Minută

DEZBATERE PUBLICA LEGEA SECURITATII CIBERNETICE

Subiect	1. Legea privind securitatea cibernetică a României, prima dezbatere publică
Data	12.02.2016
Decizii / Sarcini	• Reprezentanţii societăţii civile vor transmite şi în scris observaţii şi propuneri la proiectul de lege. • MCSI va analiza şi integra în propunerea de lege observaţiile şi propunerile primite sau pe care urmează sa le primească, în măsura în care este posibil. • MCSI va organiza o nouă dezbatere publică privind "Proiectul de lege privind Securitatea cibernetică a României"

Dezbaterea a fost organizată de către MCSI, în sediul din Bd. Libertăţii nr. 14 şi a fost prezidată de doamna ministru pentru Consultare şi Dialog Civic, Victoria-Violeta Alexandru, alături de domnul ministru al Comunicaţiilor şi pentru Societatea Informaţională, Marius-Raul Bostan. La discuţii au mai participat domnii Augustin Jianu, director general CERT-RO, Marcel Opriș, director STS, Florin Cosmoiu, Directorul Centrului National, alături de peste 60 de reprezentanți ai societății civile și jurnaliști.

Ministrul pentru Consultare şi Dialog Civic, Violeta Alexandru a precizat, încă de la începutul discuțiilor: ” Un act normativ atât de important cum este proiectul de lege privind Securitatea Cibernetică a României, care are un impact atât de mare în spațiul public, trebuie supus analizei tuturor factorilor din societatea civilă. Acesta este motivul pentru care Ministerul pentru Consultare Publică și Dialog Civic (MCPDC) a decis să sprijinire metodologic echipa Ministerul Comunicațiilor și pentru Societatea Informațională, inițiatorul proiectului de act normativ, pentru ca această primă dezbatere pe actuala variantă a textului să se desfășoare conform prevederilor legii nr. 52/2003, legea transparenței decizionale” a subliniat ministrul MCPDC.
Ministrul Violeta Alexandru a mai subliniat, în deschiderea dezbaterii: "Important este ca echipa guvernamentală să practice un proces decizional cu adevărat participativ și eficient de la momentul inițierii unui act normativ, trecând prin etapa de consultare și dezbatere publică, până la integrarea, inclusiv comunicarea, propunerilor societății civile în varianta care va fi supusă aprobării Guvernului. Astfel de exercițiu de dezbatere publică (care merge dincolo de etapa minimală de

consultare prin afișare pe internet a proiectelor de politici publice) trebuie să devină parte firească a procesului decizional. Bineînțeles, inițiatorului îi rămâne decizia de a selecta din punctele de vedere prezentate însă, înainte de a lua această decizie, într-un proces democratic firesc de elaborare a unui act normativ, mai ales un act normativ care afectează în mod cert spațiul public, asemenea exerciții de consultare publică ar trebui să devină o normalitate.
Într-una din intervențiile sale, ministrul Marius Bostan a punctat: ”Vorbim despre Big Data, Cloud, Internet of Things. Noi nu putem construi infrastructură cibernetică fără să ne asigurăm că este folosită în mod corect și în interesul cetățenilor. Nu putem folosi banii publici să construim infrastructuri, putere de calcul și capabilități, iar ele să cadă în mâna unor oameni care nu respectă nici drepturile omului și sunt adversarii democrației și ai libertății, valori pe care noi toți vrem să le apărăm. Trebuie să ne asigurăm că această putere nu este folosită în mod contrar. Este important ca partea civilă, partea privată, cetățenii să participe la acest proces. Vom lua în considerare și vom analiza toate opiniile exprimate”, a afirmat ministrul Marius Bostan.

CERT-RO, Augustin Jianu

- a susținut o prezentare tehnică referitoare la realitățile spațiului cibernetic și necesitatea securității cibernetice, explicând pe scurt cum funcționează un atac cibernetic și ce consecințe poate avea acesta.
- a prezentat o descriere succintă a sistemului național de securitate cibernetică pentru infrastructuri cibernetice
- a explicat ce înseamnă un atac cibernetic, cum se recunoaște acesta și cum se construiește o armă, livrată printr-un fișier comun de tip pdf, doc sau orice alt tip de documente.
- Raportul anual de activitate al CERT-RO a reliefat că au fost procesate 68 milioane de alerte de securitate cibernetică, din care au fost extrase 2,3 milioane de adrese IP unice, compromise sau vulnerabile. La nivel global, în 2015, durata medie de detecție a unei intruziuni a fost de 268 de zile. Asta înseamnă că atacatorul a intrat într-un sistem compromis și a stat acolo 268 de zile, până să fie depistat!

