Parlamentul European
2019-2024

Document de ședință

A9-0064/2023

10.3.2023

***I
RAPORT

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Comisia pentru industrie, cercetare și energie

Raportoare: Henna Virkkunen

Raportor pentru avizul comisiei asociate, în temeiul articolului 57 din Regulamentul de procedură:
Tomas Tobé, Comisia pentru libertăți civile, justiție și afaceri interne

Legenda simbolurilor utilizate

*	Procedura de consultare
***	Procedura de aprobare
***I	Procedura legislativă ordinară (prima lectură)
***II	Procedura legislativă ordinară (a doua lectură)
***III	Procedura legislativă ordinară (a treia lectură)

(Procedura indicată se bazează pe temeiul juridic propus în proiectul de act.)

Amendamente la un proiect de act

Amendamentele Parlamentului prezentate pe două coloane

Textul eliminat este evidențiat prin caractere ***cursive aldine*** în coloana din stânga. Textul înlocuit este evidențiat prin caractere ***cursive aldine*** în ambele coloane. Textul nou este evidențiat prin caractere ***cursive aldine*** în coloana din dreapta.

În primul și în al doilea rând din antetul fiecărui amendament se identifică fragmentul vizat din proiectul de act supus examinării. În cazul în care un amendament vizează un act existent care urmează să fie modificat prin proiectul de act, antetul conține două rânduri suplimentare în care se indică actul existent și, respectiv, dispoziția din acesta vizată de modificare.

Amendamentele Parlamentului prezentate sub formă de text consolidat

Părțile de text noi sunt evidențiate prin caractere ***cursive aldine***. Părțile de text eliminate sunt indicate prin simbolul ▌ sau sunt tăiate. Înlocuirile sunt semnalate prin evidențierea cu caractere ***cursive aldine*** a textului nou și prin eliminarea sau tăierea textului înlocuit.
Fac excepție de la regulă și nu se evidențiază modificările de natură strict tehnică efectuate de serviciile competente în vederea elaborării textului final.

CUPRINS

Pagina

PROIECT DE REZOLUȚIE LEGISLATIVĂ A PARLAMENTULUI EUROPEAN

referitoare la propunerea de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

(Procedura legislativă ordinară: prima lectură)

Parlamentul European,

– având în vedere propunerea Comisiei prezentată Parlamentului European și Consiliului (COM(2022)0122),

– având în vedere articolul 294 alineatul (2) și articolul 298 din Tratatul privind funcționarea Uniunii Europene, în temeiul cărora propunerea a fost prezentată de către Comisie (C9-0122/2022),

– având în vedere articolul 294 alineatul (3) din Tratatul privind funcționarea Uniunii Europene,

– având în vedere articolul 59 din Regulamentul său de procedură,

– având în vedere avizele Comisiei pentru libertăți civile, justiție și afaceri interne, Comisiei pentru bugete și Comisiei pentru afaceri constituționale,

– având în vedere raportul Comisiei pentru industrie, cercetare și energie (A9-0064/2023),

1. adoptă poziția sa în primă lectură prezentată în continuare;

2. solicită Comisiei să îl sesizeze din nou în cazul în care își înlocuiește, își modifică în mod substanțial sau intenționează să-și modifice în mod substanțial propunerea;

3. încredințează Președintei sarcina de a transmite Consiliului și Comisiei, precum și parlamentelor naționale poziția Parlamentului.

Amendamentul 1

AMENDAMENTELE PARLAMENTULUI EUROPEAN*

la propunerea Comisiei

2022/0085 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 298,

având în vedere Tratatul de instituire a Comunității Europene a Energiei Atomice, în special articolul 106a,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații transparente, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și proteja

* Amendamente: textul nou sau modificat este marcat cu caractere cursive aldine; textul eliminat este marcat prin simbolul ▌ .

datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației ***și comunicațiilor (TIC)***, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.

(2) Peisajul amenințărilor cibernetice cu care se confruntă ***entitățile*** Uniunii este într-o continuă evoluție. Tacticile, tehnicile și procedurile utilizate de actorii care generează amenințări sunt într-o continuă evoluție, în timp ce principalele motive ale acestor atacuri se schimbă foarte puțin, de la furtul de informații confidențiale valoroase până la sustragerea de bani, manipularea opiniei publice sau subminarea infrastructurii digitale. Ritmul în care își desfășoară atacurile cibernetice continuă să crească, în timp ce campaniile lor sunt din ce în ce mai sofisticate și automatizate, vizând suprafețe de atac expuse care continuă să se extindă și exploatând rapid vulnerabilitățile.

(3) Mediile ***TIC*** ale ***entităților*** Uniunii au interdependențe și fluxuri de date integrate, iar utilizatorii acestora colaborează îndeaproape. Această interconectare înseamnă că orice perturbare, chiar și atunci când este limitată inițial la o ***entitate*** a Uniunii, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea impacturi negative de amploare și de lungă durată asupra celorlalte. În plus, mediile ***TIC*** ale anumitor ***entități ale Uniunii*** sunt conectate cu cele ale statelor membre, ceea ce face ca un incident în cadrul unei entități a Uniunii să reprezinte un risc de securitate cibernetică a mediilor ***TIC*** ale statelor membre și viceversa.

(4) ***Entitățile*** Uniunii sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca ***entitățile*** Uniunii să atingă un nivel comun ridicat de securitate cibernetică ***prin punerea în aplicare a unor măsuri de gestionare a riscurilor*** de securitate cibernetică**,** ***proporționale cu*** riscurile ***relevante***, prin schimbul de informații și colaborarea în acest domeniu.

(5) ***Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului***[1] urmărește să îmbunătățească și mai mult capacitatea de reziliență și capacitatea de răspuns la incidente ale entităților publice și private, ale autorităților și organelor naționale competente, precum și ale Uniunii în ansamblu. Prin urmare, este necesar ca ***entitățile*** Uniunii să urmeze exemplul prin asigurarea unor norme care să fie coerente cu ***Directiva (UE) 2022/2555*** și să reflecte nivelul său de ambiție.

(6) Pentru a atinge un nivel comun ridicat de securitate cibernetică, este necesar ca fiecare ***entitate*** a Uniunii să instituie un cadru intern de gestionare a riscurilor***, administrare a incidentelor***, guvernanță și control al riscurilor de securitate cibernetică, care să asigure o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică și să țină seama de gestionarea continuității activității și de gestionarea crizelor. ***Cadrul ar trebui să stabilească politici și priorități în materie de securitate cibernetică pentru securitatea rețelelor și a sistemelor informatice, care să cuprindă întregul mediu TIC. Cadrul ar trebui revizuit periodic și cel puțin o dată la trei ani.***

(7) Diferențele dintre ***entitățile*** Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică nu ar trebui să includă nicio obligație care să interfereze în mod direct cu exercitarea misiunilor ***entităților*** Uniunii sau să aducă atingere autonomiei lor instituționale. ***De aceea***, aceste ***entități*** ar trebui să își stabilească propriile cadre pentru gestionarea riscurilor***, administrarea incidentelor***, guvernanța și controlul riscurilor de securitate cibernetică și să își adopte ***propriile măsuri de gestionare a riscurilor de securitate cibernetică și*** propriile planuri ▌de securitate cibernetică***, care să acopere întregul mediu TIC al entității. Entitățile Uniunii ar trebui să evalueze în permanență eficacitatea măsurilor de gestionare a riscurilor adoptate și proporționalitatea lor în raport cu riscurile identificate și, dacă este necesar, să își adapteze și să își revizuiască în consecință cadrele și planurile pe baza rezultatelor evaluărilor maturității în materie de securitate cibernetică.***

[1] ***Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).***

(7a) Obligația recurentă de a efectua evaluări ale maturității în materie de securitate cibernetică ar putea crea o sarcină suplimentară și disproporționată pentru entitățile mici ale Uniunii și cu resurse TIC limitate. Prin urmare, prezentul regulament ar trebui să prevadă posibilitatea ca două sau mai multe entități ale Uniunii să creeze echipe comune pentru efectuarea evaluărilor maturității în materie de securitate cibernetică și să beneficieze de avantajele care rezultă din combinarea resurselor și a expertizei.

(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra ***entităților*** Uniunii, cerințele de gestionare a riscurilor de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare ***entitate*** a Uniunii ar trebui să urmărească alocarea unui procent adecvat din bugetul său în domeniul ***TIC*** pentru a-și îmbunătăți nivelul de securitate cibernetică; pe termen lung, ar trebui să se urmărească atingerea unui obiectiv de ***cel puțin*** 10 %.

(9) Pentru asigurarea unui nivel comun ridicat de securitate cibernetică, aceasta trebuie să se afle sub supravegherea celui mai înalt nivel de conducere al fiecărei ***entități a Uniunii***, care ar trebui să ***supravegheze punerea în aplicare a dispozițiilor prezentului regulament și să*** aprobe ***instituirea și orice revizuire ulterioară a cadrului de gestionare și control al riscurilor, a măsurilor corespunzătoare de gestionare a riscurilor*** de securitate cibernetică ***care abordează*** riscurile identificate în ***cadru și a planurilor de securitate cibernetică ale fiecărei entități a Uniunii.*** Abordarea culturii securității cibernetice, adică practica zilnică în domeniul securității cibernetice, este parte integrantă a unui ***cadru de gestionare, guvernanță și control al riscurilor*** de securitate cibernetică ***și a măsurilor corespunzătoare de gestionare a riscurilor de securitate cibernetică în toate entitățile*** Uniunii.

(10) ***Entitățile*** Uniunii ar trebui să evalueze riscurile legate de relațiile cu furnizorii și prestatorii de servicii, inclusiv cu prestatorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate, și să ia măsurile adecvate pentru a combate astfel de riscuri. Aceste măsuri ***de gestionare a riscurilor*** de securitate cibernetică ***ar trebui*** să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor trebuie să se țină seama în mod corespunzător de

dreptul și politicile relevante ale **Uniunii**, inclusiv de evaluările riscurilor și de recomandările emise de ▌ Grupul de cooperare privind securitatea rețelelor și a informațiilor ***instituit prin Directiva (UE) 2022/2555***, cum ar fi evaluarea coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G. În plus, ***având în vedere peisajul amenințărilor și importanța consolidării rezilienței pentru entitățile Uniunii, trebuie să se solicite*** certificarea produselor, a serviciilor și a proceselor TIC relevante, în cadrul sistemelor ▌specifice de certificare a securității cibernetice ***ale Uniunii*** adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.

(11) În mai 2011, secretarii generali ai instituțiilor și organelor Uniunii au decis să constituie o echipă de preconfigurare a unui centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE), supervizată de un comitet director interinstituțional. În iulie 2012, secretarii generali au confirmat modalitățile practice și au convenit să mențină CERT-UE ca entitate permanentă, pentru a contribui în continuare la îmbunătățirea nivelului general de securitate a tehnologiei informației la nivelul instituțiilor, organelor și agențiilor Uniunii, ca exemplu de cooperare interinstituțională vizibilă în domeniul securității cibernetice. În septembrie 2012, CERT-UE a fost înființat ca grup operativ al Comisiei Europene, cu un mandat interinstituțional. În decembrie 2017, instituțiile și organele Uniunii au încheiat un acord interinstituțional privind organizarea și funcționarea CERT-UE[2]. Acest mecanism ar trebui să evolueze în continuare pentru a sprijini punerea în aplicare a prezentului regulament ***și ar trebui să fie evaluat periodic în lumina viitoarelor negocieri privind cadrele bugetare pe termen lung, care vor permite luarea unor decizii suplimentare în legătură cu funcționarea și rolul instituțional al CERT-UE, inclusiv posibila instituire a CERT-UE ca oficiu al Uniunii***.

(12) Denumirea CERT-UE ar trebui schimbată din „Centrul de răspuns la incidente de securitate cibernetică” în „Centrul de securitate cibernetică” pentru ***entitățile*** Uniunii, în concordanță cu evoluțiile din statele membre și de la nivel mondial, unde multe astfel de centre și-au schimbat denumirea în centre de securitate cibernetică, însă ar trebui păstrată denumirea prescurtată „CERT-UE”, deoarece este recunoscută pe scară largă.

---

[2] JO C 12, 13.1.2018, p. 1 ▌.

(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de ***entități*** ale Uniunii sau comunități de interes care includ entități ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare***, precum și redresarea în urma incidentelor semnificative***, ***entitățile*** Uniunii ar trebui să informeze CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative***, incidentele evitate la limită*** și incidentele semnificative și să facă schimb de detalii tehnice adecvate care să permită detectarea sau atenuarea ▌ incidentelor similare în alte ***entități*** ale Uniunii, precum și răspunsul ***și redresarea în urma lor***. Urmând aceeași abordare precum cea prevăzută în Directiva ***(UE) 2022/2555***, în cazul în care iau cunoștință de un incident semnificativ, entitățile ar trebui să transmită CERT-UE o ***avertizare timpurie*** în termen de 24 de ore. Acest schimb de informații ar trebui să permită CERT-UE să disemineze informațiile către alte ***entități*** ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor ***TIC*** ale Uniunii și ale omologilor Uniunii împotriva unor incidente, amenințări și vulnerabilități similare.

(13a) Prezentul regulament stabilește o abordare în mai multe etape a raportării incidentelor semnificative pentru a se ajunge la un echilibru adecvat între, pe de o parte, raportarea rapidă care contribuie la atenuarea unei eventuale răspândiri a incidentelor și le permite entităților Uniunii să solicite asistență și, pe de altă parte, o raportare aprofundată care extrage învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența diverselor entități ale Uniunii și contribuie la ameliorarea posturii generale de securitate cibernetică a administrației Uniunii. În acest sens, prezentul regulament ar trebui să includă raportarea incidentelor care, pe baza unei evaluări inițiale efectuate de entitatea în cauză a Uniunii, ar putea cauza entității respective a Uniunii perturbări operaționale ale serviciilor sau pierderi financiare substanțiale sau ar putea afecta alte persoane fizice sau juridice, provocând prejudicii materiale sau morale considerabile. O astfel de evaluare inițială ar trebui să ia în considerare, printre altele, rețelele și sistemele informatice afectate, în special importanța acestora pentru funcționarea și operațiunile entității în cauză a Uniunii, gravitatea și caracteristicile tehnice ale unei amenințări cibernetice și orice vulnerabilități subiacente care sunt exploatate, precum și experiența entității în cauză a Uniunii în ceea ce privește incidente similare. Indicatori precum măsura în care funcționarea entității Uniunii este afectată, durata unui incident sau numărul de

utilizatori afectați ar putea juca un rol important în identificarea gravității perturbării operaționale a serviciului.

(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, ar trebui instituit un Consiliu interinstituțional pentru securitate cibernetică (IICB), care să faciliteze un nivel comun ridicat de securitate cibernetică în rândul ***entităților*** Uniunii prin monitorizarea punerii în aplicare a prezentului regulament de către ***entitățile*** Uniunii, prin supravegherea punerii în aplicare a priorităților și a obiectivelor generale de către CERT-UE și prin elaborarea unor orientări strategice pentru CERT-UE. IICB ar trebui să asigure reprezentarea instituțiilor și să includă reprezentanți ai agențiilor și ai organelor prin intermediul Rețelei agențiilor UE.

(14a) IICB urmărește să sprijine entitățile pentru a își îmbunătăți posturile lor respective în materie de securitate cibernetică prin punerea în aplicare a prezentului regulament. Pentru a sprijini entitățile Uniunii, IICB ar trebui să adopte orientările și recomandările necesare pentru evaluările maturității în materie de securitate cibernetică și planurile de securitate cibernetică ale entităților Uniunii, ar putea revizui posibilele interconexiuni dintre mediile TIC ale entităților Uniunii și ar putea sprijini instituirea unui grup al responsabililor cu securitatea cibernetică în cadrul ENISA, care să reunească responsabilii locali cu securitatea cibernetică ai tuturor entităților Uniunii, cu scopul de a facilita schimbul de bune practici și de experiențe dobândite în urma punerii în aplicare a prezentului regulament.

(14b) Pentru a asigura consecvența cu Directiva (UE) 2022/2555, IICB ar putea adopta recomandări bazate pe rezultatele evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate ale lanțurilor de aprovizionare critice menționate la articolul 22 din Directiva (UE) 2022/2555 pentru a sprijini entitățile Uniunii în adoptarea unor măsuri eficace și proporționale de gestionare a riscurilor legate de securitatea lanțului de aprovizionare și ar putea elabora orientări pentru acordurile privind schimbul de informații dintre entitățile Uniunii referitoare la notificarea voluntară către CERT-UE a amenințărilor cibernetice, a incidentelor evitate la limită și a incidentelor.

(15) CERT-UE trebuie să sprijine punerea în aplicare a măsurilor pentru un nivel comun ridicat de securitate cibernetică prin propuneri de documente de orientare și recomandări adresate IICB sau prin adresarea unor apeluri la acțiune. Astfel de documente de

orientare și recomandări trebuie să fie aprobate de IICB. Atunci când este necesar, CERT-UE ar trebui să adreseze apeluri la acțiune care să descrie măsurile urgente de securitate pe care ***entitățile*** Uniunii sunt îndemnate să le adopte într-un termen stabilit.

(16) IICB ar trebui să monitorizeze respectarea regulamentului, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adresate de CERT-UE. În ceea ce privește aspectele tehnice, IICB ar trebui să beneficieze de sprijin din partea grupurilor consultative tehnice a căror componență este decisă de IICB, care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu ***entitățile*** Uniunii și cu alte părți interesate, după caz. Dacă este necesar, IICB ar trebui să emită avertismente ***și cereri de*** audituri.

(16a) În cazul în care constată că o entitate a Uniunii nu a aplicat sau nu a pus în aplicare efectiv prezentul regulament, IICB ar putea, fără a aduce atingere procedurilor interne ale entității în cauză a Uniunii, să solicite documentația relevantă și disponibilă referitoare la punerea în aplicare efectivă a dispozițiilor prezentului regulament, să comunice un aviz motivat cu lacunele observate în punerea în aplicare a prezentului regulament, să invite entitatea în cauză a Uniunii să furnizeze o autoevaluare cu privire la avizul său motivat și să emită, în cooperare cu CERT-UE, orientări pentru a asigura conformitatea cu prezentul regulament a cadrului său de gestionare, guvernanță și control al riscurilor de securitate cibernetică, a planurilor de securitate cibernetică și a obligațiilor de raportare.

(17) CERT-UE ar trebui să aibă misiunea de a contribui la securitatea mediului ***TIC*** al tuturor ***entităților*** Uniunii. ***După caz și în coordonare cu entitățile Uniunii, CERT-UE poate supune IICB spre aprobare o propunere de politică coordonată de asigurare cibernetică care să acopere entitățile Uniunii, pentru a stabili o asigurare împotriva pagubelor proprii și ale terților cu scopul de a aborda impactul potențial al incidentelor.*** CERT-UE ar trebui să acționeze ca ***coordonator*** desemnat pentru ***entitățile*** Uniunii, în scopul divulgării coordonate a vulnerabilităților către ***baza de date europeană*** a vulnerabilităților, astfel cum se menționează la articolul ***12*** din Directiva ***(UE) 2022/2555***.

(18) În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate ***entitățile*** Uniunii, cu o amploare și o profunzime adecvate, precum și o adaptare continuă la

amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a dispozitivelor conectate prin internetul obiectelor. Acest obiectiv strategic include, de asemenea, centre de operațiuni pentru securitate (SOC) cu spectru larg, care monitorizează rețelele, precum și monitorizarea permanentă a amenințărilor deosebit de grave. CERT-UE ar trebui să ofere sprijin echipelor de securitate ***TIC*** ale ***entităților*** mai mari ale Uniunii, inclusiv prin monitorizarea non-stop din prima linie. Pentru ***entitățile*** mai mici și unele medii ale Uniunii, CERT-UE ar trebui să furnizeze toată gama de servicii.

(19) De asemenea, CERT-UE trebuie să își îndeplinească rolul prevăzut în Directiva ***(UE) 2022/2555*** privind cooperarea și schimbul de informații cu rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT). În plus, în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei[3], CERT-UE trebuie să coopereze cu părțile interesate relevante pentru a identifica un răspuns coordonat. Pentru a contribui la un nivel ridicat de securitate cibernetică în întreaga Uniune, CERT-UE ar trebui să facă schimb de informații referitoare la incidente cu omologii naționali. CERT-UE trebuie, de asemenea, să colaboreze cu alți omologi din sectorul public și privat, inclusiv din cadrul NATO, sub rezerva aprobării prealabile de către IICB.

(20) În sprijinirea securității cibernetice operaționale, CERT-UE ar trebui să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate Cibernetică ***(ENISA)*** prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[4]. ▌Între cele două entități ar trebui încheiate acorduri specifice ***în termen de doi ani de la data intrării în vigoare a prezentului Regulament,*** pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE ar trebui să coopereze cu ***ENISA*** în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.

---

3 Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

4 Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

(21) În sprijinul unității cibernetice comune, create în conformitate cu Recomandarea Comisiei din 23 iunie 2021[5], este necesar ca CERT-UE să coopereze și să facă schimb de informații cu părțile interesate pentru a încuraja cooperarea operațională și pentru a permite rețelelor existente să își valorifice pe deplin potențialul de protejare a Uniunii.

(22) Toate datele cu caracter personal prelucrate în temeiul prezentului regulament trebuie prelucrate în conformitate cu ***dreptul*** în domeniul protecției datelor, inclusiv cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ▌[6]**.** ***Prezentul regulament nu ar trebui să afecteze aplicarea dreptului Uniunii care reglementează prelucrarea datelor cu caracter personal, inclusiv sarcinile și competențele conferite Autorității Europene pentru Protecția Datelor (AEPD). CERT-UE și IICB ar trebui să lucreze în strânsă cooperare cu AEPD și cu personalul specializat în protecția datelor din entitățile Uniunii, pentru a asigura respectarea deplină a dreptului Uniunii în domeniul protecției datelor.***

(22a) Sistemele și serviciile de securitate cibernetică implicate în prevenirea, detectarea și răspunsul la amenințările cibernetice ar trebui să respecte dreptul Uniunii în domeniul protecției datelor și a vieții private și să adopte măsuri de salvgardare tehnice și organizatorice relevante pentru a asigura că această conformitate se realizează într-un mod responsabil.

(22b) Instrumentele și aplicațiile de securitate cibernetică cu sursă deschisă pot contribui la un grad mai mare de deschidere. Standardele deschise înlesnesc interoperabilitatea dintre instrumentele de securitate, aducând beneficii securității părților interesate. Instrumentele și aplicațiile de securitate cibernetică cu sursă deschisă pot stimula comunitatea mai largă a dezvoltatorilor, permițând diversificarea furnizorilor. Sursa deschisă poate duce la un proces mai transparent de verificare a instrumentelor legate de securitatea cibernetică și la un proces de descoperire a vulnerabilităților bazat pe comunitate. Prin urmare, entitățile Uniunii ar trebui să fie în măsură să promoveze utilizarea de software cu sursă deschisă și de standarde deschise prin aplicarea de

---

5 Recomandarea Comisiei C(2021) 4520 din 23.6.2021 privind crearea unei unități cibernetice comune.

6 Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

politici privind utilizarea datelor deschise și a surselor deschise ca parte a securității prin transparență.

(23) CERT-UE și ***entitățile*** Uniunii trebuie să gestioneze informațiile în conformitate cu normele ***privind securitatea informațiilor, în special cele*** prevăzute în regulament [propunerea de regulament privind securitatea informațiilor]. Pentru a asigura coordonarea în materie de securitate, orice contacte cu CERT-UE inițiate sau solicitate de serviciile naționale de securitate și de informații trebuie comunicate fără întârzieri nejustificate Direcției Securitate a Comisiei și președintelui IICB.

(24) Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor ***entităților*** Uniunii, fiecare ***entitate*** a Uniunii cu cheltuieli în domeniul ***TIC*** ar trebui să contribuie în mod echitabil la aceste servicii și sarcini. Contribuțiile respective nu aduc atingere autonomiei bugetare a ***entităților*** Uniunii.

(24a) Prezentul regulament ar trebui să țină seama de faptul că, în afară de instituțiile Uniunii, majoritatea entităților Uniunii, în special cele mici, nu dispun de resursele financiare și umane necesare pentru îndeplinirea sarcinilor suplimentare în materie de securitate cibernetică.

(25) IICB, cu sprijinul CERT-UE, trebuie să revizuiască și să evalueze punerea în aplicare a prezentului regulament și trebuie să raporteze constatările sale Comisiei. Pe baza acestui input, Comisiei îi revine sarcina de a transmite rapoarte Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor.

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I

DISPOZIȚII GENERALE

Articolul 1

Obiect

Prezentul regulament stabilește măsuri care vizează atingerea unui nivel comun ridicat de securitate cibernetică în entitățile Uniunii. În acest scop, prezentul regulament stabilește:

(a) obligații ***care le impun entităților*** Uniunii ***să instituie*** un cadru ▌ de gestionare a riscurilor***, administrare a incidentelor***, guvernanță și control al riscurilor de securitate cibernetică;

(b) obligații de gestionare a riscurilor de securitate cibernetică și de raportare pentru ***entitățile*** Uniunii;

(ba) norme care stau la baza obligațiilor privind schimbul de informații și facilitarea acordurilor voluntare privind schimbul de informații pentru entitățile Uniunii;

(c) norme privind organizarea, ***sarcinile*** și funcționarea Centrului de securitate cibernetică pentru ***entitățile*** Uniunii (CERT-UE) și privind organizarea și funcționarea Consiliului interinstituțional pentru securitate cibernetică ***(IICB)***.

