



AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ

O EUROPĂ DE ÎNCREDERE ȘI SIGURĂ DIN PUNCT DE VEDERE CIBERNETIC

Strategia ENISA

Iunie 2020



O EUROPĂ DE
ÎNCREDERE
ȘI SIGURĂ DIN
PUNCT DE
VEDERE CIBERNETIC

AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ



CUVÂNT ÎNAINTE

De mai bine de 15 ani, ENISA – Agenția Uniunii Europene pentru Securitate Cibernetică – joacă un rol cheie în stimularea obiectivului ambițios al UE de a consolida încrederea și securitatea digitală în întreaga Europă, împreună cu statele membre și cu instituțiile și agențiile UE. Reunind comunitățile, ENISA a contribuit cu succes la consolidarea capacităților de pregătire și răspuns ale Europei la incidentele cibernetice.

În același timp, digitalizarea economiei și a societății noastre s-a intensificat mult, după cum s-a demonstrat în timpul crizei COVID-19, când un apel colectiv și masiv la soluții IT la distanță a fost esențial pentru a menține multe activități. Această criză a evidențiat cât de mult profită atacatorii cibernetici de dependența noastră de aceste tehnologii. De asemenea, a revelat modul în care amenințările cibernetice s-au extins de la atacuri țintite la noi forme de amenințări de masă pentru milioane de companii și cetățeni, inclusiv un număr tot mai mare de incidente sofisticate de tip ransomware. Dezvoltarea rapidă a produselor și serviciilor digitale, de la cele de tip cloud și videoconferință la 5G și IA, a adus, de asemenea, noi provocări de descoperit și de abordat.

Cu un mandat permanent și sarcini și capacități îmbunătățite, ENISA are, mai mult ca oricând, menirea de a juca un rol de lider în a ajuta UE și statele sale membre să țină pasul cu aceste provocări, în contextul apariției unei noi ere pentru securitatea cibernetică în Europa.

Pentru a face acest lucru, ENISA va depune eforturi pentru a anticipa tendințele relevante și pentru a atrage și disemina expertiză și cunoștințe de ultimă oră pentru toți.

Agenția va sprijini Comisia Europeană și statele membre în demersurile lor de a ajuta actorii publici și privați și cetățenii să prevină și să gestioneze riscurile asociate incidentelor cibernetice. Odată cu punerea în aplicare a cadrului pentru certificarea de securitate cibernetică, ENISA va contribui la o schimbare de paradigmă prin îmbunătățirea nivelului de securitate a soluțiilor digitale implementate în Europa. Procedând astfel, va crește capacitatea tuturor de a alege și de a investi încredere. De asemenea, agenția va sprijini în mod activ comunitatea operațională europeană în materie de securitate cibernetică în cooperarea strânsă și pregătirea unui răspuns comun atunci când următorul incident cibernetic la scară largă va lovi Europa.

Pe măsură ce ENISA își asumă noul său rol, deschiderea, agilitatea și fiabilitatea vor fi factori-cheie în operațiunile sale zilnice în cadrul colaborării mai strânse cu statele membre și cu Comisia Europeană în alinierea abordărilor. ENISA se va strădui, de asemenea, să își îmbunătățească impactul asupra mediului în contextul crizei climatice actuale și să fie un mediu de lucru favorabil incluziunii și responsabil din punct de vedere social.

Acest document de strategie, elaborat prin implicarea întregului personal al ENISA, a membrilor Consiliului său de administrație și a grupului său consultativ într-un proces de colaborare și incluziune, stabilește obiectivele clare care vor conduce activitatea ENISA în următorii ani pentru a face față numeroaselor provocări viitoare.