Directorul STS, Marcel Opriș

- Evoluțiile din societate și tehnologice conduc la nevoia de schimbare și adecvare a cadrului legislativ
- interesul STS a fost constant pentru stabilirea de reguli în acest domeniu
- invită la consultarea rapoartelor de activitate STS

- remarcă privind calificarea personalului: din 2700 de angajați, peste 1000 sunt ingineri. S-a produs o mutație în competențele tehnice ale personalului, 800- 900 de ingineri supercalificați, tineri
- Diviziile de software și cele de tehnologie avansată s-au dezvoltat în cadrul STS
- accentul constant pus de STS de a lungul activității sale pe nevoia de exchange-uri naționale democratice și de dezvoltare a educației populației în ceea ce privește mijloacele electronice. România este totuși ruptă în două în ceea ce privește ritmul în care populația are acces și competențe în acest domeniu. Este nevoie de dezvoltarea de instrumente cu ajutorul tehnologiei pentru creșterea înțelegerii acestui domeniu.
- 400.000 de computere din administrația publică sunt conectate la nodul de internet STS, conectat la rândul său cu exchange-ul național, toate intraneturile publice funcționează prin STS, cu atât mai mult, este importantă responsabilitatea și crearea de reguli, pentru a corecta problemele; principiul separației puterilor este important.

SRI Florin Cosmoiu- dir. gen Centrul Cyberint

- SRI a promovat întotdeauna nevoia de responsabilizare a deținătorilor de structuri cibernetice pentru a asigura protecția infrastructurilor pe care le dețin precum și principiul esențial al asigurării dreptului la viață privată a tuturor cetățenilor țării.
- Autoritățile statului trebuie să aibă acces la date private doar cu mandat judecătoresc. Această lege urmărește însă să protejeze cetățenii de multiple amenințări, ex. grupurile de criminalitate, personae răuvoitoare, entități statale.

Ministrul MCSI- Marius Bostan

- sunt multe atacuri indirecte, cyberspaceul nu are granițe, apărarea trebuie să fie activă în fața acestor amenințări
- libertatea e importantă dar trebuie definită și în funcție de raportarea la alte valori, principii
- legiferăm nu doar de dragul legiferării ci pentru că există o problemă
- expertiza din partea civilă și militară trebuie pusă în comun
- pentru a operaționaliza o strategie este nevoie de o bază legală
- există un plan de măsuri în acest an pentru CERT RO care va fi aprobat în curând
- au fost elaborate ghiduri pentru funcționarii publici

- opiniile pertinente vor fi cuprinse în textul legii
- dacă va fi nevoie de o alta dezbatere, se va face
- au fost primiți în sală și cei care s-au înscris după terminarea procedurilor, reprezentanții presei tocmai din dorința de a arăta totala deschidere pentru o dezbatere reală
- orice cetățean care face o cerere ar trebui să poată participa la dezbaterile publice
- mulțumiri pentru efort celor care au trimis observații în scris

Reprezentanții societății civile dar și ziariștii prezenți la dezbatere au ridicat probleme concrete referitoare la conținutul proiectului de lege (cum ar fi: argumentarea necesității acestui demers de reglementare legislativă cu date statistice din partea CERT-RO privind amenințările reale în domeniul securității cibernetice; corelarea proiectului de act normativ cu proiectul de directivă europeană NIS şi cu legislaţia naţională în domeniu; asumarea de către mediul privat a dublei responsabilităţi în domeniul raportării incidentelor de securitate, faţă de stat şi faţă de clienţi), dar şi aspecte legate de semantică ale textului proiectului. În acest sens, au fost exprimate următoarele opinii:

Doamna Valentina Pavel, Asociatia pentru Tehnologie si Internet - ApTI (Anexa 1):