Articolul 2

Domeniul de aplicare

Prezentul regulament se aplică ***tuturor entităților*** Uniunii, precum și organizării și funcționării CERT-UE și ***IICB***.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „***entități*** ale Uniunii” înseamnă instituțiile, organele***, oficiile*** și agențiile Uniunii înființate prin Tratatul privind Uniunea Europeană, Tratatul privind funcționarea Uniunii Europene sau Tratatul de instituire a Comunității Europene a Energiei Atomice sau în temeiul acestora;

(2) „rețea și sistem informatic” înseamnă rețea și sistem informatic ***astfel cum sunt definite la articolul 6 punctul 1*** din Directiva ***(UE) 2022/2555***;

(3) „securitatea rețelelor și a sistemelor informatice” înseamnă securitatea rețelelor și a sistemelor informatice ***astfel cum sunt definite la articolul 6 punctul 2*** din Directiva ***(UE) 2022/2555***;

(4) „securitate cibernetică” înseamnă securitate cibernetică ***astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) 2019/881***;

(5) „cel mai înalt nivel de conducere” înseamnă un manager, un organ de conducere sau de coordonare și supraveghere ***responsabil de funcționarea entității în cauză a Uniunii***, la cel mai înalt nivel administrativ***, cu mandatul de a adopta sau autoriza decizii în conformitate cu*** mecanismele de guvernanță la nivel înalt ***din entitatea în cauză, fără a aduce atingere responsabilităților oficiale ale altor niveluri de conducere în ceea ce privește conformitatea și gestionarea riscurilor în domeniile lor de responsabilitate respectiv***e;

(5a) „incident evitat la limită” înseamnă un incident evitat la limită astfel cum este definit la articolul 6 punctul 5 din Directiva (UE) 2022/2555;

(6) „incident” înseamnă un incident ***astfel cum este definit la articolul 6 punctul 6*** din Directiva ***(UE) 2022/2555***;

I

(8) „***incident*** major” înseamnă ***un*** incident care ***cauzează o perturbare ce depășește capacitatea unei entități afectate a*** Uniunii ***și a CERT-UE de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două entități din Uniune sau în cazul căruia un incident de securitate cibernetică de mare amploare astfel cum este definit la articolul 6 punctul 7 din Directiva (UE) 2022/2555 are un impact semnificativ asupra cel puțin unei entități din Uniune***;

(9) „administrarea incidentelor” înseamnă o administrare a incidentelor ***astfel cum este definită la articolul 6 punctul 8*** din Directiva ***(UE) 2022/2555***;

(10) „amenințare cibernetică” înseamnă o amenințare cibernetică ***astfel cum este definită la articolul 2 punctul 8*** din Regulamentul (UE) 2019/881;

(11) „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică ***astfel cum este definită la articolul 6 punctul 11 din Directiva (UE) 2022/2555***;

(12) „vulnerabilitate” înseamnă vulnerabilitate ***astfel cum este definită la articolul 6 punctul 15*** din Directiva ***(UE) 2022/2555***;

(13) „vulnerabilitate semnificativă” înseamnă o vulnerabilitate care prezintă riscul de a cauza un incident semnificativ dacă este exploatată;

(14) „risc ▌” înseamnă ***un risc astfel cum este definit la articolul 6 punctul 9 din Directiva (UE) 2022/2555***;

(14a) „standard” înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[8];

(14b) „specificație tehnică” înseamnă o specificație tehnică astfel cum este definită la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012;

(14c) „produs TIC” înseamnă un produs astfel cum este definit la articolul 2 punctul 12 din Regulamentul (UE) 2019/881;

(14d) „serviciu TIC” înseamnă un serviciu TIC astfel cum este definit la articolul 2 punctul 13 din Regulamentul (UE) 2019/881;

(14e) „proces TIC” înseamnă un proces TIC astfel cum este definit la articolul 2 punctul 14 din Regulamentul (UE) 2019/881;

(14f) „mediu TIC” înseamnă orice produs TIC, serviciu TIC și proces TIC de la fața locului sau virtual, orice rețea și sistem informatic, indiferent dacă este deținut și operat de o entitate, sau găzduit sau operat de o parte terță, inclusiv dispozitive mobile, rețele corporative și rețele de afaceri care nu sunt conectate la internet și orice dispozitive conectate la mediul TIC, precum și orice spații separate și birouri descentralizate, cum ar fi birourile de legătură, reprezentanțele sau birourile locale;

(15) „unitate cibernetică comună” înseamnă o platformă virtuală și fizică de cooperare pentru diferitele comunități de securitate cibernetică din Uniune, cu accent pe coordonarea operațională și tehnică împotriva amenințărilor și incidentelor cibernetice transfrontaliere majore în sensul Recomandării Comisiei din 23 iunie 2021;

(16) „***măsuri*** de securitate cibernetică” înseamnă un set de norme ***și măsuri*** minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și

---

[8] Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

operatorii și utilizatorii acestora trebuie să le respecte, pentru a reduce la minimum riscurile de securitate cibernetică.

Capitolul II

MĂSURI PENTRU UN NIVEL COMUN RIDICAT DE SECURITATE CIBERNETICĂ

Articolul 4

Cadrul de gestionare ***a riscurilor, administrare a incidentelor***, guvernanță și control al riscurilor

(1) ***Pe baza unui audit complet de securitate cibernetică,*** fiecare ***entitate*** a Uniunii își stabilește propriul cadru ▌de gestionare a riscurilor***, administrare a incidentelor***, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul”) pentru a sprijini misiunea entității ***Uniunii*** și pentru a-și exercita autonomia instituțională. ***Crearea acestui cadru*** este supravegheată de cel mai înalt nivel de conducere al entității ***Uniunii și se află sub responsabilitatea sa pentru a*** asigura o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică. Cadrul se instituie până ▌la …[15 luni de la ***data intrării*** în vigoare a prezentului regulament].

(2) Cadrul acoperă întregul mediu ***TIC*** al ***entității Uniunii*** în cauză▌. Cadrul ține seama de gestionarea continuității activității și de gestionarea crizelor și ia în considerare securitatea lanțului de aprovizionare, precum și gestionarea riscurilor umane ***și a tuturor celorlalte riscuri tehnice, operaționale și organizaționale relevante*** care ar putea avea un impact asupra securității cibernetice a ***entității*** Uniunii în cauză.

(2a) Cadrul menționat la alineatul (1) definește obiective strategice pentru a asigura un nivel ridicat de securitate cibernetică în entitățile Uniunii. Cadrul respectiv stabilește politici de securitate cibernetică pentru securitatea rețelelor și a sistemelor informatice, care cuprind întregul mediu TIC, și definește rolurile și responsabilitățile personalului entităților Uniunii însărcinat cu asigurarea punerii în aplicare eficace a prezentului regulament. Cadrul include, de asemenea, indicatorii-cheie de performanță (ICP) pentru măsurarea eficacității punerii în aplicare pe baza listei ICP menționată la articolul 12 alineatul (2) litera (eb).

(2b) ***Cadrul menționat la alineatul (1) se revizuiește periodic și cel puțin o dată la trei ani. Prima astfel de revizuire se efectuează până la... [trei ani de la data intrării în vigoare a prezentului regulament]. După caz și la cererea IICB, un cadru al unei entități a Uniunii se actualizează pe baza orientărilor primite din partea CERT-UE cu privire la incidentele identificate sau la posibilele lacune observate la punerea în aplicare a prezentului regulament.***

(3) Cel mai înalt nivel de conducere din fiecare ***entitate*** a Uniunii ***este responsabil cu punerea în aplicare și supraveghează respectarea*** de către propria organizație ***și funcționarea acesteia pe baza*** obligațiilor legate de ***cadru***, fără a aduce atingere responsabilităților formale ale altor niveluri de conducere în ceea ce privește conformitatea și gestionarea riscurilor în domeniile lor respective de responsabilitate***, cum ar fi protecția datelor***.

(4) Fiecare ***entitate*** a Uniunii dispune de mecanisme eficace pentru a se asigura că un procent adecvat din bugetul în domeniul ***TIC*** este cheltuit pentru securitatea cibernetică.

(5) Fiecare ***entitate*** a Uniunii numește un responsabil local cu securitatea cibernetică sau o funcție echivalentă care acționează ca punct unic de contact în ceea ce privește toate aspectele securității cibernetice. ***Responsabilii locali cu securitatea cibernetică pot fi partajați de mai multe entități ale Uniunii.***

Articolul 5

Măsuri de gestionare a riscurilor de securitate cibernetică

(1) Cel mai înalt nivel de conducere din fiecare ***entitate*** a Uniunii își aprobă ***propriile măsuri*** de ***gestionare a riscurilor*** de securitate cibernetică pentru a aborda riscurile identificate în cadrul menționat la articolul 4 punctul 1***, în conformitate cu orientările și recomandările formulate de IICB și CERT-UE***. ***Având în vedere stadiul actual al tehnologiei și, după caz, standardele europene și internaționale aplicabile sau certificatele europene de securitate cibernetică disponibile, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (UE) 2019/881, aceste măsuri de gestionare a riscurilor asigură un nivel de securitate a rețelelor și a sistemelor informatice în întregul mediu TIC proporțional cu riscurile identificate în cadrul menționat la articolul 4 alineatul (1). Atunci când se evaluează proporționalitatea***

măsurilor respective, se ține seama în mod corespunzător de gradul de expunere a entității Uniunii la riscuri, de dimensiunea acesteia, de probabilitatea producerii unor incidente și de gravitatea acestora, inclusiv de impactul lor societal, economic și interinstituțional.

(1a) Entitățile Uniunii includ cel puțin următoarele domenii în punerea în aplicare a măsurilor de gestionare a riscurilor de securitate cibernetică:

(a) politica în materie de securitate cibernetică, inclusiv măsurile necesare pentru atingerea obiectivelor și priorităților menționate la articolul 4 și la alineatul (2a) de la prezentul articol;

(b) obiectivele de politică privind utilizarea serviciilor de cloud computing, astfel cum sunt definite la articolul 6 punctul 30 din Directiva (UE) 2022/2555, și modalitățile tehnice pentru a permite și a susține munca la distanță;

(c) pentru a evalua dacă entitățile Uniunii dispun de un control suficient asupra securității sistemelor lor TIC, ar trebui să se efectueze o analiză inițială completă a securității cibernetice, inclusiv o evaluare a riscurilor, a vulnerabilității și a amenințărilor, precum și un test de penetrare a sistemelor și dispozitivelor TIC ale entităților Uniunii, de către o parte terță eminentă și verificată, externă entităților Uniunii, cum ar fi o companie eminentă de securitate cibernetică, la ... [data intrării în vigoare a prezentului regulament] și, ulterior, în fiecare an, ținând seama în mod corespunzător de cerințele de securitate a informațiilor ale instituțiilor relevante;

(d) în lumina revizuirilor menționate la litera (c), atenuarea riscurilor și vulnerabilităților raportate în actualizările de securitate cibernetică și punerea în aplicare a recomandărilor prin intermediul politicii de securitate cibernetică, care poate include înlocuirea sistemelor TIC infectate;

(e) organizarea securității cibernetice, inclusiv definirea rolurilor și a responsabilităților;

(f) gestionarea mediului TIC, inclusiv inventarul activelor TIC și cartografierea rețelelor TIC;

(g) controlul accesului, gestionarea identității și gestionarea accesului privilegiat;

(h) securitatea operațiunilor și securitatea resurselor umane;

(i) securitatea comunicațiilor;

(j) achiziționarea, dezvoltarea, întreținerea și transparența codului sursă;

(k) auditurile de securitate cibernetică;

(l) volumul de muncă al personalului TIC și nivelul general de satisfacție;

(m) securitatea lanțului de aprovizionare și relațiile cu furnizorii dintre entitățile Uniunii și furnizorii și prestatorii lor de servicii direcți;

(n) gestionarea incidentelor, inclusiv abordări pentru a îmbunătăți nivelul de pregătire, detectarea, analiza, limitarea incidentelor, precum și răspunsul și capacitatea de recuperare în urma acestora, și cooperarea cu CERT-UE, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate;

(o) gestionarea continuității activității și gestionarea crizelor; și

(p) programele și exercițiile dezvoltare a competențelor, educație, sensibilizare și formare.

(2) Personalul de conducere de nivel superior din fiecare ***entitate*** a Uniunii***, precum și întregul personal relevant însărcinat cu punerea în aplicare a măsurilor și a obligațiilor de gestionare a riscurilor de securitate cibernetică prevăzute în prezentul regulament*** urmează periodic cursuri de formare specifice pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor ***entității Uniunii***.

(2a) Entitățile Uniunii abordează cel puțin următoarele măsuri și controale secundare specifice când implementează măsurile de gestionare a riscurilor de securitate cibernetică și când își concep planurile de securitate cibernetică, în conformitate cu documentele de orientare și recomandările din partea IICB:

(a) pași concreți înspre o arhitectură bazată pe modelul de încredere zero („zero trust”), adică un model de securitate compus dintr-un set de principii de proiectare a sistemului și o strategie coordonată de securitate cibernetică și de gestionare a sistemelor, bazată pe recunoașterea faptului că există amenințări atât în interiorul, cât și în afara granițelor tradiționale ale rețelei;

(b) adoptarea autentificării multifactor ca normă pentru toate rețelele și sistemele informatice;

(c) utilizarea criptografiei și a criptării, în special criptarea de la un capăt la altul, criptarea în tranzit și criptarea în repaus, precum și semnăturile digitale securizate;

(d) comunicații securizate de voce, video și text și sisteme securizate de comunicații de urgență, dacă este cazul;

(e) stabilirea unor capacități de scanare frecventă și ad-hoc a dispozitivelor cu punct final și a altor componente ale mediului TIC pentru a detecta și a elimina programele informatice malware, cum ar fi programele spion;

(f) asigurarea protecției vieții private începând cu momentul conceperii și a securității sporite a tuturor datelor cu caracter personal;

(g) asigurarea securității lanțului de aprovizionare cu software prin criterii de dezvoltare și evaluare securizată a software-ului

(h) formarea periodică a membrilor personalului în materie de securitate cibernetică;

(i) participarea la analizele de risc privind interconectivitatea între entitățile Uniunii;

(j) consolidarea normelor privind achizițiile publice pentru a facilita un nivel comun ridicat de securitate cibernetică prin:

(i) eliminarea barierelor contractuale care limitează schimbul de informații între furnizorii de servicii informatice și CERT-UE cu privire la incidente, vulnerabilități și amenințări cibernetice;

(ii) obligația contractuală de a raporta incidentele, vulnerabilitățile, incidentele evitate la limită și amenințările cibernetice, precum și de a institui măsuri adecvate de răspuns la incidente și de monitorizare a acestora;

(k) stabilirea și adoptarea unor programe de formare privind securitatea cibernetică, proporționale cu sarcinile prevăzute și cu capacitățile preconizate pentru cel mai înalt nivel de conducere și personalul tehnic și operațional.

(2b) ***IICB poate recomanda cerințe tehnice și metodologice pentru domeniile și măsurile de gestionare a riscurilor de securitate cibernetică menționate la alineatele (1a) și (2a) de la prezentul articol și, dacă este necesar, poate recomanda adaptări pentru a reflecta evoluțiile metodelor de atac cibernetic, ale amenințărilor cibernetice și ale progreselor tehnologice, în scopul revizuirii menționate la articolul 24.***

Articolul 6

Evaluări ale maturității ***în materie de securitate cibernetică***

(1) Fiecare ***entitate*** a Uniunii efectuează o evaluare a nivelului de maturitate al securității cibernetice ***până la ... [18 luni de la data intrării în vigoare a prezentului regulament] și, ulterior,*** cel puțin o dată la ***doi*** ani, încorporând toate elementele mediului său ***TIC***, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în temeiul articolului 13.

(2) ***Entitățile mici din Uniune cu sarcini sau structuri similare pot efectua o evaluare combinată a maturității în materie de securitate cibernetică.***

(3) ***După consultarea Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) și după primirea de orientări din partea CERT-UE, IICB elaborează, până la [un an de la data intrării în vigoare a prezentului regulament], orientări pentru entitățile din Uniune în scopul efectuării de evaluări ale maturității în materie de securitate cibernetică. Evaluarea maturității în materie de securitate cibernetică trebuie să se bazeze pe audituri în materie de securitate cibernetică.***

(4) ***La cererea IICB și cu acordul explicit al entității în cauză a Uniunii, rezultatele unei evaluări a maturității în materie de securitate cibernetică pot fi discutate în cadrul IICB sau al rețelei instituite de ofițeri locali în materie de securitate cibernetică, pentru a învăța din experiențele legate de punerea în aplicare a prezentului regulament și pentru a face schimb de bune practici și de rezultate ale cazurilor de utilizare.***

Articolul 7

Planuri de securitate cibernetică

(1) În urma concluziilor desprinse din evaluarea nivelului de maturitate ***în materie de securitate cibernetică*** și luând în considerare ▌ riscurile identificate în temeiul

articolului 4, cel mai înalt nivel de conducere din fiecare ***entitate*** a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului ▌ și a ***măsurilor*** de ***gestionare a riscurilor*** de securitate cibernetică. Planul ***de securitate cibernetică*** vizează creșterea gradului de securitate cibernetică în ansamblu a entității ***Uniunii*** și contribuie, astfel, la atingerea sau îmbunătățirea unui nivel comun ridicat de securitate cibernetică în ***interiorul*** Uniunii. Pentru a sprijini misiunea entității Uniunii pe baza autonomiei sale instituționale, planul ***de securitate cibernetică*** include cel puțin ▌ măsurile ***de gestionare a riscurilor de securitate cibernetică menționate la articolul 5 alineatele (1a) și (2a)***. Planul ***de securitate cibernetică*** se revizuiește cel puțin o dată la ***doi*** ani ***sau, dacă este necesar, cu ocazia oricărei revizuiri substanțiale a cadrului menționat la articolul 4,*** în urma evaluărilor nivelului de maturitate ***în materie de securitate cibernetică*** efectuate în temeiul articolului 6.

(2) Planul de securitate cibernetică include rolurile***, nivelul necesar de competențe*** și responsabilitățile ***relevante*** ale membrilor personalului pentru punerea sa în aplicare***, inclusiv fișe de post detaliate pentru personalul tehnic și operațional, precum și toate procesele relevante care stau la baza evaluării performanței***.

(2a) Planul de securitate cibernetică include planul de gestionare a crizelor cibernetice al entității Uniunii pentru incidentele majore.

(3) Planul de securitate cibernetică ia în considerare toate documentele de orientare și recomandările aplicabile emise de CERT-UE ***în conformitate cu articolul 13 sau orice recomandări aplicabile sau specifice emise de IICB și CERT-UE***.

(3a) Entitățile Uniunii transmit IICB planurile lor de securitate cibernetică.

Articolul 8

Punerea în aplicare

(1) După finalizarea evaluărilor ***lor respective*** ale nivelului de maturitate ***al securității cibernetice menționate la articolul 6 și a planurilor de securitate cibernetică menționate la articolul 7***, ***entitățile*** Uniunii le prezintă ***IICB***. ▌ La cererea ***IICB***, ele raportează cu privire la aspecte specifice din prezentul capitol.

(2) Documentele de orientare și recomandările emise în temeiul articolului 13 sprijină punerea în aplicare a dispozițiilor prevăzute în prezentul capitol.

Capitolul III

IICB

Articolul 9

IICB

(1) Se instituie ▌IICB▌.

(2) IICB este responsabil cu:

(a) monitorizarea punerii în aplicare a prezentului regulament de către ***entitățile*** Uniunii ***și prezentarea de recomandări pentru atingerea unui nivel comun ridicat de securitate cibernetică***;

(b) supravegherea punerii în aplicare a priorităților și obiectivelor generale de către CERT-UE și de elaborarea de orientări strategice pentru CERT-UE.

(3) IICB este format din***:***

(a) ***doi*** reprezentanți numiți ▌de fiecare dintre următoarele entități:

(i) Parlamentul European;

(ii) Consiliul Uniunii Europene;

(iii) Comisia Europeană;

(b) ***un reprezentant numit de fiecare dintre următoarele entități:***

(i) Curtea de Justiție a Uniunii Europene;

(ii) Banca Centrală Europeană;

(iii) Curtea de Conturi Europeană;

(iv) Serviciul European de Acțiune Externă;

(v) Comitetul Economic Și Social European;

(vi) Comitetul European al Regiunilor;

(vii) Banca Europeană de Investiții;

(viii) ENISA;

(ix) Autoritatea Europeană pentru Protecția Datelor (AEPD);

(x) Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică;

(xi) Agenția Uniunii Europene pentru Programul Spațial;

(c) un reprezentant desemnat de Rețeaua agențiilor Uniunii (EUAN) la propunerea Comitetului consultativ pentru TIC pentru a reprezenta interesele agențiilor, oficiilor și organismelor, altele decât cele menționate la litera (b) punctele (viii) (x) și (xi), care își gestionează propriul mediu TIC.

Se urmărește obținerea unui echilibru de gen în rândul reprezentanților numiți.

(3a) Membrii pot fi asistați de un supleant. Alți reprezentanți ai organizațiilor enumerate mai sus sau ai altor ***entități*** ale Uniunii pot fi invitați de președinte să participe la reuniunile IICB, fără drept de vot.

(3b) Șeful CERT-UE și președinții Grupului de cooperare, ai rețelei CSIRT și ai EU-CyCLONe, menționați la articolele 14, 15 și 16 din Directiva (UE) 2022/2555, sau supleanții acestora pot participa la reuniunile IICB în calitate de observatori. În cazuri excepționale și în conformitate cu regulamentul intern de procedură al IICB, IICB poate decide altfel.

(4) IICB își stabilește regulamentul intern de procedură.

(5) IICB numește un președinte din rândul membrilor săi, în conformitate cu regulamentul intern de procedură, pentru o perioadă de patru ani. Supleantul acestuia devine membru titular ***cu drept de vot*** al IICB pentru aceeași durată.

(6) IICB se reunește la inițiativa președintelui ***și cel puțin de două ori pe an,*** la cererea CERT-UE sau a oricăruia dintre membrii săi.

(7) Fiecare membru al IICB dispune de un vot. Deciziile IICB sunt adoptate cu majoritate simplă, cu excepția cazurilor în care se prevede altfel în prezentul regulament. Președintele votează numai în caz de egalitate de voturi, situație în care poate exprima un vot decisiv.

(8) IICB poate acționa printr-o procedură scrisă simplificată inițiată în conformitate cu regulamentul intern de procedură. În temeiul procedurii respective, decizia relevantă se consideră aprobată în termenul stabilit de președinte, cu excepția cazului în care un membru formulează obiecții.

▌

(10) Secretariatul IICB este asigurat de Comisie.

(11) ***Reprezentantul numit*** de Rețeaua agențiilor UE ▌informează agențiile și întreprinderile comune ale Uniunii cu privire la deciziile adoptate de IICB. Orice agenție și organ al Uniunii are dreptul să supună atenției reprezentanților și președintelui IICB orice chestiune care, în opinia sa, ar trebui adusă în atenția IICB.

▌

(13) IICB poate numi un comitet executiv care să îl asiste în activitatea sa și căruia să îi delege o parte din sarcinile și competențele sale. IICB stabilește regulamentul de procedură al comitetului executiv, inclusiv sarcinile și competențele acestuia, precum și mandatul membrilor săi.

Articolul 10

Sarcinile IICB

Când își exercită responsabilitățile, IICB trebuie în special:

(-a) să sprijine entitățile Uniunii în punerea în aplicare a prezentului regulament, cu scopul de a crește nivelurile lor respective de securitate cibernetică;

(-aa) să monitorizeze în mod eficace punerea în aplicare a obligațiilor prevăzute în prezentul regulament în entitățile Uniunii, fără a aduce atingere autonomiei lor instituționale și echilibrului instituțional general;

(-ab) să ofere orientări strategice șefului CERT-UE;

(a) ***să solicite*** rapoarte ▌ de la CERT-UE cu privire la stadiul punerii în aplicare a prezentului regulament de către ***entitățile*** Uniunii;

(aa) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, recomandări pentru atingerea unui nivel comun ridicat de securitate cibernetică, adresate uneia sau mai multor entități ale Uniunii;

(ab) să instituie un cadru pentru efectuarea de evaluări inter pares pentru entitățile Uniunii pentru a învăța din experiențele celorlalți, a consolida încrederea reciprocă, a atinge un nivel comun ridicat de securitate cibernetică și a consolida capacitățile

entităților din Uniune, care să fie efectuate de experți tehnici de securitate cibernetică desemnați de o entitate diferită de entitatea examinată;

(b) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, programul anual de lucru al CERT-UE și să monitorizeze implementarea acestuia;

(c) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, catalogul de servicii al CERT-UE;

(d) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, planificarea anuală a veniturilor și cheltuielilor, inclusiv a personalului, pentru activitățile CERT-UE;

(e) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, modalitățile pentru acordurile privind nivelul serviciilor;

(f) să examineze și să aprobe raportul anual întocmit de șeful CERT-UE, referitor la activitățile și gestionarea fondurilor de către CERT-UE;

(g) să aprobe și să monitorizeze indicatorii cheie de performanță pentru CERT-UE, definiți pe baza propunerii șefului CERT-UE;

(h) să aprobe acordurile de cooperare, acordurile privind nivelul serviciilor sau contractele dintre CERT-UE și alte entități în temeiul articolului 17;

(ha) să adopte documente de orientare sau recomandări pe baza propunerilor CERT-EU;

(hb) dacă este necesar, să solicite CERT-UE să emită, să retragă sau să modifice o propunere de document de orientare sau de recomandare sau un apel la acțiune;

(i) să instituie ▌grupuri consultative tehnice ***cu sarcini concrete*** pentru a sprijini activitatea IICB, să stabilească mandatul și să desemneze președinții acestor grupuri***;***

(ia) să examineze și, la cerere, pe baza orientărilor relevante din partea CERT-UE, să furnizeze feedback entităților Uniunii despre evaluările maturității în materie de securitate cibernetică menționate la articolul 6 și la planurile de securitate cibernetică menționate la articolul 7;

(ib) să faciliteze schimbul de bune practici între responsabilii locali cu securitatea cibernetică; să ofere, după caz, recomandări privind rolul lor în cadrul entităților Uniunii;

(ic) să revizuiască posibilele interconexiuni între mediile TIC ale entităților Uniunii și să mențină un inventar al componentelor comune ale produselor TIC, serviciilor TIC și proceselor TIC;

(id) după caz, să adopte recomandări privind interoperabilitatea mediilor TIC ale entităților Uniunii sau a componentelor acestora;

(ie) să sprijine instituirea unui grup al responsabililor cu securitatea cibernetică, coordonat de ENISA, care să reunească responsabilii locali cu securitatea cibernetică ai tuturor entităților Uniunii, cu scopul de a facilita schimbul de bune practici și de experiențe dobândite în urma punerii în aplicare a prezentului regulament;

(if) să elaboreze un plan de răspuns la incidente majore și să coordoneze adoptarea planurilor individuale de gestionare a crizelor cibernetice ale entităților Uniunii menționate la articolul 7 alineatul (2a);

(ig) să adopte recomandări bazate pe rezultatele evaluărilor coordonate la nivelul UE ale riscurilor lanțurilor de aprovizionare critice menționate la articolul 22 din Directiva (UE) 2022/2555 pentru a sprijini entitățile Uniunii în adoptarea măsurilor de securitate cibernetică eficace și proporționale de gestionare a riscurilor legate de securitatea lanțului de aprovizionare menționate la articolul 5 alineatul (1a) litera (m);

(ih) să elaboreze orientări pentru acordurile privind schimbul de informații menționate la articolul 19.

