Noua strategie de securitate cibernetică a UE pentru Deceniul Digital și impactul său pentru România

29.12.2020

Pe 16 decembrie 2020, Comisia Europeană și Înaltul Reprezentant al Uniunii pentru afaceri externe și politică de securitate au prezentat noua **Strategie de Securitate Cibernetică a Uniunii Europene (UE)**. Aceasta are implicații semnificative pentru toate Statele Membre ale UE.

Elementele principale ale strategiei

Noua strategie de securitate cibernetică stabilește modul în care UE va reacționa mai bine la atacurile cibernetice pe scară largă asupra cetățenilor, guvernelor, industriilor și instituțiilor, precum și modul în care UE ar putea fi lider global pentru un Internet securizat și deschis.

Strategia se bazează pe 3 instrumente principale, care abordează 4 domenii de intervenție a UE:

1. **Reziliență, suveranitate tehnologică și poziția de lider** prin reformarea normelor pentru securitatea rețelelor și a sistemelor informatice în cadrul unei Directive privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune.

2. **Consolidarea capacității operaționale** de prevenire, descurajare și reacție la atacurile și crizele cibernetice. Sprijinirea statelor membre UE în vederea protejării cetățenilor și a intereselor de securitate națională.

3. **Promovarea unui spațiu cibernetic global și deschis.** UE va colabora cu partenerii externi pentru promovarea unui model politic și a unei viziuni comune în care statul de drept, drepturile omului, libertatea și democrația să fie respectate.

4. **Securitatea cibernetică în instituțiile, organismele și agențiile UE.** Comisia Europeană dorește o abordare interinstituțională la nivel UE, atât privind modul de gestionare a informațiilor clasificate, cât și a informațiilor sensibile neclasificate.

Detalii ale domeniilor de intervenție ale Uniunii Europene

Inițiativele strategice ale Comisiei Europene în cadrul pilonului „Reziliență, suveranitate tehnologică și poziția de lider”

- Adoptarea Directivei NIS 2.0
- Revizuirea propunerii unei noi Directive a UE privind reziliența infrastructurilor critice
- Construirea unui scut european de securitate cibernetică
- Propunerea pentru un cod de rețea pentru securitatea cibernetică în fluxurile transfrontaliere de energie electrică
- Propunerea de Regulament privind reziliența operațională digitală a sectorului financiar
- Infrastructură de comunicații ultra-securizată
- Securizarea rețelelor mobile 5G
- Reglementare privind cerințele de securitate cibernetică pentru IoT și serviciile asociate
- O securitate sporită a Internetului prin crearea unui serviciu securizat de tip DNS european

Adoptarea Directivei NIS 2.0:

- Comisia propune reformarea normelor privind securitatea rețelelor și a sistemelor informatice în cadrul unei Directive NIS (Directiva NIS 2.0) cu obiectivul de a întări reziliența cibernetică a sectoarelor publice și private critice: spitalele, rețelele energetice, căile ferate, dar și centrele de date, administrația publică, laboratoarele de cercetare și centrele care fabrică dispozitive medicale și medicamente, precum și alte infrastructuri și servicii critice.
- Propunerea de Directivă NIS 2.0 va fi supusă spre dezbatere și aprobare în Parlamentul European. NIS 2.0 va rămâne în continuare o directivă și nu un regulament.
- Definiția Operatorilor de Servicii Esențiale (OES) se va transforma în „entități esențiale” pentru a include organizații din sectorul de sănătate, infrastructura digitală, industria aerospațială și administrația publică.
- Furnizorii de servicii digitale se vor transforma în „entități importante”, inclusiv companiile poștale, de curierat, de producție, de tehnologie (magazine și piețe online, motoare de căutare, platforme de servicii de rețele sociale și altele).
- În ceea ce privește intrarea în vigoare/aplicarea Directivei NIS 2.0, autoritățile competente trebuie să supravegheze ex-ante „entitățile esențiale”, în timp ce „entitățile importante” vor fi supravegheate atunci când există dovezi sau indicii că entitatea nu îndeplinește cerințele de securitate prevăzute.
- Amenzile prevăzute pot consta în minimum 2% din cifra de afaceri anuală, fără a depăși însă suma de 10.000.000 euro.
- Companiile vor avea obligația de a-și informa clienții și furnizorii atunci când infrastructurile au fost compromise în urma unui atac cibernetic.
- O bază de date gestionată de ENISA pentru publicarea coordonată a vulnerabilităților.
- Statele Membre ale UE vor intensifica schimbului de informații și cooperarea privind gestionarea riscurilor, a incidentelor și crizelor cibernetice la nivel național și la nivelul UE.

