ANALIZA PRELIMINARĂ A IMPACTULUI DE REGLEMENTARE

efectuată la proiectul Hotărârii Consiliului de Administraţie al ANRCETI privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice

I. INTRODUCERE

Analiza Preliminară a Impactului de Reglementare (AIR) pentru proiectul de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie întreprinse de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice a fost elaborată de către Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei, denumită în continuare ANRCETI, în conformitate cu prevederile art.13 din Legea nr.235-XVI din 20 iulie 2006 cu privire la principiile de bază de reglementare a activităţii de întreprinzător (Monitorul Oficial nr.126-130 art. 627 din 11.08.2006) şi Metodologia de analiză a impactului de reglementare şi de monitorizare a eficienţei actului de reglementare, aprobată prin Hotărârea Guvernului Republicii Moldova nr.1230 din 24.10.2006 (Monitorul Oficial nr.170-173, art. 1321 din 03.11.2006).

AIR prezintă argumentarea vizînd necesitatea elaborării Hotărârii cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de reţele şi servicii publice de comunicaţii electronice pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, prin prisma impactului său asupra activităţii tuturor participanţilor pe piaţa comunicaţiilor electronice.

II. SCOP ŞI OBIECTIVE

Scopul iniţiativei de elaborare a Hotărârii cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice constă în asigurarea unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, în special pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor, astfel încât să asigure continuitatea furnizării serviciilor publice de comunicaţii electronice.

Obiectivele reglementării sunt următoarele:

- ajustarea cadrului normativ-legislativ la dinamica ameninţărilor specifice spaţiului cibernetic;
- asigurarea stării de securitate prin cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa reţelelor şi serviciilor publice de comunicaţii electronice;
- asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice precum şi a confidenţialităţii datelor şi informaţiilor;
- asigurarea disponibilităţii şi a calităţii serviciilor oferite;
- asigurarea continuităţii afacerii;
- reducerea semnificativă a numărului de incidente/întreruperi operaţionale şi a riscului de apariţie al acestora;
- reducerea prejudiciilor ce pot fi aduse persoanelor juridice şi fizice;
- dezvoltarea unui mediu dinamic bazat pe interoperabilitate;
- respectarea drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională.

III. DEFINIREA PROBLEMEI

Circumstanţe şi justificarea intervenţiei

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

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

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

Gradul de interconectare a reţelelor de comunicaţii electronice devine din ce în ce mai mare, iar ameninţările la adresa acestora devin din ce în ce mai complexe şi pot avea un caracter global.

Orice agent economic care folosește cel puțin un computer conectat la Internet poate fi victima unui atac sau a unor scurgeri de informații valoroase pentru companie. Date confidențiale, informații despre clienți sau parteneri de afaceri pot ajunge online și pot deschide ușa unor atacuri ulterioare care sa înghețe activitatea companiei.

În ultimele luni, companii mari precum Adobe, Google, Facebook sau Twitter au fost victimele unor atacuri cibernetice, dovada ca nimeni nu este total invulnerabil.

Exemple recente ale unor astfel de situații, în Republica Moldova, fiind atacurile cibernetice asupra companiei StarNet. Datele personale ale clienţilor companiei StarNet au fost plasate pe internet, fiind considerată cea mai mare scurgere de informaţii private: numele şi prenumele clienţilor, adresele, numerele de telefoane, dar şi codurile personale. Fişierele apărute în spaţiul virtual conţineau datele personale ale tuturor clienţilor - peste 100 de mii de persoane fizice şi 4.000 de persoane juridice. Astfel, au devenit publice numele, prenumele, adresa de domiciliu, numerele de telefon, datele personale: seria şi numărul buletinului, dar şi IDNP-ul clienţilor. În baza de date mai poate fi găsită informaţia despre toţi angajaţii StarNet, contractele semnate de furnizor cu clienţii săi, informaţii despre companiile cu care colaborează.

În prezent, la nivel mondial, atacurile cibernetice capătă o frecvenţă, complexitate şi o amploare din ce în ce mai mare, aducând pagube enorme sectorului guvernamental, privat şi cetăţenilor. Conform raportului Norton pentru anul 2013 - 378 de milioane de victime pe an sau 1 milion de victime pe zi sunt afectate de incidente informatice cărora li s-au adus pagube de 113 miliarde de dolari. Numărul atacurilor cibernetice asupra companiilor a crescut cu 38% în lume în ultimele 12 luni, potrivit unui studiu al cabinetului de consultanță PricewaterhouseCoopers (PwC). 'Cine nu se poate proteja se poate asigura', notează PwC, care estimează că piața mondială de asigurări din domeniu, care au drept scop atenuarea efectelor financiare ale unui atac cibernetic, se va tripla în acest an.

Majoritatea amenințărilor (34%) vin de la angajați ai companiei atacate, conform studiului desfășurat între 7 mai și 12 iunie pe un eșantion de peste 10.000 de responsabili din

127 de țări. O parte tot mai mare a celor ce comit atacuri cibernetici provin din rândul furnizorilor şi prestatorilor de servicii, potrivit aceluiași studiu.

Mai mult ca atît, Republica Moldova se află geografic între 2 ţări din topul celor 10, originare pentru atacuri cibernetice cu intensitate sporită (Ucraina (4) şi România (7), conform raportului Origin of Hacks 2012. Accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice, restricţionarea ilegală a accesului la aceste date şi spionajul cibernetic constituie constrângeri la nivel global. Pe de alta parte, situaţiile excepţionale cu caracter natural, tehnogen şi ecologic pun la încercare rezistenţa reţelelor de comunicaţii electronice, cum s-a întâmplat în cazul cutremurului cu magnitudinea de 8,9 grade pe scara Richter ce a zguduit coasta de nord-est a Japoniei pe 11 martie 2011, provocând colosale pagube umane și materiale. Infrastructura de comunicaţii electronice a fost afectată esenţial şi în special reţeaua de telefonie fixă. Au fost deteriorate cablurile magistrale Internet, inclusiv cablurile submarine lipsind un număr considerabil de cetățeni și autoritățile din zonă de comunicații. Compania NTT, furnizor de servicii de telefonie şi Internet, a semnalat distrugerea a circa un milion și jumătate de linii de telefonie, optice şi ISDN.