Articolul 11

Respectarea dispozițiilor

(1) IICB monitorizează punerea în aplicare de către ***entitățile*** Uniunii a prezentului regulament și a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adoptate. În cazul în care constată că ***entitățile*** Uniunii nu au pus în aplicare în mod eficace prezentul regulament sau documentele de orientare, recomandările și apelurile la acțiune adoptate în temeiul prezentului regulament, IICB poate, fără a aduce atingere procedurilor interne ale ***entității*** respective:

(-a) să solicite documentația relevantă și disponibilă a entității în cauză a Uniunii;

(-aa) să comunice entității în cauză a Uniunii un aviz motivat despre lacunele constatate în punerea în aplicare a prezentului regulament;

(-ab) să invite entitatea în cauză a Uniunii să furnizeze o autoevaluare cu privire la avizul său motivat într-un anumit interval de timp;

(-ac) să ofere, după consultarea CERT-UE, orientări entității Uniunii pentru a asigura conformitatea cu prezentul regulament a cadrului respectiv, a măsurilor de gestionare a riscurilor în materie de securitate cibernetică, a planurilor de securitate cibernetică și a obligațiilor de raportare, într-o perioadă specificată;

(a) să emită un avertisment; dacă este necesar, având în vedere un risc semnificativ de securitate cibernetică, categoria de public căreia i se adresează avertismentul este restricționată în mod corespunzător;

(b) ***să solicite*** un serviciu de audit relevant pentru efectuarea unui audit;

(ba) să informeze Curtea de Conturi cu privire la presupusa lipsă de conformitate.

Toate avertismentele și recomandările se adresează celui mai înalt nivel de conducere al entității în cauză a Uniunii.

(2) În cazul în care entitățile mici din Uniune notifică faptul că nu sunt în măsură să respecte termenele stabilite la articolul 4 alineatul (1) și la articolul 5 alineatul (1), IICB poate, în cazuri excepționale, să autorizeze prelungirea acestora și să stabilească termenele pentru conformare.

Capitolul IV

CERT-UE

Articolul 12

Misiunea și sarcinile CERT-UE

(1) Misiunea CERT-UE, Centrul autonom de răspuns la incidente de securitate cibernetică pentru ***entitățile*** UE, este de a contribui la securitatea mediului ***TIC*** neclasificat al tuturor ***entităților*** Uniunii ***și de a le furniza acestora servicii similare CSIRT instituite de statele membre în temeiul Directivei (UE) 2022/2555, în special prin*** consiliere în

materie de securitate cibernetică, ajutându-le să prevină, să detecteze, ***să abordeze,*** să atenueze**,** să răspundă la incidente ***și să se redreseze după acestea*** și acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.

(2) CERT-UE îndeplinește următoarele sarcini pentru ***entitățile*** Uniunii:

(a) le oferă sprijin pentru punerea în aplicare a prezentului regulament și contribuie la coordonarea punerii în aplicare a prezentului regulament prin intermediul măsurilor enumerate la articolul 13 alineatul (1) sau al rapoartelor ad-hoc solicitate de IICB;

(b) le oferă sprijin printr-un pachet de servicii de securitate cibernetică descrise în catalogul său de servicii („servicii de referință”);

(ba) operează pentru entitățile Uniunii care nu au capacitatea de a o face singure, un centru de operațiuni de securitate (SOC) cu spectru larg care monitorizează rețelele, inclusiv monitorizarea non-stop din prima linie a amenințărilor deosebit de grave;

(c) menține o rețea de omologi și parteneri pentru a sprijini serviciile, astfel cum se prevede la articolele 16 și 17;

(d) aduce în atenția IICB orice problemă legată de punerea în aplicare a prezentului regulament și a ***articolului 13 și prezintă propuneri de recomandări***;

(e) prezintă ***entităților Uniunii*** un raport referitor la amenințările cibernetice ***relevante*** și contribuie la conștientizarea situației amenințărilor la adresa securității cibernetice în ***Uniune, ținând seama de avizul ENISA, și transmite astfel de rapoarte IICB, rețelei CSIRT menționate la articolul 15 din Directiva (UE) 2022/2555 și Centrului de situații și de analiză a informațiilor al UE (INTCEN UE)***;

(ea) acționează drept coordonator desemnat pentru entitățile Uniunii, în scopul divulgării coordonate a vulnerabilităților către baza de date europeană a vulnerabilităților, astfel cum se menționează la articolul 12 din Directiva (UE) 2022/2555;

(eb) propune IICB, după consultarea ENISA, criteriile de securitate, o listă de posibili indicatori cheie de performanță și scara de securitate utilizată în cadrele de securitate cibernetică folosite de entitățile Uniunii;

(ec) propune IICB și acordă prioritate, după consultarea ENISA, domeniilor de securitate cibernetică și măsurilor de securitate cibernetică pe care entitățile Uniunii trebuie să le ia în considerare în cadrul lor de securitate cibernetică;

(ed) furnizează entităților din Uniune unul sau mai multe modele de maturitate în materie de securitate cibernetică, care trebuie să fie utilizate în cadrele lor de securitate cibernetică și care reflectă dimensiunea lor și domeniile de securitate cibernetică pe care le utilizează;

(ee) furnizează servicii care sprijină, cu un nivel ridicat de transparență și fiabilitate, schimburile de informații, în special în ceea ce privește notificările entităților Uniunii către CERT-UE;

(ef) efectuează periodic analize de risc ale interconectivității dintre entitățile Uniunii pentru a sprijini sarcinile IICB.

(3) CERT-UE contribuie la activitatea unității cibernetice comune, create în conformitate cu Recomandarea Comisiei din 23 iunie 2021, inclusiv în următoarele domenii:

(a) pregătirea, coordonarea în materie de incidente, schimbul de informații și răspunsul la situații de criză la nivel tehnic în cazurile legate de ***entitățile*** Uniunii;

(b) cooperarea operațională în ceea ce privește rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT), inclusiv în materie de asistență reciprocă, și comunitatea mai largă a specialiștilor din domeniul securității cibernetice;

(ba) coordonarea gestionării incidentelor și crizelor majore la nivel operațional și schimbul periodic de informații relevante între statele membre și entitățile Uniunii în cadrul rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe);

(c) informații privind amenințările cibernetice, inclusiv conștientizarea situației;

(ca) scanarea proactivă a rețelelor și a sistemelor informatice;

(d) orice subiect care necesită expertiză tehnică în materie de securitate cibernetică din partea CERT-UE.

(4) CERT-UE desfășoară o cooperare structurată cu ***ENISA*** în ceea ce privește consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice, în temeiul Regulamentului (UE) 2019/881 ▌. ***CERT-UE poate coopera și face schimb de informații cu Centrul european de combatere a criminalității informatice al Europol.***

(5) CERT-UE poate furniza ***entităților Uniunii*** următoarele servicii care nu sunt descrise în catalogul său de servicii („servicii contra cost”):

(a) servicii care sprijină securitatea cibernetică a mediului ***TIC*** al ***entităților*** Uniunii, altele decât cele menționate la alineatul (2), în temeiul unor acorduri privind nivelul serviciilor și sub rezerva resurselor disponibile***, inclusiv, prin intermediul centrului său de operațiuni de securitate menționat la alineatul (2) litera (ba), monitorizarea rețelelor și monitorizarea non-stop din prima linie a amenințărilor grave pentru entitățile mai mari ale Uniunii***;

(b) servicii care sprijină operațiunile sau proiectele în materie de securitate cibernetică ale ***entităților*** Uniunii, altele decât cele care vizează protejarea mediului lor ***TIC***, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB;

(c) servicii care sprijină securitatea mediului ***TIC*** al altor organizații decât ***entitățile*** Uniunii, care cooperează îndeaproape cu ***entitățile*** Uniunii, de exemplu, cărora li s-au atribuit sarcini sau responsabilități în temeiul dreptului Uniunii, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB.

(6) CERT-UE ***organizează*** exerciții de securitate cibernetică sau ***recomandă*** participarea la exercițiile existente, în strânsă cooperare cu ***ENISA***, dacă este cazul, pentru a testa ***periodic*** nivelul de securitate cibernetică al ***entităților*** Uniunii.

(7) CERT-UE ***oferă entităților*** Uniunii asistență referitoare la incidentele din medii ***TIC*** clasificate, dacă entitatea în cauză îi solicită acest lucru în mod expres. ***Dispozițiile și obligațiile care revin tuturor entităților Uniunii prevăzute în capitolul V nu se aplică incidentelor din mediile TIC clasificate, cu excepția cazului în care o entitate a Uniunii le aplică în mod explicit și voluntar pentru a solicita asistență din partea***

CERT-UE sau pentru a contribui în alt mod la conștientizarea situației la nivelul Uniunii.

(7a) CERT-UE prezintă Parlamentului European, în condiții de confidențialitate adecvate, un raport anual privind activitățile sale. Acest raport include informații relevante și precise despre incidentele majore și modul în care acestea au fost tratate.

(7b) CERT-UE cooperează cu AEPD pentru a sprijini entitățile Uniunii în incidentele care implică o încălcare a securității datelor cu caracter personal, astfel cum este definită la articolul 3 punctul 16 din Regulamentul (UE) 2018/1725.

(7c) Prelucrarea datelor cu caracter personal efectuată de CERT- UE în temeiul prezentului regulament face obiectul Regulamentului (UE) 2018/1725.

(7d) CERT-UE poate oferi asistență entităților Uniunii în ceea ce privește punerea în aplicare a unei cooperări adecvate în materie de securitate cibernetică între acestea în ceea ce privește cunoștințele de securitate cibernetică, personalul și resursele TIC, precum și expertiza de securitate cibernetică.

(7e) CERT-UE informează AEPD atunci când abordează vulnerabilități semnificative, incidente semnificative sau atacuri majore care au potențialul de a conduce la încălcări ale securității datelor cu caracter personal și/sau la încălcarea confidențialității comunicațiilor electronice.

(7f) CERT-UE informează AEPD cu privire la activitățile preventive de securitate cibernetică care ar conduce la colectarea de date cu caracter personal.

Articolul 13

Documente de orientare, recomandări și apeluri la acțiune

(1) CERT-UE sprijină punerea în aplicare a prezentului regulament prin adoptarea unor:

(a) apeluri la acțiune care descriu măsurile urgente de securitate pe care ***entitățile*** Uniunii sunt invitate să le adopte într-un termen stabilit;

(b) propuneri de documente de orientare, transmise IICB, care se adresează tuturor ***entităților*** Uniunii sau doar unei părți a acestora;

(c) propuneri de recomandări, transmise IICB, care se adresează ***entităților individuale sau tuturor entităților*** Uniunii.

(2) Documentele de orientare și recomandările pot include:

(a) modalități sau îmbunătățiri ale gestionării riscurilor de securitate cibernetică și ale ***măsurilor de gestionare a riscurilor*** de securitate cibernetică;

(b) ***acorduri*** de evaluare a nivelului maturității ***securității cibernetice*** și de elaborare a planurilor de securitate cibernetică; și

(c) după caz, utilizarea tehnologiei ***comune*** și a arhitecturii ***cu sursă deschisă***, precum și a celor mai bune practici asociate în scopul realizării controlului, interoperabilității și a standardelor comune***;***

(ca) după caz, înlesnirea achiziționării în comun a serviciilor TIC și a produselor TIC relevante.

▌

Articolul 14

Șeful CERT-UE

După obținerea aprobării cu o majoritate de două treimi din membrii IICB, Comisia numește șeful CERT-UE. IICB este consultat în toate etapele procedurii care precedă numirea șefului CERT-UE, în special în ceea ce privește elaborarea anunțurilor privind posturile vacante, examinarea dosarelor de candidatură și desemnarea comitetelor de selecție pentru acest post. Lista finală a candidaților include cel puțin un bărbat și o femeie.

Șeful CERT-UE prezintă IICB și președintelui IICB ***cel puțin o date pe an*** rapoarte ▌ privind ***activitățile și*** performanța CERT-UE ***în perioada de referință***, ***inclusiv privind***, execuția bugetară, acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 ▌. ***Rapoartele respective includ programul de lucru pentru perioada următoare, planificarea financiară a veniturilor și cheltuielilor, inclusiv a personalului, actualizările planificate ale catalogului de servicii al CERT-UE și o evaluare a impactului preconizat pe care aceste actualizări l-ar putea avea asupra resurselor financiare și umane.***

La cererea IICB, șeful CERT-UE prezintă IICB și rapoarte ad-hoc.

Articolul 15

Aspecte financiare și de personal

(1) ***CERT-UE este un furnizor de servicii interinstituțional autonom pentru toate entitățile Uniunii, integrat în structura administrativă a unei direcții generale a Comisiei, pentru a beneficia de structurile de sprijin administrativ, financiar, contabil și în materie de gestiune ale Comisiei.*** ▌ Comisia ***informează IICB cu privire la amplasarea administrativă a*** CERT-UE ***și la eventuale modificări ale acesteia***. ***Această abordare trebuie evaluată periodic pentru a permite luarea unor măsuri adecvate, inclusiv posibila transformare a CERT-UE într-un oficiu al Uniunii.***

(1a) Toate deciziile referitoare la asigurarea personalului și la alocarea bugetului CERT-UE sunt supuse aprobării oficiale a IICB.

(2) În ceea ce privește aplicarea procedurilor administrative și financiare, șeful CERT-UE acționează sub autoritatea Comisiei ***și sub supravegherea IICB***.

(3) Sarcinile și activitățile CERT-UE, inclusiv serviciile furnizate de CERT-UE în temeiul articolului 12 alineatele (2), (3), (4) și (6) și al articolului 13 alineatul (1) ***entităților*** Uniunii finanțate în cadrul rubricii „Administrația publică europeană” din cadrul financiar multianual, sunt finanțate printr-o linie bugetară separată a bugetului Comisiei. Posturile alocate CERT-UE sunt detaliate într-o notă de subsol la schema de personal a Comisiei.

(4) ***Entitățile*** Uniunii, altele decât cele menționate la alineatul (3), aduc o contribuție anuală la bugetul CERT-UE pentru a acoperi serviciile furnizate de CERT-UE în temeiul alineatului menționat. Contribuțiile respective se bazează pe orientările oferite de IICB și convenite între fiecare entitate și CERT-UE în cadrul acordurilor privind nivelul serviciilor. Contribuțiile reprezintă un procent echitabil și proporțional din costurile totale ale serviciilor furnizate. Acestea sunt primite în cadrul liniei bugetare separate menționate la alineatul (3) ca venituri alocate, astfel cum se prevede la articolul 21 alineatul (3) litera (c) din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului[9].

[9] Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de

(5) Costurile aferente sarcinilor definite la articolul 12 alineatul (5) se recuperează de la ***entitățile*** Uniunii beneficiare ale serviciilor furnizate de CERT-UE. Veniturile sunt alocate liniilor bugetare prin care se suportă costurile.

Articolul 16

Cooperarea CERT-UE cu omologii din statele membre

(1) CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, inclusiv CERT, centrele naționale de securitate cibernetică, CSIRT și punctele unice de contact menționate la articolul 8 din ***Directiva (UE) 2022/2555***, cu privire la amenințările cibernetice, vulnerabilități, incidente, ***incidente evitate la limită și la*** posibilele contramăsuri***, precum și la cele mai bune practici*** și la toate aspectele relevante pentru îmbunătățirea protecției mediilor ***TIC*** ale ***entităților*** Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul ***15*** din ***Directiva (UE) 2022/2555***. ***CERT-UE sprijină Comisia în cadrul EU-CyCLONe menționat la articolul 16 din Directiva (UE) 2022/2555 în ceea ce privește gestionarea coordonată a incidentelor și crizelor de mare amploare.***

(2) CERT-UE poate face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare fără ***autorizarea*** entității afectate***, cu condiția ca datele cu caracter personal să fie protejate în conformitate cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului***[10]. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul de securitate cibernetică numai cu ***autorizarea*** entității afectate ***și cu respectarea Regulamentului (UE) 2016/679***.

---

modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 (JO L 193, 30.7.2018, p. 1).

[10] ***Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).***

Articolul 17

Cooperarea CERT-UE cu omologii din statele terțe

(1) CERT-UE poate coopera cu omologii din statele terțe***, care sunt supuși cerințelor Uniunii în materie de securitate cibernetică sau unor cerințe similare,*** inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice formă de cooperare cu astfel de omologi, inclusiv într-un cadru în care omologii din afara UE cooperează cu omologii naționali din statele membre, CERT-UE solicită aprobarea prealabilă a IICB.

(2) CERT-UE poate coopera cu alți parteneri, precum entități comerciale ***(inclusiv entități din cadrul sectorului)***, organizații internaționale, entități naționale din afara Uniunii Europene sau experți individuali, pentru a colecta informații cu privire la amenințările cibernetice generale și specifice, ***la incidente evitate la limită***, la vulnerabilități și la posibilele contramăsuri. Pentru o cooperare mai extinsă cu astfel de parteneri, CERT-UE solicită aprobarea prealabilă a IICB.

(3) Cu acordul entității afectate de un incident, CERT-UE poate să furnizeze informații referitoare la incident partenerilor care pot contribui la analiza acestuia.

Capitolul V

OBLIGAȚII DE COOPERARE ȘI DE RAPORTARE

Articolul 18

Gestionarea informațiilor

(1) CERT-UE și ***entitățile*** Uniunii respectă obligația de a nu divulga informații care constituie secret profesional, în conformitate cu articolul 339 din Tratatul privind funcționarea Uniunii Europene sau cu cadrele echivalente aplicabile.

(2) Dispozițiile Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[11] se aplică în ceea ce privește cererile de acces public la documentele

[11] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

deținute de CERT-UE, inclusiv obligația care decurge din regulamentul menționat de a consulta alte ***entități*** ale Uniunii ***sau, după caz, statele membre,*** ori de câte ori o cerere se referă la documentele lor.

(3) Prelucrarea datelor cu caracter personal efectuată în temeiul prezentului regulament face obiectul Regulamentului (CE) nr. 2018/1725 ▌.

Orice prelucrare, schimb, colectare sau păstrare a datelor cu caracter personal de către CERT-UE, IICB și entitățile Uniunii se limitează la prelucrarea, schimbul, colectarea sau păstrarea care este strict necesară și se efectuează exclusiv în scopul îndeplinirii obligațiilor care le revin în temeiul prezentului regulament.

(3a) În termen de ... [un an de la intrarea în vigoare a prezentului regulament], Comisia adoptă un act delegat în conformitate cu articolul 24a pentru a specifica activitățile de prelucrare a datelor cu caracter personal permise în temeiul prezentului regulament, inclusiv scopul prelucrării, categoriile de date cu caracter personal, categoriile de persoane vizate, condițiile de prelucrare a datelor, perioadele maxime de păstrare, definirea operatorilor de date și a persoanelor împuternicite de operatori și destinatarii în cazul transmiterii.

Actul delegat menționat la primul paragraf limitează activitățile de prelucrare la cele strict necesare și impune ca aceste activități de prelucrare să fie cât mai specifice posibil și să nu includă păstrarea nediferențiată a datelor privind traficul sau conținutul.

Comisia modifică actul delegat menționat la primul paragraf atunci când identifică modificări semnificative în ceea ce privește necesitatea, scopurile specifice sau entitățile implicate în prelucrarea datelor cu caracter personal în sensul prezentului regulament.

(4) CERT-UE și ***entitățile*** Uniunii gestionează informațiile în conformitate cu normele prevăzute în [propunerea de regulament privind securitatea informațiilor]. ***Atunci când cooperează cu alți omologi, CERT-UE folosește norme echivalente referitoare la gestionarea informațiilor.***

(5) Orice contact cu CERT-UE inițiat sau solicitat de serviciile naționale de securitate și de informații trebuie comunicat fără întârzieri nejustificate Direcției Securitate a Comisiei***, Europol*** și președintelui IICB.

(5a) Informațiile privind finalizarea planurilor de securitate de către entitățile Uniunii sunt comunicate autorităților care acordă descărcarea de gestiune.

(5b) Documentele de orientare și recomandările, precum și apelurile la acțiune emise de IICB sunt comunicate autorităților care acordă descărcarea de gestiune.

Articolul 19

Acorduri și obligații privind schimbul de informații ***în materie de securitate cibernetică***

(-1) Entitățile Uniunii pot să transmită și să furnizeze în mod voluntar CERT-UE informații privind amenințările cibernetice, incidentele, incidentele evitate la limită și vulnerabilitățile care le afectează. CERT-UE se asigură că sunt adoptate măsuri eficace pentru a garanta confidențialitatea și protecția adecvată a informațiilor furnizate de entitatea Uniunii care transmite informația. CERT-UE se asigură că sunt disponibile mijloace eficiente de comunicare, în scopul de a facilita schimbul de informații cu entitățile Uniunii. Atunci când prelucrează notificările, CERT-UE poate acorda prioritate notificărilor obligatorii față de notificările voluntare. Notificarea voluntară nu impune entității Uniunii care transmite informația nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.

(1) Pentru a ***permite CERT-UE să-și îndeplinească în mod eficace misiunea și sarcinile prevăzute la articolul 12 din prezentul regulament, în special să coordoneze*** gestionarea vulnerabilităților ▌, CERT-UE poate solicita ***entităților*** Uniunii să îi furnizeze informații din inventarele lor de sisteme ***TIC*** care sunt relevante pentru sprijinul CERT-UE. ***Entitatea Uniunii*** care primește o astfel de solicitare ***poate*** transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.

Fără a aduce atingere Regulamentului (UE) 2018/1725, orice schimb de date între CERT-UE și entitățile Uniunii se desfășoară respectând principiile unor garanții clare pentru cazuri de utilizare specifice și folosesc tratatele de asistență juridică reciprocă și alte acorduri pentru a asigura un nivel ridicat de protecție a drepturilor atunci când prelucrează cereri de acces transfrontalier la date.

▌

(3) CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea ***entității*** Uniunii afectate de incident numai cu consimțământul entității respective. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea țintei incidentului de securitate cibernetică numai cu consimțământul entității afectate de incident. ***Având în vedere sarcinile sale de control, Parlamentul European poate solicita astfel de informații chiar și fără consimțământul entității Uniunii în cauză. Dacă Parlamentul European solicită informațiile fără consimțământul entității în cauză, deliberările sale nu sunt făcute publice și toate documentele relevante sunt analizate numai pe baza principiului necesității de a cunoaște.***

(4) Acordurile ***și obligațiile*** privind schimbul de informații ***în materie de securitate cibernetică*** nu se aplică în cazul informațiilor UE clasificate (IUEC) și al informațiilor pe care o ***entitate*** a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o agenție de aplicare a legii, ***cu excepția cazului în care serviciul de securitate sau de informații al statului membru sau agenția de aplicare a legii în cauză permite ca aceste informații să*** fie comunicate CERT-UE.

Articolul 20

Obligații de ***raportare***

(1) Toate ***entitățile*** Uniunii ***raportează*** CERT-UE***, în conformitate cu alineatul (1d), orice incident care are un impact semnificativ***. ***Un incident este considerat a fi semnificativ dacă:***

(a) a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză;

(b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile.

(1a) Entitățile Uniunii notifică, printre altele, orice informații care permit CERT-UE să stabilească orice impact între entități, orice impact asupra statului membru gazdă sau orice impact transfrontalier în urma unui incident semnificativ. Simpla notificare nu expune entitatea notificatoare unei răspunderi sporite.