În numele Consiliului de administrație

Jean-Baptiste Demaison

Președintele Consiliului de administrație

Krzysztof Silicki

Vicepreședintele Consiliului de administrație

VIZIUNE

O Europă de încredere și sigură din punct de vedere cibernetic

MISIUNE

Misiunea Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) este de a atinge un nivel comun înalt de securitate cibernetică în întreaga Uniune, în cooperare cu comunitatea extinsă. Acest lucru se realizează acționând ca un centru de expertiză în domeniul securității cibernetică, colectând și oferind consultanță tehnică independentă și de înaltă calitate, precum și asistență statelor membre și organismelor UE în domeniul securității cibernetică. Agenția contribuie la dezvoltarea și punerea în aplicare a politicilor cibernetică ale Uniunii.

Scopul nostru este de a consolida încrederea în economia conectată, de a spori reziliența și încrederea în infrastructura și serviciile Uniunii și de a menține securitatea digitală a societății și a cetățenilor. Aspirăm să fim o organizație agilă, responsabilă din punct de vedere ecologic și social și concentrată pe oameni.

VALORI

Atitudine axată pe comunitate

ENISA lucrează cu comunitățile, respectându-le competențele și expertiza, și încurajează sinergiile și încrederea pentru a-și îndeplini cel mai bine misiunea.

Exelență

În activitatea sa, ENISA își propune să folosească expertiză de ultimă oră, susține cele mai înalte standarde de calitate ale operațiunilor și își evaluează performanța pentru îmbunătățirea continuă prin inovare și previziune.

Integritate/etică

ENISA susține principiile etice, precum și normele și obligațiile relevante ale UE în serviciile sale și mediul său de lucru, asigurând echitate și incluziune.

Respect

ENISA respectă drepturile și valorile fundamentale europene care acoperă toate serviciile sale și mediul său de lucru, precum și așteptările părților interesate.