La 27 februarie 2014, în conformitate cu articolul 29 alineatul (2) din Regulamentul de procedură, Comitetul Economic și Social European a hotărât să elaboreze un aviz din proprie inițiativă pe tema *Atacurile cibernetice în UE* (Avizul CESE 2014/C 451/05). Potrivit acestui Aviz:

- ✓ Întreprinderile ar trebui obligate la o abordare proactivă pentru a se proteja împotriva atacurilor cibernetice, inclusiv tehnologii ale informației și comunicațiilor (TIC) sigure și flexibile, care să ofere pregătirea necesară pentru angajaţi în ceea ce priveşte politicile de securitate cibernetică, așa cum se întâmplă deja în domeniul sănătății și siguranţei la locul de muncă;
- ✓ Organele de conducere la nivel de întreprinderi şi organizaţii ar trebui sensibilizate cu privire la responsabilitatea ce le revine pentru securitatea cibernetică. Directorii organizațiilor ar trebui informaţi în mod explicit în legătură cu consecințele pe care le pot avea politicile şi măsurile inadecvate în materie de securitate cibernetică.

Comitetul European consideră că măsurile voluntare sunt insuficiente și că trebuie să se impună obligații ferme în materie de reglementare pentru a se asigura armonizarea, guvernanța și punerea în aplicare a securității cibernetice în Europa. De asemenea, este necesară adoptarea unei legislații pentru a impune obligaţia de notificare a incidentelor grave de securitate cibernetică la nivelul tuturor întreprinderilor și organizațiilor, nu doar pentru furnizorii de infrastructuri critice. Aceasta ar putea îmbunătăți răspunsul Europei la ameninţări și ar contribui la creșterea nivelului de cunoștințe și înțelegere cu privire la atacurile cibernetice, permițând dezvoltarea unor sisteme de apărare mai bune.

Reieşind din faptul că nivelul dezvoltării Societăţii informaţionale în Republica Moldova este destul de avansat, spaţiul cibernetic al ţării este expus unor noi riscuri, care finalizându-se în atacuri cibernetice sau calamități, pot afecta grav ţara.

Prin urmare, asigurarea unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, în special pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor, astfel încât să asigure continuitatea furnizării serviciilor de comunicaţii electronice precum și integrarea în societatea informațională constituie un obiectiv primordial pentru ANRCETI cît şi pentru întreaga economie.

Astfel, prin proiectul de Hotărâre privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele și/sau servicii publice de comunicaţii electronice, ANRCETI urmăreşte să reducă semnificativ numărul de incidente, întreruperi operaţionale şi fraude, să prevină pierderea, distrugerea, furtul sau compromiterea diverselor resurse ale

furnizorilor, dar şi să optimizeze calitatea serviciilor de comunicaţii oferite utilizatorilor şi să crească încrederea acestora în furnizorii de reţelele şi/sau servicii de comunicaţii electronice.

Potrivit proiectului de Hotărâre, furnizorii de reţele şi/sau servicii de comunicaţii electronice vor trebui să stabilească măsuri tehnice şi organizatorice în vederea asigurării unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Printre obligaţiile ce vor fi impuse în sarcina furnizorilor se află atât stabilirea unui management al riscului, a unui sistem de detectare a incidentelor, cât şi a unei strategii proprii pentru asigurarea continuităţii furnizării reţelelor şi/sau serviciilor de comunicaţii electronice în situaţiile generate de perturbări grave ale funcţionării acestora, precum şi asigurarea protecţiei reţelelor şi serviciilor împotriva atacurilor informatice.

Proiectul de Hotărâre propune, de asemenea, stabilirea unei proceduri de raportare a incidentelor de securitate cu impact semnificativ, incidentele reprezentând acele evenimente care pot afecta sau ameninţa, direct sau indirect, securitatea şi integritatea reţelelor şi/sau serviciilor de comunicaţii electronice. Astfel, furnizorii de reţele şi/sau servicii de comunicaţii electronice vor avea obligaţia de a transmite ANRCETI, informaţii cu privire la încălcarea securităţii sau pierderea integrităţii care are un impact semnificativ asupra furnizării reţelelor sau serviciilor de comunicaţii electronice. În plus, ANRCETI poate informa publicul sau poate solicita furnizorilor să informeze publicul în cazul producerii incidentelor cu impact semnificativ.

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

Importanţa colectării datelor privind incidentele care afectează securitatea şi integritatea reţelelor şi serviciilor este incontestabilă. Accesul la informaţii complete, corecte, comparabile şi actualizate referitoare la incidente constituie un element necesar pentru a obţine o mai bună înţelegere a nevoii de acţiuni în scopul asigurării securităţii, precum şi pentru a evalua rezultatele măsurilor puse în aplicare anterior (legale, de reglementare, organizatorice şi tehnice).

De asemenea, Guvernul a emis Strategia Naţională de dezvoltare a societăţii informaţionale "Moldova Digitală 2020" (Hotărîrea Guvernului nr.857 din 31.10.2013). În Strategie se expune viziunea complexă şi obiectivele de dezvoltare a societăţii informaţionale în Republica Moldova, inclusiv obiectivul privind "Crearea condiţiilor pentru sporirea gradului de securitate şi încredere în spaţiul digital".