(1b) ***După caz, entitățile Uniunii notifică, fără întârzieri nejustificate, utilizatorilor rețelei și ai sistemelor informatice afectate sau ai altor componente ale mediului TIC care ar putea fi afectate de un incident semnificativ sau de o amenințare cibernetică semnificativă legată de orice măsuri sau măsuri corective care pot fi luate ca răspuns la incident sau amenințare. După caz, entitățile Uniunii informează utilizatorii despre amenințare.***

(1c) ***În cazul în care un incident semnificativ sau o amenințare cibernetică semnificativă afectează o rețea și un sistem informatic sau o componentă a mediului TIC al unei entități a Uniunii care știe că este conectată la mediul TIC al unei alte entități a Uniunii, CERT-UE notifică, fără întârzieri nejustificate, entitatea afectată a Uniunii.***

(1d) ***Toate entitățile Uniunii transmit CERT-UE:***

(a) ***fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care au luat cunoștință de incidentul semnificativ, o avertizare timpurie, care, după caz, indică dacă există suspiciuni că incidentul semnificativ este cauzat de acțiuni ilegale sau răuvoitoare sau ar putea avea un impact transfrontalier sau în mai multe entități;***

(b) ***fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, un raport al incidentului, care, după caz, actualizează informațiile menționate la litera (a) și prezintă o evaluare inițială a incidentului semnificativ, a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili;***

(c) ***la cererea CERT-UE, un raport intermediar privind actualizările relevante ale situației.***

(2) ***Entitățile*** Uniunii ***prezintă*** apoi CERT-UE ***un raport final, în termen de cel mult o lună de la prezentarea raportului incidentului menționat la alineatul (1d) litera (b)***. ***În cazul unor incidente semnificative în curs la momentul transmiterii raportului final, se prezintă un raport privind progresele înregistrate la momentul respectiv și un raport final în termen de o lună de la soluționarea incidentului. Raportul incidentului*** include ***cel puțin următoarele informații***, dacă sunt ***disponibile***:

(a) ***o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia;***

(b) ***tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;***

(c) ***măsurile de atenuare care au fost aplicate sau sunt în curs de aplicare;***

(d) ***dacă este cazul, impactul potențial al incidentului asupra altor entități ale Uniunii sau impactul transfrontalier.***

(2a) În cazuri justificate corespunzător și în acord cu CERT-UE, entitatea în cauză a Uniunii poate folosi o derogare de la termenul prevăzut la alineatul (2). Entitatea în cauză a Uniunii prezintă un raport privind progresele înregistrate până la termenul de prezentare a raportului final, în cazul în care se convine asupra unei derogări.

(2b) Entitățile Uniunii, la cererea CERT-UE și fără întârzieri nejustificate, îi furnizează CERT-UE informații digitale create prin utilizarea dispozitivelor electronice implicate în incidentele respective. CERT-UE poate stabili mai în detaliu tipurile de informații digitale de care are nevoie pentru o cunoaștere detaliată a situației și pentru răspunsul la incidente.

(3) CERT-UE transmite lunar ENISA un raport de sinteză cu date anonimizate și agregate privind incidentele ***semnificative***, amenințările cibernetice ▌, ***incidentele, incidentele evitate la limită și*** vulnerabilitățile ▌ notificate în conformitate cu alineatul ***(1d) de la prezentul articol și cu articolul 19 alineatul (-1)***.

(4) ***În termen de ... [un an de la intrarea în vigoare a regulamentului], CERT-UE*** emite documente de orientare sau recomandări ***despre acordurile referitoare la rapoarte și la*** conținutul ***acestora***. ***Atunci când elaborează astfel de documente de orientare sau recomandări, CERT-UE ține seama de specificațiile prevăzute de actele de punere în aplicare adoptate de Comisie care precizează tipul de informații, formatul și procedura unei notificări transmise în temeiul articolului 23 alineatul (11) din Directiva (UE) 2022/2555.*** CERT-UE difuzează detaliile tehnice adecvate pentru a permite detectarea proactivă, răspunsul la incidente sau adoptarea unor măsuri de atenuare de către ***entitățile*** Uniunii.

(5) Obligațiile de ***raportare*** nu se aplică în cazul informațiilor IUEC și al informațiilor pe care o ***entitate*** a Uniunii le-a primit de la un serviciu de securitate sau de informații al

unui stat membru sau de la o autoritate de aplicare a legii cu condiția explicită ca acestea să nu fie comunicate CERT-UE.

Articolul 21

Coordonarea răspunsului la incidente și cooperarea cu privire la incidente ▌

(1) Acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente, CERT-UE facilitează schimbul de informații cu privire la amenințările cibernetice, vulnerabilități***, incidentele evitate la limită*** și incidente, între:

(a) ***entitățile*** Uniunii;

(b) omologii menționați la articolele 16 și 17.

(2) CERT-UE facilitează coordonarea între ***entitățile*** Uniunii în ceea ce privește răspunsul la incidente, inclusiv prin:

(a) contribuția la o comunicare externă coerentă;

(b) asistență reciprocă;

(c) utilizarea optimă a resurselor operaționale;

(d) coordonarea cu alte mecanisme de răspuns la situații de criză la nivelul Uniunii.

(3) ***În cooperare cu ENISA,*** CERT-UE sprijină ***entitățile*** Uniunii în ceea ce privește conștientizarea situației amenințărilor cibernetice, a vulnerabilităților***, a incidentelor evitate la limită*** și a incidentelor***, precum și schimburile legate de cele mai recente evoluții în domeniul securității cibernetice***.

(4) ***În termen de ... [un an de la intrarea în vigoare a regulamentului],*** IICB elaborează orientări privind coordonarea răspunsului la incidente și cooperarea în cazul incidentelor semnificative. În cazul în care se suspectează că un incident este de natură penală, ***IICB și*** CERT-UE furnizează orientări privind raportarea incidentului către autoritățile de aplicare a legii ***fără întârzieri nejustificate***.

Articolul 22

Incidente majore

(1) CERT-UE coordonează***, la nivelul entităților*** Uniunii***, gestionarea incidentelor*** majore. ***În această privință,*** CERT-UE menține un inventar al expertizei tehnice necesare pentru răspunsul la incidente în cazul unor astfel de ***incidente majore și sprijină IICB în coordonarea planurilor de gestionare a crizelor cibernetice ale entităților Uniunii pentru incidentele majore menționate la articolul 7 alineatul (2a)***.

(2) ***Entitățile*** Uniunii contribuie la inventarul expertizei tehnice prin transmiterea unei liste, actualizate anual, de experți disponibili în cadrul organizațiilor respective, în care sunt detaliate competențele tehnice specifice ale acestora.

(3) Cu aprobarea ***entităților*** Uniunii în cauză, CERT-UE poate apela, de asemenea, la experții de pe lista menționată la alineatul (2) pentru a contribui la identificarea răspunsului la un ***incident*** major într-un stat membru, în conformitate cu procedurile operaționale ale ***EU-CyCLONe***. ***Normele specifice privind accesul și folosirea experților tehnici din entitățile Uniunii sunt aprobate de IICB la propunerea CERT-UE.***

Capitolul VI

DISPOZIȚII FINALE

Articolul 23

Acorduri bugetare inițiale

(1) În propunerea sa pentru primul buget care urmează să fie adoptat după ... [data intrării în vigoare a prezentului regulament], Comisia ține seama de creșterea nevoilor bugetare și de personal ale tuturor entităților Uniunii, în special cele ale entităților mici ale Uniunii, care țin de noile obligații care decurg din prezentul regulament.

(2) Pentru a asigura funcționarea corectă și stabilă a CERT-UE, Comisia ***poate*** propune realocarea personalului și a resurselor financiare ***din bugetele TIC ale anumitor entități ale Uniunii*** către bugetul Comisiei ***pentru a fi utilizate în operațiunile CERT-UE, pe baza unor criterii clare și fără a aduce atingere securității cibernetice a***

acestor entități. Realocarea produce efecte în același timp cu primul buget adoptat după intrarea în vigoare a prezentului regulament.

Articolul 24

Revizuire

(1) ***Cel puțin o dată pe an,*** IICB, cu sprijinul CERT-UE, raportează ▌ Comisiei cu privire la punerea în aplicare a prezentului regulament. IICB poate, de asemenea, să facă recomandări Comisiei pentru a propune modificarea prezentului regulament.

(2) Comisia prezintă Parlamentului European și Consiliului ***o evaluare și*** un raport privind punerea în aplicare a prezentului regulament ***și privind experiența acumulată la nivel strategic și operațional până la ... [36 de*** luni de la data intrării în vigoare a prezentului regulament***]*** și, ulterior, o dată la ***doi*** ani.

(2a) Rapoartele menționate la prezentul articol alineatul (2) evaluează, ținând seama de articolul 15 alineatul (1a), posibilitatea transformării CERT-UE în oficiu al Uniunii.

(3) Comisia evaluează funcționarea prezentului regulament și prezintă un raport Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor nu mai devreme de cinci ani de la data intrării în vigoare.

Articolul 24a

Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Competența de a adopta acte delegate menționată la articolul 18 alineatul (3a) se conferă Comisiei pe o perioadă nedeterminată de la ... [o zi după data intrării în vigoare a prezentului regulament].

(3) Delegarea de competențe menționată la articolul 18 alineatul (3a) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene

sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(5) Un act delegat adoptat în temeiul articolului 18 alineatul (3a) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 25

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

I

EXPUNERE DE MOTIVE

CONTEXT

În propunerea sa privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii (IOAUE), Comisia a prevăzut măsuri pentru ca toate entitățile Uniunii să stabilească un cadru pentru norme și măsuri comune în materie de securitate cibernetică pentru a îmbunătăți reziliența și capacitățile lor de răspuns la incidente. Acesta este primul act legislativ al Uniunii care se axează pe securitatea cibernetică a IOAUE.

Scopul propunerii este de a îmbunătăți reziliența și capacitățile de răspuns la incidente ale entităților Uniunii și de a extinde mandatul și finanțarea CERT-UE, care va fi redenumit din „Centrul de răspuns la incidente de securitate cibernetică” în „Centrul de securitate cibernetică”. Propunerea instituie, de asemenea, un Consiliu interinstituțional pentru securitate cibernetică (IICB), care are sarcina de a monitoriza aplicarea regulamentului de către IOAUE și de a supraveghea aplicarea priorităților și obiectivelor generale de către CERT-UE.

RAPORTOAREA

Raportoarea salută propunerea Comisiei și este de acord cu alegerea unui regulament ca instrument adecvat pentru a aborda tendința de proliferare a amenințărilor cibernetice, deoarece numărul incidentelor semnificative ce afectează IOAUE și sunt provocate de actori care generează amenințări persistente avansate (APT) a crescut dramatic în perioada 2019-2021. Prin urmare, aspectele legate de securitatea cibernetică ar trebui să beneficieze de o atenție sporită și de un buget adecvat.

Raportoarea este de părere că această propunere este esențială pentru a îmbunătăți reziliența și protecția administrației publice a UE, având în vedere numărul tot mai mare de amenințări cibernetice care devin mai sofisticate. În acest sens, cooperarea interinstituțională este valoroasă pentru detectarea, prevenirea și monitorizarea amenințărilor și riscurilor cibernetice, precum și pentru răspunsul la ele. IOAUE urmează să își elaboreze măsurile în materie de securitate cibernetică și răspunsurile la amenințările cibernetice și la potențialele atacuri. În consecință, se impune o abordare comună.

Raportoarea consideră că instituțiile, organele și agențiile UE ar trebui să dispună de resurse adecvate pentru a face față provocărilor reprezentate de amenințările cibernetice tot mai mari. În special, cunoștințele și competențele în domeniul securității cibernetice ar trebui protejate în cadrul IOAUE.

Propunerea abordează problema resurselor umane prin centralizarea resurselor către CERT-UE. Modelul centralizat propus este menit să îmbunătățească recrutarea experților în cadrul IOAUE. Raportoarea salută consolidarea mandatului CERT-UE și consideră că este nevoie să i se pună la dispoziție resursele necesare pentru îndeplinirea acestuia, iar structura sa ar trebui analizată cu atenție în viitor.

IOAUE variază considerabil în ceea ce privește dimensiunea și rolul lor. Unele dintre ele au

rețele internaționale semnificative. Prin urmare, raportoarea subliniază că ar trebui să li se permită un nivel suficient de flexibilitate și o abordare bazată pe riscuri pentru a-și putea îndeplini sarcinile. În același timp, ar trebui găsită o abordare uniformă pentru combaterea amenințărilor cibernetice, deoarece toate IOAUE sunt interconectate și nu ar trebui să existe nicio verigă slabă în lanț.

1.3.2023

AVIZ AL COMISIEI PENTRU LIBERTĂȚI CIVILE, JUSTIȚIE ȘI AFACERI INTERNE

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Raportor pentru aviz (*): Tomas Tobé

(*) Procedura comisiei asociate – articolul 57 din Regulamentul de procedură

AMENDAMENTE

Comisia pentru libertăți civile, justiție și afaceri interne recomandă Comisiei pentru industrie, cercetare și energie, care este comisie competentă, să ia în considerare următoarele amendamente:

Amendamentul 1

Propunere de regulament
Considerentul 4

Textul propus de Comisie	*Amendamentul*
(4) Instituțiile, organele și agențiile Uniunii sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca instituțiile, organele și agențiile Uniunii să	(4) Instituțiile, organele și agențiile Uniunii ***au fost și*** sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca instituțiile, organele și agențiile Uniunii să

atingă un nivel comun ridicat de securitate cibernetică printr-un „nivel de referință în materie de securitate cibernetică” (un set de norme minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte pentru a reduce la minimum riscurile de securitate cibernetică), prin schimbul de informații și colaborarea în acest domeniu.	atingă un nivel comun ridicat de securitate cibernetică printr-un „nivel de referință în materie de securitate cibernetică” (un set de norme minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte pentru a reduce la minimum riscurile de securitate cibernetică), prin schimbul de informații și colaborarea în acest domeniu.

Amendamentul 2

Propunere de regulament
Considerentul 5

Textul propus de Comisie	*Amendamentul*
(5) [Propunerea de Directivă NIS 2] privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune urmărește să îmbunătățească și mai mult capacitatea de reziliență și capacitatea de răspuns la incidente ale entităților publice și private, ale autorităților și organelor naționale competente, precum și ale Uniunii în ansamblu. Prin urmare, este necesar ca instituțiile, organele și agențiile Uniunii să urmeze exemplul prin asigurarea unor norme care să fie coerente cu [propunerea de Directivă NIS 2] și să reflecte nivelul său de ambiție.	(5) [Propunerea de Directivă NIS 2] privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune urmărește să îmbunătățească și mai mult capacitatea de reziliență și capacitatea de răspuns la incidente ale entităților publice și private, ale autorităților și organelor naționale competente, precum și ale Uniunii în ansamblu. Prin urmare, este necesar ca instituțiile, organele și agențiile Uniunii să urmeze exemplul prin asigurarea unor norme care să fie coerente cu [propunerea de Directivă NIS 2] și să reflecte nivelul său de ambiție. ***Cerințele de securitate ar trebui să fie cel puțin egale cu cerințele minime de securitate ale entităților prevăzute în Directiva (UE) 2022/2555 sau mai mari decât acestea.***

Amendamentul 3

Propunere de regulament
Considerentul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	(6a) Instituțiile, organele, oficiile și agențiile Uniunii ar trebui să dispună de

	mijloace și instrumente adecvate prin care să își consolideze reziliența cibernetică. Este esențial, prin urmare, să se asigure că există mecanisme de coordonare adecvate pentru ca procesul decizional să se desfășoare într-un mod eficient și eficace.

Amendamentul 4

Propunere de regulament
Considerentul 22

Textul propus de Comisie	*Amendamentul*
(22) Toate datele cu caracter personal prelucrate în temeiul prezentului regulament trebuie prelucrate în conformitate cu legislația privind protecția datelor, inclusiv cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului.[7]	(22) Toate datele cu caracter personal prelucrate în temeiul prezentului regulament trebuie prelucrate în conformitate cu legislația ***Uniunii*** privind protecția datelor, inclusiv cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului.[7] ***Prezentul regulament nu ar trebui să afecteze aplicarea legislației Uniunii care reglementează prelucrarea datelor cu caracter personal, inclusiv sarcinile și competențele conferite AEPD. CERT-UE și IICB ar trebui să lucreze în strânsă cooperare cu AEPD și cu personalul specializat în protecția datelor din instituțiile, organele, oficiile și agențiile Uniunii, pentru a asigura respectarea deplină a legislației Uniunii în materie de protecție a datelor.***
[7] Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).	[7] Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

Amendamentul 5

Propunere de regulament
Considerentul 22 a (nou)

Textul propus de Comisie	*Amendamentul*
	(22a) Sistemele și serviciile de securitate cibernetică implicate în prevenirea, detectarea și răspunsul la amenințările cibernetice ar trebui să respecte legislația privind protecția datelor și a vieții private și să adopte măsuri de salvgardare tehnice și organizatorice relevante pentru a asigura că această conformitate se realizează într-un mod responsabil.

Amendamentul 6

Propunere de regulament
Considerentul 23

Textul propus de Comisie	*Amendamentul*
(23) CERT-UE și instituțiile, organele și agențiile Uniunii ***trebuie*** să gestioneze informațiile în conformitate cu normele prevăzute în regulament [propunerea de regulament privind securitatea informațiilor]. Pentru a asigura coordonarea în materie de securitate, orice contacte cu CERT-UE inițiate sau solicitate de serviciile naționale de securitate și de informații trebuie comunicate fără întârzieri nejustificate Direcției Securitate a Comisiei și președintelui IICB.	(23) CERT-UE și instituțiile, organele și agențiile Uniunii ***ar trebui*** să gestioneze informațiile în conformitate cu normele ***Uniunii privind securitatea informațiilor, în special cele*** prevăzute în regulament [propunerea de regulament privind securitatea informațiilor]. Pentru a asigura coordonarea în materie de securitate, orice contacte cu CERT-UE inițiate sau solicitate de serviciile naționale de securitate și de informații trebuie comunicate fără întârzieri nejustificate Direcției Securitate a Comisiei și președintelui IICB.

Amendamentul 7

Propunere de regulament
Considerentul 25 a (nou)

Textul propus de Comisie	*Amendamentul*
	(25a) Autoritatea Europeană pentru

	Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 și a emis un aviz la 17 mai 2022.

Amendamentul 8

Propunere de regulament
Articolul 4 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Fiecare instituție, organ și agenție a Uniunii numește un responsabil local cu securitatea cibernetică sau o funcție echivalentă care acționează ca punct unic de contact în ceea ce privește toate aspectele securității cibernetice.	5. Fiecare instituție, organ și agenție a Uniunii numește un responsabil local cu securitatea cibernetică sau o funcție echivalentă care acționează ca punct unic de contact în ceea ce privește toate aspectele securității cibernetice. ***Responsabilul local cu securitatea cibernetică cooperează cu responsabilul cu protecția datelor desemnat în conformitate cu articolul 43 din Regulamentul (UE) 2018/1725 atunci când se ocupă de activități care se suprapun, cum ar fi aplicarea protecției datelor începând cu momentul conceperii și a protecției implicite a datelor în cazul măsurilor de securitate cibernetică, selectarea măsurilor de securitate cibernetică care implică protecția datelor cu caracter personal, gestionarea integrată a riscurilor și gestionarea integrată a incidentelor de securitate.***

Amendamentul 9

Propunere de regulament
Articolul 9 – alineatul 3 – paragraful 1 – litera ka (nouă)

Textul propus de Comisie	*Amendamentul*
	(ka) Autoritatea Europeană pentru Protecția Datelor;

Amendamentul 10

Propunere de regulament
Articolul 9 – alineatul 3 – paragraful 1 – litera kb (nouă)

Textul propus de Comisie	*Amendamentul*
	(kb) Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii.

Amendamentul 11

Propunere de regulament
Articolul 12 – alineatul 2 – litera ea (nouă)

Textul propus de Comisie	*Amendamentul*
	(ea) informează Autoritatea Europeană pentru Protecția Datelor cu privire la orice indiciu privind o încălcare de către o instituție, un organ, un oficiu sau o agenție a Uniunii a obligațiilor prevăzute în prezentul regulament care includ o prelucrare ilegală a datelor cu caracter personal;

Amendamentul 12

Propunere de regulament
Articolul 12 – alineatul 2 – litera eb (nouă)

Textul propus de Comisie	*Amendamentul*
	(eb) lucrează în strânsă cooperare cu Autoritatea Europeană pentru Protecția Datelor la soluționarea incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal sau încălcarea confidențialității comunicațiilor electronice.

Amendamentul 13

Propunere de regulament
Articolul 12 – alineatul 7 a (nou)

Textul propus de Comisie	*Amendamentul*
	7a. CERT-UE informează Autoritatea Europeană pentru Protecția Datelor atunci când tratează vulnerabilități semnificative, incidente semnificative sau atacuri majore care au potențialul de a conduce la încălcări ale securității datelor cu caracter personal sau la încălcarea confidențialității comunicațiilor electronice.

Amendamentul 14

Propunere de regulament
Articolul 18 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Dispozițiile Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[9] se aplică în ceea ce privește cererile de acces public la documentele deținute de CERT-UE, inclusiv obligația care decurge din regulamentul menționat de a consulta alte instituții, organe și agenții ale Uniunii ori de câte ori o cerere se referă la documentele lor.	2. Dispozițiile Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[9] se aplică în ceea ce privește cererile de acces public la documentele deținute de CERT-UE, inclusiv obligația care decurge din regulamentul menționat de a consulta alte instituții, organe și agenții ale Uniunii***, sau, dacă este cazul, statele membre,*** ori de câte ori o cerere se referă la documentele lor.
[9] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).	[9] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

Amendamentul 15

Propunere de regulament
Articolul 18 – alineatul 3 – paragraful 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	Orice prelucrare, schimb, colectare sau păstrare a datelor cu caracter personal de către CERT-UE, IICB și instituțiile, organele, oficiile și agențiile Uniunii se limitează la prelucrarea, schimbul, colectarea sau păstrarea care este strict necesară și se efectuează exclusiv în scopul îndeplinirii obligațiilor care le revin în temeiul prezentului regulament.

Amendamentul 16

Propunere de regulament
Articolul 18 – alineatul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3a. În termen de... [un an de la intrarea în vigoare a prezentului regulament], Comisia adoptă un act delegat pentru a specifica activitățile de prelucrare a datelor cu caracter personal permise în temeiul prezentului regulament, inclusiv scopul prelucrării, categoriile de date cu caracter personal, categoriile de persoane vizate, condițiile de prelucrare a datelor, perioadele maxime de păstrare, definirea operatorilor de date și a persoanelor împuternicite de operatori și destinatarii în cazul transmiterii.
	Actul delegat menționat la primul paragraf limitează activitățile de prelucrare la cele strict necesare și impune ca aceste activități de prelucrare să fie cât mai specifice posibil și să nu includă păstrarea nediferențiată a datelor privind traficul sau conținutul.
	Comisia modifică actul delegat menționat la primul paragraf atunci când identifică modificări semnificative în ceea ce privește necesitatea, scopurile specifice sau entitățile implicate în prelucrarea datelor cu caracter personal în sensul

prezentului regulament.

Amendamentul 17

Propunere de regulament
Articolul 18 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. CERT-UE și instituțiile, organele și agențiile Uniunii gestionează informațiile în conformitate cu normele prevăzute în [propunerea de regulament privind securitatea informațiilor].	4. CERT-UE și instituțiile, organele și agențiile Uniunii gestionează informațiile în conformitate cu normele ***Uniunii privind securitatea informațiilor, în special cele*** prevăzute în [propunerea de regulament privind securitatea informațiilor].

Amendamentul 18

Propunere de regulament
Articolul 18 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Orice contact cu CERT-UE inițiat sau solicitat de serviciile naționale de securitate și de informații trebuie comunicat fără întârzieri nejustificate Direcției Securitate a Comisiei și președintelui IICB.	5. Orice contact cu CERT-UE inițiat sau solicitat de serviciile naționale de securitate și de informații trebuie comunicat fără întârzieri nejustificate Direcției Securitate a Comisiei***, Europol*** și președintelui IICB.

Amendamentul 19

Propunere de regulament
Articolul 19 – titlu

Textul propus de Comisie	*Amendamentul*
Obligații privind schimbul de informații	Schimbul de informații

Amendamentul 20

Propunere de regulament
Articolul 19 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Pentru a coordona gestionarea vulnerabilităților și răspunsul la incidente, ***CERT-UE le poate solicita instituțiilor, organelor și agențiilor Uniunii să îi furnizeze*** informații din inventarele lor de sisteme ***informatice*** care sunt relevante pentru sprijinul CERT-UE***. Instituția, organul sau agenția*** care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.	1. ***Pentru a îndeplini sarcinile stabilite la articolul 12, în special*** pentru a coordona gestionarea vulnerabilităților și răspunsul la incidente, ***instituțiile, organele sau agențiile Uniunii îi furnizează CERT-UE, la solicitarea acestuia,*** informații din inventarele lor de sisteme ***TIC*** care sunt relevante pentru sprijinul CERT-UE***, inclusiv orice modificare a mediului lor informatic. Entitatea*** care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate. ***Fără a aduce atingere Regulamentului (UE) 2018/1725, orice schimb de date între CERT-UE și instituțiile, organele și agențiile Uniunii se desfășoară respectând principiile unor garanții clare pentru cazuri de utilizare specifice și utilizează tratatele de asistență juridică reciprocă și alte acorduri pentru a asigura un nivel ridicat de protecție a drepturilor atunci când prelucrează cereri de acces transfrontalier la date.***

Amendamentul 21

Propunere de regulament
Articolul 19 – alineatul 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	1a. Instituțiile, organele, oficiile și agențiile Uniunii pot furniza CERT-UE în mod voluntar informații privind amenințările cibernetice, incidentele, incidentele evitate la limită și vulnerabilitățile care le afectează. Acestea pot solicita, de asemenea, din partea CERT-UE asistență tehnică suplimentară și consiliere pentru combaterea incidentelor de securitate cibernetică și a atacurilor majore. CERT-UE poate

acorda prioritate prelucrării notificărilor obligatorii în detrimentul notificărilor voluntare, cu excepția cazului în care primește cereri voluntare urgente și justificate în mod corespunzător din partea instituțiilor, organelor, oficiilor și agențiilor Uniunii.