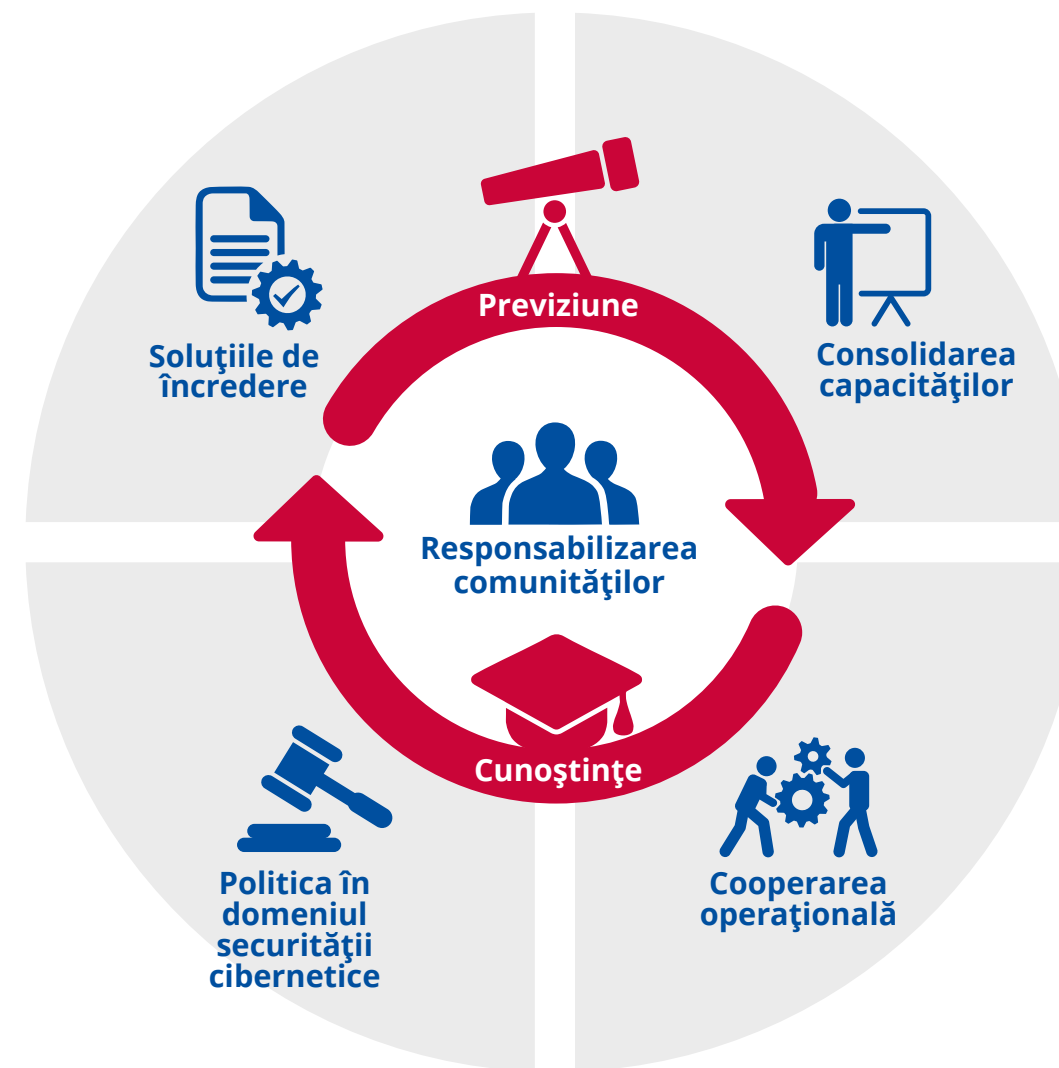
Responsabilitate

ENISA își asumă responsabilitatea, asigurând astfel integrarea dimensiunilor sociale și de mediu în practici și proceduri.

Transparență

ENISA adoptă proceduri, structuri și procese deschise, factuale și independente, limitând astfel prejudecățile, ambiguitățile, fraudă și lipsa de transparență.

OBIECTIVE STRATEGICE



OS1

Obiectiv strategic

“

COMUNITĂȚI RESPONSABILIZATE ȘI IMPLICATE ÎN ECOSISTEMUL DE SECURITATE CIBERNETICĂ

Context

Securitatea cibernetică este o responsabilitate comună. Europa își propune să creeze un cadru de cooperare transsectorială integrală . ENISA joacă un rol cheie în stimularea cooperării active între părțile interesate în materie de securitate cibernetică din statele membre și instituțiile și agențiile UE. Agenția dorește să asigure complementaritatea eforturilor comune, adăugând valoare părților interesate, explorând sinergiile și utilizând în mod eficient expertiza și resursele limitate în domeniul securității cibernetică. Comunitățile ar trebui să aibă capacitatea să amplifice modelul de securitate cibernetică.

Ce dorim să realizăm

- Un ansamblu de cunoștințe de ultimă oră la nivelul UE cu privire la conceptele și practicile de securitate cibernetică, care să stimuleze cooperarea între actorii-cheie în materie de securitate cibernetică, care să promoveze lecțiile învățate și expertiza UE și care să creeze noi sinergii.
- Un ecosistem cibernetic responsabil, care să cuprindă autoritățile statelor membre, instituțiile, agențiile și organismele UE, asociații, centre de cercetare și universități, industria, actori privați și cetățeni, care joacă toți un rol în asigurarea securității cibernetică a Europei.

OS2

Obiectiv strategic

“

SECURITATEA
CIBERNETICĂ, PARTE
INTEGRANTĂ A
POLITICILOR UE

Context

Securitatea cibernetică este piatra de temelie a transformării digitale, iar necesitatea sa se resimte în toate sectoarele, prin urmare, trebuie avută în vedere într-o gamă largă de domenii și inițiative politice. Securitatea cibernetică nu trebuie limitată la o comunitate specializată de experți tehnici în domeniul ciberneticii. Prin urmare, securitatea cibernetică trebuie să fie încorporată în toate domeniile politicii UE. Evitarea fragmentării și necesitatea unei abordări coerente sunt esențiale, luând în considerare în același timp particularitățile fiecărui sector.

