplice proceduri interne specifice, detaliate, aplicabile în cazul particular al avariilor electrice, respectiv separate de fluxul comun de gestionare a incidentelor generale de rețea.

8. Raportarea incidentelor de securitate cu impact semnificativ

În ceea ce privește raportarea incidentelor de securitate cu impact semnificativ, prezentul proiect de decizie are în vedere revizuirea parametrilor în funcție de care este determinată amploarea impactului unui incident de securitate.

De asemenea, au fost luate în considerare definițiile conceptelor de „Securitate(a) rețelelor și serviciilor", respectiv de „incident de securitate" prevăzute de Ordonanța de urgență a Guvernului nr. 111/2011. Astfel, conform art. 4 alin. (1) pct. 54^1 din legea mai sus amintită, „*securitatea rețelelor și serviciilor reprezintă capacitatea rețelelor și serviciilor de comunicații electronice de a rezista, la un anumit nivel de încredere, oricărei acțiuni care afectează disponibilitatea, autenticitatea, integritatea sau confidențialitatea acestor rețele și servicii, a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de rețelele ori serviciile de comunicații electronice respective sau accesibile prin intermediul acestora"*.

De asemenea, conform pct. 54^2 din cadrul aceluiași alineat, „*incidentul de securitate este un eveniment care are un efect real negativ asupra securității rețelelor sau serviciilor de comunicații electronice*".

Pe lângă definițiile notate în capitolul 3 din prezentul document, în continuare vor fi date o serie de exemple de incidente ce afectează diversele dimensiuni ale securității, exemple furnizate de ENISA în *Technical Guideline on Incident Reporting under the EECC, March 2021*:

- disponibilitatea – întreruperi de apeluri pentru un anumit interval de timp sau scăderea vitezei de transfer pentru serviciile de acces la internet. În aceste cazuri, percepția utilizatorului final poate fi că serviciul de comunicații electronice nu mai corespunde scopului pentru care este folosit;

- confidențialitate – criptarea nu funcționează în mod corespunzător și conținutul schimbului de mesaje private a ajuns disponibil atacatorilor, o bază de date care conține jurnale de sistem (cum ar fi lista de convorbiri, IMSI) a fost compromisă, email-urile se direcționează către destinatari necunoscuți sau a avut loc un atac asupra unui server de autentificare, iar credențialele obținute au fost utilizate pentru a avea acces la informații;

- integritatea - există o afectare/compromitere a integrității datelor sau metadatelor, ca de exemplu: modificarea datelor apelantului/IP-ului (spoofing), modificarea fișierelor jurnal, modificarea unor fișiere de configurare sau de rutare, malware sau software instalat ilicit pe un server capabil să identifice și să modifice date din diverse fișiere etc. sau exploatarea unei vulnerabilități în protocolul rețelei care permite interceptarea comunicațiilor. În acest caz, pe lângă afectarea integrității, incidentul afectează și confidențialitatea;

- autenticitatea - aplicația nu asigură protecția corespunzătoare a procesului de autentificare pentru accesul neautorizat din exterior. Prin urmare, are loc un atac cibernetic de tip „*man-in-the-middle*" sau interceptarea serviciilor de comunicații/aplicațiilor care conduc la furtul sau utilizarea incorectă, rău intenționată a credenţialelor de autentificare.

Având în vedere definiția incidentului de securitate şi recomandările în domeniu (ghidul ENISA *Technical Guideline on Incident Reporting under the EECC, March 2021*), proiectul de decizie definește incidentul de securitate care are un impact semnificativ. Astfel, această definiție are în vedere, pe lângă praguri cantitative, şi praguri calitative. În cazul unui incident care atinge cel puțin unul dintre praguri (fie ele cantitative sau calitative) se impune obligația raportării către ANCOM.

Așadar, incidentul de securitate care are un impact semnificativ este acel incident care atinge cel puțin unul dintre pragurile cantitative sau calitative definite în proiectul de decizie.

Astfel, furnizorii vor avea obligația de a raporta care dintre praguri a fost depășit şi ce anume a declanșat raportarea acestuia. Spre deosebire de definiția din prezent, noile modificări prevăd raportarea incidentelor nu numai în funcție de anumite praguri cantitative, ci şi în funcție de o serie de praguri calitative.