Totodată, în conformitate cu prevederile Strategiei securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr.153 din 15.07.2011, Acordului de Asociere între Republica Moldova şi Uniunea Europeană, ratificat prin Legea nr.112 din 02.07.2014, precum şi actelor normative subsidiare acestuia, sunt prevăzute întreprinderea unui set de măsuri pentru transpunerea legislaţiei Uniunii Europene în domeniu, în legislaţia naţională, şi în primul rînd: Directiva 2002/21/CE a Parlamentului European şi a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru reţelele şi serviciile de comunicaţii electronice, astfel cum a fost modificată prin Directiva 2009/140/CE a Parlamentului European şi a Consiliului din 25 noiembrie 2009, Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, astfel cum a fost modificată prin Directiva 2009/136/CE al Parlamentului European şi al Consiliului din 25 noiembrie 2009, Directiva 2000/31/CE a Parlamentului European şi a Consiliului din 8 iunie 2000 privind anumite

aspecte juridice ale serviciilor societăţii informaţionale, în special ale comerţului electronic, pe piaţa internă, Directiva 1999/93/CE a Parlamentului European şi a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, Strategia UE pentru Securitate Cibernetică: un spaţiu deschis, sigur şi securizat, precum și a altor documente europene aprobate sau în proces de elaborare ce vizează securitatea rețelelor de comunicații electronice și a sistemelor informatice.

La nivelul Uniunii Europene a fost recunoscută importanţa comunicaţiilor electronice, precum şi necesitatea de a extinde eforturile pentru a asigura rezilienţa acestora.

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

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

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

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

Întru respectarea Acordului de Asociere între Republica Moldova şi Uniunea Europeană, ratificat prin Legea nr.112 din 02.07.2014, la data de 29 octombrie 2015 prin Hotărârea de Guvern cu nr. 811 a fost aprobat Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (Monitorul Oficial al Republicii Moldova, 2015, nr. 306-310, art. 905). Conform pct.2.2 al Planului de acţiuni privind implementarea Programului menţionat ANRCETI, în perioada anilor 2016-2017, urmează să stabilească *măsuri minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii, non-repudierii şi integrităţii reţelelor şi/sau serviciilor de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra acestora*.

Potrivit pct. 1 din Concepţia securităţii naţionale a Republicii Moldova, aprobată prin Legea nr. 112-XVI din 22.05.2008 (Monitorul Oficial nr.97-98/357 din 03.06.2008), ameninţările din domeniul tehnologiei informaţiei/instabilitatea şi disfuncţionalitatea sistemelor informaţionale pot să reprezinte ameninţări accentuate la adresa securităţii naţionale. Dezvoltarea progresivă a sistemelor electronice de informaţii din Republica Moldova, gradul lor înalt de interconexiune cu sistemele informaţionale internaţionale facilitează activitatea factorului criminogen în sfera informaţională şi fac să sporească vulnerabilitatea sistemelor respective, inclusiv în sferele de importanţă primordială pentru securitatea naţională.

Prin urmare, este certă necesitatea elaborării unei reglementări cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor publice de comunicaţii electronice. Proiectul propus de autor, care, de fapt, va asigura implementarea unui șir de prevederi din Legea comunicaţiilor electronice nr.241-XVI din 15.11.2007, denumită în continuare Legea nr.241/2007, precum:

- ✓ art. 8 alin. (6) lit. e) din Legea nr.241/2007: ANRCETI promovează interesele utilizatorilor finali prin: e) menţinerea de către furnizori a securităţii şi integrităţii reţelelor publice de comunicaţii electronice;
- ✓ art. 20. alin. (2) lit. e) din Legea nr.241/2007:

Furnizorii de reţele şi/sau servicii publice de comunicaţii electronice publice au obligaţia să asigure: e) întreprinderea acţiunilor tehnice şi organizatorice corespunzătoare în vederea asigurării securităţii serviciilor şi protecţiei datelor personale ale utilizatorilor vine să acopere această necesitate.

Măsurile de securitate, definire şi scop

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

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

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

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

Măsurile de securitate sunt selectate luând în considerare riscurile existente în cadrul organizaţiei. Cerinţele de securitate pot fi identificate doar printr-o evaluare sistematică a riscurilor la adresa securităţii. Rezultatele evaluării riscurilor vor ajuta la determinarea acţiunilor corespunzătoare şi a priorităţilor implementării măsurilor de securitate în scopul protejării împotriva acestor riscuri. Măsurile de securitate pot preveni posibile incidente, pot limita consecinţele incidentelor atunci când acestea au loc sau pot asigura rectificarea rapidă şi eficientă a întreruperilor serviciilor de comunicaţii electronice, restabilind furnizarea la condiţii normale şi trebuie să acopere orice condiţii de operare, diverse tipuri de incidente şi evenimente de securitate, precum şi situaţii de urgenţă, cazuri de dezastru sau crize majore.

Asigurarea unui nivel adecvat de securitate este un proces continuu de punere în aplicare, revizuire, actualizare a măsurilor de securitate. Efectele măsurilor de securitate trebuie monitorizate. Este posibil ca setul măsurilor de securitate selectate să nu poată realiza o

securitate „totală”, fiind astfel necesare acţiuni suplimentare pentru monitorizarea, evaluarea şi îmbunătăţirea eficienţei măsurilor de securitate în sprijinul atingerii obiectivelor de securitate.

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

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

Ca rezultat al implementării măsurilor de securitate adecvate, furnizorii de reţele şi servicii de comunicaţii electronice vor fi capabili să asigure o securitate şi integritate adecvată a reţelelor şi serviciilor de comunicaţii electronice, vor avea o abordare clară şi completă asupra tuturor activităţilor aferente acestui domeniu, vor deţine capacităţile restabilirii serviciilor la condiţii normale de funcţionare în cazul apariţiei incidentelor, vor reuşi să conştientizeze personalul organizaţiilor şi utilizatorii asupra importanţei securităţii şi vor spori încrederea acestora în serviciile oferite, ansamblul măsurilor de securitate contribuind semnificativ la îmbunătăţirea calităţii serviciilor şi la asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice.