Amendamentul 22

Propunere de regulament
Articolul 19 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea instituției, organului sau agenției Uniunii afectate de incident numai cu ***consimțământul*** entității respective. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea țintei incidentului de securitate cibernetică numai cu ***consimțământul*** entității afectate de incident.	3. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea instituției, organului sau agenției Uniunii afectate de incident numai cu ***autorizarea*** entității respective. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea țintei incidentului de securitate cibernetică numai cu ***autorizarea*** entității afectate de incident. ***În cazul în care acest lucru este necesar pentru îndeplinirea sarcinilor sale, CERT-UE poate face schimb de informații specifice incidentului, inclusiv în absența autorizării din partea instituției, organului, oficiului sau agenției Uniunii afectate de incident. Instituția, organul, oficiul sau agenția Uniunii este notificată în prealabil cu privire la orice astfel de schimb de informații.***

Amendamentul 23

Propunere de regulament
Articolul 19 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Obligațiile privind schimbul de	4. Obligațiile privind schimbul de

informații nu se aplică în cazul informațiilor UE clasificate (IUEC) și al informațiilor pe care o instituție, ***un*** organ sau ***o*** agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o agenție de aplicare a legii cu ***condiția explicită*** ca ***acestea să nu*** fie comunicate CERT-UE.	informații nu se aplică în cazul informațiilor UE clasificate (IUEC) și al informațiilor pe care o instituție, organ sau agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o agenție de aplicare a legii***,*** cu ***excepția cazului în care serviciul de securitate sau de informații al statului membru sau agenția de aplicare a legii în cauză permite*** ca ***aceste informații să*** fie comunicate CERT-UE.

Amendamentul 24

Propunere de regulament
Articolul 20 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. CERT-UE transmite lunar ENISA un raport de sinteză cu date anonimizate și agregate privind amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative notificate în conformitate cu alineatul (1).	3. CERT-UE transmite lunar ENISA un raport de sinteză cu date anonimizate și agregate privind amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative notificate în conformitate cu alineatul (1). ***Raportul respectiv este făcut public, sub rezerva normelor aplicabile ale Uniunii privind securitatea informațiilor, în special a celor prevăzute în [propunerea de regulament privind securitatea informațiilor].***

Amendamentul 25

Propunere de regulament
Articolul 20 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Obligațiile de notificare nu se aplică în cazul informațiilor IUEC și al informațiilor pe care o instituție, un organ sau o agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o autoritate de aplicare a legii cu ***condiția explicită*** ca	5. Obligațiile de notificare nu se aplică în cazul informațiilor IUEC și al informațiilor pe care o instituție, un organ sau o agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o autoritate de aplicare a legii***,*** cu ***excepția cazului în care***

acestea să ***nu*** fie comunicate CERT-UE.	***serviciul de securitate sau de informații al statului membru în cauză permite*** ca ***aceste informații*** să fie comunicate CERT-UE.

Amendamentul 26

Propunere de regulament
Articolul 21 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. IICB elaborează orientări privind coordonarea răspunsului la incidente și cooperarea în cazul incidentelor semnificative. În cazul în care se suspectează că un incident este de natură penală, CERT-UE ***furnizează orientări privind raportarea incidentului*** către autoritățile de aplicare a legii.	4. IICB elaborează orientări privind coordonarea răspunsului la incidente și cooperarea în cazul incidentelor semnificative. În cazul în care se suspectează că un incident este de natură penală, CERT-UE ***sau IICB raportează incidentul*** către autoritățile de aplicare a legii***, fără întârzieri nejustificate***.

Amendamentul 27

Propunere de regulament
Articolul 24 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 24a
	Exercitarea delegării
	1. Competența de a adopta acte delegate se conferă Comisiei în condițiile prevăzute la prezentul articol.
	2. Competența de a adopta acte delegate menționată la articolul 18 alineatul (3a) se conferă Comisiei pe o perioadă nedeterminată de la ... [o zi după data intrării în vigoare a prezentului regulament].
	3. Delegarea de competențe menționată la articolul 18 alineatul (3a) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia

	respectivă. Decizia produce efecte din ziua următoare datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.
	4. De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.
	5. Un act delegat adoptat în temeiul articolului 18 alineatul (3a) intră în vigoare numai dacă nici Parlamentul European, nici Consiliul nu a ridicat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau dacă, înaintea expirării termenului respectiv, ambele instituții au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Amendamentul 28

Propunere de regulament
Anexa II – paragraful 1 – punctul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	(2a) utilizarea criptării în repaus, a criptării în tranzit, precum și a criptării de la un capăt la altul ori de câte ori este posibil;

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
Referințe	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Comisie competentă Data anunțului în plen	ITRE 4.4.2022
Aviz emis de către Data anunțului în plen	LIBE 4.4.2022
Comisii asociate - data anunțului în plen	15.9.2022
Raportor/Raportoare pentru aviz Data numirii	Tomas Tobé 12.12.2022
Examinare în comisie	31.1.2023
Data adoptării	1.3.2023
Rezultatul votului final	+: 62 –: 0 0: 1
Membri titulari prezenți la votul final	Magdalena Adamowicz, Abir Al-Sahlani, Malik Azmani, Katarina Barley, Pietro Bartolo, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Caterina Chinnici, Clare Daly, Lena Düpont, Lucia Ďuriš Nicholsonová, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Erik Marquardt, Nuno Melo, Maite Pagazaurtundúa, Karlo Ressler, Diana Riba i Giner, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Yana Toom, Milan Uhrík, Tom Vandendriessche, Jadwiga Wiśniewska
Membri supleanți prezenți la votul final	Susanna Ceccardi, Gwendoline Delbos-Corfield, Loucas Fourlas, Beata Kempa, Philippe Olivier, Dragoş Tudorache, Petar Vitanov, Tomáš Zdechovský
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Gheorghe Falcă, Jean-François Jalkh, Petra Kammerevert, Marisa Matias, Martina Michels, Ljudmila Novak, Stanislav Polčák, Mick Wallace, Bernhard Zimniok

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA SESIZATĂ PENTRU AVIZ

62	+
ECR	Patryk Jaki, Assita Kanko, Beata Kempa, Vincenzo Sofo, Jadwiga Wiśniewska
ID	Susanna Ceccardi, Patricia Chagnon, Jean-François Jalkh, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche, Bernhard Zimniok
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Lena Düpont, Gheorghe Falcă, Loucas Fourlas, Andrzej Halicki, Jeroen Lenaers, Nuno Melo, Ljudmila Novak, Stanislav Polčák, Karlo Ressler, Sara Skyttedal, Tomas Tobé, Tomáš Zdechovský
Renew	Abir Al-Sahlani, Malik Azmani, Lucia Ďuriš Nicholsonová, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Ramona Strugariu, Yana Toom, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Petra Kammerevert, Łukasz Kohut, Juan Fernando López Aguilar, Birgit Sippel, Petar Vitanov
The Left	Clare Daly, Marisa Matias, Martina Michels, Mick Wallace
Verts/ALE	Patrick Breyer, Saskia Bricmont, Gwendoline Delbos-Corfield, Alice Kuhnke, Erik Marquardt, Diana Riba i Giner, Tineke Strik

0	-

1	0
NI	Milan Uhrík

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri

13.7.2022

AVIZ AL COMISIEI PENTRU BUGETE

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Raportor pentru aviz: Nils Ušakovs

JUSTIFICARE SUCCINTĂ

Raportorul salută propunerea Comisiei privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii (IOAUE). El consideră că propunerea este necesară pentru a îmbunătăți reziliența și securitatea administrației publice a UE, având în vedere creșterea numărului de amenințări, din ce în ce mai sofisticate, la adresa securității cibernetice. Acest lucru este cu atât mai valabil în contextul geopolitic actual.

Raportorul consideră că cooperarea interinstituțională este esențială pentru a preveni, detecta, monitoriza și răspunde în mod adecvat amenințărilor și riscurilor. Fiecare IOAUE, indiferent de dimensiunea sa, are un rol de jucat și o responsabilitate de asumat în protejarea IOAUE împotriva atacurilor cibernetice, deoarece o singură lacună mică poate pune în pericol toate celelalte IOAUE. Prin urmare, raportorul sprijină ideea unor măsuri de referință în materie de securitate cibernetică. În plus, el consideră că cooperarea interinstituțională, pe lângă faptul că permite IOAUE să își îmbunătățească securitatea cibernetică și răspunsurile la atacurile cibernetice, ar trebui, de asemenea, să analizeze sinergiile potențiale la nivelul metodelor de lucru și al canalelor de comunicare, cu scopul de a reduce sarcina administrativă, de a evita duplicarea eforturilor și de a îmbunătăți pregătirea și protecția.

Contrar celor propuse de Comisie, raportorul este convins că sunt necesare 42 de posturi în loc de 21 pentru ca CERT-UE să funcționeze cu servicii pe deplin operaționale și de ultimă generație. Nu este de acord cu propunerea Comisiei de a compensa parțial posturile suplimentare dedicate CERT-UE prin reducerea numărului de agenți contractuali.

Raportorul susține că, având în vedere dimensiunea sa relativă și posturile suplimentare în domeniul securității cibernetice pe care le-a solicitat în situația estimărilor de venituri și cheltuieli pentru 2023, Parlamentul European ar trebui să aloce CERT-UE primele 48 de posturi în primul buget adoptat după intrarea în vigoare a prezentului regulament. În următorii trei ani, 14 dintre aceste posturi vor fi realocate anual Parlamentului, lăsându-se la sfârșit șase posturi permanente în cadrul CERT-UE. Acest transfer treptat înapoi spre Parlament va permite

stabilitatea personalului și gestionarea cunoștințelor. În același timp, celelalte IOAUE relevante, după primul an, vor aloca treptat posturi CERT-UE. Acest lucru va permite crearea unui grup de 42 de noi membri permanenți ai personalului în cadrul CERT-UE de la început.

Raportorul propune îmbunătățirea mecanismelor actuale ale acordurilor privind nivelul serviciilor pentru serviciile contra cost, astfel cum a recomandat Curtea de Conturi Europeană în Raportul său special 05/2022[1], pentru a se asigura o mai bună gestionare a fluxurilor de numerar și a se reduce activitatea administrativă.

În cele din urmă, raportorul recomandă să se înscrie în buget investițiile și posturile dedicate securității cibernetice în IOAUE. Acest lucru va permite schimbul de bune practici și identificarea eventualelor nevoi de finanțare la nivelul IOAUE.

[1] Raportul special 05/2022: Securitatea cibernetică a instituțiilor, organelor și agențiilor UE: per ansamblu, nivelul de pregătire nu este proporțional cu amenințările

AMENDAMENTE

Comisia pentru bugete recomandă Comisiei pentru industrie, cercetare și energie, care este comisie competentă, să ia în considerare următoarele amendamente:

Amendamentul 1

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) Diferențele dintre instituțiile, organele și agențiile Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică nu ar trebui să includă nicio obligație care să interfereze în mod direct cu exercitarea misiunilor instituțiilor, organelor și agențiilor Uniunii sau să aducă atingere autonomiei lor instituționale. Astfel, aceste instituții, organe și agenții trebuie să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică.	(7) Diferențele dintre instituțiile, organele și agențiile Uniunii***, inclusiv în ceea ce privește dimensiunea resurselor lor umane și financiare,*** necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică nu ar trebui să includă nicio obligație care să interfereze în mod direct cu exercitarea misiunilor instituțiilor, organelor și agențiilor Uniunii sau să aducă atingere autonomiei lor instituționale. Astfel, aceste instituții, organe și agenții trebuie să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică.

Justificare

Nu se poate aștepta aceeași contribuție din partea unei agenții sau a unui organism de dimensiune redusă ca din partea unei instituții a Uniunii.

Amendamentul 2

Propunere de regulament
Considerentul 8

Textul propus de Comisie	*Amendamentul*
(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra instituțiilor, organelor și agențiilor Uniunii, cerințele de gestionare a riscurilor de securitate	(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra instituțiilor, organelor și agențiilor Uniunii, cerințele de gestionare a riscurilor de securitate

cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare instituție, organ sau agenție a Uniunii ***trebuie*** să urmărească alocarea ***unui procent adecvat*** din bugetul său în domeniul tehnologiei informației pentru a-și îmbunătăți nivelul de securitate cibernetică***;*** pe termen lung, ar trebui să ***se urmărească atingerea unui obiectiv*** de ***10 %***.	cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare instituție, organ sau agenție a Uniunii ***ar trebui*** să urmărească alocarea ***unor resurse adecvate*** din bugetul său în domeniul tehnologiei informației pentru a-și îmbunătăți nivelul de securitate cibernetică ***și pentru a asigura cel puțin un nivel minim de securitate cibernetică corespunzător evaluării riscurilor. Costul asigurării securității cibernetice depinde de mai mulți factori, cum ar fi dimensiunea entității, necesitatea de a asigura protecții specifice, suprafața atacurilor și profilul amenințărilor, și include costuri fixe și o parte variabilă. Din cauza amenințărilor tot mai mari,*** pe termen lung ***ar putea fi necesare până la 10 % din bugetul unei entități pentru a asigura un nivel de securitate adecvat***, ***în conformitate cu standardele din sector. În conformitate cu recomandarea Autorității Europene pentru Protecția Datelor formulată în avizul acesteia 8/2022 din 17 mai 2022, cerințele minime de securitate prevăzute în prezentul regulament*** ar trebui să ***fie egale cu sau mai mari decât cerințele minime*** de ***securitate pentru entități prevăzute în Directiva NIS și propunerea de directivă NIS 2.0***.

Justificare

Conform standardelor din sector, 10 % din bugetul pentru informații, comunicații și tehnologie (TIC) ar trebui cheltuit pentru securitatea cibernetică. Bugetul în domeniul tehnologiei informației ar trebui să fie proporțional cu riscurile la nivelul fiecărei IOAUE, în conformitate cu mediile lor externe și interne. În avizul său 8/2022, AEPD recomandă să se adauge în propunere că cerințele minime de securitate ar trebui să fie cel puțin egale cu sau mai mari decât cerințele minime de securitate pentru entități prevăzute în Directiva NIS și propunerea de directivă NIS 2.0.

Amendamentul 3

Propunere de regulament
Considerentul 8 a (nou)

Textul propus de Comisie	*Amendamentul*
	(8a) Pentru a recupera costurile serviciilor contra cost de la instituțiile, organele și agențiile Uniunii care beneficiază de aceste servicii, CERT-UE ar trebui să se asigure că acordurile privind nivelul serviciilor, din care a rezultat peste 90 % din bugetul CERT-UE pentru 2020, nu creează sarcini administrative inutile și reprezintă un instrument util pentru planificarea viitoarelor venituri din fluxurile de numerar.

Justificare

Potrivit Raportului special 05/2022 al CCE, acordurile privind nivelul serviciilor trebuie reînnoite separat în fiecare an. Acest lucru reprezintă o sarcină administrativă și creează probleme legate de fluxul de numerar, întrucât fondurile pe care CERT-UE le primește în temeiul acordurilor nu ajung toate în același timp. Agențiile pot încheia acordurile respective în orice moment, ceea ce poate iniția un cerc vicios în care, din cauza pierderii de venituri, CERT-UE va fi nevoit să își reducă serviciile și nu poate ține pasul cu cererea, determinând alte IOAUE să își rezilieze acordurile și să se mute la furnizori privați. Prin urmare, actualul model de finanțare nu este ideal pentru asigurarea unui nivel stabil și optim al serviciilor.

Amendamentul 4

Propunere de regulament
Considerentul 8 b (nou)

Textul propus de Comisie	*Amendamentul*
	(8b) Pentru a putea garanta un cadru eficace de securitate cibernetică și pentru a oferi o gamă largă de servicii instituțiilor, organelor și agențiilor Uniunii, CERT-UE are nevoie de personal stabil, înalt calificat și specializat. În plus, pentru a asigura gestionarea eficace a cunoștințelor, o mare parte a personalului afectat CERT-

UE ar trebui să fie permanent. Personalul respectiv ar trebui să aibă acces la programe de formare continuă.

Justificare

Trebuie să se aloce CERT-UE 42 de posturi permanente suplimentare pentru a păstra cunoștințele în cadrul CERT-UE. Parlamentul ar trebui să aloce primele 48 de posturi CERT-UE în primul buget adoptat după intrarea în vigoare a prezentului regulament. În următorii trei ani, 14 dintre aceste posturi vor fi realocate anual Parlamentului, șase posturi rămânând permanent în cadrul CERT-UE. În același timp, alte IOAUE relevante, după primul an, vor aloca treptat posturi CERT-UE. Acest mecanism va permite crearea unui grup de 42 de posturi permanente de la început, cu acces adecvat la programe de formare.

Amendamentul 5

Propunere de regulament
Considerentul 8 c (nou)

Textul propus de Comisie	*Amendamentul*
	(8c) În contextul geopolitic actual, este esențial ca echipe specializate și operaționale să protejeze în permanență confidențialitatea datelor împotriva amenințărilor cibernetice.

Amendamentul 6

Propunere de regulament
Considerentul 8 d (nou)

Textul propus de Comisie	*Amendamentul*
	(8d) Înainte de alocarea de resurse umane suplimentare, Comisia ar trebui să efectueze o analiză a nevoilor, ținând seama de perspectiva pe termen lung.

Amendamentul 7

Propunere de regulament
Considerentul 10 a (nou)

Textul propus de Comisie	*Amendamentul*
	(10a) Cooperarea și încrederea

interinstituțională sunt esențiale pentru protejarea, în mod eficient și eficace, a mediului informatic al Uniunii și, prin urmare, a vocii sale democratice. Toate părțile interesate în cauză ar trebui să urmărească în permanență creșterea sinergiilor, reducerea sarcinii administrative și evitarea duplicării eforturilor.

Justificare

Mai multe organisme și rețele sunt implicate în pregătirea orientărilor și colectarea de informații cu privire la incidentele IT, la răspunsurile date etc. Cooperarea dintre toate aceste părți interesate este esențială pentru a evita suprapunerea eforturilor, a găsi sinergii și a asigura fluxuri de comunicare rapide și eficace între acestea.

Amendamentul 8

Propunere de regulament
Considerentul 10 b (nou)

Textul propus de Comisie	*Amendamentul*
	(10b) Pentru a fi în concordanță cu politica pe care Uniunea o promovează în raport cu statele membre, instituțiile, organele, oficiile și agențiile Uniunii ar trebui să renunțe la utilizarea și dezvoltarea de programe informatice, cum ar fi Pegasus, care ar putea încălca dreptul la viață privată și ordinea juridică a Uniunii;

Justificare

În raportul său din 15 februarie 2022 intitulat „Preliminary Remarks on Modern Spyware” (Observații preliminare privind programele informatice de spionaj moderne), AEPD a invitat statele membre să renunțe la utilizarea și dezvoltarea pe teritoriul european a unor programe informatice precum Pegasus, care ar putea afecta dreptul la viață privată, democrația și statul de drept și, prin urmare, ar putea fi incompatibile cu valorile democratice și cu ordinea juridică a Uniunii.

Amendamentul 9

Propunere de regulament
Considerentul 11

Textul propus de Comisie	*Amendamentul*
(11) În mai 2011, secretarii generali ai instituțiilor și organelor Uniunii au decis să constituie o echipă de preconfigurare a unui centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE), supervizată de un comitet director interinstituțional. În iulie 2012, secretarii generali au confirmat modalitățile practice și au convenit să mențină CERT-UE ca entitate permanentă, pentru a contribui în continuare la îmbunătățirea nivelului general de securitate a tehnologiei informației la nivelul instituțiilor, organelor și agențiilor Uniunii, ca exemplu de cooperare interinstituțională vizibilă în domeniul securității cibernetice. În septembrie 2012, CERT-UE a fost înființat ca grup operativ al Comisiei Europene, cu un mandat interinstituțional. În decembrie 2017, instituțiile și organele Uniunii au încheiat un acord interinstituțional privind organizarea și funcționarea CERT-UE[3]. Acest mecanism ar trebui să evolueze în continuare pentru a ***sprijini punerea*** în ***aplicare a prezentului*** regulament.	(11) În mai 2011, secretarii generali ai instituțiilor și organelor Uniunii au decis să constituie o echipă de preconfigurare a unui centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE), supervizată de un comitet director interinstituțional. În iulie 2012, secretarii generali au confirmat modalitățile practice și au convenit să mențină CERT-UE ca entitate permanentă, pentru a contribui în continuare la îmbunătățirea nivelului general de securitate a tehnologiei informației la nivelul instituțiilor, organelor și agențiilor Uniunii, ca exemplu de cooperare interinstituțională vizibilă în domeniul securității cibernetice. În septembrie 2012, CERT-UE a fost înființat ca grup operativ ***permanent*** al Comisiei Europene, cu un mandat interinstituțional. În decembrie 2017, instituțiile și organele Uniunii au încheiat un acord interinstituțional privind organizarea și funcționarea CERT-UE[3]. Acest mecanism ***interinstituțional*** ar trebui să evolueze în continuare pentru a ***fi*** în ***conformitate cu prezentul*** regulament ***și a sprijini punerea sa în aplicare***.
[3] JO C 12, 13.1.2018, p. 1–11.	[3] JO C 12, 13.1.2018, p. 1–11.

Justificare

Potrivit considerentului 11, CERT-UE a fost instituit ca entitate permanentă. Acordul interinstituțional din 2018 ar trebui revizuit pentru a ține seama de repartizarea posturilor din anexa IIa (nouă).

Amendamentul 10

Propunere de regulament
Considerentul 14

Textul propus de Comisie	*Amendamentul*
(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, este necesară instituirea unui Consiliu interinstituțional pentru securitate cibernetică (IICB), care să faciliteze un nivel comun ridicat de securitate cibernetică în rândul instituțiilor, organelor și agențiilor Uniunii prin monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii, prin supravegherea punerii în aplicare a priorităților și a obiectivelor generale de către CERT-UE și prin elaborarea unor orientări strategice pentru CERT-UE. IICB ***trebuie*** să asigure reprezentarea instituțiilor și să includă reprezentanți ai agențiilor și ai organelor prin intermediul Rețelei agențiilor UE.	(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, este necesară instituirea unui Consiliu interinstituțional pentru securitate cibernetică (IICB), care să faciliteze un nivel comun ridicat de securitate cibernetică în rândul instituțiilor, organelor și agențiilor Uniunii prin monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii, prin supravegherea punerii în aplicare a priorităților și a obiectivelor generale de către CERT-UE și prin elaborarea unor orientări strategice pentru CERT-UE. IICB ***ar trebui*** să asigure reprezentarea instituțiilor și să includă reprezentanți ai agențiilor și ai organelor prin intermediul Rețelei agențiilor UE ***și să aplice o procedură de numire care respectă echilibrul de gen. IICB ar trebui să solicite ca toți membrii săi să desemneze o reprezentare echilibrată din punctul de vedere al genului.***

Justificare

Este important să se asigure că principiul echilibrului de gen este respectat în cadrul IICB nou înființat.

Amendamentul 11

Propunere de regulament
Considerentul 24

Textul propus de Comisie	*Amendamentul*
(24) Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor instituțiilor, organelor și agențiilor Uniunii, fiecare instituție, organ și agenție a Uniunii cu cheltuieli în domeniul tehnologiei informației ***trebuie*** să contribuie în mod echitabil la aceste servicii și sarcini. Contribuțiile respective nu aduc atingere autonomiei bugetare a instituțiilor, organelor și agențiilor Uniunii.	(24) Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor instituțiilor, organelor și agențiilor Uniunii, fiecare instituție, organ și agenție a Uniunii cu cheltuieli în domeniul tehnologiei informației ***ar trebui*** să contribuie în mod echitabil la aceste servicii și sarcini***, sub formă de posturi, de contribuții financiare, sau în ambele moduri, în funcție de dimensiunea instituțiilor,***

	organelor și agențiilor, precum și de serviciile și sarcinile furnizate. Contribuțiile respective nu aduc atingere autonomiei bugetare a instituțiilor, organelor și agențiilor Uniunii.

Justificare

În funcție de dimensiunea instituțiilor, organelor și agențiilor Uniunii, contribuțiile la CERT-UE ar putea lua forma alocării de posturi și a contribuțiilor financiare.

Amendamentul 12

Propunere de regulament
Considerentul 24 a (nou)

Textul propus de Comisie	*Amendamentul*
	(24a) Toate instituțiile, organele și agențiile Uniunii ar trebui să aplice principiile egalității de gen și echilibrului de gen atunci când efectuează numirile lor pentru CERT-UE și când alocă resursele lor umane în domeniul tehnologiei informației și al securității cibernetice. În cadrul tuturor instituțiilor, organelor și agențiilor Uniunii, ar trebui să se prevadă cursuri de formare specifice și resurse adecvate pentru promovarea angajării femeilor în domeniul securității cibernetice, contribuind la eliminarea decalajului digital dintre femei și bărbați.

Justificare

Este important să se includă în regulament principiile egalității de gen și echilibrului de gen.

Amendamentul 13

Propunere de regulament
Considerentul 25 a (nou)

Textul propus de Comisie	*Amendamentul*
	(25a) În concluziile sale din 23 mai 2022 privind dezvoltarea posturii de securitate cibernetică a Uniunii Europene, Consiliul

	a invitat autoritățile relevante și Comisia să consolideze reziliența rețelelor și infrastructurilor de comunicații în cadrul Uniunii Europene. Prin urmare, este important să se consolideze suveranitatea și reziliența infrastructurilor și controlul conexiunii, inclusiv în cazul instituțiilor, agențiilor și organelor Uniunii;

Justificare

În concluziile Consiliului privind dezvoltarea posturii de securitate cibernetică a Uniunii Europene din 23 mai 2022, Consiliul solicită să se consolideze reziliența cibernetică a UE și capacitatea sa de a se proteja împotriva atacurilor cibernetice.

