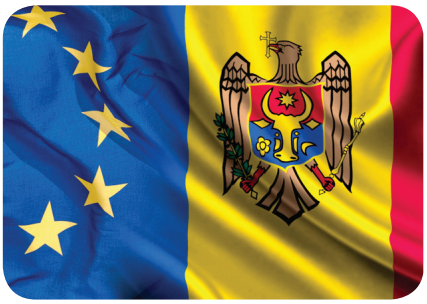
BULETIN INFORMATIV



nr. 14 | 2019

Serghei Popovici:

Securitate cibernetică necesită resurse financiare și umane importante

pag. 3

Cadrul legal privind transpunerea Acordului de Asociere în noiembrie 2019

pag. 7

Evenimente desfășurate în noiembrie 2019 în relația Republica Moldova–UE

pag. 7

Infrastructura critică în contextul atacurilor teroriste și amenințărilor cibernetice

Reglementarea și protecția infrastructurii critice este o necesitate în era tehnologiilor informaționale și a daunelor provocate de atacurile teroriste. Infrastructură critică înseamnă un bun, un sistem sau o parte componenta a acestuia care este esențială pentru menținerea funcțiilor vitale ale societății, a sănătății și a bunăstării economice sau sociale a oamenilor.

Fiind un domeniu relativ nou de reglementare, Republica Moldova trebuie să dezvolte cadrul legal și instituțional pentru a face față provocărilor la adresa securității naționale din care face parte și segmentul infrastructurii critice. Distrugerea sau perturbarea acesteia din cauza dezastrelor naturale, a terorismului, a activității infracționale sau a comportamentului rău intenționat poate avea un impact negativ semnificativ asupra securității Republicii Moldova și a bunăstării cetățenilor săi.

Acest domeniu cuprinde două importante care se completează reciproc – infrastructura critică fizică (clădiri și edificii) și infrastructura critică informațională. Protecția clădirilor/edificiilor aglomerate sau a celor care au funcții vitale pentru societate (alimentație, sănătate, transport) a devenit un subiect important pe agenda politicii de securitate din cauza atacurilor teroriste comise asupra acestora. Totodată, ținând cont de rolul crescând al tehnologiilor informaționale în activitatea obiectivelor incluse în lista infrastructurii critice, subiectul combaterii crimei informaționale și asigurării securității cibernetice devine esențial pe agenda politicii de securitate.

sursa foto: www.moldova.europalibera.org

Republica Moldova este în proces de dezvoltare a cadrului legal și instituțional pentru protecția infrastructurii critice. Planul Național de Acțiuni pentru Implementarea Acordului de Asociere prevede explorarea posibilităţilor de cooperare specifică în domeniul protecţiei infrastructurilor critice, referindu-se la *Directiva 2008/114/CE a Consiliului privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora* și la *Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.*

Astfel, autoritățile naționale au elaborat documente de politici în vederea prevenirii și combaterii terorismului, verificării stării și aprecierii nivelului de protecție antiteroristă a obiectivelor incluse în infrastructurilor critice. Menționăm elaborarea *Nomenclatorului național al infrastructurii critice* care cuprinde o listă de obiective dotate cu pașaport antiterorist.

Dezvoltarea cadrului legal și instituțional care se referă la combaterea criminalității informatice se confruntă cu unele probleme. Pe de o parte, au fost adoptate mai multe documente importante (Strategia securității informaționale) și create instituții care au scopul să gestioneze problema securității cibernetice (CERT-GOV), pe de altă parte sunt restanțe în procesul de implementare a mai multor acțiuni necesare pentru combaterea criminalității cibernetice, cum ar fi crearea unei echipe naționale de intervenție în caz de incidente de securitate informatică la nivel național.

Dacă în cazul protecției infrastructurii critice fizice constatăm elaborarea și implementarea majorității măsurilor prevăzute, atunci în domeniul securității informatice constatăm anumite mai multe deficiențe. Acest fapt se explică, în mare parte, prin lipsa resurselor financiare și umane necesare pentru a implementa toate obiectivele stabilite. În acest context, menționăm importanța adoptării în 2018 a Strategiei securității informaționale pentru anii 2019-2024 care trebuie să dezvolte capacitățile statului pentru asigurarea securității informaționale. Realizarea obiectivelor acestui document vor contribuie la sporirea nivelului de securitate cibernetică a infrastructurilor critice naţionale (autorităţi/instituţii publice, reţele de comunicaţii electronice, apeducte, reţele energetice, reţele de transport etc.) și sporirea competenţelor instituționale în securitatea cibernetică.