Nivelul actual al securităţii şi integrităţii reţelelor şi serviciilor

Conform datelor Centrului pentru Securitatea Cibernetică (CERT-GOV-MD), numai în perioada de 1 Aprilie - 30 Septembrie 2014 CERT-GOV-MD a primit 2 700 000 de alerte, mai mult de 1,7 milioane provin din scanarea serverelor Guvernamentale (efectuate pentru a identifica eventualele vulnerabilități). Dispozitivele de securitate au blocat de asemenea, un număr de 900 000 de mesaje de tip spam, 23 000 de atacuri de rețea, au fost neutralizate 12 000 de e-mailuri care conțineau numeroși viruși, au fost depistate mai mult de 1 900 de alerte de la adrese IP. În total în perioada dată au fost identificate 2 758 027 incidente numai la rețelele și serviciile guvernamentale.

În luna martie curent, în vederea analizării/estimării nivelului de securitate şi integritate al reţelelor şi serviciilor de comunicaţii electronice existent la momentul actual şi identificării măsurilor ce sunt deja implementate în acest sens, ANRCETI a transmis către cei mai importanţi 30 de furnizori de reţele şi/sau servicii de comunicaţii electronice, din punct de vedere al numărului de utilizatori, un chestionar privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Chestionarul a cuprins 43 de întrebări structurate în 7 teme mari: aspecte generale privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, managementul riscului, măsuri privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, monitorizarea incidentelor, informarea utilizatorilor cu privire la incidentele semnificative, testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, costul şi beneficiile măsurilor de securitate.

În urma analizării răspunsurilor primite de la furnizori, la chestionarul transmis de ANRCETI, a rezultat că doar o mică parte dintre aceştia au o preocupare activă în asigurarea securităţii şi integrităţii reţelelor şi serviciilor. De asemenea, doar o mică parte dintre furnizori au proceduri clare şi documentate pentru asigurarea continuităţii reţelelor şi serviciilor, în majoritatea cazurilor stabilirea unor măsuri de securitate efectuându-se reactiv, în momentul apariţiei unui incident. În plus, puţini dintre furnizori au o abordare completă a domeniului securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, majoritatea axându-se doar pe anumite domenii de interes.

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

Managementul riscului este un proces continuu şi trebuie să fie parte integrantă a tuturor activităţilor desfăşurate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor. Cu toate că managementul riscurilor constituie un domeniu fundamental pe baza căruia ar trebui luată decizia stabilirii măsurilor de securitate, din răspunsurile multor furnizori a rezultat că acestui domeniu i se acordă un interes scăzut, analiza de risc nefiind completă în multe cazuri sau chiar lipsind cu desăvârşire.

Majoritatea furnizorilor chestionaţi monitorizează incidentele petrecute în reţea, însă nu toţi au proceduri în vederea tratării incidentelor.

În ceea ce priveşte testarea securităţii şi integrităţii reţelelor şi serviciilor, o mare parte a furnizorilor nu efectuează o astfel de activitate, nefiind la curent cu vulnerabilităţile existente/actuale. Din răspunsurile primite, a reieşit că doar 4 furnizori efectuează audituri de securitate pentru a se asigura că securitatea şi integritatea reţelelor este una adecvată.

Doar un număr relativ redus din furnizorii chestionaţi (practic doar furnizorii cu cote semnificative pe piaţa comunicaţiilor electronice) au recunoscut necesitatea/beneficiile implementării măsurilor de securitate şi integritate a reţelelor şi serviciilor de comunicaţii electronice, printre cele mai importante beneficii regăsindu-se asigurarea continuităţii afacerii, asigurarea disponibilităţii şi integrităţii serviciilor de comunicaţii electronice, protejarea datelor personale ale clienţilor şi angajaţilor, păstrarea confidenţialităţii, identificarea rău făcătorilor şi tehnicelor de fraudare, oferirea unor garanţii suplimentare abonaţilor în protejarea drepturilor sale, reducerea numărului incidentelor de securitate şi a reclamaţiilor la adresa securităţii, îmbunătăţirea controlului sistemelor şi proceselor interne ale organizaţiilor, îmbunătăţirea calităţii serviciului, reducerea riscurilor în privinţa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

În ceea ce priveşte informarea utilizatorilor cu privire la incidentele semnificative, din răspunsurile furnizorilor a reieşit că o bună parte dintre aceştia îşi informează utilizatorii. Majoritatea furnizorilor însă au raportat că nu au suferit careva incidente semnificative care ar afecta securitatea şi integritatea reţelelor. Doar un furnizor a adus detalii privind desfăşurarea (în ultimele 12 luni) a unor campanii pentru conştientizarea de către clienţi a unor aspecte ce pot afecta securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Ca urmare a recepţionării şi examinării răspunsurilor la Chestionar, ANRCETI consideră că domeniul securităţii şi integrităţii nu este abordat la un nivel suficient de către furnizorii de reţele şi/sau servicii de comunicaţii electronice şi că este necesară stabilirea unor orientări sumare în scopul asigurării unei securităţi şi integrităţi adecvate a reţelelor şi serviciilor.

Având în vedere cele expuse mai sus, este certă necesitatea asigurării unui nivel adecvat al securităţii şi integrităţii reţelelor şi serviciilor publice de comunicaţii electronice, în special pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor, astfel încât să asigure continuitatea furnizării serviciilor de comunicaţii electronice.

Definirea problemei

Problema generală este cauzată de nivelul redus de preocupare din partea furnizorilor de reţele şi/sau servicii de comunicaţii electronice în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor, precum şi de vulnerabilitatea sporită a acestor reţele şi servicii la atacurile şi incidentele cibernetice, care ar putea compromite disponibilitatea, autenticitatea, integritatea şi confidenţialitatea datelor stocate sau transmise şi a serviciilor asociate, oferite sau accesibile prin aceste reţele şi servicii.

Deoarece niveluri diferite de conectivitate Internet devin esențiale pentru menținerea competitivității companiilor, asigurarea securității infrastructurii de rețea devine o cerință esențială. Companiile trebuie să conceapă o arhitectură a securității rețelelor, bazată pe o

politică de securitate a companiei. Soluția completă de securitate a rețelelor este necesară companiei pentru aşi proteja datele şi resursele informatice. Această soluție trebuie să includă autentificare şi autorizare, confidențialitatea datelor şi securitatea perimetrului.

