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 şi raportarea incidentelor cu impact semnificativ asupra acestora

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 şi raportarea incidentelor cu impact semnificativ asupra acestora 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.126-130/627 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.170-173/1321 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 şi raportarea incidentelor cu impact semnificativ asupra acestora 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.

Exemple recente ale unor astfel de situaţii fiind atacurile cibernetice asupra companiei Starnet.

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.

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 si 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 cetăţeni şi autorităţile din zonă de comunicaţii. Compania NTT, furnizor de servicii de telefonie şi Internet, a semnalat distrugerea a circa un milion şi jumătate de linii de telefonie, optice şi ISDN.

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 calamităţi, 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).

Proiectul de Hotărâre stabileşte cadrul legal pentru implementarea prevederilor Legii comunicaţiilor electronice nr.241-XVI din 15.11.2007, denumită în continuare Legea nr.241/2007, precum şi ale altor acte de reglementare emise de către ANRCETI, după cum urmează:

- 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;

- art. 23. alin. (13) din Legea nr.241/2007:

ANRCETI elaborează, actualizează şi modifică, în conformitate cu prezenta lege, condiţiile autorizării generale pentru diverse tipuri de reţele şi servicii, prin care stabileşte condiţiile în care acestea pot fi furnizate, definind astfel drepturile şi obligaţiile care revin furnizorilor fiecărui tip de reţea sau de serviciu. Condiţiile autorizării generale prevăd:

o) asigurarea securităţii reţelelor publice de comunicaţii electronice împotriva accesului neautorizat;

- 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.

De asemenea, Guvernul a aprobat Strategia Naţională de dezvoltare a societăţii informaţionale "Moldova Digitală 2020" (HG 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 spațiu deschis, sigur și 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 şi a Consiliului privind un cadru de reglementare comun pentru reţelele şi serviciile de comunicaţii electronice (Directiva cadru), astfel cum a fost modificată de Directiva 2009/140/CE a Parlamentului European şi 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 şi organizatorice corespunzătoare pentru a gestiona în mod corespunzător riscurile privind securitatea reţelelor şi serviciilor. Ţinând seama de progresele ştiinţifice de la momentul respectiv din domeniu, aceste măsuri trebuie să garanteze un nivel de securitate adecvat riscului existent. În special, trebuie luate măsuri pentru a preveni şi limita impactul incidentelor de securitate asupra utilizatorilor şi asupra reţelelor interconectate.

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

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

După caz, autoritatea naţională de reglementare informează autorităţile naţionale de reglementare din celelalte state şi Agenţia Europeană pentru Securitatea Reţelelor şi a Informaţiei (ENISA). Autoritatea naţională de reglementare respectivă poate informa publicul sau poate solicita întreprinderilor să facă acest lucru, în cazul în care consideră că dezvăluirea încălcării serveşte interesului public. O dată pe an, autoritatea naţională de reglementare în cauză prezintă Comisiei şi ENISA un raport de sinteză privind notificările primite şi măsurile luate în conformitate cu prezentul alineat

(4) Comisia, ţinând cont în cea mai mare măsură de avizul ENISA, poate să adopte măsuri corespunzătoare de natură tehnică de punere în aplicare cu scopul de a armoniza măsurile menţionate la alineatele (1), (2) şi (3), inclusiv măsurile care definesc circumstanţele, formatul şi procedurile aplicabile în cazul cerinţelor de notificare. Respectivele măsuri de natură tehnică de punere în aplicare se vor baza pe cât posibil pe standarde europene şi internaţionale şi nu împiedică statele membre să adopte cerinţe suplimentare în vederea urmăririi obiectivelor prevăzute la alineatele (1) şi (2).

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 (operare normală, cu întreruperi), diverse tipuri de incidente şi evenimente de securitate, precum şi situaţii de urgenţă, cazuri de dezastru sau crize majore.

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

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

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

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

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 vulnerabilităţi). Dispozitivele de securitate au blocat de asemenea, un număr de 900 000 de mesaje de tip spam, 23 000 de atacuri de reţea, au fost neutralizate 12 000 de e-mailuri care conţineau numeroşi viruşi, 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 reţelele şi 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.

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 securităţii reţelelor şi serviciilor publice de comunicaţii electronice.

IV. GRUPURILE DE INTERESE

Impactul noilor reglementări care vor fi introduse prin modificarea şi completarea Regulamentul nr.57/2010vor 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

Măsurile minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii reţelelor şi 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 cerinţele de securitate existente (şi anume menţinerea de către furnizori a securităţii şi integrităţii reţelelor publice de comunicaţii electronice).

De asemenea, menţionăm 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.).

Beneficii:

Printre beneficiile enumerate de respondenţi, se remarcă: asigurarea continuităţii 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.

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 şi 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; 7. 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 comunicaţii electronice	1. Îmbunătăţirea rezilienţei reţelelor şi serviciilor de comunicaţii electronice; 2. Asigurarea disponibilităţii şi integrităţii reţelele şi serviciilor de comunicaţii electronice; 3. Protejare împotriva utilizării neautorizate a resurselor; 4. Asigurarea confidenţialităţii informaţiilor; 5. Reducerea numărului incidentelor de securitate şi a reclamaţiilor la adresa securităţii; 6. Răspuns rapid la incidente şi prevenirea apariţiei unor incidente similare; 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. Creşterea eficienţei şi productivităţii companiilor în livrarea serviciilor către clienţi; 10. Reducerea efortului material şi uman de recuperare a datelor importante ce s-ar putea pierde în cazul incidentelor care afectează securitatea informaţiei 11. Îmbunătăţirea controlului sistemelor şi proceselor interne ale furnizorilor.	Nu au fost identificate.

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 securității și integrității rețelelor și serviciilor de comunicații 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 privește 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 privește asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, precum şi inexistența 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 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 și 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 necesităţilor 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 securității rețelelor și 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, este expus spre consultare publică pe pagina de Internet a ANRCETI: www.anrceti.md, solicitându-se părţilor interesate de a-şi expune propunerile şi comentariile asupra acestui proiect conform termenilor stabiliţi în comunicatul de presă.

VIII. IMPLEMENTAREA

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 este atribuită ANRCETI.

IX. MONITORIZAREA

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 va fi în sarcina ANRCETI.

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.