Amendamentul 14

Propunere de regulament
Articolul 4 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Fiecare instituție, organ și agenție a Uniunii dispune de mecanisme eficace pentru a se asigura că ***un procent adecvat*** din bugetul în domeniul tehnologiei informației ***este*** cheltuit pentru securitatea cibernetică.	4. Fiecare instituție, organ și agenție a Uniunii dispune de mecanisme eficace pentru a se asigura că ***sunt cheltuite resurse adecvate*** din bugetul în domeniul tehnologiei informației ***pentru securitatea cibernetică, ținând seama de procentul minim din bugetul IT care urmează să fie*** cheltuit pentru securitatea cibernetică ***în conformitate cu standardele din sector, pentru a-și proteja în mod eficace mediul informatic. Instituțiile, organele și agențiile Uniunii înscriu în bugetele lor resursele alocate CERT-UE pentru o mai mare transparență.***

Justificare

Nu se înțelege clar din propunerea Comisiei ce înseamnă mecanisme eficace și procent adecvat. Cel puțin, un criteriu de evaluare a unui procent adecvat este standardul din sector. Înscrierea în bugetul IOAUE ar crea mai multă transparență pentru investițiile în securitatea cibernetică și identificarea posibilelor lacune financiare și schimbul de bune practici.

Amendamentul 15

Propunere de regulament
Articolul 4 – alineatul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	4a. Fiecare instituție, organ și agenție a Uniunii aplică principiile egalității de gen și echilibrului de gen atunci când efectuează numirile lor pentru CERT-UE și când alocă resursele lor umane în domeniul securității cibernetice. În cadrul tuturor instituțiilor, organelor și agențiilor Uniunii se prevăd cursuri de formare specifice și resurse adecvate pentru promovarea angajării femeilor în domeniul securității cibernetice, contribuind la eliminarea decalajului digital dintre femei și bărbați.

Justificare

Este important să se includă în regulament principiile egalității de gen și echilibrului de gen.

Amendamentul 16

Propunere de regulament
Articolul 9 – alineatul 3 – paragraful 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	Membrii sunt numiți ținând seama în mod corespunzător de principiul echilibrului de gen.

Justificare

Este important să se includă în regulament principiile egalității de gen și echilibrului de gen.

Amendamentul 17

Propunere de regulament
Articolul 12 – alineatul 7 a (nou)

Textul propus de Comisie	*Amendamentul*
	7a. În cazul în care cererea de servicii contra cost este mai mare decât resursele disponibile ale CERT-UE pentru furnizarea acestor servicii, CERT-UE

	acordă prioritate cererilor pe baza unei analize a riscurilor, ținând seama de gestionarea riscurilor în materie de securitate cibernetică de către instituțiile, organele și agențiile Uniunii solicitante, asupra cărora dimensiunea relativă a resurselor lor financiare și umane are impact.

Justificare

IOAUE ar trebui să aibă prioritate pe baza profilului lor de risc și ținând seama de dimensiunea relativă a resurselor lor financiare și umane.

Amendamentul 18

Propunere de regulament
Articolul 14

Textul propus de Comisie	*Amendamentul*
Șeful CERT-UE prezintă IICB și președintelui IICB rapoarte periodice privind performanța CERT-UE, planificarea financiară, veniturile, execuția bugetară, acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 alineatul (1).	Șeful CERT-UE prezintă IICB și președintelui IICB rapoarte periodice privind performanța CERT-UE, planificarea financiară, veniturile, execuția bugetară, ***inclusiv privind posturile și personalul extern,*** acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 alineatul (1).

Justificare

Acest amendament urmărește să clarifice faptul că raportul privind execuția bugetară ar trebui să includă situația posturilor și a personalului extern din CERT-UE.

Amendamentul 19

Propunere de regulament
Articolul 15 – alineatul 2

Textul propus de Comisie	*Amendamentul*

2. În ceea ce privește aplicarea procedurilor administrative și financiare, șeful CERT-UE acționează sub autoritatea Comisiei.	***eliminat***

Amendamentul 20

Propunere de regulament
Articolul 15 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Sarcinile și activitățile CERT-UE, inclusiv serviciile furnizate de CERT-UE în temeiul articolului 12 alineatele (2), (3), (4) și (6) și al articolului 13 alineatul (1) instituțiilor, organelor și agențiilor Uniunii finanțate în cadrul rubricii „Administrația publică europeană” din cadrul financiar multianual sunt finanțate printr-o linie bugetară separată a bugetului Comisiei. Posturile alocate CERT-UE sunt detaliate într-o notă de subsol la schema de personal a Comisiei.	3. Sarcinile și activitățile CERT-UE, inclusiv serviciile furnizate de CERT-UE în temeiul articolului 12 alineatele (2), (3), (4) și (6) și al articolului 13 alineatul (1) instituțiilor, organelor și agențiilor Uniunii finanțate în cadrul rubricii „Administrația publică europeană” din cadrul financiar multianual sunt finanțate printr-o linie bugetară separată a bugetului Comisiei. Posturile alocate CERT-UE sunt detaliate într-o notă de subsol la schema de personal a Comisiei. ***Posturile repartizate temporar se păstrează în schema de personal a instituției donatoare pe durata repartizării temporare și sunt semnalate printr-o notă de subsol. Această schemă de personal face obiectul unei evaluări o dată la 2,5 ani.***

Amendamentul 21

Propunere de regulament
Articolul 15 – alineatul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3a. Transferul unui total de 42 de posturi de către instituțiile, organele și agențiile relevante ale Uniunii, astfel cum se prevede în anexa IIa (nouă), fără compensare parțială prin reducerea numărului de agenți contractuali în cadrul CERT-UE, nu aduce atingere prerogativelor autorității bugetare a Uniunii. Contribuțiile reprezintă un

procent echitabil, care este proporțional cu ponderea respectivă a posturilor AD permanente ale organizației și ține seama în mod corespunzător de principiul echilibrului de gen.

Justificare

Se consideră necesar să se aloce CERT-UE 42 de posturi permanente suplimentare. Repartizarea posturilor între instituțiile, agențiile și organele relevante ale Uniunii ar trebui convenită între cele două componente ale autorității bugetare în cursul negocierilor interinstituționale pentru prezenta propunere, sub rezerva prerogativelor autorității bugetare a Uniunii. Este important să se asigure că principiul echilibrului de gen este respectat în regulament.

Amendamentul 22

Propunere de regulament
Articolul 23 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Comisia propune realocarea ***personalului și a*** resurselor financiare de la instituțiile, organele și agențiile relevante ale Uniunii către bugetul Comisiei. ***Realocarea*** produce efecte în același timp cu primul buget adoptat după intrarea în vigoare a prezentului regulament.	Comisia propune realocarea resurselor financiare de la instituțiile, organele și agențiile relevante ale Uniunii către bugetul Comisiei. ***Această realocare*** produce efecte în același timp cu primul buget adoptat după intrarea în vigoare a prezentului regulament.

Justificare

Repartizarea posturilor alocate CERT-UE este detaliată în anexa IIa (nouă).

Amendamentul 23

Propunere de regulament
Anexa II a (nouă)

Textul propus de Comisie

Amendamentul

Anexa II a (nouă)

IOAUE/an	*Total personal*	*Posturi alocate CERT-UE în anul N*	*Posturi alocate CERT-UE în anul N + 1*	*Posturi alocate CERT-UE în anul N + 2*	*Posturi alocate CERT-UE în anul N + 3*	*Posturi alocate permanent CERT-UE*
CERT-UE, din anul precedent		*Nu se aplică*	*48*	*42*	*42*	
PE	*6 773*	*48*	*-14*	*-14*	*-14*	*6*
CE	*23 474*	*0*	*8*	*9*	*6*	*23*
Agenții descentralizate	*7 717*	*0*	*0*	*3*	*4*	*7*
CSL	*3 029*	*0*	*0*	*2*	*1*	*3*
CJUE	*2 110*	*0*	*0*	*0*	*2*	*2*
SEAE	*1 753*	*0*	*0*	*0*	*1*	*1*
CCE	*873*	*0*	*0*	*0*	*0*	*0*
Agenții executive	*840*	*0*	*0*	*0*	*0*	*0*
CESE	*669*	*0*	*0*	*0*	*0*	*0*
ÎC + inițiative tehnologice comune + Institutul European de Inovare și Tehnologie	*556*	*0*	*0*	*0*	*0*	*0*
CoR	*496*	*0*	*0*	*0*	*0*	*0*
AEPD	*84*	*0*	*0*	*0*	*0*	*0*
Ombudsmanul European	*73*	*0*	*0*	*0*	*0*	*0*
Total personal nou		*48*	*42*	*42*	*42*	*42*

Justificare

Repartizarea celor 42 de posturi care urmează să fie alocate CERT-UE pentru a asigura funcționarea corespunzătoare și stabilă a acestuia.

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
Referințe	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Comisie competentă Data anunțului în plen	ITRE 4.4.2022
Aviz emis de către Data anunțului în plen	BUDG 4.4.2022
Raportor pentru aviz Data numirii	Nils Ušakovs 22.4.2022
Examinare în comisie	20.6.2022 21.6.2022
Data adoptării	12.7.2022
Rezultatul votului final	+: 28 –: 0 0: 4
Membri titulari prezenți la votul final	Rasmus Andresen, Anna Bonfrisco, Olivier Chastel, Lefteris Christoforou, Andor Deli, José Manuel Fernandes, Eider Gardiazabal Rubial, Vlad Gheorghe, Francisco Guerreiro, Valérie Hayer, Eero Heinäluoma, Niclas Herbst, Monika Hohlmeier, Moritz Körner, Joachim Kuhs, Zbigniew Kuźmiuk, Janusz Lewandowski, Margarida Marques, Siegfried Mureșan, Victor Negrescu, Dimitrios Papadimoulis, Bogdan Rzońca, Nicolae Ștefănuță, Nils Torvalds, Nils Ušakovs, Johan Van Overtveldt, Rainer Wieland
Membri supleanți prezenți la votul final	Damian Boeselager, Jan Olbrycht
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Alexander Bernhuber, Helmut Scholz, Birgit Sippel

VOT FINAL PRIN APEL NOMINAL ÎN COMISIA SESIZATĂ PENTRU AVIZ

28	+
ID	Anna Bonfrisco
NI	Andor Deli
PPE	Alexander Bernhuber, Lefteris Christoforou, José Manuel Fernandes, Niclas Herbst, Monika Hohlmeier, Janusz Lewandowski, Siegfried Mureşan, Jan Olbrycht, Rainer Wieland
Renew	Olivier Chastel, Vlad Gheorghe, Valérie Hayer, Moritz Körner, Nils Torvalds, Nicolae Ştefănuță
S&D	Eider Gardiazabal Rubial, Eero Heinäluoma, Margarida Marques, Victor Negrescu, Birgit Sippel, Nils Ušakovs
The Left	Dimitrios Papadimoulis, Helmut Scholz
Verts/ALE	Rasmus Andresen, Damian Boeselager, Francisco Guerreiro

0	-

4	0
ECR	Zbigniew Kuźmiuk, Bogdan Rzońca, Johan Van Overtveldt
ID	Joachim Kuhs

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri

31.1.2023

AVIZ AL COMISIEI PENTRU AFACERI CONSTITUȚIONALE

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Raportoare pentru aviz: Markéta Gregorová

JUSTIFICARE SUCCINTĂ

Instituțiile, organele și agențiile Uniunii Europene își desfășoară activitatea în ultimii ani într-un context tot mai digitalizat, caracterizat de evoluții tehnologice constante și de niveluri în continuă evoluție ale amenințărilor la adresa securității cibernetice. Această situație a fost exacerbată de declanșarea crizei sanitare provocate de pandemia de COVID-19 și, printre altele, de intensificarea practicilor de telemuncă, în cursul cărora numărul atacurilor sofisticate provenite dintr-o gamă largă de surse a continuat să crească.

În prezent, peisajul securității cibernetice, inclusiv guvernanța, igiena cibernetică, capacitatea generală și maturitatea, diferă considerabil între instituțiile, organele și agențiile Uniunii, ceea ce creează un obstacol suplimentar în calea unei administrații europene deschise, eficiente și independente.

Prin urmare, raportoarea este de acord că ar fi necesară o abordare de bază în rândul instituțiilor, organelor și agențiilor Uniunii pentru instituirea unor sisteme și cerințe comune în materie de securitate cibernetică pentru a se asigura că securitatea cibernetică evoluează în aceeași direcție, contribuind astfel la eficiența și independența administrației europene.

Raportoarea consideră, de asemenea, că un cadru de securitate solid și coerent este extrem de important pentru protejarea personalului, a datelor, a rețelelor de comunicații, a sistemelor informatice și a proceselor decizionale ale UE în ansamblu, contribuind astfel și la funcționarea democratică a Uniunii Europene. O cultură a securității consolidată la nivelul instituțiilor, organelor și agențiilor Uniunii ar face, totodată, ca Europa să fie pregătită pentru era digitală și ar construi o economie adaptată exigențelor viitorului, în serviciul cetățenilor.

AMENDAMENTELE

Comisia pentru afaceri constituționale recomandă Comisiei pentru industrie, cercetare și energie, care este comisie competentă, să ia în considerare următoarele amendamente:

Amendamentul 1

Propunere de regulament
Considerentul 1

Textul propus de Comisie	*Amendamentul*
(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații transparente, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și proteja datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.	(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații transparente, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și proteja datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației ***și comunicațiilor (TIC)***, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.

Justificare

Propunerea Comisiei folosește „tehnologia informației” acolo unde ar trebui să fie „tehnologia informației și comunicațiilor”, termenul standard utilizat în NIS2 și Regulamentul UE privind securitatea cibernetică.

Amendamentul 2

Propunere de regulament
Considerentul 2

Textul propus de Comisie	*Amendamentul*
(2) Peisajul amenințărilor cibernetice cu care se confruntă instituțiile, organele și agențiile Uniunii este într-o continuă evoluție. Tacticile, tehnicile și procedurile utilizate de actorii care generează amenințări sunt într-o continuă evoluție, în timp ce principalele motive ale acestor atacuri se schimbă foarte puțin, de la furtul de informații confidențiale valoroase până la sustragerea de bani, manipularea opiniei publice sau subminarea infrastructurii digitale. Ritmul în care își desfășoară atacurile cibernetice continuă să crească, în timp ce campaniile lor sunt din ce în ce mai sofisticate și automatizate, vizând suprafețe de atac expuse care continuă să se extindă și exploatând rapid vulnerabilitățile.	(2) Peisajul amenințărilor cibernetice cu care se confruntă instituțiile, organele***, oficiile*** și agențiile Uniunii este într-o continuă evoluție. Tacticile, tehnicile și procedurile utilizate de actorii care generează amenințări sunt într-o continuă evoluție, în timp ce principalele motive ale acestor atacuri se schimbă foarte puțin, de la furtul de informații confidențiale valoroase până la sustragerea de bani, manipularea opiniei publice sau subminarea infrastructurii digitale. Ritmul în care își desfășoară atacurile cibernetice continuă să crească, în timp ce campaniile ***și metodele*** lor sunt din ce în ce mai sofisticate și automatizate, vizând suprafețe de atac expuse care continuă să se extindă și exploatând rapid vulnerabilitățile.

Amendamentul 3

Propunere de regulament
Considerentul 3

Textul propus de Comisie	*Amendamentul*
(3) Mediile ***informatice*** ale instituțiilor, organelor și agențiilor Uniunii au interdependențe și fluxuri de date integrate, iar utilizatorii acestora colaborează îndeaproape. Această interconectare înseamnă că orice perturbare, chiar și atunci când este limitată inițial la o instituție, un organ sau o agenție a Uniunii, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea impacturi negative de amploare și de lungă durată asupra celorlalte. În plus, mediile ***informatice*** ale anumitor instituții, organe și agenții sunt conectate cu cele ale statelor membre, ceea ce face ca un incident în cadrul unei entități a Uniunii să reprezinte un risc de securitate cibernetică a mediilor ***informatice*** ale statelor membre și viceversa.	(3) Mediile ***TIC*** ale instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii au interdependențe și fluxuri de date integrate, iar utilizatorii acestora colaborează îndeaproape. Această interconectare înseamnă că orice perturbare, chiar și atunci când este limitată inițial la o instituție, un organ***, un oficiu*** sau o agenție a Uniunii, poate avea efecte în cascadă în sens mai larg, ceea ce ar putea avea impacturi negative de amploare și de lungă durată asupra celorlalte. În plus, mediile ***TIC*** ale anumitor instituții, organe***, oficii*** și agenții sunt conectate cu cele ale statelor membre, ceea ce face ca un incident în cadrul unei entități a Uniunii să reprezinte un risc de securitate cibernetică a mediilor ***TIC*** ale statelor membre și viceversa.

Amendamentul 4
Propunere de regulament
Considerentul 4

Textul propus de Comisie	*Amendamentul*
(4) Instituțiile, organele și agențiile Uniunii sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca instituțiile, organele și agențiile Uniunii să atingă un nivel comun ridicat de securitate cibernetică printr-un „nivel de referință în materie de securitate cibernetică” (un set de norme minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte pentru a ***reduce la minimum*** riscurile de securitate cibernetică), ***prin schimbul*** de informații și ***colaborarea*** în acest domeniu.	(4) Instituțiile, organele***, oficiile*** și agențiile Uniunii sunt ținte atractive, care se confruntă cu actori care generează amenințări cu înaltă calificare și care dispun de resurse suficiente, precum și cu alte amenințări. În același timp, nivelul și maturitatea rezilienței cibernetice și capacitatea de a detecta și de a răspunde activităților cibernetice răuvoitoare variază semnificativ între aceste entități. Prin urmare, pentru buna funcționare a administrației europene este necesar ca instituțiile, organele***, oficiile*** și agențiile Uniunii să atingă un nivel comun ridicat de securitate cibernetică printr-un „nivel de referință în materie de securitate cibernetică” (un set de norme ***comune*** minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte pentru a ***limita*** riscurile de securitate cibernetică), ***printr-un schimb*** de informații și ***o colaborare periodică și eficace*** în acest domeniu***, precum și prin formarea în materie de securitate cibernetică***.

Amendamentul 5

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) Diferențele dintre instituțiile, organele și agențiile Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate	(7) Diferențele dintre instituțiile, organele***, oficiile*** și agențiile Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate

cibernetică ***nu*** ar trebui să ***includă nicio obligație care să interfereze în mod direct cu*** exercitarea misiunilor instituțiilor, organelor și agențiilor Uniunii ***sau*** să ***aducă atingere autonomiei*** lor ***instituționale***. Astfel, aceste instituții, organe și agenții ***trebuie*** să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică.	cibernetică ar trebui să ***sprijine*** exercitarea misiunilor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii ***și*** să ***țină seama de autonomia*** lor ***instituțională***. Astfel, aceste instituții, organe***, oficii*** și agenții ***ar trebui*** să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică***, ținând seama de coerența și interoperabilitatea cadrelor lor respective și pe baza cadrului comun stabilit de prezentul regulament***.

Amendamentul 6
Propunere de regulament
Considerentul 8

Textul propus de Comisie	*Amendamentul*
(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra instituțiilor, organelor și agențiilor Uniunii, cerințele de gestionare a riscurilor de securitate cibernetică ar trebui să ***fie proporționale cu riscurile*** la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare instituție, organ ***sau*** agenție a Uniunii ***trebuie*** să urmărească alocarea ***unui procent adecvat*** din bugetul său în domeniul ***tehnologiei informației*** pentru a-și îmbunătăți nivelul de securitate cibernetică***;*** pe termen ***lung, ar trebui să se urmărească atingerea unui obiectiv de 10 %***.	(8) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, cerințele de gestionare a riscurilor de securitate cibernetică ar trebui să ***corespundă riscurilor*** la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Fiecare instituție, organ***, oficiu și*** agenție a Uniunii ***ar trebui*** să urmărească alocarea ***a cel puțin 10 %*** din bugetul său în domeniul ***TIC*** pentru a-și îmbunătăți nivelul de securitate cibernetică pe termen ***mediu și mai mult pe termen lung dacă este necesar***.

Amendamentul 7

Propunere de regulament
Considerentul 9

Textul propus de Comisie	*Amendamentul*
(9) Pentru asigurarea unui nivel comun ridicat de securitate cibernetică, aceasta trebuie să se afle sub supravegherea ***celui*** mai înalt nivel de conducere al fiecărei instituții, agenții și al fiecărui organ al Uniunii, care ***trebuie*** să aprobe un nivel de referință în materie de securitate cibernetică, care să abordeze riscurile identificate în cadrul stabilit de fiecare instituție, organ și agenție. Abordarea culturii securității cibernetice, adică practica zilnică în domeniul securității cibernetice, ***este*** parte integrantă a unui nivel de referință în materie de securitate cibernetică în toate instituțiile, organele și agențiile Uniunii.	(9) Pentru asigurarea unui nivel comun ridicat de securitate cibernetică, aceasta trebuie să se afle sub supravegherea ***unui consiliu comun al UE, implicând cel*** mai înalt nivel de conducere al fiecărei instituții, agenții și al fiecărui organ ***sau oficiu*** al Uniunii, care ***ar trebui*** să aprobe un nivel de referință în materie de securitate cibernetică, care să abordeze riscurile identificate în cadrul stabilit de fiecare instituție, organ***, oficiu*** și agenție. Abordarea culturii securității cibernetice, adică practica zilnică în domeniul securității cibernetice, ***ar trebui să devină*** parte integrantă a unui nivel de referință în materie de securitate cibernetică în toate instituțiile, organele***, oficiile*** și agențiile Uniunii.

Amendamentul 8

Propunere de regulament
Considerentul 10

Textul propus de Comisie	*Amendamentul*
(10) Instituțiile, organele și agențiile Uniunii ***trebuie*** să evalueze riscurile legate de relațiile cu furnizorii și prestatorii de servicii, inclusiv cu prestatorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate, și să ia măsurile adecvate pentru a combate astfel de riscuri. Aceste măsuri ***trebuie*** să facă parte din nivelul de referință în materie de securitate cibernetică și să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor ***trebuie*** să se țină seama în mod corespunzător de legislația și politicile relevante ale UE, inclusiv de evaluările riscurilor și de recomandările emise de Grupul de cooperare privind securitatea rețelelor și a informațiilor, cum ar fi evaluarea	(10) Instituțiile, organele***, oficiile*** și agențiile Uniunii ***ar trebui*** să evalueze riscurile legate de relațiile cu furnizorii și prestatorii de servicii, inclusiv cu prestatorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate, și să ia măsurile adecvate pentru a combate astfel de riscuri. ***Acești furnizori și prestatori de servicii ar trebui să fie verificați cu atenție, ținându-se seama de întregul lanț de aprovizionare și de mediul economic și politic în care își desfășoară activitatea. În cazul în care relațiile cu astfel de furnizori și prestatori de servicii reprezintă un risc pentru integritatea proceselor democratice din Uniune, ar trebui să înceteze fără întârzieri nejustificate.*** Aceste măsuri ***ar trebui*** să facă parte din nivelul de referință

coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G. În plus, ar ***putea fi necesară*** certificarea produselor, a serviciilor și a proceselor TIC relevante, în cadrul sistemelor europene specifice de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.

în materie de securitate cibernetică și să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor ***ar trebui*** să se țină seama în mod corespunzător de legislația și politicile relevante ale UE, inclusiv de evaluările riscurilor și de recomandările emise de Grupul de cooperare privind securitatea rețelelor și a informațiilor, cum ar fi evaluarea coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G. În plus, ***având în vedere peisajul amenințărilor și importanța consolidării rezilienței,*** ar ***trebui să se solicite*** certificarea produselor, a serviciilor și a proceselor TIC relevante ***utilizate în instituțiile, organele, oficiile și agențiile Uniunii***, în cadrul sistemelor europene specifice de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.

Amendamentul 9

Propunere de regulament
Considerentul 13

Textul propus de Comisie	*Amendamentul*
(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de instituții, organe și agenții ale Uniunii sau comunități de interes care includ instituții, organe și agenții ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare, instituțiile, organele și agențiile Uniunii ***trebuie*** să informeze CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative și să facă schimb de detalii tehnice adecvate care să permită detectarea sau	(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de instituții, organe***, oficii*** și agenții ale Uniunii sau comunități de interes care includ instituții, organe***, oficii*** și agenții ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare, instituțiile, organele***, oficiile*** și agențiile Uniunii ***ar trebui*** să informeze CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative și să facă schimb de detalii tehnice adecvate care să permită

atenuarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor similare în alte instituții, organe și agenții ale Uniunii, precum și răspunsul la astfel de amenințări, vulnerabilități și incidente. Urmând aceeași abordare precum cea prevăzută în Directiva [propunerea NIS 2], în cazul în care iau cunoștință de un incident semnificativ, entitățile ar trebui să transmită CERT-UE o ***notificare inițială*** în ***termen*** de 24 de ore. Acest schimb de informații ***trebuie*** să permită CERT-UE să disemineze informațiile către alte instituții, organe și agenții ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor ***informatice*** ale Uniunii și ale omologilor Uniunii împotriva unor incidente, amenințări și vulnerabilități similare.

detectarea sau atenuarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor similare în alte instituții, organe***, oficii*** și agenții ale Uniunii, precum și răspunsul la astfel de amenințări, vulnerabilități și incidente. Urmând aceeași abordare precum cea prevăzută în Directiva [propunerea NIS 2], în cazul în care iau cunoștință de un incident semnificativ, entitățile ar trebui să transmită CERT-UE o ***avertizare timpurie fără întârzieri nejustificate și,*** în ***orice caz, nu mai târziu*** de 24 de ore. ***Instituțiilor, organelor, oficiilor și agențiilor Uniunii ar trebui să li se aloce resurse suficiente pentru a-și îndeplini obligațiile de raportare în mod rapid și eficient, astfel încât să se asigure funcționarea corectă a sistemului conceput.*** Acest schimb de informații ***ar trebui*** să permită CERT-UE să disemineze informațiile către alte instituții, organe***, oficii*** și agenții ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor ***TIC*** ale Uniunii și ale omologilor Uniunii împotriva unor incidente, amenințări și vulnerabilități similare.