Creşterea numărului de ameninţări informatice precum viruşi, spam, spyware sau phising au determinat creşterea importanţei atingerii acestor obiective.

În acest sens, şi pentru îndeplinirea prevederilor Legii nr.241/2007, apare necesitatea elaborării proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice.

IV. GRUPURILE DE INTERESE

Impactul noilor reglementări care vor fi introduse prin proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor şi serviciilor publice de comunicaţii electronice vor fi resimţite în măsuri diferite şi adverse de câteva părţi interesate:

1) furnizorii de reţele şi servicii publice de comunicaţii electronice publice;
2) Statul, Guvernul RM;
3) utilizatorii finali de servicii de comunicaţii electronice.

V. COSTURI ŞI BENEFICII ANTICIPATE

Costuri

Realizarea unor măsuri de securitate implică și costuri însă acestea trebuie puse în legătură cu avantajele oferite.

Studiile efectuate au arătat ca jumătate din costurile implicate de incidente sunt datorate acțiunilor voit distructive, un sfert dezastrelor accidentale și un sfert greşelilor umane. Acestea din urma pot fi evitate sau, în cele din urmă, reparate printr-o mai buna aplicare a regulilor de securitate (salvări regulate de date, discuri oglindite, limitarea drepturilor de acces).

Indiferent de dimensiunea companiei, pericolele pot fi evitate sau controlate cu un minim de atenție acordat nivelului de securitate. Protejarea datelor digitale ar trebui să fie o prioritate pentru orice companie, indiferent de dimensiunea ei.

Dincolo de softuri specializate și investiții costisitoare, securitatea firmei ține foarte mult de practici sănătoase și proceduri interne. Câteva masuri simple ar trebui însa sa facă sistemele folosite mult mai greu de compromis.

Care sunt datele esențiale pentru activitatea companiei?

In termeni mai pretențioși, clasificarea datelor în funcție de importanță poartă numele de „audit de securitate“. Practic, este crucial să se știe exact ce anume se poate pierde în cazul unei breșe de securitate. Ierarhizarea informațiilor în funcție de gradul de confidențialitate, importanta pentru activitatea companiei, clienți sau angajați e utila pentru ca odată ce se știe ce anume se protejează, se va ști și cum se protejează.

Parole „puternice“

Simplu! O parola de 8-12 semne care combina majuscule, litere mici, semne și cifre este debutul perfect pentru creșterea securității firmei. Este important să se evite numele proprii, datele de naștere, modificarea parolei cel puțin o data la 90 de zile. Parolele nu trebuie notate on sau off-line. Datele de logare în rețea sau pe serverul de e-mail ale unui angajat care și-a încheiat colaborarea cu firma trebuie șterse imediat.

Un antivirus performant

Un pachet de securitate complet include un antivirus actualizat și dotat cu tehnologii anti-spam, anti-malware - vitale împotriva atacurilor de tip phishing sau exploit.

Whitelisting

Internetul are mai multe zone râu famate, site-uri considerate periculoase pentru securitatea computerului. Fiecare departament IT dintr-o companie are deja un „blacklist“ (lista neagra) al site-urilor, linkurilor sau aplicațiilor care ar putea duce la infectări. Mai utilă însa ar putea fi o listare a site-urilor curate, pe care angajații pot sa le acceseze pentru a-și duce la sfârșit îndatoririle fără a risca o infecție. Blocarea website-urilor nepermise printr-un firewall performant și un training de securitate pentru angajați pot limita considerabil riscul unui atac.

Arhitectura rețelei

Odată infectat, un computer trebuie izolat cat mai repede de restul rețelei astfel încît aplicația nocivă sa nu se răspândească.

Limitarea accesului fizic în spațiul de muncă

Eforturile de a proteja un sistem de posibilele amenințări venite din afara se pot dovedi inutile atât timp cat cineva reușește să scoată din firmă informații pe un banal stick USB sau poate folosi același dispozitiv pentru a introduce în firma un soft periculos. Informațiile secrete trebuie stocate în locații izolate și protejate care sa limiteze la minim accesul persoanelor autorizate.

Mobil înseamnă mai vulnerabil

Tabletele, laptopurile și telefoanele inteligente cresc considerabil eficienta angajaților, dar deschid drumul către noi vulnerabilități. De la furtul, pierderea sau distrugerea informațiilor de pe ele la exploatarea de către hackeri, dispozitivele mobile trebuie tratate la fel ca un PC conectat la rețea prin cablu sau chiar mai atent. Fiecare dispozitiv de pe care pot fi accesate date confidențiale trebuie protejat. Se recomanda criptarea datelor, protejarea telefoanelor prin coduri de blocare și activarea unui serviciu de ștergere de la distanta.

Punctele de acces neautorizate trebuie interzise

Un hacker poate accesa informații confidențiale prin simpla conectare la rețeaua wi-fi a companiei. De aceea, orice dispozitiv care se conectează la rețeaua aprobata de companie trebuie sa permită doar autentificarea bazată pe datele de conectare din domeniu sau cu certificate digitale.

Back-up, back-up, back-up

Odată ce lista informațiilor esențiale pentru companie a fost pusă la punct, cele mai importante date trebuie salvate pe un suport mai puțin vulnerabil la atacuri: un hard-disk extern, un serviciu cloud sau chiar DVD-uri, în funcție de necesitățile sistemelor incluse în back-up.

Pregătirea angajaților

Proceduri stricte de securitate și angajați conștienți de riscurile la care se expun reprezintă protecția excelentă împotriva amenințărilor. Fiecare dintre ei trebuie sa fie capabil sa facă diferența intre pagina oficiala a unei bănci și un mesaj de tip phishing, sa știe cum sa trateze atașamentele din e-mailuri și sa raporteze departamentului IT incidentele suspecte.