În funcţie de situație, furnizorii vor trebui să raporteze incidentele care depășesc cel puțin unul dintre următoarele:

a) *praguri cantitative*:

a1) dacă, din perspectiva disponibilității, incidentul a afectat mai mult de 5.000 de utilizatori timp de cel puțin 60 de minute. Acest prag a fost păstrat din Decizia președintelui ANCOM nr. 512/2013 deoarece şi-a dovedit utilitatea din raportările anterioare.

a2) dacă incidentul depășește pragul de 500.000 de ore–utilizator. A fost adăugat acest nou prag cantitativ pentru a fi notificate şi incidentele care afectează un număr foarte mare de utilizatori și, prin urmare, au impact semnificativ, dar care până în prezent nu întruneau condiția de durată. Pragul ore-utilizator se calculează folosind formula:

Ore-utilizator = (Număr utilizatori afectați de incident x durata incidentului, exprimată în minute) / 60.

a3) dacă, din perspectiva confidențialității, integrității sau autenticității, sunt afectați cel puțin 5.000 de utilizatori, indiferent de durata incidentului.

b) *praguri calitative*:

b1) dacă incidentul a afectat, direct sau indirect, pe o perioadă de cel puțin 15 minute, rutarea comunicațiilor de urgență către Serviciul de urgență 112 – în cadrul acestui criteriu vor fi raportate incidentele care afectează echipamentele de rutare către rețeaua Serviciului de Telecomunicații Speciale (denumit în continuare „STS"). STS este administratorul Sistemului național unic pentru apeluri de urgență. Incidentele care afectează serviciul de comunicații de voce şi, implicit, apelarea către serviciul unic pentru apeluri de urgență nu vor fi raportate conform acestui prag, ci conform pragului cantitativ;

b2) dacă incidentul a avut impact transfrontalier – se va selecta acest prag dacă furnizorul are informații cu privire la afectarea unor utilizatori ai unor furnizori de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului din afara granițelor României;

b3) dacă incidentul a afectat securitatea rețelelor și serviciilor altui furnizor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și i-a cauzat acestuia un incident care are un impact semnificativ în măsura în care această situație era cunoscută - acest prag va fi selectat în situația în care un incident din rețeaua proprie afectează un furnizor partener și îi provoacă acestuia un incident care are un impact semnificativ, indiferent dacă este atins sau nu un prag cantitativ în rețeaua proprie. Dacă furnizorul care provoacă incidentul nu cunoaște numărul de utilizatori afectați în rețeaua parteneră, acesta va fi informat de către ANCOM. Această raportare este necesară deoarece doar notificarea incidentului de către furnizorul impactat colateral conduce la o încadrare eronată a incidentului respectiv (atât în ce privește cauza producerii, cât şi resursele afectate), precum și la lipsa unor detalii esențiale privind incidentul. În acest context, şi pentru a avea o evidență a acestui tip de incidente, se impune obligația ca incidentele cauzate de problemele în rețelele partenere să fie notificate și de către furnizorul în a cărui rețea a avut loc incidentul.

Pentru a veni în ajutorul furnizorilor şi pentru a colecta/analiza mai eficient informațiile furnizate, ANCOM a luat decizia modificării semnificative a **formularului de raportare**. Aceste modificări includ nu doar eliminarea și simplificarea unor câmpuri, ci şi adăugarea unora noi, considerate necesare pentru simplificarea procesului de raportare și colectare a datelor.

Monitorizarea incidentelor de securitate pe parcursul anilor precedenți a relevat faptul că sunt destul de multe incidente care se repetă şi ele ar trebui diferențiate şi analizate suplimentar. În acest sens, a fost adăugat un nou câmp care să evidențieze natura repetitivă a incidentelor. Un incident repetitiv este acel incident de securitate care are un impact semnificativ şi care cumulează următoarele 3 caracteristici:

a) afectează aceleași resurse;

b) are aceeași cauză;

c) a mai fost raportat în precedentele 12 luni.

Implementarea unor măsuri de securitate adecvate ar trebui să preîntâmpine apariția incidentelor repetitive. Aceste incidente vor fi monitorizate suplimentar pentru a verifica dacă au fost implementate măsuri de către furnizori, dacă acele măsuri au fost eficiente în vederea limitării repetării incidentelor precum și eventuale probleme pe care le întâmpină furnizorii în adoptarea unor măsuri eficiente.