Ce dorim să realizăm

- Sprijin și recomandări proactive pentru toți actorii relevanți la nivelul UE, care să integreze dimensiunea securității cibernetică în ciclul de viață al dezvoltării politicilor, prin orientări tehnice viabile și bine direcționate.
- Cadre de gestionare a riscurilor de securitate cibernetică care să fie implementate în toate sectoarele și respectate pe tot parcursul ciclului de viață al politicii de securitate cibernetică.

OS3

Obiectiv strategic

“

COOPERAREA EFICIENTĂ ÎNTRE ACTORII OPERAȚIONALI DIN CADRUL UNIUNII ÎN CAZ DE INCIDENTE CIBERNETICE MASIVE.

Context

Beneficiile economiei și societății digitale europene pot fi realizate pe deplin numai sub premisa securității cibernetice. Atacurile cibernetice nu cunosc frontiere. Pot fi afectate toate păturile sociale, iar Uniunea trebuie să fie pregătită să răspundă atacurilor cibernetice masive (la scară largă și transfrontaliere) și crizelor provocate de astfel de atacuri cibernetice. Interdependențele transfrontaliere au evidențiat necesitatea unei cooperări eficiente între statele membre și instituțiile UE pentru un răspuns mai rapid și o coordonare adecvată a eforturilor la toate nivelurile (strategic, operațional, tehnic și de comunicare).

Ce dorim să realizăm

- Sprijin transfrontalier și intersectorial continuu pentru cooperarea între statele membre, precum și cu instituțiile UE. Având în vedere în special potențialele incidente și crize la scară largă, sprijin pentru extinderea cooperării tehnice operaționale, politice și strategice între actorii operaționali cheie pentru a permite răspunsul în timp util, schimbul de informații, conștientizarea situației și comunicarea crizelor în întreaga Uniune.
- O abordare tehnică rapidă și cuprinzătoare, la cererea statelor membre, pentru a facilita nevoile tehnice și operaționale în gestionarea incidentelor și a crizelor.

OS4

Obiectiv strategic

“

COMPETENȚE ȘI CAPACITĂȚI DE VÂRF ÎN MATERIE DE SECURITATE CIBERNETICĂ ÎN ÎNTREAGA UNIUNE.

Context

Frecvența și complexitatea atacurilor cibernetice cresc într-un ritm rapid, în vreme ce utilizarea infrastructurilor și tehnologiilor TIC de către persoane, organizații și industrii crește cu aceeași rapiditate. Necesarul de cunoștințe și competențe privind securitatea cibernetică depășește resursele. UE trebuie să investească în dezvoltarea competențelor și talentelor în materie de securitate cibernetică la toate nivelurile, de la persoane nespecializate la profesioniști cu înaltă calificare. Investițiile ar trebui să se concentreze nu numai pe dezvoltarea capacităților în materie de securitate cibernetică în statele membre, ci și pe asigurarea faptului că diferitele comunități operaționale posedă capacitatea adecvată de a face față mediului marcat de amenințări cibernetice.

Ce dorim să realizăm

- Competențe cibernetice, experiență profesională și structuri educaționale aliniate pentru a satisface nevoile în continuă creștere de cunoștințe și competențe în materie de securitate cibernetică în UE.
- Un nivel de bază ridicat al conștientizării și competențelor în materie de securitate cibernetică în întreaga UE, integrând în același timp cibernetica în noile discipline.
- Capacități bine pregătite și testate, care să poată face față mediului caracterizat prin tot mai multe amenințări la nivelul UE.