Astfel, măsurile minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice nu vor constitui o sarcină împovărătoare pentru aceştia. Costurile implementării acestor măsuri fiind neînsemnate mai ales în contextul în care, conform prevederilor Legii nr.241/2007 şi Regulamentului cu privire la regimul de autorizare generală, furnizorii ar trebui deja să se conformeze cu cerințele de securitate existente (şi anume menţinerea de către furnizori a securităţii şi integrităţii reţelelor publice de comunicaţii electronice).

De asemenea, menționăm că conform Chestionarului cu privire la securitatea şi integritatea reţelelor furnizorii urmau să prezinte informaţii inclusiv privind costurile şi beneficiile măsurilor de securitate implementate.

Majoritatea respondenţilor au afirmat că costul este dificil de cuantificat. Unii respondenţi au afirmat că costurile efectuate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice se integrează în cheltuielile curente de dezvoltare, modernizare şi menţinere a reţelei şi serviciilor de comunicaţii electronice. În mare parte costurile fiind aferente implementării tehnice (hardware şi software) şi a celor operaţionale. Conform răspunsurilor primite, costurile depind în mare măsură de mărimea organizaţiei (ca şi număr de utilizatori, angajaţi, cifră de afaceri etc.).

Costurile pentru realizarea acțiunii ce ține de stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi/sau serviciilor de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra acestora fi suportate din bugetul ANRCETI format și utilizat în condiției legislației în vigoare.

Beneficii:

Este de menţionat faptul, că an de an, atacurile cibernetice provoacă daune economice considerabile. Astfel, la calcularea costurilor de organizare și furnizare a serviciilor trebuie avute în vedere următoarele:

- ✓ pierderea proprietății intelectuale și a datelor sensibile;
- ✓ costurile de oportunitate, inclusiv cele referitoare la întreruperea serviciilor și a muncii;
- ✓ deteriorarea imaginii mărcii și a reputației întreprinderii;
- ✓ sancțiuni și plăți compensatorii către clienți (pentru inconveniente sau pierderile conexe), compensații contractuale (pentru întârzieri etc.);
- ✓ costurile contramăsurilor și asigurărilor;
- ✓ costurile strategiilor de atenuare și redresare în urma unor atacuri informatice;
- ✓ pierderi comerciale și de competitivitate;
- ✓ denaturarea comerţului și pierderile de locuri de muncă.

Costul mediu pentru o organizație mare ca urmare a celei mai grave încălcări a securității cibernetice ar putea ajunge la 1400 000,00 Euro, respectiv la 140.000,00 Euro pentru o organizație mijlocie sau mică.

Chiar dacă atacurile nu reușesc, costurile de atenuare cresc cu rapiditate. În 2014, la nivel mondial, creșterea pieței de securitate a informațiilor a ajuns la 8,6 % și a depășit 73 de miliarde de dolari.

Aceste costuri depășesc cu mult costurile de implementare a reglementării propuse.

Astfel, printre beneficiile obținute în rezultatul implementării reglementării propuse, beneficii enumerate și de respondenţi, se remarcă: asigurarea continuității serviciilor, reducerea numărului incidentelor de securitate, evitarea întreruperii activităţilor de bază ale organizaţiilor, reducerea efortului material şi uman de recuperare a datelor importante ce s-ar putea pierde în cazul incidentelor care afectează securitatea informaţiei, posibilitatea ofertării de servicii critice cu disponibilitate foarte ridicată, îmbunătăţirea calităţii serviciilor furnizate, protejarea clienţilor de eventuale atacuri informatice, creşterea încrederii în rândul clienţilor şi a partenerilor de afaceri, controlul sporit al fluxurilor de informaţii din organizaţii, asigurarea integrităţii şi disponibilităţii sistemelor şi aplicaţiilor IT utilizate pentru operarea, livrarea şi asigurarea serviciilor companiei, reducerea costurilor de întreţinere a reţelelor, securizarea fizică a ariilor protejate, extinderea capacităţii reţelelor, promovarea afacerilor, asigurarea dreptului de autor etc.

După cum se poate observa, avantajele sunt atît de ordin economic cît şi social şi vor aduce beneficii întregii economii în ansamblu. Cu toate acestea, ele sunt dificil de cuantificat.

VI. EVALUAREA ABORDĂRILOR ALTERNATIVE

În urma definirii problemei şi scopului/obiectivelor au fost identificate 3 opţiuni. În tabelul de mai jos au fost expuse posibilele avantaje şi dezavantaje pentru fiecare opţiune:

- Opţiunea 1 – „A nu face nimic”.
- Opţiunea 2 – „Reglementarea clasică” – aprobarea proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice;
- Opţiunea 3 –„Co-reglementarea” - în baza altor acte normative şi legislative.

Opţiunea	**Avantaje**	**Dezavantaje**
1. A nu face nimic	Nu sunt identificate.	1) Vulnerabilitate sporită a reţelelor şi serviciilor de comunicaţii electronice; 2) Capacitate limitată de alertă rapidă şi de reacţie în caz de incidente; 3) Abordări inegale și necoordonate în ceea ce priveşte asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice; 4) Inexistenţa unor procese și practici de monitorizare și de raportare a incidentelor de securitate a rețelelor; 5) Nivel scăzut de încredere în rîndul utilizatorilor finali; 6) Risc sporit de întrerupere a proceselor de afaceri; 2) Compromiterea disponibilităţii, autenticităţii, integrităţii şi confidenţialităţii datelor stocate sau transmise şi a serviciilor asociate, oferite sau accesibile prin reţelele şi serviciile de comunicaţii electronice.
2.Reglementarea clasică – elaborarea şi aprobarea proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de	1) Îmbunătăţire a rezilienţei reţelelor şi serviciilor de comunicaţii electronice; 2) Asigurare a disponibilităţii şi integrităţii reţelele şi serviciilor de comunicaţii electronice;Protecție în timp real, împotriva unui număr mare de amenințări informatice, inclusiv împotriva atacurilor de tip Denial of Service, spamului sau fraudei. 3) Protejare împotriva utilizării neautorizate a resurselor; 4) Asigurare a confidenţialităţii informaţiilor; 5) Reducere a numărului incidentelor de securitate şi a reclamaţiilor la adresa securităţii; 6) Răspuns rapid la incidente şi prevenirea apariţiei unor incidente similare;	Nu au fost identificate.

