5 principii pentru o securitate informatică sănătoasă pentru întreaga societate

Scrisoare deschisă

Securitatea informatică este o problemă care ne privește pe toți.

Dar securitatea informatică NU înseamnă doar **securitatea** sistemelor informatice care sunt de interes **pentru stat**, **ci şi securitatea informaţiilor noastre electronice**. Fie că vorbim despre securitatea informațiilor personale (ex. date personale, informații private) sau de securitatea informațiilor unei companii (ex. liste de clienți, informații confidențiale de serviciu).

Dar, uneori, **informaţiile noastre nu trebuie partajate cu statul**. Fie că vorbim despre o anchetă cu informații din surse care nu se fac publice, de baza de date de clienți ai unei firme sau de chestiuni strict personale ale unei persoane fizice. Deci cu atât mai mult **securitatea informaţiilor noastre nu trebuie să fie comunicată statului**, decât atunci când există un interes public superior interesului privat în cauză.

Propunerea legii securității cibernetice nu reușește să facă această distincție și creează iluzia că am putea fi într-o insulă de siguranță informatică într-un ocean de Internet. **Propunem 5 modificări de concepţie** pentru a putea avea un act normativ coerent și care să răspundă acestor principii:

Ce propune propunerea de **lege actuală**	**Ce propunem noi**
Practic **toate persoanele juridice sunt subiecţii legii** [1].	**Subiecţii legii trebuie să fie exclusiv infrastructurile naţionale de interes public.** Acestea trebuie definite clar prin lege, nu să avem definiții neclare, ca în Anexa II din directiva NIS.
În ciuda principiilor (art. 4 lit. e) [2]), **sectorul privat este tratat în textul propus ca un simplu raportor** de incidente de securitate. Mai mult, **furnizorii de servicii de securitate cibernetică sunt obligaţi să devină nişte delatori**, având obligația să notifice SRI de posibile amenințări informatice, dar nu au	La ora actuală **sectorul privat are cea mai mare competenţă în domeniul securităţii informatice, el trebuie să fie implicat activ** în domeniul securității cibernetice (*de ex. să fie reprezentat în organele de conducere ale CERT-RO*), dar în același timp

aceiaşi obligaţie faţă de propriul client (art. 20 alin. (1) [3]).	**respectându-se de stat obligaţiile sale de confidenţialitate** faţă de clienţii săi sau datele personale colectate de la persoanele fizice *(de ex. un furnizor de servicii de securitate nu ar trebui să poată să trimită o notificare fără acceptul scris al clientului său).*
Textul actual **nominalizează 12 instituţii** cu diverse atribuţii (art. 9 [4]) cu obligaţia de comunicare reciprocă de date între ele (art. 12 lit. j) [5]). **Toate incidentele de securitate cibernetică trebuie raportate** (art. 3 lit. m) [6], art. 20 alin. (1) b) [7], art. 24 [8]).	**Raportarea incidentelor de securitate se va face doar către o singură instituţie civilă cu competenţe tehnice reale (CERT RO)** şi doar pentru incidente majore.
Proiectul de lege include o serie de obligaţii pentru deţinătorii de infrastructuri cibernetice (cam orice persoană juridică), ce pot fi contractate către „furnizori de servicii de securitate". Proiectul este foarte ambiguu cu privire la aceşti furnizori. **În schimb în art. 22 alin. (3) [9]) se ascunde o obligaţie de înregistrare şi creare a unui Registrul Furnizorilor de Audit de Securitate Cibernetică**, în condiţiile unui simplu ordin de ministru.	Dacă aceşti furnizori au un rol important în această lege, rolul lor trebuie precizat clar într-un capitol special. Dacă se cere înregistrarea furnizorilor de servicii de securitate cibernetică pentru a realiza audit, aceste **norme trebuie stabilite de lege** şi nu prin legislaţie secundară.
Legea include texte din domenii multiple fără o minimă corelare cu actele normative primare: • obligaţii pentru operatorii de date personale, ignorându-se Legea 677/2001, Ordinul 52/2002 al Avocatului Poporului şi ANSPDCP • obligaţii pentru furnizorii de comunicaţii electronice, ignorându-se prevederile Legii 506/2004, OUG 111/2011 şi	**Toate celelalte obligaţii de securitate a informaţiei trebuie incluse în legislaţia sectorială** *(ex. securitatea datelor personale în legea datele personale, securitatea comunicaţiilor electronice în legislaţia comunicaţiilor electronice, furnizorii de găzduire în Legea 365/2002, securitatea instituţiilor subordonate SPP în legislaţia SPP, etc.)*