- Directiva NIS a fost adoptată de Parlament şi de Consiliu şi nu-i mai lipseşte decât o adoptare formală, având un termen de transpunere de 21 luni. Propunerea de lege nu este armonizată cu directiva şi MCSI ar trebui să anticipeze nevoia de modificare a propunerii de lege.
- Toate persoanele juridice fac obiectul propunerii de lege, în timp ce directiva NIS detaliază în anexă lista persoanelor ce fac obiectul directivei.
- Propunerea de lege nu este corelată cu o serie de alte acte normative. - Legea nr. 677/2001- privind operatorii de date cu caracter personal, Autoritatea pentru Protectia Datelor nu este menționată
- Potrivit propunerii de lege, persoanele juridice ce intră sub incidenţa legii sunt raportori de incidente de securitate cibernetică faţă de instituţiile publice responsabile, nu și faţă de clienți. Securitatea cibernetică este o responsabilitate pentru fiecare dintre noi, nu este o responsabilitate exclusivă a statutului şi toţi actorii trebuie implicaţi în egală măsura pentru a asigura această securitate cibernetică.

Asociaţia Naţională Internet Service Providerilor din Romania (ANISP):

- Nu dorește susținerea unui punct de vedere, nu a trimis observaţii la propunerea de lege, dar va transmite.

Asociatia Pentru Apăararea Drepturilor Omului în România – Comitetul Helsinki (APADOR-CH) (ANEXA1):

- Punctul de vedere transmis de APADOR-CH este cel pe care, în mare, l-a prezentat Valentina Pavel. Este un punct de vedere comun.
- Legea prevede un număr de 12 institutii publice cu diverse atribuţii în domeniul securitatii cibernetice, număr care este prea mare. Propunerea a fost ca raportarea să se realizeze către o singură instituţie publică civilă, de preferinţă CERT-RO
- COSC este compus din prea multe instituţii militare și este coordonat tehnic de către SRI, având un regulament aprobat de CSAT, în baza unor decizii secrete – astfel, informațiile despre COSC și activitatea sa sunt secrete.

Asociatia Civică din Hunedoara, Filiala Bucureşti (ANEXA 2):

- Propunerea de lege încalcă decizia din 2014 a Curții Constitutionale, privind propunerea anterioară de lege a securităţii cibernetice.
- Expunerea de motive nu este suficient de clară, deoarece:
  - nu conține motivele privind necesitatea elaborării acestei legi
  - Mass media este trecută ca și resursă de protejat
  - Nu este clar de ce este necesară protejarea resurselor energetice
- Care este rolul MAI, având în vedere faptul ca în urma unor probleme a fost necesară prezentarea unor probe video și a rezultat că poliția nu are calculatoare cu care sa poată vizualiza DVD-uri?
- Ce face SRI, care este protejat de atacuri din interior, nevoia fiind însă a ne proteja de atacuri din exterior?

Domnul Ambrosie Ionut-Marius a transmis observații în scris (ANEXA 3):

- Nu a dorit să intervină

Domnul George Popescu, freelancer :

•A dorit să prezinte 5 puncte:

1. Suspiciuni în loc de transparență, deoarece:

- Formularul postat de MCSI pe propriul site web pentru înregistrarea la dezbatere conține un cod macros care poate reprezenta un risc de securitate și poate fi activat.
- Există dovezi că RCS a deviat traficul de Internet al Asociaţiei Civice DREPTATE din Hunedoara către ICI, fapt pentru care va fi făcută o plângere penală.

2. Controlul – arta de a fi dictator prin iluzii:
- Privitor la Art. 6.3 care desemnează SRI ca și coordonator tehnic al activităţilor COSC, cine asigură serviciul tehnic deține cu adevărat controlul.
3. Conceptul strategie subversivă pe termen lung – denumirea legii ca fiind a securităţii cibernetice a României) pune sub semnul întrebării intenţiile iniţiatorului proiectului:
- denumirea propunerii de lege și preferarea sintagmei „cibernetice" în loc de „informatice", duc către un domeniu prea mare de aplicare a acesteia.
4. Apărarea – legislatia existența nu a împiedicat niciun serviciu să-și facă treaba
- Nu este clară necesitatea unei astfel de legi.
5. Kybernete– provine din limba greacă – înseamnă conducerea poporului. Expresia a fost extinsă de-a lungul timpului către așa de multe domenii de știința, încât putem fi oricând puși în situația de a ni se implementa orice altceva printr-o lege de așa anvergură.

Domnul avocat Cristian Driga (ANEXA 4):

- A transmis observaţii scrise la propunerea de lege și nu dorește sustinerea verbală.