Veaceslav BERBECA


sursa foto: www.popor.md

Serghei POPOVICI:

director al I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică”

Securitate cibernetică necesită resurse financiare și umane importante

Cum evaluați procesul de transpunere a măsurilor prevăzute în Planului Național de Acțiuni privind Implementarea Acordului de Asociere în domeniul infrastructurii critice?

Din păcate, trebuie să constatăm că ne-am mișcat mai lent decât ne-am fi dorit în privința cooperării specifice privind protecția infrastructurii critice. Serviciul Informații și Securitate a predat din 2019 MEI ștafeta de transpune prevederile Directivei (UE) 2016/1148 a Parlamentului European și ale Consiliului European privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Anul trecut a fost creat un grup de lucru pentru coordona procesul transpunerii, dar, din cauza fluctuațiilor politice, activitatea acestuia a rămas la nivel de intenție și, respectiv, membrii săi nu au reușit să se întrunească. Grupul de lucru, creat printr-o decizie internă a Ministerului Economiei și Infrastructurii, este constituit din reprezentanți ai mai multor instituții de stat care au tangență directă cu sectorul infrastructurii critice. Recent, s-a pus din nou problema transpunerii prevederilor

Directivei (UE) 2016/1148, domeniul infrastructurii critice fiind o prioritate pentru MEI.

Există și progrese evidente la care trebuie să ne referim. La nivel de politici au fost elaborate și adoptate mai multe documente importante în ultimii doi ani. Vreau să menționez, în mod special, Legea nr. 299 din 21.12.2017 privind aprobarea *Concepției securității informaționale* a Republicii Moldova. Acest act se referă la procesul de prevenire și combatere a criminalității informatice, definind, inclusiv, noțiuni legale precum *amenințarea hibridă de securitate* și *războiul informațional.*

Pentru asigurarea securității cibernetice a fost foarte important să adoptăm *Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia* prin HG nr. 257 din 22.11.2018. Acest document este un angajament al Republicii Moldova în cadrul Planului Național de Acțiuni privind Implementarea Acordului de Asociere.

Ce reprezintă securitatea cibernetică?

Este un lucru foarte costisitor și solicită resurse umane și financiare importante. Securitatea cibernetică este o problemă globală. Tehnologia nu a fost integrată în sistemul de securitate și, respectiv, există provocări enorme ce țin de gestionarea acestei probleme. Tehnologia e un trend cu mare viteză care depășește cadrul legal și instituțional creat de ani de zile. Trebuie să fie elaborate documente și regulamente pentru administrarea securității cibernetice. Este foarte important ca în fiecare instituție să fie numită o persoană responsabilă de gestionarea acestui sector. Menționez că problema este mult mai mare și nu trebuie să se rezume doar la un expert responsabil de acest domeniu. Este nevoie de specialiști de diferite calificări. Măsurile de protecție a securității cibernetice înseamnă, de asemenea, actualizarea programelor anti-virus și instruirea personalului în privința procedurilor interne și conștientizării riscurilor. Angajații nu au voie să folosească dispozitive proprii în rețelele instituționale pentru activități ce țin de activitatea profesională la locul. E o problemă mare și utilizarea telefoanelor mobile, deoarece informația se transmite foarte ușor prin fotocopiere. De asemenea, constatăm de multe ori că instruirile profesionale de anul trecut nu mai sunt actuale în anumite circumstanțe. Virușii s-au mutat pe rețelele sociale și pe telefonia mobilă. Oamenii trebuie să-și asume responsabilitatea în privința informației plasate pe rețelele de socializare.

Care sunt principalele probleme ce țin de securitatea cibernetică?

Există probleme la nivel instituțional, din perspectiva coordonării acestei probleme, dar și la nivel legal. La nivel național nu au fost efectuate procese de audit complexe de securitate cibernetică și nici nu există rapoarte care ar evalua situaţia privind criminalitatea informatică. Practica internațională spune că trebuie creat un Centrul de Răspuns la Incidente Cibernetice la nivel național (CERT-național) pe lângă prim-ministru sau președinte, mai aproape de factorul de decizie, pentru ca un număr cât mai limitat de persoane să fie implicat în lanțul procesului de luare a deciziilor.