obligaţii deja existente de la ANCOM de raportare a incidentelor de securitate • obligaţii pentru furnizorii de găzduire (art. 23 [10]) care contrazic Legea 365/2002 etc.	

Prezentul document va fi înaintat în cadrul dezbaterii publice organizate de MCSI din data de 12.02.2015.

Semnatari - persoane fizice şi juridice

Asociaţia pentru Tehnologie şi Internet - ApTI - www.apti.ro

Referinţe:

[1] Legea se aplică „persoanelor juridice, deținătoare de infrastructuri cibernetice care prelucrează date cu caracter personal" (art. alin. (2) lit. b). Definiţia largă a infrastructurilor cibernetice face ca orice persoană juridică să fie inclusă în această categorie. Spre exemplu:
- orice firmă care are o bază de date cu clienţi persoane fizice
- orice ONG care lucrează cu datele personale ale beneficiarilor pe un calculator
- orice instituţie publică, oricât de mică
Toate acestea vor fi obligate să facă diverse raportări sau chiar audituri, de la caz la caz, generând costuri suplimentare pentru ele.

[2] Art. 4 lit. e) asigurarea unei guvernanțe participative, democratice şi eficiente a spațiului cibernetic prin cooperarea autorităților competente cu sectorul privat;

[3] Art. 20 alin. (1) Deținătorii de infrastructuri cibernetice prevăzuţi la art. 2 lit. a) - c) au următoarele obligații:
a) să asigure implementarea cerințelor minime de securitate cibernetică;
b) să notifice deîndată autoritatea competentă cu privire la incidentele de securitate cibernetică identificate;
c) să se asigure că datele şi/sau informațiile referitoare la configurarea şi protecția infrastructurilor cibernetice sunt diseminate exclusiv persoanelor autorizate să le Cunoască;
d) să nu permită accesul la datele de conținut din infrastructurile cibernetice deținute sau aflate în competență, în lipsa unei înştiințări scrise din partea autorităților abilitate, privind existența unei autorizații emise de judecător, în condițiile legii;
e) să gestioneze incidentele de securitate cibernetică;
f) să nu afecteze, prin acțiunile proprii, securitatea altor infrastructuri cibernetice.

[4] Art. 9 Pentru asigurarea securității cibernetice, instituțiile publice din România au atribuții după cum urmează:

a) Ministerul Comunicațiilor şi pentru Societatea informațională, cu rol de autoritate de reglementare şi control al implementării măsurilor privitoare la asigurarea securității cibernetice, cu excepția instituțiilor prevăzute la lit. d) şi e);
b) Centrul Național de Răspuns la Incidente de Securitate Cibernetică, desemnat punct național de contact cu entitățile de tip CERT naționale şi internaționale şi autoritate competentă pentru coordonarea activităților în domeniul securității cibernetice a infrastructurilor cibernetice, altele decât cele menționate la lit. c), d) şi e);
c) Serviciul Român de informații, prin Centrul Național de Securitate Cibernetică, desemnat autoritate competentă pentru coordonarea activităţilor în domeniul securității cibernetice organizate şi desfăşurate la nivelul infrastructurilor cibernetice de interes național, cu excepția infrastructurilor cibernetice de interes național aflate în administrarea sau responsabilitatea celorlalte autorități prevăzute la lit. d) şi e);
d) Autoritatea Națională pentru Administrare şi Reglementare în Comunicații, desemnată autoritate competentă pentru coordonarea activităţilor în domeniul securității cibernetice a furnizorilor de reţele publice de comunicații electronice sau furnizorilor de servicii de comunicații electronice destinate publicului;
e) Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Autoritatea Națională pentru Administrare şi Reglementare în Comunicații, Serviciul Român de Informații, Serviciul de Informaţii Externe, Serviciul de Telecomunicații Speciale şi Serviciul de Protecție şi Pază sunt autorități responsabile de securitate cibernetică cu rol în stabilirea de structuri şi implementarea de măsuri proprii privind coordonarea şi controlul activităților referitoare la asigurarea securității cibernetice pentru infrastructurile cibernetice, inclusiv infrastructurile cibernetice de interes național, aflate în domeniul lor de activitate şi responsabilitate.

[5] Art. 12 lit. j) să coopereze şi să-şi comunice reciproc date referitoare la securitatea cibernetică, inclusiv către celelalte autorități şi instituții publice sau deținători de infrastructuri cibernetice;

[6] Art. 3 lit. m) incident de securitate cibernetică - eveniment survenit în spațiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;

[7] Art. 20 alin. 1 lit. b) să notifice deîndată autoritatea competentă cu privire la incidentele de securitate cibernetică identificate;

[8] Art. 24 (1) Notificarea incidentelor de securitate cibernetică se transmite în modalitatea stabilită de autoritatea competentă şi trebuie să conțină, în mod obligatoriu, următoarele elemente:
a) elementele de identificare ale infrastructurii cibernetice afectate;
b) descrierea incidentului;
c) perioada de desfăşurare a incidentului;
d) impactul incidentului.
(2) Pentru gestionarea incidentelor de securitate cibernetică, deţinătorii de infrastructuri cibernetice pot solicita sprijinul furnizorilor de servicii de securitate cibernetică sau al autorităţilor prevăzute de art. 9 lit. b) - e), potrivit competenţelor acestora, cărora le pot pune la dispoziție date tehnice referitoare la incidentele şi atacurile cibernetice pe care le gestionează, cu asigurarea anonimizării datelor cu caracter personal deținute.
(3) Datele tehnice transmise în condițiile prevăzute la alin. (2) nu vor conține:
a) informații clasificate;
b) date care pot aduce atingere drepturilor şi libertăților cetățeneşti ori intereselor legitime ale unor terțe entități implicate.

[9] Art. 22 alin. (3) Furnizorii de servicii de securitate cibernetică care realizează audit de securitate pentru infrastructuri cibernetice de interes național au obligația de a se înregistra la Ministerul Comunicațiilor şi pentru Societatea Informațională, potrivit normelor aprobate prin ordin al ministrului, care stabilesc condițiile pentru înregistrarea şi radierea acestora din Registrul Furnizorilor de Audit de Securitate Cibernetică.

[10] Art. 23 (1) Furnizorii de servicii de găzduire internet care desfăşoară activități pe teritoriul României au obligația să acorde sprijin autorităților competente, respectiv organelor de urmărire penală, pentru punerea în aplicare, potrivit legii, a oricărui act de autorizare a restrângerii temporare a exercițiului drepturilor şi libertăților persoanelor, emis de judecător.
(2) Furnizorii de servicii de găzduire internet au obligația de a înregistra şi stoca date de jurnalizare a activităților din sistemele informatice deținute care fac obiectul actului de autorizare de la alin. (1), pe toată perioada de valabilitate a acestuia.
(3) Persoanele care sunt chemate să acorde spriijn tehnic la punerea în executare a actelor de autorizare, precum şi persoanele care iau la cunoştință despre aceasta au obligația să păstreze secretul operațiunii efectuate, sub sancțiunea legii penale