Domnul Toma Cîmpeanu, Asociatia Naţională pentru Securitatea Sistemelor Informatice (ANSSI) (ANEXA 5):

- ANSSI, reprezentantă a specialiştilor în securitate cibernetica, reprezintă aproximativ 30% din piața.
- Remarcă, în primul rând, preocuparea iniţiatorului legii de a prelua observaţiile care au venit de la Curtea Constituţională și de a încerca să creeze un echilibru necesar între nevoia de cunoaştere a faptelor care ar putea constitui vulnerabilităti, respectarea libertăţilor cetăţenilor, precum și o bună cooperare între organizaţiile publice și mediul privat, precum și cetăteni. Este necesară identificarea și menţinerea unui echilibru între libertăţile cetăţeneşti și nevoile comunitare.
- ANSSI a transmis MCSI un numar de 40 de propuneri și observații privind propunerea de lege și normele sale de aplicare**.**

Sorin Manea ANISP:

- e nevoie de lege ținând cont de evoluțiile globale, România e țară NATO dar scopul propunerii de lege excede nevoia reală.
- O serie de prevederi, precum Art. 4.b), sunt deja implementate în practică.

- Art. 4 duce către o eventuală asemănare între România și Turcia, creând temeri.
- Potrivit Art. 2 și 3, orice furnizor de servicii sau deținător de infrastructuri cibernetice face obiectul propunerii de lege, în timp ce aceasta ar trebui să vizeze numai infrastructurile ICIN.

Asociatia Civică Dreptate:

- Sintagma „cibernetic" nu își are sensul în denumirea și textul propunerii de lege; propunerea este de inlocuire cu sintagma „informatic".
- Nu este clară necesitatea propunerii de lege, știind faptul că acela care deține informația are puterea.
- ICI este controlat de către SRI.

Domnul Mircea Toma, ActiveWatch (ANEXA 1):

- Există suspiciunea întreruperii principiului "checks and balances" al puterilor în stat."Există o poziţie exagerat de importantă a unui actor în aceasta structură, şi anume SRI. Aşa cum am văzut în tentativele precedente de legi Big Brother care au fost oprite în diverse instanţe, inclusiv la CCR, s-a semnalat tendinţa excesului de autoritate pe care această structură şi-l atribuie";
- În actualul proiect de lege, SRI apare ca operând Centrul Naţional de Securitate Cibernetică desemnat autoritate competentă pentru coordonarea activităţii în domeniul securităţii cibernetice. Cuvântul desemnat este cel care generează îngrijorare. Cine desemnează CNSC din cadrul SRI ca și autoritate competentă pentru infrastructuri ICIN, știind că deciziile CSAT sunt cel puțin influentate de SRI? Prima cerere concretă este să apară documentul transparent prin care un departament din interiorul SRI este desemnat să opereze/ să aibă autoritate asupra tuturor structurilor, mai puțin două care sunt ale statului.
- De ce SRI este la prezidiu și nu în sală?

Domnul Mihai Eftimie, Enigma System:

- Propunerea de lege duce la un paralelism legislativ, interzis de legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative.
- Privitor la Art. 16, ce reprezintă „infrastructura critică" și de ce nu este definită în propunerea de lege?
- Propunerea de lege nu prevede un audit al persoanelor ce vor activa în domeniul securității cibernetice.

- Oficiul Național pentru Jocuri de Noroc a solicitat furnizorilor de servicii de acces la Internet să blocheze accesul la site-uri de jocuri de noroc de pe lista „blacklist”, acțiune ce se realizează prin atacuri cibernetice de tip DNS Poisoning. Astfel, potrivit ONJN furnizorii ar trebui să își atace cibernetic propria infrastructură cibernetică și proprii clienți, iar potrivit propunerii de lege ar trebui să se raporteze la instituțiile statului cu privire la atacuri.
- Există şi alte probleme de genul salariilor mici din administraţia publică, promovarea unor personalităţi a căror competenţă şi profesionalism pot fi puse sub semnul întrebării. Acest lucru este coroborat cu obligaţia de livrare a unor informaţii confidenţiale. Credem că acest lucru reprezintă o adevărată ameninţare cibernetică şi nu alte aspecte care au fost omise.

Domnul Adrian Aciu, persoana fizică:

- Propunerea de lege este prea vagă, are nevoie de o serie de clarificări.
- Este nevoie ca toți cetăţenii să fie protejaţi de autoritățile publice din România.