OS5

Obiectiv strategic

“

UN NIVEL RIDICAT
DE ÎNCREDERE ÎN
SOLUȚII DIGITALE
SIGURE

Context

Produsele și serviciile digitale aduc atât beneficii, cât și riscuri, iar aceste riscuri trebuie identificate și atenuate. În procesul de evaluare a securității soluțiilor digitale și de asigurare a fiabilității acestora, este esențial să se adopte o abordare comună, cu scopul de a ajunge la un echilibru între nevoile societale, de piață, economice și de securitate cibernetică. O entitate neutră care acționează într-un mod transparent va crește încrederea clienților în soluțiile digitale și în mediul digital în ansamblu.

Ce dorim să realizăm

- Un mediu digital cibernetic securizat în întreaga UE, în care cetățenii să poată avea încredere în produsele, serviciile și procesele TIC, prin implementarea de sisteme de certificare în domeniile tehnologice cheie.

OS6

Obiectiv strategic

“

PREVIZIUNI ASUPRA
PROVOCĂRILOR
EMERGENTE ȘI VIITOARE
ÎN DOMENIUL SECURITĂȚII
CIBERNETICE

Context

Numeroase tehnologii noi, încă în fază incipientă sau aproape de adoptarea generală, ar putea profita de utilizarea metodelor de previziune. Prin intermediul unui proces structurat care să permită dialogul între părțile interesate, factorii de decizie și decidenții politici ar putea să definească strategii de atenuare timpurii care să îmbunătățească reziliența UE la amenințările de securitate cibernetică și să găsească soluții pentru a aborda provocările emergente.

Ce dorim să realizăm

- Înțelegerea tendințelor și tiparelor emergente folosind previziuni și scenarii viitoare care să contribuie la atenuarea provocărilor cibernetică cu care se confruntă părțile interesate.
- Evaluarea timpurie a provocărilor și riscurilor care decurg din adoptarea opțiunilor viitoare emergente și adaptarea la acestea, colaborând în același timp cu părțile interesate referitor la strategiile adecvate de atenuare.

OS7

Obiectiv strategic

“

GESTIONAREA EFICIENTĂ ȘI EFICACE A INFORMAȚIILOR ȘI CUNOȘTINȚELOR PRIVIND SECURITĂȚEA CIBERNETICĂ PENTRU EUROPA.

Context

Energia care alimentează „motorul” securității cibernetice o reprezintă informațiile și cunoștințele. Pentru ca profesioniștii în materie de securitate cibernetică să fie eficienți în abordarea obiectivelor noastre, să lucreze într-un mediu în continuă evoluție – în ceea ce privește atât progresele digitale, cât și actorii – pentru a face față provocărilor actuale, avem nevoie de un proces continuu de colectare, organizare, sintetizare, analizare, comunicare și întreținere informațiilor și cunoștințelor privind securitatea cibernetică. Toate fazele sunt esențiale pentru a se asigura că informațiile și cunoștințele sunt distribuite și extinse în cadrul ecosistemului UE de securitate cibernetică.

Ce dorim să realizăm

- Gestionarea partajată a informațiilor și a cunoștințelor pentru ecosistemul de securitate cibernetică al UE într-o formă accesibilă, personalizată, oportună și aplicabilă, cu metodologie, infrastructuri și instrumente adecvate, cuplate cu măsuri de asigurare a calității, pentru a realiza îmbunătățirea continuă a serviciilor.

DESPRE ENISA

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Legea UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică contribuie la politica cibernetică a UE, îmbunătățește fiabilitatea produselor, serviciilor și proceselor TIC prin sistemele de certificare a securității cibernetică, cooperează cu statele membre și cu organismele UE și ajută Europa să se pregătească pentru provocările cibernetică de mâine. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa pot fi găsite la adresa www.enisa.europa.eu



ENISA

Agenția Uniunii Europene pentru Securitate
Cibernetică

Biroul din Atena

1 Vasilissis Sofias
151 24 Marousi, Attiki, Grecia

Biroul din Heraklion

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grecia

enisa.europa.eu



9 789292 043537