Din punct de vedere legal, există problema acumulării probelor pentru a demonstra daunele materiale. Un incident de securitate este criptarea informației și, drept impact, se pierde informația. În acest caz, nu avem consecințe fizice care pot fi demonstrate. Probele din cibernetică sunt complicat de demonstrat.

Mai mult, criminalitatea cibernetică e doar o componentă. Mai este și securitate cibernetică și securitate informațională, amenințările hibride, problema spionajului care, odată instalat de răufăcători, este foarte greu de identificat și, respectiv, de a înțelege toate pericolele pe care le prezintă. O problemă mare este criptomining-ul, fiindcă se conectează la rețele și consumă energie pentru producerea valutei virtuale.

Crima cibernetică urmărește, de regulă, profit financiar. Vorbim de spioni din punct de vedere geopolitic care doresc să acumuleze informație, sau este vorba de tineri care vor să testeze

capacitățile noastre de reacție și organizează atacuri. Există o piață neagră în domeniul tehnologiilor informaționale care este foarte bine protejată și inventivă.

Pentru atacatori este important să găsească veriga slabă. Cauzele problemelor pot fi diferite – de la vulnerabilitățile rețelei până la oamenii care activează în aceste instituții. Atacurile cibernetice nu sunt o noutate. Acestea constituie o problemă globală. Problema nu e în atacurile care se operează, ci cât de rapid reușim să reacționăm la aceste incidente pentru a recupera daunele provocate.

Factorul uman este foarte important în întregul proces legat de asigurarea securității cibernetice, fiindcă oamenii sunt implicați în procesele de dezvoltare a rețelelor și cea mai mică eroare sau scăpare poate afecta funcționarea rețelelor. Pe de altă parte, sistemele din instituții se învechesc, iar menținerea lor în pas cu tendințele din domeniul tehnologiilor informaționale este costisitoare. Pentru securizare avem nevoie de oameni instruiți și de resurse financiare. Este importantă dezvoltarea culturii cibernetice în rândurile cetățenilor.

Când va fi creat CERT național?

Trebuie să fie luată o decizie în viitorul apropiat pentru crearea acestui instrument de reacție la incidentele și atacurile cibernetice. Conform Planului de Acțiuni, anul viitor urmează a fi creat CERT-național. Crearea acestuia presupune implicarea tuturor factorilor de decizie, inclusiv prestatorilor de servicii internet care sunt foarte sensibili la subiectul de a raporta și a informa despre incidente sau alte tipuri de informație sensibilă. Deocamdată, CERT-GOV-MD din cadrul Serviciului Tehnologiei Informaționale și a Securității Cibernetice este unicul punct de contact în materie de raportare a incidentelor cibernetice la nivel autorităților centrale**.** Suntem membri ai comunității internaționale TF – CSIRT Trusted Introducer - o comunitate la nivel european și FIRST (Forumul de reacție la incidente și echipele de securitate) care este lider global de răspuns la incidente de securitate cibernetică la nivel internațional. Sunt două comunități foarte importante. Noi participăm la conferințele internaționale și regionale, unde discutăm despre bunele practici în domeniul securității cibernetice. Cea mai mare problemă în raport cu activitatea noastră este că nu primim reacții la incidentele cibernetice raportate instituțiilor responsabile de asigurarea ordinii publice. Am vrea să știm dacă cei care încalcă legea au fost reținuți, care sunt pagubele comise de activitatea infracțională și cum am îmbunătăți activitatea noastră.

CERT-național va rezolva problema raportării tuturor celor vizați și va facilita comunicarea. Sectorul privat a fost interesat și e deschis pentru colaborare și a ridicat nivelul de reziliență cibernetică prin proceduri sau politici proprii.

Trebuie să decidem competențele instituționale în domeniul securității cibernetice și să dotăm tehnic autoritățile și agențiile de stat. Trebuie să fie alocate mai multe resurse financiare din bugetul de stat pentru instruirea personalului, deoarece securitatea solicită sume importante de bani.

Care sunt platformele de colaborare la nivel internațional?

Amenințările provenite din spaţiul cibernetic sunt caracterizate de dinamism şi asimetrie, având caracteristici globale. Aceste trăsături le fac greu de identificat şi neutralizat prin măsuri izolate la nivelul statelor. Astfel, devine pregnantă necesitatea de cooperare a tuturor entităților care au atribuții ce țin de asigurarea securității cibernetice, atât în spațiul public, cât şi în cel privat.