Dl. Florin Cosmoiu, SRI:

- Mandatul emis de către un judecător este obligatoriu, potrivit prevederilor propunerii de lege.
- Informarea furnizorului de servicii se face printr-o înstiinţare cu privire la existența mandatului. Înștiintarea nu este mandat în sine.
- Accesul la datele solicitate se face în prezent în baza Codului Penal și Codului de Procedură Penală, precum și în baza legii nr. 51/1991 privind securitatea națională a României.
- Mandatul de Securitate națională este un document clasificat, iar accesul la acesta se poate realiza de persoanele care dețin un certificate de acces la date clasificate. Mandatul de supraveghere tehnică prevăzut de Codul Penal este un document neclasificat, dar acesta devine public doar în faza de judecată. Pentru respectarea legislației incidente, s-a ales soluția înștiințării.
-

APADOR CH -Reprezentanții societății civile prezenţi la discuţii au solicitat ca mandatul, atunci când există și se poate arăta, să fie arătat. De asemenea, mandatul emis în baza legii nr. 51/1991 trebuie să reprezinte excepție, nu sa devină regulă.

Domnul Augustin Jianu, CERT-RO:

- Nu s-a făcut abstracție de directiva NIS, dar, deocamdată, aceasta reprezintă doar un acord politic în mecanismul de negociere, nu se știe când va fi aprobată

- statele membre au libertatea de a merge dincolo de obiectivele directivei
- în anexă se spune *"cel puțin aceștia"*- în referirea la tipul de operatori
- neclaritățile care apar în lege pot proveni din nevoia de adaptare a legii la schimbările tehnologice, în așa fel încât să nu fie necesar să se revină asupra ei foarte curând, ținând cont de ritmul alert de dezvoltare în acest domeniu.
- Nu toate persoanele juridice fac obiectul legii, în înțelegerea sa, ci doar (art. 2)- persoanele juridice care folosesc date cu caracter personal
- există aspecte care pot fi mai bine conturate în privința corelării cu legea datelor cu caracter personal
- e normal ca un srl de apartament să notifice dacă sunt breșe de securitate pentru că pot fi afectați și cetățenii
- nu e o lege big brother, această etichetă doar ascunde ceea ce legea spune
- sigur e nevoie de dotări tehnice mai bune pentru Poliție
- pentru a sprijini eforturile de apărare este nevoie de informație - instituții și companii pot fi compromise
- media generală de detectare a unei infractiuni de acest tip este de 268 de zile, multe rămân nedescoperite
- în lumea modernă, sunt multe sisteme digitale care trebuie susținute și care pot fi periclitate la un atac pe scară largă

Ministrul MCSI-Marius Raul- Bostan

- problema e de fapt nu că sunt multe instituții ci că acestea trebuie bine coordonate, comparația se poate face cu SMURD
- partea civilă trebuie să participe la acest efort de siguranță, oamenii pot alerta și preveni
- există o strategie privind agenda digitală, vorbim de cloud, de big data, dar si de drepturi care trebuie apărate împotriva adversarilor libertății
- legea impune responsabilități deținătorilor de infrastructuri

Domnul Matei Vasile, ApTI:

- De ce este necesar ca propunerea de lege să meargă peste anexa la Directiva NIS? Propunerea de lege are un obiect de activitate prea mare, am înțeles că propunerea de directivă permite statelor membre să se meargă peste dar de ce să nu se meargă peste ea în spiritul ei
- nu trebuie aruncată o pătură peste toți, unii se vor sufoca, firmele mici nu vor putea din punct de vedere financiar să securizeze sistemul. Care sunt şi cine suportă costurile pentru firmele mici?
- vrem să avem grijă de securitatatea informatică, înțelegem, dar nu cu prețul diminuării mediului informatic

- Este necesar ca notificarea emisă de furnizorul de servicii să se facă şi către clienţi, nu doar către instituţiile publice.
- Responsabilitatea în ceea ce priveşte securitatea cibernetică trebuie să fie atât a Statului, cât si a persoanei juridice ce a pierdut date ale clienţilor săi.