Pentru a facilita completarea informațiilor în aplicația informatică de raportare a incidentelor, s-a decis introducerea unui câmp, în format text, ce va conține informații despre impact (numărul de utilizatori afectați de incident, durata incidentului şi aria/răspândirea geografică). Astfel, se dorește eliminarea secțiunilor cu fiecare tip de serviciu afectat în parte şi numărul de utilizatori afectați. Fiecare furnizor va avea posibilitatea de a introduce, sub formă de text, numărul de utilizatori afectați pe fiecare tip de serviciu. În cazul în care incidentul afectează și alte dimensiuni ale securității, în afară de disponibilitate, furnizorul va specifica numărul de utilizatori, precum şi o descriere a ce anume a fost afectat. În ceea ce privește durata incidentului, se va specifica intervalul de timp dintre momentul în care serviciul începe să se degradeze sau s-a întrerupt și momentul în care acesta este restabilit la parametrii inițiali. Timpul va fi exprimat în minute. Pe de altă parte, în situația unui incident ce afectează autenticitatea, integritatea sau confidențialitatea, durata va fi măsurată ca intervalul de timp dintre ora (estimată) a producerii breșei de securitate şi ora rezolvării sau încheierii acesteia.

În vederea îmbunătățirii calității informațiilor raportate în cadrul notificărilor, s-a ales comasarea unor câmpuri care să cuprindă informații detaliate referitoare la succedarea evenimentelor din cadrul incidentului începând cu cauza inițială, resursele afectate şi continuând cu cauza subsecventă. Furnizorii vor avea libertatea de a scrie informațiile pe care le consideră relevante însă vor avea în vedere inserarea, în mod obligatoriu, a informațiilor cu privire la succesiunea evenimentelor care a dus la incident, tehnologia/protocolul afectat de incident, cauza incidentului (incluzând şi cauzele tehnice), resursele afectate de incident, localizarea echipamentelor afectate în cadrul rețelei şi nivelul la care componentele au fost afectate.

Pentru clarificare, urmează să exemplificăm însemnătatea termenilor de mai sus. Astfel, la cauză inițială furnizorii vor avea obligația să noteze ce anume a dus la apariția incidentului în momentul producerii acestuia, iar dacă, pe parcurs, s-au declanșat şi alte evenimente este necesară relatarea cauzei subsecvente. În această categorie de cauze inițială/subsecventă se încadrează cauze precum:

acțiune rău intenționată, eroare umană, eroare de sistem, fenomen natural, parte terță - accident (secționare FO de către terți, accident auto, incendiu etc.), parte terță - cauză necunoscută sau parte terță - discontinuitate în alimentarea cu energie electrică datorată furnizorului/distribuitorului.

Înlănțuirea evenimentelor şi explicarea evenimentelor care se succed pot oferi informații utile şi permit o mai bună înțelegere a celor petrecute, în plus, ajută la eliminarea pasului de solicitare suplimentară de informații. Mai mult decât atât, furnizorii vor trebui să detalieze şi ce s-a întâmplat din punct de vedete tehnic transmițând ce s-a petrecut efectiv (dacă au fost ascultate convorbiri ori a fost vorba de un atac cibernetic, sau dacă elemente de rețea au fost congestionate ori s-au defectat sau dacă au fost probleme procedurale, furturi sau ce fel de fenomen natural a produs un anume incident etc.).

Elemente precum resursele afectate de incident, localizarea echipamentelor afectate în cadrul rețelei şi nivelul la care componentele au fost afectate sunt păstrate din Decizia președintelui ANCOM nr. 512/2013 şi sunt în continuare utile a fi știute, dar vor fi cuprinse în câmpul text pentru a simplifica formularul.

O serie de câmpuri au rămas neschimbate. Acestea se referă la acțiunile de răspuns şi la măsurile luate sau planificate pentru a împiedica producerea unui incident similar inclusiv momentul când au fost/vor fi luate şi lecțiile învățate. Aceste două câmpuri furnizează informații utile pentru înțelegerea acțiunilor desfășurate de furnizori. Se vor detalia acțiunile întreprinse pentru a aduce serviciul la un nivel acceptabil, precum şi pentru a restabili serviciul la parametrii inițiali în cazul afectării disponibilității, acțiunile întreprinse în ceea ce privește limitarea pierderii suplimentare a datelor, evaluarea pierderilor survenite prin colectarea faptelor și evaluarea riscurilor, inclusiv a potențialelor prejudicii aduse persoanelor afectate, în cazul afectării autenticității, integrității sau confidențialității. Se vor menționa alte autorități care au fost contactate și acțiunile de informare a persoanelor implicate in incident, dacă este cazul. Totodată, se vor detalia acțiunile realizate pentru a minimiza nivelul de risc şi pentru a preîntâmpina reapariția incidentului (de exemplu: revizuire măsuri de securitate şi proceduri, renegociere SLA-uri, instruiri de personal, achiziție de echipamente sau sisteme de back-up etc.), precum şi momentul când au fost luate sau când vor fi luate aceste măsuri. Nu în ultimul rând, vor fi necesare informații despre lecțiile învățate - aceasta presupune realizarea unui bilanț al incidentului, ajungerea la sursa problemei, ce anume s-a întâmplat în concret și motivul pentru care acest eveniment a avut loc, evaluarea a cât de bine a funcționat planul de răspuns la incident pentru a rezolva problema și identificarea îmbunătățirilor care trebuie făcute.

De reținut faptul că deși s-a luat decizia eliminării anumitor câmpuri din formularul de raportare, o parte dintre informațiile legate de acestea se regăsesc în câmpul dedicat descrierii incidentului. Informațiile despre resurse, cauze, localizarea echipamentelor etc. vor fi analizate şi clasificate în cadrul procesului de monitorizare a raportării incidentelor. Ghidul de raportare a incidentelor cu impact semnificativ asupra furnizării rețelelor şi serviciilor de comunicații electronice[29] va fi actualizat după emiterea deciziei, iar furnizorii vor fi invitați să îl consulte. Alte eventuale probleme sau nelămuriri legate de completarea informațiilor în formularul de raportare vor fi discutate în Grupul Consultativ prevăzut la art. 8 din proiectul de decizie.

În prezentul proiect de decizie a fost adăugat un nou alineat la art. 5, și anume alin. (8), cu privire la procesul de notificare a incidentelor. Din practică, s-a observat că furnizorii introduc incidentele direct în aplicația informatică, pusă la dispoziție de ANCOM, sărind peste pasul notificării inițiale. În situația în care un incident a fost finalizat și se cunosc toate informațiile cu privire la incident până la ora transmiterii notificării inițiale, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului pot raporta incidentul direct în aplicația informatică.

Din punct de vedere procedural, notificarea inițială a incidentelor cu impact semnificativ se va realiza prin transmiterea către ANCOM a unui înscris în formă electronică la adresa de poștă electronică incidente@ancom.ro. Diferența față de prevederile actuale ale Deciziei președintelui ANCOM nr. 512/2013 constă în obligația furnizorilor de a transmite notificarea inițială până la ora 13.00 a următoarei zile calendaristice celei în care a fost detectat incidentul de securitate care are un impact

[29] Disponibil în prezent la următoarea adresă:
https://www.ancom.ro/uploads/links_files/20141219_GHID_DE_RAPORTARE_A_INCIDENTELOR.pdf

semnificativ pentru incidentele care afectează mai mult de 100.000 de utilizatori. Instituirea pragului de 100.000 de utilizatori în zilele de sărbători legale sau în zilele considerate libere este justificată de faptul că un număr atât de mare de utilizatori afectați este posibil să devină un incident cu impact societal, caz în care este necesar ca și Autoritatea să fie înștiințată din timp astfel încât să poată să își exercite atribuțiile de supraveghere în mod adecvat, dacă este cazul. ANCOM reamintește că notificarea inițială, așa cum este prevăzută în Proiect, trebuie să conțină informații sumare despre incident, astfel că termenul mai scurt de transmitere a acesteia implică un efort suplimentar minim în procesul de raportare. Faptul că transmiterea notificării inițiale se realizează exclusiv prin intermediul e-mail-ului, fără necesitatea accesării vreunei aplicații informatice, ar trebui să contribuie la simplificarea procesului și la minimizarea impactului asupra resurselor necesare la nivelul furnizorilor de rețele și servicii publice de comunicații electronice.

Totodată, proiectul de decizie prevede obligația furnizorilor care au un număr de cel puțin 5.000 de utilizatori de a transmite ANCOM datele de contact ale persoanelor responsabile de notificarea inițială a incidentelor de securitate care au un impact semnificativ în conformitate cu dispozițiile art. 5, în termen de 5 zile de la intrarea în vigoare a prezentei decizii, precum şi orice modificare a acestor date, în termen de 5 zile de la survenirea modificărilor.

În ceea ce privește notificarea finală, precum și cea suplimentară a incidentului cu impact semnificativ, precizăm că acestea se vor realiza exclusiv prin intermediul aplicației informatice prevăzute de dispozițiile art. 5 alin. (1) din Decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații nr. 336/2013 privind mijloacele şi modalitatea de transmitere de către furnizori a unor documente, date sau informaţii către Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, cu modificările și completările ulterioare, prevederile acesteia fiind aplicabile în mod corespunzător.

9. Consultarea publică

Prevederile art. 135 alin. (1)-(3) din Ordonanţa de urgenţă a Guvernului nr. 111/2011 se aplică în mod corespunzător.