Cooperarea a fost intensificată în ultima perioadă pe plan internaţional în vederea adoptării unor răspunsuri adecvate la ameninţările provenite din mediul virtual.

Am pus accentul pe intensificarea eforturilor de colaborare la nivel bilateral, precum și în cadrul organizaţiilor internaţionale. Obiectivul este de a dezvolta proiecte în domeniul securității cibernetice de instruire a specialiștilor pentru a răspunde noilor ameninţări cibernetice. De asemenea, suntem interesați de cele mai bune practici și tehnici de remediere a daunelor

provocate de atacurile cibernetice, dezvoltând programe de cooperare bilaterală pentru asigurarea securităţii cibernetice. Colaborarea cu Uniunea Internațională a Telecomunicațiilor (UIT), Departamentul de Stat al Statelor Unite ale Americii și Pacific Northwest National Laboratory (PNNL), Institutul de Inginerie Software (SEI), Universitatea Carnegie Mellon, OSCE (Capacity Building Measures), FIRST, George C. Marshall Center, NATO oferă posibilitatea de a prelua cele mai bune practici, de a organiza în comun conferințe, workshop-uri, exerciții, vizite de lucru. Rezultatele acestor colaborări sunt ulterior implementate în Republica Moldova.

Colaborăm cu UE prin *Programul „EU4Digital în Republica Moldova: Armonizarea piețelor digitale în Parteneriatul Estic”* care sprijină țările Parteneriatului Estic, inclusiv în domeniul securității cibernetice.

Dezvoltăm cooperarea bilaterală cu CERT din România, Ucraina și Georgia. E foarte important să ai prieteni și să știi cine sunt prietenii pe care poți să contezi în cazul unor atacuri cibernetice. Timpul de reacție este important și, de aceea, trebuie aplicate cele mai bune practici existente pentru a răspunde la incidentele cibernetice.

Cadrul legal privind transpunerea Acordului de Asociere în noiembrie 2019

ORDINUL MINISTERULUI AFACERILOR EXTERNE ȘI INTEGRĂRII EUROPENE

Ordinul nr. 182-s-10 din 12 noiembrie 2019 cu privire la alinierea la măsuri restrictive internaţionale ale Uniunii Europene, Monitorul Oficial nr. 315-319 din 25.10.2019 Alinierea Republicii Moldova la măsurile restrictive internaţionale instituite prin Decizia Consiliului 2019/1596 din 26.09.2019 de modificare a Deciziei 2017/2074 privind măsurile restrictive având în vedere situaţia din Venezuela.

Evenimente desfășurate în noiembrie 2019 în relația Republica Moldova–UE

12 noiembrie

Uniunea Europeană oferă 39,94 milioane de euro pentru construcția stației Back-to-Back în Vulcănești

Cabinetul de miniștri a aprobat Proiectul Hotărârii de Guvern cu privire la aprobarea proiectului de lege privind ratificarea Acordului de grant dintre Republica Moldova, Î.S. „Moldelectrica” şi Banca Europeană pentru Reconstrucție și Dezvoltare (BERD) privind implementarea proiectului „Interconectarea rețelelor de energie electrică dintre Republica Moldova şi România, faza I”, în valoare de 39,94 milioane de euro, semnat la 26 septembrie 2019.

Scopul proiectului este de a interconecta sistemul electroenergetic al Republicii Moldova cu cel al României și integrarea în piața regională de energie electrică a Uniunii Europene.

12 noiembrie

La Copenhaga s-a desfășurat Cea de-a 4-a reuniune a Comitetului de Supraveghere a Proiectului ENI SEIS II

Copenhaga a găzduit cea de-a 4-a reuniune a Comitetului de Supraveghere a Proiectului ENI SEIS II, care a prezentat informații despre implementarea proiectului pentru perioada anului 2019 în țările din cadrul Parteneriatului Estic. Totodată au fost discutați pașii următori, activitățile planificate pentru anii 2019-2020 și perspectivele viitoare.

Proiectul regional ENI-SEIS II East este finanţat de către Uniunea Europeană, prin Instrumentul Vecinătăţii Estice şi implementat de către Agenţia Europeană de Mediu (AEM).

Obiectivul general al proiectului este de a sprijini punerea în aplicare a principiilor și practicilor sistemului comun/partajat de informaţii privind mediul (SEIS) și de a consolida procesul de raportare periodică, inclusiv elaborarea și implementarea indicatorilor de mediu.

13–15 noiembrie

Centrul Național pentru Protecția Datelor cu Caracter Personale a organizat un curs de instruire despre protecția datelor cu caracter personal în domeniul educației

În perioada 13-15 noiembrie 2019, experți europeni din cadrul Proiectului Twinning UE „Consolidarea capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal" în colaborare cu CNPDCP au organizat un curs de instruire în domeniul educației. Au participat 84 de reprezentanți ai instituțiilor de învățământ timpuriu, primar și secundar (gimnanzii și licee) din municipiul Chișinău.

Participanții au discutat despre drepturile subiecților de date cu caracter personal prin prisma proiectului de lege privind protecția datelor cu caracter personal, analiza comparativă a drepturilor subiecților de date cu caracter personal din legea actuală privind protecția datelor cu caracter personal, principiile de prelucrare a datelor cu caracter personal, atribuțiile și obligațiile CNPDCP, etc.

14 noiembrie

A fost organizat seminarul privind implementarea și aplicarea Eurocodurilor în Republica Moldova

Seminarul a fost organizat în cadrul Proiectului „Implementarea și aplicarea Eurocodurilor în Republica Moldova și sporirea accesului la standardele europene". Scopul proiectului este de a fortifica capacitățile instituțiilor implicate în procesul de proiectare, producere a materialelor de construcții şi inginerie.

Utilizarea standardelor europene în construcții va facilita accesul investitorilor străini pe piața Republicii Moldova, precum şi va contribui la participarea companiilor de construcții din țară, în cadrul proiectelor internaționale.

20–22 noiembrie

Centrul Național pentru Protecția Datelor cu Caracter Personale a organizat un curs de instruire despre protecția datelor cu caracter personal în domeniul administrației publice centrale și locale

Experții europeni din cadrul Proiectului Twinning al UE „Consolidarea capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal" au organizat în colaborare cu CNPDCP un nou curs de instruire în domeniul de activitate a administrației publice centrale și locale.

Au participat aproximativ 60 de angajați ai cancelariei de Stat, inclusiv din cadrul oficiilor teritoriale din republică. Agenda cursului de instruire a inclus subiecte cu privire la legislația internațională din domeniul protecției datelor cu caracter personal, precum și noile prevederi ale proiectului de lege național privind protecția datelor cu caracter personal. Participanții au fost familiarizați cu conceptele de „operator de date", „persoană împuternicită", determinarea rolului părților în cadrul

unei prelucrări, principiile și temeiurile legale de prelucrare a datelor cu caracter personal, obținerea și administrarea consimțământului subiectului de date, drepturile subiecților de date și modul de realizare ale acestora.

27 noiembrie

Reuniunea Consiliului Consultativ al EUBAM a fost organizată la Chișinău

În incinta Ministerului Afacerilor Externe și Integrării Europene s-a desfășurat cea de-a 33-a reuniune a Consiliului Consultativ al Republicii Moldova și Ucrainei – EUBAM la care au participat reprezentanții serviciilor vamale și de frontieră ale Republicii Moldova și Ucrainei, precum și reprezentanții Delegației UE în Moldova, Misiunii OSCE în Moldova și Organizației Internaționale pentru Migrație.

A fost audiat raportul șefului Misiunii EUBAM, generalul Slavomir Pichor, cu privire la activitatea desfășurată în perioada iunie – octombrie 2019, în care au fost elucidate măsurile întreprinse în vederea modernizării managementului integrat al frontierei de stat moldo-ucrainene, inclusiv pe sectorul transnistrean al acesteia, în conformitate cu standardele europene în acest domeniu.

IDIS "Viitorul" reprezintă o instituție de cercetare, instruire și inițiativă publică, care activează pe o serie de domenii legate de: analiză economică, guvernare, cercetare politică, planificare strategică și management al cunoștințelor în Republica Moldova

www.viitorul.org

Acest buletin informativ apare în cadrul proiectului „Fact Checking of the Association Agreement Implementation" susținut financiar de Ambasada Regatului Țărilor de Jos

Kingdom of the Netherlands