Domnul Marcel Opris, STS:

- Art. 21.1) prevede faptul că şi clientul este informat Din punctul nostru de vedere subiectul este închis pentru că utilizatorul este îndreptățit să fie notificat, conform legii, este de fapt o completare la drepturile consumatorului
- există sancțiuni în alte legi pentru utilizatorul care a pierdut datele

Domnul Adrian Sturdza, Epoch Times:

- Nu sunt disponibile suficiente informaţii privind atacuri cibernetice efectuate asupra infrastructurilor cibernetice din România.
- Ar trebui ca propunerea de lege să trateze numai apărarea cibernetică, nu să încerce să trateze tot domeniul.

Domnul Marcel Opriș, STS: de fapt este un domeniu nou pentru România, cu instrumente într-o dinamică extraordinară, cu toate acestea există rapoarte, exemplu CERT RO, STS însuși este un serviciu care are o secțiune de CERT, prima de acest fel

- Există rapoarte publice cu informaţii referitoare la securitatea cibernetică şi atacuri cibernetice.

Doamna Valentina Pavel, ApTI:

- Notificarea prevazută de Art. 21.1) din propunerea de lege este deja prevazută în legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vietii private în sectorul comunicaţiilor electronice.
- Garanţia oferită prin propunerea de lege privind mandatul nu este suficientă, având în vedere faptul că legea nr. 677/2001 privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, oferă deja o excepţie pentru SRI.

Domnul Mihai Spirache, Asociaţia Creştină Sfântul Arhanghel Mihail:

- Sunt respectate drepturile şi libertăţile din Constituţia României? Cum este asigurată respectarea acestora?
- Ce interese sunt urmărite prin propunerea de lege?

- Care este scopul în reluarea propunerii de lege, după ce propunerea anterioară a fost respinsă la Curtea Constituţională?

Domnul Marcel Opris, STS:

- Atacurile cibernetice au surse diferite, pot veni de la orice calculator, din toată lumea.
- Ca de exemplu, formularul 112 al MFP a adus un efect benefic în societate; dacă formularul 112 este atacat şi infrastructura cibernetică nu mai functionează, care sunt efectele asupra societăţii?

Domnul Mihai Bumbes, Mişcarea Civică Miliţia Spirituală:

- Cine este directorul CNSC din cadrul SRI şi de ce nu este prezent în sală?
- Cine controlează CNSC?

Domnul Doru Dragomir, jurnalist:

- S-a ţinut cont la elaborarea legii de 2 hotărâri CSAT, o decizie ANCOM si o decizie CSAT. SRI mai pune în aplicare hotărârea CSAT din 2008 prin care furnizorii de comunicaţii de date pun la dispoziţia SRI serverele de management şi consolele de management ale reţelelor?
- Hotărârile CSAT conţin prevederi ce se suprapun propunerii de lege şi deciziei preşedintelui ANCOM?

Domnul Andrei Nicoara:

Privind prevederile Art. 19.c), există şi obligaţia primirii suportului solicitat? Dacă există resurse disponibile la instituţiile publice specializate, suportul se poate acorda; dacă nu există resurse disponibile, suportul trebuie contractat din piaţă, prin achiziţie publică, proces care durează o perioadă de timp, în care este neclar ce se întamplă cu infrastructura cibernetică. Este necesară tratarea corespunzătoare a acestor situaţii. Problema achiziţiilor publice de furnizori privaţi de securitate care durează foarte mult!

Cum poate face faţă CERT RO la ameninţări simultane când există aceste slăbiciuni ale sistemului?

Domnul Matei Vasile, ApTI:

- Dacă serviciul 112 cade, o să se stea la cozi.

Domnul Adrian Herciu:

- Daca un ONG nu prelucrează date cu caracter personal, intră sub incidenţa propunerii de lege?
- Statul transferă date cu caracter personal către terţi?
- SRI este în incompatibilitate, relativ la propunerea de lege: cineva, care are interesul să afle date, este pus să le păzească.
- Instituţiile care fac abuzuri trebuie să nu se mai ocupe de managementul securităţii cibernetice.
- Dorim ca dezbaterea să se reia, să ştim în ce măsură se ține cont de părerea noastră, exprimarea dorinței ca ideile primate, dar care au fost response, să primească și o justificare corespunzătoare a motivului respingerii lor

Doamna ministru Violeta Alexandru:

- rog reprezentanţii societatii civile prezenţi la dezbatere să trimită observaţiile şi propunerile privind proiectul de lege pe e-mail, către MCSI, la adresa:biroupresa@msinf.ro

Domnul Florin Cosmoiu, SRI:

- CyberInt s-a înființat în baza deciziei CSAT din 2008, la început, fără statut juridic. Din 2013, printr-o decizie CSAT, a devenit unitate distinctă în cadrul SRI.
- CNSC va fi o structură operaţională a SRI şi va include şi atribuțiile CyberInt.
- Comisia parlamentară de control a SRI-ului este cea care controlează SRI.