comunicaţii electronice	7) Garantarea utilizării infrastructurilor TIC la întregul potențial pentru a profita, în acest sens, de oportunitățile economice și sociale ale societății informaționale; 8) Nivel ridicat de încredere în rîndul utilizatorilor finali; 9) Creştere a eficienţei şi productivităţii companiilor în livrarea serviciilor către clienţi; 10) Reducere a efortului material şi uman de recuperare a datelor importante ce s-ar putea pierde în cazul incidentelor care afectează securitatea informaţiei 11) Îmbunătăţire a controlului sistemelor şi proceselor interne ale furnizorilor. 12) Reduce costurile și sporește profitabilitatea pe termen scurt și lung. 13) Asigură funcționarea optimă a rețelei, dispozitivelor și aplicațiilor. 14) Permite existența breșelor de securitate care pot produce pagube importante. 15) Oferă control asupra traficului din rețea, astfel încât utilizatorii din interior pot accesa în siguranță resurse externe, iar utilizatorii din exterior pot accesa resurse interne. 16) Permite monitorizarea și administrarea datelor care intră sau ies din companie pentru a asigura lipsa codului periculos, virușilor sau conținutului ofensiv.	
3. Co-reglementare în baza altor acte normative şi legislative	Nu au fost identificate	1) Dificultăţi identificate la punerea în aplicare a cadrului normativ existent; 2) Nerespectarea cadrului legal de către toţi participanţii la piaţa comunicaţiilor electronice; 3) Abordări inegale și necoordonate în ceea ce privește asigurarea securităţii şi integrităţii rețelelor și serviciilor de comunicaţii electronice; 4) Inexistența unor procese și practici de monitorizare și de raportare a incidentelor de securitate a rețelelor; 5) Nivel de sensibilizare insuficient pentru elaborarea de măsuri protective și de contramăsuri adecvate.

Opţiunea 1. Opţiunea 1 nu prevede realizarea din partea statului a unor măsuri şi acţiuni.

Lipsa unor măsuri minime de securitate a reţelelor şi serviciilor de comunicaţii electronice, poate compromite servicii vitale în funcție de integritatea sistemelor rețelelor și a informațiilor. Acest lucru poate împiedica buna funcţionare a întreprinderilor, genera pierderi financiare substanțiale pentru economie şi afecta negativ bunăstarea societății.

Furnizorii de reţele şi/sau servicii de comunicaţii electronice au niveluri foarte diferite de capacități și de pregătire, ceea ce duce la abordări fragmentate în ceea ce priveşte asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. Având în vedere faptul că rețelele de comunicaţii electronice sunt interconectate, securitatea generală a acestora este slăbită de acei furnizori cu un nivel insuficient de protecție.

Prin urmare, lipsa unor abordări consecvente în ceea ce priveşte asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, precum şi inexistenţa unor linii directoare ar putea compromite disponibilitatea, autenticitatea, integritatea şi confidenţialitatea datelor stocate sau transmise şi a serviciilor asociate, oferite sau accesibile prin aceste reţele şi sisteme.

În cazul acestei opţiuni nu sunt prevăzute careva beneficii esenţiale.

Opţiunea 2. Opţiunea 2 prevede elaborarea şi aprobarea proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice. Inițiativa dată va oferi o viziune mai clară şi orientări sumare furnizorilor privind acţiunile ce urmează a fi întreprinse în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

Aceasta va contribui la sporirea capacităţii reţelelor sau a sistemelor informatice de a rezista, la un anumit nivel de încredere, la evenimente accidentale sau la acţiuni ilegale sau răuvoitoare, în special pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor, astfel încât să asigure continuitatea furnizării serviciilor de comunicaţii electronice.

De asemenea, aceste măsuri ar oferi garanţii suplimentare utilizatorilor finali în protejarea drepturilor sale: confidenţialitate a corespondenţei, protecţiei datelor cu caracter personal şi informaţiilor transmise pe calea comunicaţiilor electronice, securitatea aplicaţiilor folosite.

Aceste măsuri de securitate vor fi complementare prevederilor Legii nr.241/2007 precum şi Regulamentului privind regimul de autorizare generală şi nu vor avea un impact împovărător asupra furnizorilor de reţele şi servicii de comunicaţii electronice.

Opţiunea 3. Această opţiune constă în existenţa unor acte normative şi legislative care ar reglementa subiectul analizat.

Potrivit art. 20. alin. (2) lit. e) din Legea nr.241/2007:

Furnizorii de reţele şi/sau servicii publice de comunicaţii electronice publice au obligaţia să asigure:

e) întreprinderea acţiunilor tehnice şi organizatorice corespunzătoare în vederea asigurării securităţii serviciilor şi protecţiei datelor personale ale utilizatorilor.

De asemenea, conform pct.29, subpct. 9 al Regulamentul privind regimul de autorizare generală şi eliberare a licenţelor de utilizare a resurselor limitate pentru furnizarea reţelelor şi serviciilor publice de comunicaţii electronice aprobat prin Hotărârea Consiliului de Administraţie al ANRCETI nr. 57 din 21.12.2010.

29. Furnizorul are următoarele obligaţii:

9) privind securitatea reţelelor şi a serviciilor publice de comunicaţii electronice

a) să întreprindă măsuri tehnice şi organizatorice adecvate în vederea asigurării securităţii reţelelor şi a serviciilor împotriva accesului neautorizat, inclusiv, privind asigurarea inviolabilităţii secretului corespondenţei;

b) să informeze abonaţii săi, precum şi Agenţia, în situaţia în care ia cunoştinţă de apariţia unui risc de încălcare a securităţii reţelei prin intermediul căreia se furnizează serviciul public de comunicaţii electronice.