Amendamentul 10

Propunere de regulament
Considerentul 14

Textul propus de Comisie	*Amendamentul*
(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, este necesară instituirea unui Consiliu interinstituțional pentru securitate cibernetică (IICB), care să faciliteze un nivel comun ridicat de securitate cibernetică în rândul instituțiilor, organelor și agențiilor Uniunii prin monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii, prin supravegherea punerii în aplicare a priorităților și a obiectivelor generale de către CERT-UE și prin	(14) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, este necesară instituirea unui Consiliu interinstituțional pentru securitate cibernetică (IICB), care să faciliteze un nivel comun ridicat de securitate cibernetică în rândul instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii prin monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele***, oficiile*** și agențiile Uniunii, prin supravegherea punerii în aplicare a priorităților și a obiectivelor generale de

elaborarea unor orientări strategice pentru CERT-UE. IICB ar trebui să asigure reprezentarea instituțiilor și să includă reprezentanți ai agențiilor și ai organelor prin intermediul Rețelei agențiilor UE.

către CERT-UE și prin elaborarea unor orientări strategice pentru CERT-UE. IICB ar trebui să asigure reprezentarea ***egală a*** instituțiilor și să includă reprezentanți ai agențiilor***, ai oficiilor*** și ai organelor prin intermediul Rețelei agențiilor UE.

Amendamentul 11

Propunere de regulament
Considerentul 16

Textul propus de Comisie	*Amendamentul*
(16) IICB ar trebui să monitorizeze respectarea regulamentului, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adresate de CERT-UE. În ceea ce privește aspectele tehnice, IICB ***trebuie*** să beneficieze de sprijin din partea grupurilor consultative tehnice ***a căror componență este decisă de IICB***, care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu instituțiile, organele și agențiile Uniunii și cu alte părți interesate, după caz. Dacă este necesar, IICB ***trebuie*** să emită avertismente ***fără caracter obligatoriu*** și ***să recomande*** audituri.	(16) IICB ar trebui să monitorizeze respectarea regulamentului, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adresate de CERT-UE. În ceea ce privește aspectele tehnice, IICB ***ar trebui*** să beneficieze de sprijin din partea grupurilor consultative tehnice, care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu instituțiile, organele***, oficiile*** și agențiile Uniunii și cu alte părți interesate, după caz. Dacă este necesar, IICB ***ar trebui*** să emită avertismente și ***recomandări pentru*** audituri.

Amendamentul 12

Propunere de regulament
Considerentul 17

Textul propus de Comisie	*Amendamentul*
(17) CERT-UE ***trebuie*** să aibă misiunea de a contribui la securitatea mediului ***informatic*** al tuturor instituțiilor, organelor și agențiilor Uniunii. CERT-UE ***trebuie*** să acționeze ca echivalent al coordonatorului desemnat pentru instituțiile, organele și agențiile Uniunii, în scopul divulgării coordonate a vulnerabilităților către registrul european al vulnerabilităților, astfel cum se menționează la articolul 6 din	(17) CERT-UE ***ar trebui*** să aibă misiunea de a contribui la securitatea mediului ***TIC*** al tuturor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii. CERT-UE ***ar trebui*** să acționeze ca echivalent al coordonatorului desemnat pentru instituțiile, organele***, oficiile*** și agențiile Uniunii, în scopul divulgării coordonate a vulnerabilităților către registrul european al vulnerabilităților,

[propunerea de Directivă NIS 2].	astfel cum se menționează la articolul 6 din ***Directiva [propunerea*** NIS 2].

Amendamentul 13

Propunere de regulament
Considerentul 18

Textul propus de Comisie	*Amendamentul*
(18) În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate instituțiile, organele și agențiile Uniunii, cu o amploare și o profunzime adecvate, precum și o adaptare continuă la amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a dispozitivelor conectate prin internetul obiectelor. Acest obiectiv strategic include, de asemenea, centre de operațiuni pentru securitate (SOC) cu spectru larg, care monitorizează rețelele, precum și monitorizarea permanentă a amenințărilor deosebit de grave. CERT-UE ***trebuie*** să ofere sprijin echipelor de securitate ***informatică*** ale instituțiilor, organelor și agențiilor mai mari ale Uniunii, inclusiv prin monitorizarea non-stop din prima linie. Pentru instituțiile, organele și agențiile mai mici și unele medii ale Uniunii, CERT-UE trebuie să furnizeze toată gama de servicii.	(18) În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate instituțiile, organele***, oficiile*** și agențiile Uniunii, cu o amploare și o profunzime adecvate, precum și o adaptare continuă la amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a dispozitivelor conectate prin internetul obiectelor. Acest obiectiv strategic include, de asemenea, centre de operațiuni pentru securitate (SOC) cu spectru larg, care monitorizează rețelele, precum și monitorizarea permanentă a amenințărilor deosebit de grave. CERT-UE ***ar trebui*** să ofere sprijin echipelor de securitate ***TIC*** ale instituțiilor, organelor***, oficiilor*** și agențiilor mai mari ale Uniunii, inclusiv prin monitorizarea non-stop din prima linie. Pentru instituțiile, organele***, oficiile*** și agențiile mai mici și unele medii ale Uniunii, CERT-UE trebuie să furnizeze toată gama de servicii.

Amendamentul 14

Propunere de regulament
Considerentul 19 a (nou)

Textul propus de Comisie	*Amendamentul*
	(19a) Pentru a asigura o mai bună punere în aplicare a măsurilor și a orientărilor în materie de securitate cibernetică pentru instituțiile, organele,

	oficiile și agențiile Uniunii și pentru a consolida o cultură a securității cibernetice în cadrul acestora, CERT-UE ar trebui, de asemenea, să consolideze cooperarea cu Rețeaua și Centrul european de competențe în materie de securitate cibernetică.

Amendamentul 15

Propunere de regulament
Considerentul 20

Textul propus de Comisie	*Amendamentul*
(20) În sprijinirea cooperării operaționale în domeniul securității cibernetice, CERT-UE ***trebuie*** să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate Cibernetică prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[5]. ***Dacă este cazul,*** între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE ***trebuie*** să coopereze cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.	(20) În sprijinirea cooperării operaționale în domeniul securității cibernetice, CERT-UE ***ar trebui*** să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate Cibernetică prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[5]. Între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE ***ar trebui*** să coopereze cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.
[5] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).	[5] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

Amendamentul 16
Propunere de regulament
Considerentul 24

Textul propus de Comisie	*Amendamentul*
(24) Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor instituțiilor, organelor și agențiilor Uniunii, fiecare instituție, organ și agenție a Uniunii cu cheltuieli în domeniul ***tehnologiei informației trebuie*** să contribuie în mod ***echitabil*** la aceste servicii și sarcini. Contribuțiile respective nu aduc atingere ***autonomiei*** bugetare a instituțiilor, organelor și agențiilor Uniunii.	(24) Întrucât serviciile și sarcinile CERT-UE sunt în interesul tuturor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, fiecare instituție, organ***, oficiu*** și agenție a Uniunii cu cheltuieli în domeniul ***TIC ar trebui*** să contribuie în mod ***proporțional*** la aceste servicii și sarcini. Contribuțiile respective nu aduc atingere ***capacității*** bugetare a instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii.

Amendamentul 17

Propunere de regulament
Considerentul 25

Textul propus de Comisie	*Amendamentul*
(25) IICB, cu sprijinul CERT-UE, trebuie să revizuiască și să evalueze punerea în aplicare a prezentului regulament și trebuie să raporteze constatările sale Comisiei. Pe baza acestui input, ***Comisiei îi revine sarcina de a transmite rapoarte*** Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor.	(25) IICB, cu sprijinul CERT-UE, trebuie să revizuiască și să evalueze punerea în aplicare a prezentului regulament și trebuie să raporteze constatările sale Comisiei. Pe baza acestui input, ***Comisia ar trebui să transmită rapoarte, cel puțin o dată la trei ani,*** Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor.

Amendamentul 18

Propunere de regulament
Articolul 1 – alineatul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) obligații pentru instituțiile, organele și agențiile Uniunii de a institui un cadru intern de gestionare, guvernanță și control	(a) obligații pentru instituțiile, organele***, oficiile*** și agențiile Uniunii de a institui un cadru intern de gestionare,

al riscurilor de securitate cibernetică;	guvernanță și control al riscurilor de securitate cibernetică;

Amendamentul 19

Propunere de regulament
Articolul 1 – alineatul 1 – litera c

Textul propus de Comisie	*Amendamentul*
(c) norme privind organizarea și ***funcționarea*** Centrului de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE) și privind organizarea și ***funcționarea*** Consiliului interinstituțional pentru securitate cibernetică (IICB).	(c) norme privind organizarea și ***modul de operare ale*** Centrului de securitate cibernetică pentru instituțiile, organele***, oficiile*** și agențiile Uniunii (CERT-UE) și privind ***funcționarea,*** organizarea și ***modul de operare ale*** Consiliului interinstituțional pentru securitate cibernetică (IICB).

Amendamentul 20

Propunere de regulament
Articolul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 2a
	Prelucrarea datelor cu caracter personal
	Prelucrarea datelor cu caracter personal în temeiul prezentului regulament de către CERT-UE, IICB și de către toate instituțiile, organele, oficiile și agențiile Uniunii se efectuează în conformitate cu Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului.

Amendamentul 21

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 2

Textul propus de Comisie	*Amendamentul*
(2) „rețea și sistem informatic” înseamnă rețea și sistem informatic ***în sensul articolului 4*** punctul 1 din	(2) „rețea și sistem informatic” înseamnă rețea și sistem informatic ***astfel cum sunt definite la articolul 6*** punctul 1

[propunerea de Directivă NIS 2];	din ***Directiva [propunerea*** NIS 2];

Amendamentul 22

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 4

Textul propus de Comisie	*Amendamentul*
(4) „securitate cibernetică” înseamnă securitatea cibernetică ***în sensul articolului 4*** punctul ***3 din [propunerea de Directivă NIS 2]***;	(4) „securitate cibernetică” înseamnă securitatea cibernetică ***astfel cum este definită la articolul 2*** punctul ***1 din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului***[1a];
	[1a] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

Amendamentul 23

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 5

Textul propus de Comisie	*Amendamentul*
(5) „cel mai înalt nivel de conducere” înseamnă un manager, un organ de conducere sau de coordonare și supraveghere de la cel mai înalt nivel administrativ, ținând seama de mecanismele de guvernanță la nivel înalt din fiecare instituție, organ sau agenție a Uniunii;	(5) „cel mai înalt nivel de conducere” înseamnă un manager, un organ de conducere sau de coordonare și supraveghere de la cel mai înalt nivel administrativ ***cu un mandat de a lua sau de a autoriza decizii***, ținând seama de mecanismele de guvernanță la nivel înalt din fiecare instituție, organ***, oficiu*** sau agenție a Uniunii;

Amendamentul 24

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 7

Textul propus de Comisie	*Amendamentul*
(7) „incident semnificativ” înseamnă orice incident***, cu excepția cazului*** în ***care acesta are un impact limitat și este probabil ca metoda*** sau ***tehnologia sa să fie deja bine înțeleasă***;	(7) „incident semnificativ” înseamnă orice incident ***care a cauzat sau poate cauza perturbări operaționale grave în funcționarea entității Uniunii sau pierderi financiare pentru entitatea Uniunii*** în ***cauză sau care a afectat sau poate afecta alte persoane fizice*** sau ***juridice cauzând prejudicii materiale sau morale considerabile***;

Amendamentul 25

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 11

Textul propus de Comisie	*Amendamentul*
(11) „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică ***cu intenția, oportunitatea și capacitatea de a cauza un incident semnificativ***;	(11) „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică ***astfel cum este definită la articolul 6 punctul 11 din Directiva [propunerea NIS 2]***;

Amendamentul 26

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 14

Textul propus de Comisie	*Amendamentul*
(14) ***„risc de securitate cibernetică”*** înseamnă orice ***circumstanță sau eveniment ce poate fi identificat în mod rezonabil care are un efect potențial negativ asupra securității rețelelor și a sistemelor informatice***;	(14) ***„risc”*** înseamnă orice ***risc astfel cum este definit la articolul 6 punctul 9 din Directiva [propunerea NIS 2]***;

Amendamentul 27

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 14 a (nou)

Textul propus de Comisie	*Amendamentul*
	(14a) „mediu TIC” înseamnă orice produs TIC la fața locului sau virtual, serviciu TIC și proces TIC astfel cum sunt definite la articolul 2 punctele 12, 13 și 14 din Regulamentul (UE) 2019/881, precum și orice rețea și sistem informatic, indiferent dacă este deținut și operat de o instituție, un organ, un oficiu sau o agenție a Uniunii sau este găzduit sau operat de o parte terță, inclusiv dispozitive mobile, rețele corporative și rețele organizaționale care nu sunt conectate la internet și orice dispozitive conectate la mediul TIC;

Justificare

Termen mutat de la articolul 4 alineatul (2) din prezenta propunere la articolul privind definițiile, având în vedere că acest termen este utilizat în mod consecvent în întregul text. Definiția propusă pentru acest termen se bazează pe definițiile componentelor sale de la articolul 2 din Regulamentul (UE) 2019/881 privind securitatea cibernetică.

Amendamentul 28

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 15

Textul propus de Comisie	*Amendamentul*
(15) „unitate cibernetică comună” înseamnă o platformă virtuală și fizică de cooperare pentru diferitele comunități de securitate cibernetică din Uniune, cu accent pe coordonarea operațională și tehnică împotriva amenințărilor și incidentelor cibernetice transfrontaliere majore în sensul Recomandării Comisiei din 23 iunie 2021;	***eliminat***

Amendamentul 29
Propunere de regulament
Articolul 4 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Fiecare instituție, organ și agenție a Uniunii își stabilește propriul cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul”) pentru a sprijini misiunea entității și pentru a-și exercita autonomia instituțională. Această activitate este supravegheată de cel mai înalt nivel de conducere al entității ***pentru a se putea asigura o gestionare*** eficace și ***prudentă*** a tuturor riscurilor de securitate cibernetică. Cadrul se instituie până cel târziu la …. [15 luni de la ***intrarea*** în vigoare a prezentului regulament].	1. ***Pe baza unui audit complet de securitate,*** fiecare instituție, organ***, oficiu*** și agenție a Uniunii își stabilește propriul cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul”) pentru a sprijini misiunea entității și pentru a-și exercita autonomia instituțională***, ținând totodată seama de coerența și interoperabilitatea cadrului său cu cel al altor instituții, organe, oficii și agenții relevante***. Această activitate este supravegheată de cel mai înalt nivel de conducere al entității***, care este responsabil cu asigurarea unei gestionări*** eficace și ***prudente*** a tuturor riscurilor de securitate cibernetică. Cadrul se instituie până cel târziu la …. [15 luni de la ***data intrării*** în vigoare a prezentului regulament].

Amendamentul 30

Propunere de regulament
Articolul 4 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Cadrul acoperă întregul mediu ***informatic*** al instituției, organului sau agenției în cauză, inclusiv orice mediu ***informatic*** de la fața locului, active și servicii externalizate în medii de cloud computing sau găzduite de părți terțe, dispozitive mobile, rețele corporative, rețele organizaționale care nu sunt conectate la internet și orice dispozitive conectate la mediul ***informatic***. Cadrul ține seama de gestionarea continuității activității și de gestionarea crizelor și ia în considerare securitatea lanțului de aprovizionare, precum și gestionarea riscurilor umane care ar putea avea un impact asupra securității cibernetice a instituției, organului sau agenției Uniunii în	2. Cadrul acoperă întregul mediu ***TIC*** al instituției, organului***, oficiului*** sau agenției în cauză, inclusiv orice mediu ***TIC*** de la fața locului, active și servicii externalizate în medii de cloud computing sau găzduite de părți terțe, dispozitive mobile, rețele corporative, rețele organizaționale care nu sunt conectate la internet și orice dispozitive conectate la mediul ***TIC***. Cadrul ține seama de gestionarea continuității activității și de gestionarea crizelor și ia în considerare securitatea lanțului de aprovizionare, precum și gestionarea riscurilor umane care ar putea avea un impact asupra securității cibernetice a instituției, organului***, oficiului*** sau agenției Uniunii în cauză.

cauză.

Amendamentul 31
Propunere de regulament
Articolul 4 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Fiecare instituție, organ și agenție a Uniunii dispune de mecanisme eficace pentru a se asigura că ***un procent adecvat*** din bugetul în domeniul ***tehnologiei informației*** este cheltuit pentru securitatea cibernetică.	4. Fiecare instituție, organ***, oficiu*** și agenție a Uniunii dispune de mecanisme eficace pentru a se asigura că ***minimum 10 %*** din bugetul ***agregat*** în domeniul ***TIC*** este cheltuit pentru securitatea cibernetică ***pe termen mediu***.

Amendamentul 32

Propunere de regulament
Articolul 4 – alineatul 5 a (nou)

Textul propus de Comisie	*Amendamentul*
	5a. Responsabilul local cu securitatea cibernetică cooperează cu responsabilul cu protecția datelor menționat la articolul 43 din Regulamentul (UE) 2018/1725 atunci când se ocupă de activități care se suprapun, aplicând protecția datelor începând cu momentul conceperii și protecția implicită a datelor în cazul măsurilor de securitate cibernetică, și atunci când selectează măsuri de securitate cibernetică care implică protecția datelor cu caracter personal, gestionarea integrată a riscurilor și gestionarea integrată a incidentelor de securitate.

Amendamentul 33

Propunere de regulament
Articolul 5 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Cel mai înalt nivel de conducere din fiecare instituție, organ și agenție a Uniunii își aprobă propriul nivel de referință în materie de securitate cibernetică pentru a aborda riscurile identificate în cadrul menționat la articolul 4 punctul 1. Acest nivel este stabilit în sprijinul misiunii sale și cu exercitarea autonomiei sale instituționale. Nivelul de referință în materie de securitate cibernetică se instituie până cel târziu la … [18 luni de la ***intrarea*** în vigoare a prezentului regulament] și abordează domeniile enumerate în anexa I și măsurile enumerate în anexa II.	1. Cel mai înalt nivel de conducere din fiecare instituție, organ***, oficiu*** și agenție a Uniunii își aprobă propriul nivel de referință în materie de securitate cibernetică pentru a aborda riscurile identificate în cadrul menționat la articolul 4 punctul 1. Acest nivel este stabilit în sprijinul misiunii sale și cu exercitarea autonomiei sale instituționale ***în deplină conformitate cu cerințele prezentului regulament și ținând seama de coerența și interoperabilitatea cadrului său cu cel al altor instituții, organe, oficii și agenții relevante, precum și de documentele de orientare și recomandările adoptate de IICB la propunerea CERT-UE și de sistemele UE de certificare de securitate cibernetică aplicabile***. Nivelul de referință în materie de securitate cibernetică se instituie până cel târziu la … [18 luni de la ***data intrării*** în vigoare a prezentului regulament] și abordează domeniile enumerate în anexa I și măsurile enumerate în anexa II.

Amendamentul 34

Propunere de regulament
Articolul 5 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Personalul de conducere de nivel superior din fiecare instituție, organ și agenție a Uniunii urmează periodic cursuri de formare specifice, pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor organizației.	2. Personalul de conducere de nivel superior din fiecare instituție, organ***, oficiu*** și agenție a Uniunii urmează periodic cursuri de formare specifice ***cu resurse adecvate***, pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor organizației. ***În plus față de aceste cursuri de formare specifice și în scopul construirii și consolidării culturii securității cibernetice, în planul***

	de securitate cibernetică se include o formare periodică a membrilor personalului în materie de securitate cibernetică, ce se actualizează cel puțin o dată la doi ani. Se asigură resurse suficiente pentru a asigura o formare de calitate.

Amendamentul 35

Propunere de regulament
Articolul 6 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Fiecare instituție, organ și agenție a Uniunii efectuează o evaluare a nivelului de maturitate al securității cibernetice cel puțin o dată la ***trei*** ani, încorporând toate elementele mediului său ***informatic***, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în temeiul articolului 13.	Fiecare instituție, organ***, oficiu*** și agenție a Uniunii efectuează o evaluare a nivelului de maturitate al securității cibernetice ***până la ... [6 luni de la intrarea în vigoare a prezentului regulament] și, ulterior,*** cel puțin o dată la ***doi*** ani, încorporând toate elementele mediului său ***TIC***, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în temeiul articolului 13. ***Evaluarea maturității se bazează pe audituri de securitate cibernetică independente efectuate de prestatori verificați.***

Amendamentul 36

Propunere de regulament
Articolul 7 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În urma concluziilor desprinse din evaluarea nivelului de maturitate și luând în considerare activele și riscurile identificate în temeiul articolului 4, cel mai înalt nivel de conducere din fiecare instituție, organ și agenție a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului de gestionare, guvernanță și	1. În urma concluziilor desprinse din evaluarea nivelului de maturitate și luând în considerare activele și riscurile identificate în temeiul articolului 4, cel mai înalt nivel de conducere din fiecare instituție, organ***, oficiu*** și agenție a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului de gestionare, guvernanță și

control al riscurilor și a nivelului de referință în materie de securitate cibernetică. Planul vizează creșterea gradului de securitate cibernetică în ansamblu a entității în cauză și contribuie, astfel, la atingerea sau îmbunătățirea unui nivel comun ridicat de securitate cibernetică în toate instituțiile, organele și agențiile Uniunii. Pentru a sprijini misiunea entității pe baza autonomiei sale instituționale, planul include cel puțin domeniile enumerate în anexa I, măsurile enumerate în anexa II, precum și măsuri legate de pregătirea pentru incidente, răspunsul la incidente și redresarea în urma incidentelor, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate. Planul se revizuiește cel puțin o dată la ***trei*** ani, în urma evaluărilor nivelului de maturitate, efectuate în temeiul articolului 6.	control al riscurilor și a nivelului de referință în materie de securitate cibernetică. Planul vizează creșterea gradului de securitate cibernetică în ansamblu a entității în cauză și contribuie, astfel, la atingerea sau îmbunătățirea unui nivel comun ridicat de securitate cibernetică în toate instituțiile, organele***, oficiile*** și agențiile Uniunii. Pentru a sprijini misiunea entității pe baza autonomiei sale instituționale, planul include cel puțin domeniile enumerate în anexa I, măsurile enumerate în anexa II, precum și măsuri legate de pregătirea pentru incidente, răspunsul la incidente și redresarea în urma incidentelor, cum ar fi ***evaluarea securității prestatorilor și serviciilor,*** monitorizarea și jurnalizarea evenimentelor de securitate. Planul se revizuiește cel puțin o dată la ***doi*** ani, în urma evaluărilor nivelului de maturitate, efectuate în temeiul articolului 6.

Amendamentul 37

Propunere de regulament
Articolul 7 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Planul de securitate cibernetică include rolurile și responsabilitățile ***ce revin*** membrilor personalului în legătură cu implementarea acestui plan.	2. Planul de securitate cibernetică include rolurile***, pregătirea*** și responsabilitățile membrilor personalului în legătură cu implementarea acestui plan.

Amendamentul 38

Propunere de regulament
Articolul 7 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Planul de securitate cibernetică ***ia în considerare orice document*** de orientare și ***orice recomandare aplicabilă adoptată*** de CERT-UE.	3. Planul de securitate cibernetică ***include toate măsurile propuse cuprinse în documentele*** de orientare și ***recomandările aplicabile adoptate*** de

CERT-UE.

Amendamentul 39

Propunere de regulament
Articolul 7 – alineatul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3 a. Instituțiile, organele, oficiile și agențiile Uniunii transmit IICB planurile lor de securitate cibernetică. Aceste planuri sunt comunicate, în măsura posibilului, fără a risca dezvăluirea sau divulgarea de informații sensibile sau confidențiale cu privire la mecanismele și capacitățile tehnice specifice în materie de securitate cibernetică ale entității Uniunii către părți terțe neautorizate.

Amendamentul 40

Propunere de regulament
Articolul 9 – alineatul 2 – litera a

Textul propus de Comisie	*Amendamentul*
(a) monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele și agențiile Uniunii;	(a) monitorizarea punerii în aplicare a prezentului regulament de către instituțiile, organele***, oficiile*** și agențiile Uniunii ***și formularea de recomandări pentru atingerea unui nivel comun ridicat de securitate cibernetică***;

Amendamentul 41

Propunere de regulament
Articolul 9 – alineatul 3 – paragraful 1 – partea introductivă

Textul propus de Comisie	*Amendamentul*
IICB este format din trei reprezentanți numiți de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta	IICB este format din trei reprezentanți numiți de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta

interesele agențiilor și organelor care își gestionează propriul mediu ***informatic*** și câte un reprezentant numit de fiecare dintre următoarele entități:	interesele ***oficiilor,*** agențiilor și organelor care își gestionează propriul mediu ***TIC*** și câte un reprezentant numit de fiecare dintre următoarele entități:

Amendamentul 42

Propunere de regulament
Articolul 9 – alineatul 3 – paragraful 1 – litera ka (nouă)

Textul propus de Comisie	*Amendamentul*
	(ka) Autoritatea Europeană pentru Protecția Datelor.