Domnul Ion Dedu, colonel în rezervă:

- **CNSC a fost deja constituit; potrivit unei note de fundamentare semnată de premierul Victor Ponta în 2015, el deja functionează.**

Domnul Marius-Raul Bostan, MCSI:

- Vă rog transmiteţi-ne toată solicitarea dumneavoastră în scris, vom cerceta şi vă raspundem.

Domnul Mihai Spirache, Asociatia Crestina Sfantul Arhanghel Mihail:

- Propunerea de lege se subscrie Planului pentru Piaţa Digitală Unică?

Domnul Augustin Jianu, CERT-RO:

- Da, contribuie la implementarea planului. Într-adevar ar trebui menționat în expunerea de motive
- Este necesar să găsim mijloacele prin care propunerea de lege să nu sufoce firmele mici.
- Notificările privind incidentele de securitate cibernetică trebuie să ajungă şi la clienţii afectați.
- Pentru domnul Adrian Sturdza, Epoch Times: consideraţi că persoanele juridice ce au suferit atacuri cibernetice şi au pierdut date personale, trebuie să faca aceste informaţii publice? Există riscul ca, dacă CERT-RO face aceste date publice, poate provoca prejudicii de imagine.
- În prezent se răspunde la atacurile cibernetice imediat cum sunt identificate; dacă notificarea ar fi obligatorie către CERT-RO, răspunsul ar putea fi mai eficient decât în prezent.

Domnul Florin Cosmoiu, SRI:

- Nu vor exista şi CyberInt şi CNSC în cadrul SRI.

Domnul Marius-Raul Bostan, MCSI:

- Exprimarea poate fi deficitară în nota de fundamentare, poate fi modificată.
- În ceea ce priveste terminologia – cibernetică vs informatică –, aceasta trebuie armonizată cu termenii folosiţi pe plan comunitar; vom face totuşi şi o analiză semantică a textului.
- Legea aceasta pune nişte responsabilități și deținătorilor de infrastructure, pentru a avea grijă de aceste date, întrucât în momentul de față, acest aspect nu este reglementat.
- Vă rog ca, dacă aveţi şi alte observații şi propuneri la proiectul de lege, să ni le transmiteţi în scris.
- MCSI va organiza o nouă dezbatere publică privind legea securităţii cibernetice, pe care o va anunţa public.

DEZBATEREA A AJUTAT LA CLARIFICAREA URMĂTOARELOR ÎNTREBĂRI DIN PARTEA SOCIETĂȚII CIVILE

- Cum se armonizează proiectul de lege cu directiva europeană NIS - răspunsul a fost că directiva a fost luată în considerare la elaborarea proiectului de lege, dar intenția legiuitorului este de se folosi permisiunea oferită de directiva statelor membre de a merge dincolo de ea, lărgind de exemplu definiția operatorilor

- În ceea ce privește observațiile privind posibile probleme de tehnică legislativă, paralelisme cu alte legi în domeniu, sau absența referinței la altele, acestea au fost și sunt în continuare verificate
- S-a reținut nevoia unei expuneri de motive mai argumentată din punct de vedere statistic, privind amenințările cibernetice, luarea în calcul a unei posibile estimări a costurilor pe care le-ar avea firmele mici precum și punerea acestei legi în contextul mai larg al Pieței Digitale Unice
- S-a explicat faptul că actuala structura Cyberint și noul organism prevăzut în proiectul de lege COSC vor fuziona și că SRI nu va avea mai multă putere decât în prezent, fiind controlat prin aceleași mijloace ca și până acum, respectiv, Comisia parlamentară de specialitate
- S-a reținut opinia care a fost formulată de lideri ai organizațiilor neguvernamentale, că există o îngrijorare generală privind transparența și integritatea noului organism, care va fi creat prin lege, Consiliul Operativ pentru Securitate Cibernetică, și dorința acestora ca acest organism să fie mai degrabă civil
- Necesitatea unor clarificări terminologice cibernetic/ informatic a fost considerată importantă