Cu toate că există unele prevederi legale privind necesitatea asigurării de către furnizori a securităţii reţelelor şi a serviciilor publice de comunicaţii electronice, nivelul de sensibilizare al furnizorilor este insuficient pentru elaborarea de măsuri de protective și de contramăsuri adecvate

În rîndul furnizorilor nu există o abordare comună şi acţiuni specifice în domeniul securităţii reţelelor şi informaţiilor. Doar o parte dintre furnizori au proceduri clare şi documentate pentru asigurarea continuităţii reţelelor şi serviciilor, în majoritatea cazurilor stabilirea unor măsuri de securitate efectuându-se reactiv, în momentul apariţiei unui incident. În plus, puţini dintre furnizori au o abordare completă a domeniului securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, majoritatea axându-se doar pe anumite domenii de interes.

De asemenea, nu este prevăzută o abordare comună de raportare a incidentelor care ar furniza ANRCETI informaţii suficiente în vederea evaluării nivelului de securitate a reţelelor sau serviciilor, precum și obţinerii unor date complete și certe referitoare la incidentele reale privind securitatea, care au avut un impact semnificativ asupra funcţionării reţelelor sau serviciilor şi respectiv prevenirea apariţiei unor incidente similare.

Prin urmare, prevederile Legii nr.241/2007 şi Regulamentului privind regimul de autorizare generală şi eliberare a licenţelor de utilizare a resurselor limitate pentru furnizarea reţelelor şi serviciilor publice de comunicaţii electronice nu tratează într-o măsură suficientă aspectele legate de securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Respectiv, opţiunea de co-reglementare nu corespunde necesităților pieţei și nu va identifica careva beneficii esenţiale.

VII. STRATEGIA DE CONSULTANŢĂ

AIR preliminar precum şi proiectul de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii reţelelor şi serviciilor publice de comunicaţii electronice, în conformitate cu prevederile Legii nr.241/2007 şi ale Legii nr.239 din 13.11.2008 privind transparenţa în procesul decizional, a fost expus spre consultare publică pe pagina de Internet a ANRCETI: www.anrceti.md, în perioada 1–24 iulie 2015, solicitându-se persoanelor interesate de a se expune asupra acestui AIR.

De asemenea, ANRCETI dispune de o bază de date a furnizorilor (registrul corespondenței cu persoanele interesate: furnizori – mai mult de 100 de adrese înregistrate, autorități publice, reprezentanți ai mass-media) la e – mail-ul cărora se expediază, în timp real anunţul despre organizarea consultărilor publice a documentelor expuse pe pagina de internet a ANRCETI precum și, după caz, fiind informaţi despre actualizarea conţinutului de pe pagina web a ANRCETI.

Pe parcursul perioadei de consultare publică, în adresa ANRCETI, au parvenit propuneri şi recomandări doar din partea a doi furnizori S.A.”Moldcell” și S.A.”Orange Moldova” (7 recomandări care au fost incluse în sinteza expusă în anexă la prezentul AIR). În rezultatul examinării acestora, 1 a fost acceptată, 2 acceptate de principiu și 4 recomandări respinse, aducându-se argumentele de rigoare incluse în sinteza din anexă.

În cazul în care cetăţenii, asociaţiile constituite în corespundere cu legea, alte părţi interesate nu transmit recomandări în termenul stabilit, ANRCETI, avînd în vedere prevederile

Legii nr. 239 din 13.11.2008 privind transparenţa în procesul decizional *(Monitorul Oficial 215-217/798, 05.12.2008),* consideră că aceştia nu au obiecţii şi recomandări asupra documentului expus spre consultare publică.

VIII. IMPLEMENTARE

Aprobarea proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice este atribuită ANRCETI.

Implementarea proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice este atribuită furnizorilor.

IX. MONITORIZARE

Orice acţiune realizată trebuie monitorizată pentru măsurarea eficienţei acesteia.

Monitorizarea implementării Proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice şi evaluarea eficacităţii aplicării acestui proiect urmează a fi realizată de către ANRCETI conform legislației în vigoare.

X. CONCLUZII

În urma analizei putem menţiona că opţiunea 2 va oferi cele mai mari avantaje. Astfel, se optează pentru opţiunea 2, care răspunde criteriului de planificare a unei reglementări bune, clare pentru utilizatori.

Prevederile prezentului proiect de hotărâre vor asigura stabilirea de către furnizori a unor măsuri coerente de securitate pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice. Vor oferi proceduri clare şi documentate pentru asigurarea continuităţii reţelelor şi serviciilor, precum şi o abordare completă a domeniului securităţii.

Aceste măsuri ar oferi garanţii suplimentare utilizatorilor finali în protejarea drepturilor sale: confidenţialitate a corespondenţei, protecţiei datelor cu caracter personal şi informaţiilor transmise pe calea comunicaţiilor electronice, securitatea aplicaţiilor folosite.

XI. RECOMANDĂRI

Reieşind din cele expuse în AIR preliminară, este recomandată opţiunea 2, aprobarea şi implementarea proiectului de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securității rețelelor și serviciilor publice de comunicaţii electronice, întrucât aceasta oferă cele mai mari avantaje.

Notă:

Prezenta Analiză Preliminară a Impactului de Reglementare a fost examinată în cadrul ședinței Grupului de lucru pentru reglementarea activității de întreprinzător în Republica Moldova din data de 16 decembrie 2015 (Procesul –verbal nr. 27). În rezultatul examinării s-a decis de a accepta Analiza Preliminară a Impactului de Reglementare pentru proiectul de Hotărâre cu privire la stabilirea măsurilor minime de securitate ce trebuie întreprinse de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor publice de comunicaţii electronice.