Revizuirea propunerii unei noi Directive a UE privind reziliența infrastructurilor critice.

Construirea unui scut european de securitate cibernetică:

- Comisia propune, de asemenea, lansarea la nivelul întregii UE a unei rețele de centre de operațiuni de securitate (SOC) bazată pe Artificial Intelligence (AI, inteligență artificială). SOC-urile vor fi ajutate în detectarea incidentelor, analiză și activitățile de răspuns de capabilitățile de Artificial Intelligence (AI), Machine Learning (ML) și EU High-Performance Computing Joint Undertaking.

- Rețeaua de SOC-uri va sprijini instruirea și dezvoltarea abilităților personalului care operează aceste centre și ar putea avea un buget de până la 300.000.000 euro.
- SOC-urile vor partaja mai eficient datele cu structurile de tip ISAC, autoritățile naționale și Joint Cyber Unit (JCU), pentru a genera cunoștințe colective despre amenințările cibernetice și pentru a împărtăși cele mai bune practici.

Propunerea pentru un cod de rețea pentru securitatea cibernetică în fluxurile transfrontaliere de energie electrică (Q4 2022).

Propunerea de Regulament privind reziliența operațională digitală a sectorului financiar (Digital Operational Resilience Act – DORA).

Infrastructură de comunicații ultra-securizată. Statele membre vor colabora cu Comisia și cu Agenția Spațială Europeană pentru a dezvolta o infrastructură cuantică sigură de comunicații (QCI) construită cu tehnologie UE. Aceasta va oferi posibilitatea de a transmite informații confidențiale folosind o formă de criptare ultra-securizată.

Securizarea rețelelor mobile 5G. Se propun obiective și acțiuni cheie pentru dezvoltarea în continuare a unui cadru de securitate 5G optim. UE și statele membre vor trebui să asigure că riscurile generate de rețelele 5G sunt identificate și abordate într-un mod coordonat. Statele membre se vor concentra asupra furnizorilor cu risc ridicat, evitând dependență de aceștia.

Noi măsuri de reglementare privind cerințele de securitate cibernetică pentru Internet of Things (IoT, dispozitive conectate) și serviciile asociate. Comisia Europeană are în vedere noi reguli orizontale privind securitatea cibernetică a acestora. Acestea vor genera o noi responsabilități ale producătorilor de dispozitive conectate, care vor trebui să rezolve vulnerabilitățile, să actualizeze continuu software-ul implicat și să șteargă datele cu caracter personal la sfârșitul duratei de viață a produsului.

O securitate sporită a Internetului prin crearea unui serviciu securizat de tip DNS european. Comisia Europeană va încuraja companiile din UE, furnizorii de servicii Internet, furnizorii de browsere să adopte o decizie de diversificare a strategiei Domain Name System (DNS) pentru a reduce concentrarea pe piață, în cadrul inițiativei DNS4EU. Se va accelera adoptarea standardelor cheie precum IPv6, standarde de securitate pentru DNS, rutare sau securitate a email-ului.

Crearea unui Observator de Internet în cadrul Centrului European de Competențe Industriale, Tehnologice și de Cercetare în Domeniul Securității Cibernetice (ECCC, găzduit de București, România), pentru a monitoriza și a culege date agregate privind traficul Internet și ale potențialelor perturbări.

Inițiativele strategice ale Comisiei Europene în cadrul pilonului „Consolidarea capacității operaționale de prevenire, descurajare și reacție la atacurile și crizele cibernetice”

- Joint Cyber Unit (JCU)
- Crearea EU Cyber Intelligence Working Group
- Un plan de acțiune privind sinergia dintre industria civilă, de apărare și industria spațială

Joint Cyber Unit (JCU): până în februarie 2021 Comisia Europeană va prezenta procesul, etapele de referință și calendarul pentru definirea, pregătirea, desfășurarea și extinderea JCU. Aceasta nu necesită înființarea unei noi agenții a UE, ci se bazează pe instituțiile și mecanismele existente. Rolul principal al JCU este îmbunătățirea, accelerarea, facilitarea cooperării operaționale și tehnice în cazurile de incidente și amenințări cibernetice transfrontaliere majore. JCU va fi un loc pentru comunitățile de securitate cibernetică, inclusiv experți în domeniile civil, diplomatic, aplicarea legii și apărare, pentru a se întâlni și a schimba informații, dar și pentru a asigura o cooperare operațională deschisă cu sectorul privat.

JCU are 3 obiective principale: (i) asigurarea pregătirii pentru toate comunitățile de securitate cibernetică, (ii) asigurarea unei conștientizări situaționale continue, prin schimbul continuu de informații și (iii) consolidarea răspunsului coordonat și a revenirii la normal, în cazul unor atacuri sau crize cibernetice majore.

În plus, se va continua lucrul la proiectul SIRIUS, care se ocupă de dovezi electronice și care îmbunătățește capacitatea de tratare a elementelor criptografice specifice anchetelor penale derulate de agențiile de aplicare a legii europene;

Crearea EU Cyber Intelligence Working Group, ca grup de lucru al UE pentru analiza informațiilor din spațiu cibernetic în cadrul Centrului de situații și analiză a informațiilor al UE (INTCEN) al European External Action Service (EEAS) unde Statele membre vor participa la cooperarea strategică pe linie de informații privitor la activitățile și amenințările cibernetice.

De asemenea, UE își va consolida cooperarea cu partenerii internaționali, inclusiv cu NATO. Atât UE cât și Statele Membre își vor spori capacitatea de prevenire, descurajare și răspuns la amenințările de securitate cibernetică.

Un plan de acțiune privind sinergia dintre industria civilă, de apărare și industria spațială în primul trimestru al anului 2021 și va lucra pentru a asigura securitatea cibernetică a infrastructurii spațiale critice, responsabilitate prevăzută a fi în cadrul Programului Spațial al viitoarei Agenții Europene pentru Programul Spațial, care va fi găzduită la Praga.

Inițiativele strategice ale Comisiei Europene în cadrul pilonului „Promovarea unui spațiu cibernetic global și deschis”

- Noua strategie de standardizare în domeniul securității cibernetice
- Cooperarea cu partenerii și comunitatea părților interesate
- Rețeaua UE de diplomație cibernetică
- Consolidarea capacităților globale și atenuarea amenințărilor cibernetice
- Noua Agendă externă de consolidare a capacității cibernetice a UE

Noua strategie de standardizare în domeniul securității cibernetice, în care UE își va defini obiectivele de angajament și planul de acțiune pentru standardizarea internațională.

UE își va intensifica angajamentul și va dori să preia rolul conducător al proceselor de standardizare la nivel internațional, precum și al organismelor implicate în ceea ce privește standardele, normele și cadrele de lucru. UE va colabora cu statele membre la consolidarea și promovarea normelor internaționale și a valorilor europene în spațiul cibernetic, prin dezvoltarea unei poziții comune cu privire la aplicarea dreptului internațional în acest domeniu.

Cooperarea cu partenerii și comunitatea părților interesate. UE va continua și va întări dialogul în domeniul cibernetic cu țări terțe și organizații regionale. Se va consolida cooperarea UE-NATO în domeniile schimbului de informații, gestionării crizelor, standardelor, educației, pregătirii și exercițiilor. Uniunea va continua să lucreze la cooperarea multilaterală în probleme de securitate cibernetică, prin consolidarea dialogurilor și schimburilor periodice și regulate cu sectorul privat.

Rețeaua UE de diplomație cibernetică va fi întărită și extinsă pentru a promova activ viziunea UE asupra spațiului cibernetic, schimbul de informații și coordonarea.

Consolidarea capacităților globale și atenuarea amenințărilor cibernetice. UE va continua să sprijine partenerii săi externi pentru a-și spori reziliența cibernetică și capacitățile în domeniul investigațiilor privind criminalitatea cibernetică și amenințărilor cibernetice.

Noua Agendă externă de consolidare a capacității cibernetice a UE pentru dezvoltarea consolidată și coordonată a capacităților în țări terțe, în special pentru Balcanii de Vest și vecinătatea UE.

Inițiativele strategice ale Comisiei Europene în cadrul pilonului „Securitatea cibernetică în instituțiile, organismele și agențiile UE”

- Noi norme obligatorii privind securitatea informațiilor și cea cibernetică
- Investiții sporite pentru a ajuta instituțiile UE
- Program de conștientizare privind securitatea și igiena cibernetică
- Consolidare și un nou mandat pentru CERT-EU

Norme obligatorii privind securitatea informațiilor și cea cibernetică pentru toate instituțiile UE.

Investiții sporite pentru a ajuta instituțiile UE să ajungă la același nivel ridicat de maturitate din punct de vedere al securității cibernetice.

Program de conștientizare: securitatea și igiena cibernetică pentru personalul instituțiilor UE.

Consolidare și definirea unui nou mandat pentru CERT-EU.

Concluzie

Securitatea cibernetică este una dintre principalele priorități ale Comisiei și una dintre pietrele de temelie ale Europei digitale și conectate. Creșterea numărului de atacuri cibernetice în timpul crizei provocate de pandemia SARS-CoV-2 a demonstrat importanța protejării spitalelor, a centrelor de cercetare, a instituțiilor administrației publice și a economiei în general.

Noua Strategie de Securitate Cibernetică a Uniunii Europene propune integrarea securității cibernetice în economie, în fiecare element al lanțului de aprovizionare și corelarea într-o mai mare măsură a activităților și a resurselor UE în cadrul celor patru comunități ale securității cibernetice – piața internă, asigurarea respectării legii, sectorul diplomației și cel al apărării.

Prin această strategie, Comisia prezintă europenilor o agendă pe cât de ambițioasă, pe atât de necesară următorului Deceniu Digital.

Mai mult, având în vedere că România a lansat procesul de actualizare a **Strategiei Naționale de Securitate Cibernetică**, este important ca aceasta să ia în considerare evoluțiile la nivel european, iar cadrul normativ național să fie adaptat corespunzător pentru a răspunde la nivel instituțional noilor cerințe ale Uniunii Europene, pe care țara noastră trebuie să și le asume.

Pentru a reuși implementarea noilor obiective și priorități trasate de către Comisie prin noua Strategie de Securitate Cibernetică a UE, România are nevoie de un cadru instituțional matur, caracterizat prin stabilitate, agilitate, independență și o strânsă cooperare.

Un element pozitiv este că prin propunerea de OUG pentru înființarea **Directoratului Național de Securitate Cibernetică (DNSC)** s-au anticipat majoritatea recentelor evoluții în domeniul securității cibernetice la nivel european și s-au definit în mod transparent, obiectiv și pragmatic schimbările instituționale civile necesare a fi făcute de către Guvernul României pentru a transpune cu celeritate noile repere legislative europene.

Directoratul ar urma să fie acel actor instituțional civil cu un rol-cheie în sprijinirea sau adoptarea noilor măsuri strategice și operaționale cerute de Comisia Europeană, pentru ca **România să fie unul din liderii recunoscuți** ai implementării noii Strategii de Securitate Cibernetică a UE.

În acest context, având în vedere recentele cerințe ale securității cibernetice din partea UE precum și necesitățile naționale, este imperios necesară continuarea coordonării directe a CERT-RO și ulterior, a Directoratului de către Prim-ministrul României, pentru a se reuși implementarea obiectivelor și priorităților trasate de către Comisie prin noua Strategie de Securitate Cibernetică.

Aceasta va aduce autoritatea necesară pentru a garanta îndeplinirea responsabilităților asumate România la nivel european, prin prisma recentelor evoluții ale domeniului securității cibernetice.