Amendamentul 43

Propunere de regulament
Articolul 10 – paragraful 1 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) să aprobe, pe baza unei propuneri din partea șefului CERT-UE, recomandări pentru atingerea unui nivel comun ridicat de securitate cibernetică, care să vizeze una sau toate instituțiile, organele, oficiile și agențiile Uniunii;

Amendamentul 44

Propunere de regulament
Articolul 11 – alineatul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) să emită un avertisment; dacă este necesar, având în vedere un risc semnificativ de securitate cibernetică, categoria de public căreia i se adresează avertismentul este restricționată în mod corespunzător;	(a) să emită un avertisment; dacă este necesar, având în vedere un risc semnificativ de securitate cibernetică, categoria de public căreia i se adresează avertismentul este restricționată în mod corespunzător***, printr-o metodologie convenită de comun acord***;

Amendamentul 45

Propunere de regulament
Articolul 11 – alineatul 1 – litera b

Textul propus de Comisie	*Amendamentul*
(b) să ***recomande un*** serviciu de audit relevant ***pentru efectuarea unui*** audit.	(b) să ***solicite unui*** serviciu de audit relevant ***să efectueze un*** audit.

Amendamentul 46

Propunere de regulament
Articolul 12 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Misiunea CERT-UE, a Centrului autonom de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE, este de a contribui la securitatea mediului ***informatic*** neclasificat al tuturor instituțiilor, organelor și agențiilor Uniunii, oferindu-le consiliere în materie de securitate cibernetică, ajutându-le să prevină, să detecteze, să atenueze și să răspundă la incidente și acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.	1. Misiunea CERT-UE, a Centrului autonom de răspuns la incidente de securitate cibernetică pentru instituțiile, organele***, oficiile*** și agențiile UE, este de a contribui la securitatea mediului ***TIC*** neclasificat al tuturor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, oferindu-le consiliere în materie de securitate cibernetică, ajutându-le să prevină, să detecteze, să atenueze și să răspundă la incidente și acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.

Amendamentul 47

Propunere de regulament
Articolul 12 – alineatul 2 – litera d

Textul propus de Comisie	*Amendamentul*
(d) aduce în atenția IICB orice problemă legată de punerea în aplicare a prezentului regulament și a documentelor de orientare, recomandărilor și apelurilor la acțiune;	(d) aduce în atenția IICB orice problemă legată de punerea în aplicare a prezentului regulament și a documentelor de orientare, recomandărilor și apelurilor la acțiune ***și formulează propuneri de măsuri corective***;

Amendamentul 48

Propunere de regulament
Articolul 12 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. CERT-UE desfășoară o cooperare structurată cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice, în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului.	4. CERT-UE desfășoară o cooperare structurată cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește consolidarea capacităților, cooperarea operațională și analizele strategice pe termen lung ale amenințărilor cibernetice, în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului. ***În plus, CERT-UE poate coopera și face schimb de informații cu Centrul european de combatere a criminalității informatice.***

Amendamentul 49

Propunere de regulament
Articolul 12 – alineatul 5 – partea introductivă

Textul propus de Comisie	*Amendamentul*
5. CERT-UE poate furniza următoarele servicii care nu sunt descrise în catalogul său de servicii („servicii contra cost”):	5. CERT-UE poate furniza ***instituțiilor, organelor, oficiilor și agențiilor Uniunii*** următoarele servicii care nu sunt descrise în catalogul său de servicii („servicii contra cost”):

Amendamentul 50

Propunere de regulament
Articolul 12 – alineatul 5 – litera a

Textul propus de Comisie	*Amendamentul*
(a) servicii care sprijină securitatea cibernetică a mediului ***informatic*** al instituțiilor, organelor și agențiilor Uniunii, altele decât cele menționate la alineatul (2), în temeiul unor acorduri privind nivelul	(a) servicii care sprijină securitatea cibernetică a mediului ***TIC*** al instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, altele decât cele menționate la alineatul (2), în temeiul unor acorduri privind nivelul

serviciilor și sub rezerva resurselor disponibile;	serviciilor și sub rezerva resurselor disponibile;

Amendamentul 51

Propunere de regulament
Articolul 12 – alineatul 5 – litera b

Textul propus de Comisie	*Amendamentul*
(b) servicii care sprijină operațiunile sau proiectele în materie de securitate cibernetică ale instituțiilor, organelor și agențiilor Uniunii, altele decât cele care vizează protejarea mediului lor ***informatic***, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB;	(b) servicii care sprijină operațiunile sau proiectele în materie de securitate cibernetică ale instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, altele decât cele care vizează protejarea mediului lor ***TIC***, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB;

Amendamentul 52
Propunere de regulament
Articolul 12 – alineatul 5 – litera c

Textul propus de Comisie	*Amendamentul*
(c) servicii care sprijină securitatea mediului ***informatic*** al altor organizații decât instituțiile, organele și agențiile Uniunii, care cooperează îndeaproape cu instituțiile, organele și agențiile Uniunii, de exemplu, cărora li s-au atribuit sarcini sau responsabilități în temeiul dreptului Uniunii, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB.	(c) servicii care sprijină securitatea mediului ***TIC*** al altor organizații decât instituțiile, organele***, oficiile*** și agențiile Uniunii, care cooperează îndeaproape cu instituțiile, organele***, oficiile*** și agențiile Uniunii, de exemplu, cărora li s-au atribuit sarcini sau responsabilități în temeiul dreptului Uniunii, în temeiul unor acorduri scrise și cu aprobarea prealabilă a IICB.

Amendamentul 53

Propunere de regulament
Articolul 12 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. CERT-UE poate organiza exerciții	6. CERT-UE poate organiza exerciții

de securitate cibernetică sau poate recomanda participarea la exercițiile existente, în strânsă cooperare cu Agenția Uniunii Europene pentru Securitate Cibernetică, dacă este cazul, pentru a testa nivelul de securitate cibernetică al instituțiilor, organelor și agențiilor Uniunii.	de securitate cibernetică sau poate recomanda participarea la exercițiile existente, în strânsă cooperare cu Agenția Uniunii Europene pentru Securitate Cibernetică, dacă este cazul, pentru a testa ***periodic*** nivelul de securitate cibernetică al instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii. ***În plus, prin intermediul cooperării consolidate și al programelor comune cu Rețeaua și Centrul european de competențe în materie de securitate cibernetică (ECCC), CERT-UE poate sprijini cercetarea și inovarea și poate contribui la consolidarea capacităților în materie de securitate cibernetică ale instituțiilor, organelor, oficiilor și agențiilor Uniunii.***

Amendamentul 54

Propunere de regulament
Articolul 12 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. CERT-UE ***poate oferi*** instituțiilor, organelor și agențiilor Uniunii asistență referitoare la incidentele din medii ***informatice*** clasificate, dacă ***entitatea*** în cauză îi solicită acest lucru în mod expres.	7. CERT-UE ***oferă*** instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii asistență referitoare la incidentele din medii ***TIC*** clasificate, dacă ***instituțiile, organele, oficiile sau agențiile Uniunii*** în cauză îi solicită acest lucru în mod expres ***și dacă CERT-UE dispune de resursele necesare pentru a face acest lucru sau primește astfel de resurse de la entitatea în cauză***.

Amendamentul 55

Propunere de regulament
Articolul 14 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Șeful CERT-UE prezintă IICB și președintelui IICB rapoarte ***periodice*** privind performanța CERT-UE, planificarea financiară, veniturile, execuția	***Cel puțin o dată pe an,*** șeful CERT-UE prezintă IICB și președintelui IICB rapoarte privind performanța CERT-UE, planificarea financiară, veniturile, execuția

bugetară, acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 alineatul (1).

bugetară, acordurile privind nivelul serviciilor și acordurile scrise încheiate, cooperarea cu omologii și partenerii și misiunile desfășurate de personal, inclusiv rapoartele menționate la articolul 10 alineatul (1).

Amendamentul 56

Propunere de regulament
Articolul 16 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, inclusiv CERT, centrele naționale de securitate cibernetică, CSIRT și punctele unice de contact menționate la articolul 8 din ***[propunerea de Directivă*** NIS 2], cu privire la amenințările cibernetice, la vulnerabilități și incidente, la posibilele contramăsuri și la toate aspectele relevante pentru îmbunătățirea protecției mediilor ***informatice*** ale instituțiilor, organelor și agențiilor Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul 13 din ***[propunerea de Directivă*** NIS 2].	1. CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, inclusiv CERT, centrele naționale de securitate cibernetică, CSIRT și punctele unice de contact menționate la articolul 8 din ***Directiva [propunerea*** NIS 2], cu privire la amenințările cibernetice, la vulnerabilități și incidente, la posibilele contramăsuri și la toate aspectele relevante pentru îmbunătățirea protecției mediilor ***TIC*** ale instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul 13 din ***Directiva [propunerea*** NIS 2].

Amendamentul 57

Propunere de regulament
Articolul 16 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. CERT-UE poate face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare fără consimțământul ***entității*** afectate. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul	2. CERT-UE poate face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare fără consimțământul ***instituțiilor, organelor, oficiilor sau agențiilor Uniunii*** afectate***, atât timp cât prelucrarea datelor cu caracter personal respectă dispozițiile***

de securitate cibernetică numai cu consimțământul ***entității*** afectate.	***aplicabile din Regulamentul (UE) 2018/1725***. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul de securitate cibernetică numai cu consimțământul ***instituțiilor, organelor, oficiilor sau agențiilor Uniunii*** afectate.

Amendamentul 58

Propunere de regulament
Articolul 17 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. CERT-UE poate coopera cu omologii din statele terțe, inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice formă de cooperare cu astfel de omologi, inclusiv într-un cadru în care omologii din afara UE cooperează cu omologii naționali din statele membre, CERT-UE solicită aprobarea prealabilă a IICB.	1. CERT-UE poate coopera cu omologii din statele terțe, inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice formă de cooperare cu astfel de omologi, inclusiv într-un cadru în care omologii din afara UE cooperează cu omologii naționali din statele membre, CERT-UE solicită aprobarea prealabilă a IICB. ***Orice astfel de cooperare respectă integritatea democratică a UE.***

Amendamentul 59

Propunere de regulament
Articolul 17 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. CERT-UE poate coopera cu alți parteneri, precum entități comerciale, organizații internaționale, entități naționale din afara Uniunii Europene sau experți individuali, pentru a colecta informații cu privire la amenințările cibernetice generale și specifice, la vulnerabilități și la posibilele contramăsuri. Pentru o cooperare mai extinsă cu astfel de parteneri, CERT-	2. CERT-UE poate coopera cu alți parteneri, precum entități comerciale, organizații internaționale, entități naționale din afara Uniunii Europene sau experți individuali, pentru a colecta informații cu privire la amenințările cibernetice generale și specifice, la vulnerabilități și la posibilele contramăsuri. Pentru o cooperare mai extinsă cu astfel de parteneri, CERT-UE solicită aprobarea prealabilă a IICB.

UE solicită aprobarea prealabilă a IICB.	***Orice astfel de cooperare respectă integritatea democratică a UE.***

Amendamentul 60

Propunere de regulament
Articolul 17 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Cu acordul ***entității*** afectate de un incident, CERT-UE poate să furnizeze informații referitoare la incident partenerilor care pot contribui la analiza acestuia.	3. Cu acordul ***instituțiilor, organelor, oficiilor sau agențiilor Uniunii*** afectate de un incident, CERT-UE poate să furnizeze informații referitoare la incident partenerilor care pot contribui la analiza acestuia.

Amendamentul 61

Propunere de regulament
Articolul 19 – alineatul -1 (nou)

Textul propus de Comisie	*Amendamentul*
	-1. Instituțiile, organele, oficiile sau agențiile Uniunii pot furniza CERT-UE în mod voluntar informații privind amenințările cibernetice, incidentele, incidentele evitate la limită și vulnerabilitățile care le afectează. CERT-UE se asigură că sunt disponibile mijloace eficiente de comunicare, în scopul de a facilita schimbul de informații cu entitățile Uniunii. CERT-UE poate trata notificările obligatorii cu prioritate față de notificările voluntare.

Amendamentul 62

Propunere de regulament
Articolul 19 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Pentru ***a coordona gestionarea vulnerabilităților și răspunsul*** la	1. Pentru ***a-și îndeplini misiunea și sarcinile astfel cum sunt definite*** la

incidente, CERT-UE ***le*** poate solicita instituțiilor, organelor și agențiilor Uniunii să îi furnizeze informații din inventarele lor de sisteme ***informatice care sunt relevante pentru sprijinul CERT-UE. Instituția***, ***organul sau agenția*** care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.	***articolul 12***, CERT-UE poate solicita instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii să îi furnizeze informații din inventarele lor de sisteme ***TIC, inclusiv informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, indicatori de compromitere***, ***alerte de securitate cibernetică și recomandări privind configurarea instrumentelor de securitate cibernetică pentru detectarea incidentelor cibernetice. Entitatea*** care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.

Amendamentul 63

Propunere de regulament
Articolul 19 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Instituțiile, organele și agențiile Uniunii, la cererea CERT-UE și fără întârzieri nejustificate, îi furnizează informații digitale create prin utilizarea dispozitivelor electronice implicate în incidentele lor respective. CERT-UE poate stabili mai în detaliu tipurile de informații digitale de care are nevoie pentru o cunoaștere detaliată a situației și pentru răspunsul la incidente.	2. Instituțiile, organele***, oficiile*** și agențiile Uniunii, la cererea CERT-UE și fără întârzieri nejustificate, îi furnizează informații digitale create prin utilizarea dispozitivelor electronice implicate în incidentele lor respective. CERT-UE poate stabili mai în detaliu tipurile de informații digitale de care are nevoie pentru o cunoaștere detaliată a situației și pentru răspunsul la incidente.

Amendamentul 64
Propunere de regulament
Articolul 20 – titlu

Textul propus de Comisie	*Amendamentul*
Obligații de ***notificare***	Obligații de ***raportare***

Amendamentul 65

Propunere de regulament
Articolul 20 – alineatul 1 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Toate instituțiile, organele și agențiile Uniunii ***vor trimite*** CERT-UE o ***notificare inițială*** cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în ***termen de*** 24 de ore ***de la data la*** care au luat cunoștință de acestea.	Toate instituțiile, organele***, oficiile*** și agențiile Uniunii ***transmit*** CERT-UE o ***avertizare timpurie*** cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative, fără întârzieri nejustificate și, în orice caz, în ***cel mult*** 24 de ore ***din momentul în*** care au luat cunoștință de acestea. ***Avertizarea timpurie respectivă indică, după caz, dacă incidentul semnificativ este probabil cauzat de acțiuni ilegale sau răuvoitoare și dacă are sau ar putea avea un impact transfrontalier.***

Amendamentul 66

Propunere de regulament
Articolul 20 – alineatul 1 – paragraful 2

Textul propus de Comisie	*Amendamentul*
În cazuri justificate corespunzător și în acord cu CERT-UE, instituția, organul sau agenția Uniunii în cauză se poate abate de la termenul ***prevăzut la paragraful anterior***.	În cazuri justificate corespunzător și în acord cu CERT-UE, instituția, organul***, oficiul*** sau agenția Uniunii în cauză se poate abate de la termenul ***respectiv***.

Amendamentul 67

Propunere de regulament
Articolul 20 – alineatul 2 – partea introductivă

Textul propus de Comisie	*Amendamentul*
2. Instituțiile, organele și agențiile Uniunii transmit apoi către CERT-UE, fără întârzieri nejustificate, detalii tehnice adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea, răspunsul la incidente sau	2. Instituțiile, organele***, oficiile*** și agențiile Uniunii transmit apoi ***o notificare*** către CERT-UE, fără întârzieri nejustificate ***și***, ***în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, actualizează***

adoptarea unor măsuri de atenuare. Notificarea include, dacă sunt disponibili:	***avertizarea timpurie și furnizează o evaluare inițială a incidentului semnificativ, a gravității și a impactului acestuia, cu*** detalii tehnice adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea, răspunsul la incidente sau adoptarea unor măsuri de atenuare. Notificarea include, dacă sunt disponibili:

Amendamentul 68
Propunere de regulament
Articolul 20 – alineatul 2 – paragraful 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	În cazuri justificate corespunzător și în acord cu CERT-UE, instituția, organul, oficiul sau agenția Uniunii în cauză se poate abate de la acest termen.

Amendamentul 69

Propunere de regulament
Articolul 20 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2 a. În termen de cel mult o lună de la transmiterea notificării unui incident semnificativ, instituțiile, organele, oficiile și agențiile Uniunii prezintă CERT-UE un raport final care include cel puțin următoarele:
	(a) o descriere detaliată a incidentului semnificativ, a gravității și a impactului acestuia;
	(b) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul semnificativ;
	(c) măsurile de atenuare aplicate și în curs;
	(d) după caz, impactul transfrontalier al incidentului semnificativ.

	În cazul în care incidentul semnificativ este încă în curs la momentul transmiterii raportului final menționat la primul paragraf, se transmit un raport privind progresele înregistrate la momentul respectiv și un raport final în termen de o lună de la incident.

Amendamentul 70

Propunere de regulament
Articolul 20 – alineatul 2 b (nou)

Textul propus de Comisie	*Amendamentul*
	2 b. În cazuri justificate corespunzător și în acord cu CERT-UE, instituția, organul, oficiul sau agenția Uniunii în cauză se poate abate de la termenul prevăzut la alineatul (2a).

Amendamentul 71

Propunere de regulament
Articolul 20 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. CERT-UE transmite lunar ENISA un raport de sinteză cu date anonimizate și agregate privind amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative notificate în conformitate cu alineatul (1).	3. CERT-UE transmite lunar ENISA un raport de sinteză cu date anonimizate și agregate privind amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative notificate în conformitate cu alineatul (1). ***Raportul respectiv constituie o contribuție la raportul bienal privind situația în materie de securitate cibernetică în Uniune, în temeiul articolului 18 din Directiva [propunerea NIS 2].***

Amendamentul 72

Propunere de regulament
Articolul 20 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. IICB ***poate*** emite documente de orientare sau recomandări privind modalitățile și conținutul notificării. CERT-UE difuzează detaliile tehnice adecvate pentru a permite detectarea proactivă, răspunsul la incidente sau adoptarea unor măsuri de atenuare de către instituțiile, organele și agențiile Uniunii.	4. IICB emite documente de orientare sau recomandări privind modalitățile și conținutul notificării. CERT-UE difuzează detaliile tehnice adecvate pentru a permite detectarea proactivă, răspunsul la incidente sau adoptarea unor măsuri de atenuare de către instituțiile, organele***, oficiile*** și agențiile Uniunii.

Amendamentul 73

Propunere de regulament
Articolul 20 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Obligațiile de notificare nu se aplică în cazul informațiilor IUEC și al informațiilor pe care o instituție, un organ sau o agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o autoritate de aplicare a legii cu condiția explicită ca acestea să nu fie comunicate CERT-UE.	***eliminat***

Amendamentul 74

Propunere de regulament
Articolul 24 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Comisia prezintă Parlamentului European și Consiliului un raport privind punerea în aplicare a prezentului regulament în termen de cel mult ***48*** luni de la data intrării în vigoare a prezentului regulament și, ulterior, o dată la ***trei*** ani.	2. Comisia prezintă Parlamentului European și Consiliului un raport privind punerea în aplicare a prezentului regulament în termen de cel mult ***36 de*** luni de la data intrării în vigoare a prezentului regulament și, ulterior, o dată la ***doi*** ani.

Amendamentul 75

Propunere de regulament

Articolul 24 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Comisia evaluează funcționarea prezentului regulament și prezintă un raport Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor nu mai devreme de ***cinci*** ani de la data intrării în vigoare.	3. Comisia evaluează funcționarea prezentului regulament și prezintă un raport Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor nu mai devreme de ***trei*** ani de la data intrării în vigoare***, având în vedere evoluția rapidă a peisajului amenințărilor cibernetice***.

Amendamentul 76

Propunere de regulament
Anexa I – paragraful 1 – partea introductivă

Textul propus de Comisie	*Amendamentul*
Domeniile următoare trebuie abordate în cadrul nivelului de referință în materie de securitate cibernetică:	***Cel puțin*** domeniile următoare trebuie abordate în cadrul nivelului de referință în materie de securitate cibernetică:

Amendamentul 77

Propunere de regulament
Anexa I – paragraful 1 – punctul 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	(1 a) formarea membrilor personalului în materie de securitate cibernetică;

Amendamentul 78

Propunere de regulament
Anexa I – paragraful 1 – punctul 3

Textul propus de Comisie	*Amendamentul*
(3) gestionarea activelor, inclusiv inventarul activelor ***informatice*** și cartografierea rețelelor ***informatice***;	(3) ***achiziționarea și*** gestionarea activelor, inclusiv inventarul activelor ***TIC*** și cartografierea rețelelor ***TIC***;

Amendamentul 79

Propunere de regulament
Anexa I – paragraful 1 – punctul 7

Textul propus de Comisie	*Amendamentul*
(7) achiziționarea, dezvoltarea și întreținerea de sisteme;	(7) achiziționarea, dezvoltarea și întreținerea de sisteme***, inclusiv dezvoltarea internă de software cu sursă deschisă***;

Amendamentul 80

Propunere de regulament
Anexa I – paragraful 1 – punctul 7 a (nou)

Textul propus de Comisie	*Amendamentul*
	(7a) auditurile de securitate cibernetică;

Amendamentul 81

Propunere de regulament
Anexa I – paragraful 1 – punctul 9

Textul propus de Comisie	*Amendamentul*
(9) gestionarea incidentelor, inclusiv abordări privind îmbunătățirea gradului de pregătire, a răspunsului la incidente și a capacității de recuperare în urma acestora, precum și cooperarea cu CERT-UE, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate;	(9) gestionarea incidentelor, inclusiv abordări privind îmbunătățirea gradului de pregătire, a răspunsului la incidente și a capacității de recuperare în urma acestora, ***respectarea și scurtarea termenelor obligațiilor de raportare,*** precum și cooperarea cu CERT-UE, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate;

Amendamentul 82

Propunere de regulament
Anexa II – paragraful 1 – punctul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	(3 a) formarea periodică a membrilor personalului în materie de securitate cibernetică;

Amendamentul 83

Propunere de regulament
Anexa II – paragraful 1 – punctul 4 – litera a

Textul propus de Comisie	*Amendamentul*
(a) eliminarea barierelor contractuale care limitează schimbul de informații între furnizorii de servicii ***informatice*** și CERT-UE cu privire la incidente, vulnerabilități și amenințări cibernetice	(a) eliminarea barierelor contractuale care limitează schimbul de informații între furnizorii de servicii ***TIC*** și CERT-UE cu privire la incidente, vulnerabilități și amenințări cibernetice***;***

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
Referințe	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Comisie competentă Data anunțului în plen	ITRE 4.4.2022
Aviz emis de către Data anunțului în plen	AFCO 4.4.2022
Raportor/Raportoare pentru aviz Data numirii	Markéta Gregorová 20.6.2022
Examinare în comisie	26.10.2022 1.12.2022
Data adoptării	25.1.2023
Rezultatul votului final	+: 24 –: 0 0: 0
Membri titulari prezenți la votul final	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Membri supleanți prezenți la votul final	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Leszek Miller

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA SESIZATĂ PENTRU AVIZ

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri

PROCEDURA COMISIEI COMPETENTE

Titlu	Măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii
Referințe	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Data prezentării în PE	22.3.2022
Comisie competentă Data anunțului în plen	ITRE 4.4.2022
Comisii sesizate pentru aviz Data anunțului în plen	BUDG LIBE AFCO 4.4.2022 4.4.2022 4.4.2022
Comisii asociate Data anunțului în plen	LIBE 15.9.2022
Raportori Data numirii	Henna Virkkunen 18.5.2022
Examinare în comisie	26.10.2022
Data adoptării	9.3.2023
Rezultatul votului final	+: 58 –: 0 0: 0
Membri titulari prezenți la votul final	Nicola Beer, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Cristian-Silviu Buşoi, Jerzy Buzek, Ignazio Corrao, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Christian Ehler, Valter Flego, Niels Fuglsang, Lina Gálvez Muñoz, Claudia Gamon, Jens Geier, Nicolás González Casares, Bart Groothuis, Christophe Grudler, Henrike Hahn, Robert Hajšel, Ivo Hristov, Romana Jerković, Seán Kelly, Łukasz Kohut, Miapetra Kumpula-Natri, Marisa Matias, Dan Nica, Angelika Niebler, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Manuela Ripa, Robert Roos, Maria Spyraki, Riho Terras, Grzegorz Tobiszowski, Patrizia Toia, Pernille Weiss
Membri supleanți prezenți la votul final	Andrus Ansip, Pascal Arimont, Izaskun Bilbao Barandica, Franc Bogovič, Jakop G. Dalunde, Matthias Ecke, Cornelia Ernst, Jens Gieseke, Jutta Paulus, Marion Walsmann, Emma Wiesner
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Agnès Evren, Tilly Metz
Data depunerii	10.3.2023

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA COMPETENTĂ

58	+
ECR	Johan Nissinen, Robert Roos, Grzegorz Tobiszowski
NI	Martin Buschmann
PPE	Pascal Arimont, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Christian Ehler, Agnès Evren, Jens Gieseke, Seán Kelly, Angelika Niebler, Maria Spyraki, Riho Terras, Marion Walsmann, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Izaskun Bilbao Barandica, Nicola Danti, Valter Flego, Claudia Gamon, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Niels Fuglsang, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Robert Hajšel, Ivo Hristov, Romana Jerković, Łukasz Kohut, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia
The Left	Marc Botenga, Cornelia Ernst, Marisa Matias
Verts/ALE	Michael Bloss, Ignazio Corrao, Ciarán Cuffe, Jakop G. Dalunde, Henrike Hahn, Tilly Metz, Ville Niinistö, Jutta Paulus, Manuela Ripa

0	-

0	0

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri