2023/2841

18.12.2023

REGULAMENTUL (UE, Euratom) 2023/2841 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 13 decembrie 2023

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 ([1]),

întrucât:

(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații europene transparente, eficiente și independente. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale amplifică riscurile de securitate cibernetică, făcând entitățile Uniunii mai vulnerabile la amenințările și incidentele cibernetice, care reprezintă o amenințare la adresa continuității activității și a capacității acestora 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 caracteristici esențiale ale tuturor activităților entităților 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 actorii care generează amenințări 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 sunt interdependente și au fluxuri de date integrate, iar utilizatorii acestora colaborează îndeaproape. Această interconectare înseamnă că orice perturbare, chiar și atunci când este limitată inițial la o singură 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 altor entități ale Uniunii. 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. Partajarea informațiilor referitoare la incidente poate facilita detectarea amenințărilor sau a incidentelor cibernetice similare care afectează statele membre.

(4) Entitățile Uniunii reprezintă 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 entităților Uniunii, este necesar ca acestea să atingă un nivel comun ridicat de securitate cibernetică prin punerea în aplicare a unor măsuri de securitate cibernetică proporționale cu riscurile de securitate cibernetică identificate, prin schimbul de informații și colaborarea în acest domeniu.

([1]) Poziția Parlamentului European din 21 noiembrie 2023 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 8 decembrie 2023.

(5) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([2]) urmărește să îmbunătățească și mai mult capacitatea de reziliență cibernetică și capacitatea de răspuns la incidente cibernetice ale entităților publice și private, ale autorităților și organelor 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, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul"), care să asigure o gestionare eficace și prudentă a tuturor riscurilor de securitate cibernetică și să țină seama de continuitatea activității și de gestionarea crizelor. Cadrul ar trebui să stabilească politici în materie de securitate cibernetică, inclusiv obiective și priorități, pentru securitatea rețelelor și a sistemelor informatice, care să cuprindă întregul mediu TIC neclasificat. Cadrul ar trebui să se bazeze pe o abordare multirisc, care vizează protejarea rețelelor și a sistemelor informatice și a mediului fizic al acestor sisteme împotriva unor evenimente precum furtul, incendiile, inundațiile, penele serviciilor de telecom sau de electricitate, ori împotriva accesului fizic neautorizat și a daunelor și intruziunii la nivelul informațiilor deținute de entitatea Uniunii sau al echipamentelor acesteia de prelucrare a informațiilor, care ar putea compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise, prelucrate sau accesibile prin intermediul rețelelor și al sistemelor informatice.

(7) Pentru a gestiona riscurile de securitate cibernetică identificate în cadru, fiecare entitate a Uniunii ar trebui să ia măsuri tehnice, operaționale și organizaționale adecvate și proporționale. Aceste măsuri ar trebui să abordeze domeniile și măsurile de gestionare a riscurilor de securitate cibernetică prevăzute în prezentul regulament pentru a consolida securitatea cibernetică a fiecărei entități a Uniunii.

(8) Activele și riscurile de securitate cibernetică identificate în cadru, precum și concluziile care decurg din evaluările periodice ale nivelului de maturitate a securității cibernetice ar trebui să se reflecte în planul de securitate cibernetică stabilit de fiecare entitate a Uniunii. Planul de securitate cibernetică ar trebui să includă măsurile de gestionare a riscurilor în materie de securitate cibernetică adoptate.

(9) Întrucât asigurarea securității cibernetice este un proces continuu, caracterul adecvat și eficacitatea tuturor măsurilor luate în temeiul prezentului regulament ar trebui revizuite periodic având în vedere riscurile de securitate cibernetică, activele și maturitatea securității cibernetice în schimbare ale entităților Uniunii. Cadrul ar trebui evaluat periodic și cel puțin o dată la patru ani, în timp ce planul de securitate cibernetică ar trebui să fie revizuit o dată la doi ani sau mai des atunci când este cazul, în urma evaluărilor nivelului de maturitate a securității cibernetice ori în urma oricărei revizuiri semnificative a cadrului.

(10) Măsurile de gestionare a riscurilor de securitate cibernetică instituite de entitățile Uniunii ar trebui să includă politici menite, atunci când este posibil, să asigure transparența codului sursă, ținând seama de garanțiile prin care se protejează drepturile terților sau ale entităților Uniunii. Aceste politici ar trebui să fie proporționale cu riscul de securitate cibernetică și sunt menite să faciliteze analiza amenințărilor cibernetice, fără a crea, în același timp, obligații de divulgare sau drepturi de acces la codul terților în afara clauzelor contractuale aplicabile.

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

([2]) 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).

(12) Diferențele dintre entitățile Uniunii necesită o anumită flexibilitate în punerea în aplicare a prezentului regulament. Măsurile pentru nivelul comun ridicat de securitate cibernetică prevăzut în prezentul regulament 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. Prin urmare, aceste entități ar trebui să își stabilească propriile cadre și să își adopte propriile măsuri de gestionare a riscurilor de securitate cibernetică și planuri de securitate cibernetică. La punerea în aplicare a unor astfel de măsuri, ar trebui să se țină seama în mod corespunzător de sinergiile existente între entitățile Uniunii, în scopul gestionării adecvate a resurselor și al optimizării costurilor. De asemenea, ar trebui să se asigure că măsurile nu afectează în mod negativ schimbul eficient de informații între entitățile Uniunii și cooperarea dintre entitățile Uniunii și omologii din statele membre.

(13) Pentru a optimiza utilizarea resurselor, prezentul regulament ar trebui să prevadă posibilitatea ca două sau mai multe entități ale Uniunii cu structuri similare să coopereze la efectuarea evaluărilor maturității securității cibernetice pentru entitățile lor respective.

(14) 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 de securitate cibernetică la care sunt expuse rețeaua și sistemele informatice 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 indicativ de cel puțin 10 %. În aprecierea nivelului de maturitate al securității cibernetice ar trebui, de asemenea, să se evalueze dacă cheltuielile entității Uniunii în materie de securitate cibernetică sunt proporționale cu riscurile de securitate cibernetică cu care se confruntă. Fără a aduce atingere normelor referitoare la bugetul anual al Uniunii în temeiul tratatelor, Comisia ar trebui să țină seama, în propunerea sa privind primul buget anual adoptat după intrarea în vigoare a prezentului regulament, de obligațiile care decurg din prezentul regulament atunci când evaluează necesitățile bugetare și de personal ale entităților Uniunii, astfel cum rezultă din estimările lor privind cheltuielile.

(15) 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. Cel mai înalt nivel de conducere al entității Uniunii ar trebui să fie responsabil de punerea în aplicare a prezentului regulament, inclusiv de instituirea cadrului, de luarea măsurilor de gestionare a riscurilor de securitate cibernetică și de aprobarea planului de securitate cibernetică. Abordarea culturii securității cibernetice, adică practica zilnică în domeniul securității cibernetice, este parte integrantă a cadrului și a măsurilor corespunzătoare de gestionare a riscurilor de securitate cibernetică în toate entitățile Uniunii.

(16) Securitatea rețelelor și a sistemelor informatice care gestionează informații UE clasificate (IUEC) este esențială. Entitățile Uniunii care gestionează IUEC trebuie să aplice cadrele de reglementare cuprinzătoare în vigoare pentru protejarea acestor informații, inclusiv o guvernanță, politici și proceduri specifice de gestionare a riscurilor. Este necesar ca rețelele și sistemele informatice care gestionează IUEC să respecte standarde de securitate mai stricte decât rețelele și sistemele informatice neclasificate. Prin urmare, rețelele și sistemele informatice care gestionează IUEC sunt mai reziliente la amenințările și incidentele cibernetice. În consecință, deși recunoaște necesitatea unui cadru comun în această privință, prezentul regulament nu ar trebui să se aplice rețelelor și sistemelor informatice care gestionează IUEC. Cu toate acestea, în cazul în care o entitate a Uniunii solicită în mod explicit acest lucru, Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE) ar trebui să fie în măsură să ofere asistență respectivei entități a Uniunii în ceea ce privește incidentele din medii TIC clasificate.

(17) Entitățile Uniunii ar trebui să evalueze riscurile de securitate cibernetică 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. Măsurile de securitate cibernetică ar trebui să fie detaliate în orientările sau în recomandările emise de CERT-UE. La stabilirea măsurilor și a orientărilor ar trebui să se țină seama în mod corespunzător de cele mai recente evoluții și, după caz, de standardele europene și internaționale relevante, precum și de dreptul și politicile relevante ale Uniunii, inclusiv de evaluările riscurilor de securitate cibernetică și de recomandările emise de Grupul de cooperare instituit în temeiul articolului 14 din 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 pentru securitatea cibernetică a rețelelor 5G. În plus, având în vedere peisajul

amenințărilor cibernetice și importanța, pentru entitățile Uniunii, a consolidării rezilienței cibernetice, ar putea să se solicite certificarea produselor TIC, a serviciilor TIC 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 al Parlamentului European și al Consiliului ([3]).

(18) În mai 2011, secretarii generali ai instituțiilor și organelor Uniunii au decis să instituie o echipă de preconfigurare a 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, cu un mandat interinstituțional. În decembrie 2017, instituțiile și organele Uniunii au încheiat un acord interinstituțional privind organizarea și funcționarea CERT-UE ([4]). Prezentul regulament ar trebui să ofere un set cuprinzător de norme privind organizarea, funcționarea și gestionarea CERT-UE. Dispozițiile prezentului regulament prevalează asupra dispozițiilor Acordului interinstituțional privind organizarea și funcționarea CERT-UE, care a fost încheiat în decembrie 2017.

(19) CERT-UE ar trebui să fie redenumit Serviciul de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii, însă denumirea prescurtată CERT-UE ar trebui să fie păstrată datorită recunoașterii sale pe scară largă.

(20) Pe lângă atribuirea mai multor sarcini și a unui rol extins pentru CERT-UE, prezentul regulament instituie Consiliul interinstituțional pentru securitate cibernetică (IICB), pentru a facilita un nivel comun ridicat de securitate cibernetică în entitățile Uniunii. IICB ar trebui să aibă un rol exclusiv în ceea ce privește monitorizarea și sprijinirea punerii în aplicare a prezentului regulament de către entitățile Uniunii și în ceea ce privește supravegherea punerii în aplicare a priorităților și a obiectivelor generale ale CERT-UE și elaborarea unor orientări strategice pentru CERT-UE. Prin urmare, IICB ar trebui să asigure reprezentarea instituțiilor Uniunii și ar trebui să includă reprezentanți ai organelor, oficiilor și agențiilor Uniunii prin intermediul Rețelei agențiilor Uniunii (EUAN). Organizarea și funcționarea IICB ar trebui să fie reglementate în continuare de regulamentul său intern de procedură, care poate include precizări suplimentare privind reuniunile periodice ale IICB, inclusiv reuniunile anuale la nivel politic, în cadrul cărora reprezentanții de la cel mai înalt nivel de conducere al fiecărui membru al IICB ar permite IICB să poarte discuții strategice și să ofere orientări strategice pentru IICB. În plus, IICB ar trebui să poată institui un comitet executiv care să îi ofere asistență în activitatea sa și să poată să îi delege unele dintre sarcinile și competențele sale, în special sarcinile care necesită expertiza specifică a membrilor săi, de exemplu aprobarea catalogului de servicii și orice actualizări ulterioare ale acestuia, modalitățile de încheiere a acordurilor privind nivelul serviciilor, evaluările documentelor și rapoartelor transmise de entitățile Uniunii către IICB în temeiul prezentului regulament sau sarcinile legate de pregătirea deciziilor privind măsurile de conformitate emise de IICB și de monitorizarea punerii lor în aplicare. IICB ar trebui să stabilească regulamentul de procedură al comitetului executiv, inclusiv sarcinile și competențele acestuia.

(21) IICB urmărește să sprijine entitățile Uniunii pentru a îmbunătăți situația lor respectivă în materie de securitate cibernetică prin punerea în aplicare a prezentului regulament. Pentru a sprijini entitățile Uniunii, IICB ar trebui să ofere orientări șefului CERT-UE, să adopte o strategie multianuală privind creșterea nivelului de securitate cibernetică în entitățile Uniunii, să stabilească metodologia și alte aspecte ale evaluărilor *inter pares* voluntare și să faciliteze instituirea unui grup informal de responsabili locali cu securitatea cibernetică, sprijinit de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cu scopul de a face schimb de bune practici și de informații în legătură cu punerea în aplicare a prezentului regulament.

([3]) 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).

([4]) Acordul dintre Parlamentul European, Consiliul European, Consiliul Uniunii Europene, Comisia Europeană, Curtea de Justiție a Uniunii Europene, Banca Centrală Europeană, Curtea de Conturi Europeană, Serviciul European de Acțiune Externă, Comitetul Economic și Social European, Comitetul European al Regiunilor și Banca Europeană de Investiții privind organizarea și funcționarea unui Centru de răspuns la incidente de securitate cibernetică pentru instituțiile, organismele și agențiile Uniunii (CERT-UE) (JO C 12, 13.1.2018, p. 1).

(22) Pentru a atinge un nivel ridicat de securitate cibernetică în toate entitățile Uniunii, interesele organelor, oficiilor și agențiilor Uniunii care își gestionează propriul mediu TIC ar trebui să fie reprezentate în cadrul IICB de trei reprezentanți desemnați de EUAN. Securitatea prelucrării datelor cu caracter personal și, prin urmare, și securitatea cibernetică a acestora reprezintă o piatră de temelie pentru protecția datelor. Având în vedere sinergiile dintre protecția datelor și securitatea cibernetică, Autoritatea Europeană pentru Protecția Datelor ar trebui să fie reprezentată în cadrul IICB în calitatea sa de entitate a Uniunii care face obiectul prezentului regulament, cu expertiză specifică în domeniul protecției datelor, inclusiv al securității rețelelor de comunicații electronice. Având în vedere importanța inovării și a competitivității în domeniul securității cibernetice, Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică ar trebui să fie reprezentat în cadrul IICB. Având în vedere rolul ENISA de centru de expertiză în materie de securitate cibernetică și sprijinul pe care îl oferă și având în vedere importanța securității cibernetice a infrastructurii și serviciilor spațiale ale Uniunii, ENISA și Agenția Uniunii Europene pentru Programul spațial ar trebui să fie reprezentate în cadrul IICB. Având în vedere rolul atribuit CERT-UE în temeiul prezentului regulament, șeful CERT-UE ar trebui să fie invitat de președintele IICB la toate reuniunile IICB, cu excepția cazului în care IICB discută aspecte direct legate de șeful CERT-UE.

(23) IICB ar trebui să monitorizeze respectarea prezentului regulament, precum și punerea în aplicare a orientărilor, a recomandărilor și a apelurilor la acțiune. 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. Grupurile consultative tehnice respective ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu entitățile Uniunii și cu alte părți interesate, după caz.

(24) În cazul în care constată că o entitate a Uniunii nu a pus în aplicare în mod efectiv prezentul regulament sau orientările, recomandările sau apelurile la acțiune emise în temeiul acestuia, IICB poate, fără a aduce atingere procedurilor interne ale entității Uniunii în cauză, să ia măsuri de asigurare a conformității. IICB ar trebui să aplice în mod progresiv măsurile de asigurare a conformității, cu alte cuvinte, IICB ar trebui să adopte mai întâi măsura cea mai puțin severă, și anume un aviz motivat și, numai dacă este necesar, măsuri din ce în ce mai severe, culminând cu cea mai severă măsură, și anume o recomandare de suspendare temporară a fluxurilor de date către entitatea Uniunii în cauză. O astfel de recomandare ar trebui să se aplice numai în cazuri excepționale de încălcări pe termen lung, deliberate, repetitive sau grave ale prezentului regulament de către entitatea Uniunii în cauză.

(25) Avizul motivat reprezintă măsura de asigurare a conformității cea mai puțin severă, care abordează lacunele observate în ceea ce privește punerea în aplicare a prezentului regulament. IICB ar trebui să poată prezenta, după un aviz motivat, orientări pentru a ajuta entitatea Uniunii să se asigure că cadrul său, măsurile sale de gestionare a riscurilor de securitate cibernetică, planul său de securitate cibernetică și raportarea sa sunt conforme cu prezentul regulament și, apoi, un avertisment vizând remedierea într-un termen specificat a lacunelor identificate ale entității Uniunii. Dacă lacunele identificate în avertisment nu sunt remediate în mod suficient, IICB ar trebui să poată emite o notificare motivată.

(26) IICB ar trebui să poată recomanda efectuarea unui audit al unei entități a Uniunii. Entitatea Uniunii ar trebui să își poată utiliza funcția de audit intern în acest scop. De asemenea, IICB ar trebui să poată solicita efectuarea unui audit de către un serviciu de audit terț, inclusiv de către un furnizor de servicii din sectorul privat convenit de comun acord.

(27) În cazuri excepționale de încălcări pe termen lung, deliberate, repetate sau grave ale prezentului regulament de către o entitate a Uniunii, IICB ar trebui, ca măsură de ultimă instanță, să le poată recomanda tuturor statelor membre și entităților Uniunii o suspendare temporară a fluxurilor de date către entitatea Uniunii în cauză, suspendare care ar trebui să rămână în vigoare până când entitatea Uniunii încetează încălcarea. O astfel de recomandare ar trebui transmisă prin intermediul unor canale de comunicare adecvate și securizate.

(28) Pentru a asigura punerea corectă în aplicare a prezentului regulament, IICB ar trebui, în cazul în care consideră că o încălcare persistentă a prezentului regulament de către o entitate a Uniunii a fost cauzată direct de acțiunile sau omisiunile unui membru al personalului acesteia, inclusiv la cel mai înalt nivel de conducere, să solicite entității Uniunii în cauză să ia măsurile corespunzătoare, inclusiv să aibă în vedere luarea unor măsuri de natură disciplinară, în conformitate cu normele și procedurile stabilite în Statutul funcționarilor Uniunii Europene și în Regimul aplicabil celorlalți agenți ai Uniunii, prevăzute în Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([5]) (denumit în continuare „Statutul funcționarilor") și în orice alte norme și proceduri aplicabile.

(29) CERT-UE ar trebui să contribuie la securitatea mediului TIC al tuturor entităților Uniunii. Atunci când, la cererea unei entități a Uniunii, analizează dacă să ofere consiliere tehnică sau contribuții cu privire la chestiuni de politică relevante, CERT-UE ar trebui să se asigure că acest lucru nu împiedică îndeplinirea celorlalte sarcini care îi sunt conferite în temeiul prezentului regulament. CERT-UE ar trebui să îndeplinească pentru entitățile Uniunii un rol echivalent celui de coordonator desemnat în scopul divulgării coordonate a vulnerabilităților în temeiul articolului 12 alineatul (1) din Directiva (UE) 2022/2555.

(30) CERT-UE ar trebui să sprijine punerea în aplicare a măsurilor pentru un nivel comun ridicat de securitate cibernetică prin propuneri de orientări și recomandări adresate IICB sau prin adresarea unor apeluri la acțiune. Aceste orientări și recomandări ar trebui 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. IICB ar trebui să îi solicite CERT-UE să emită, să retragă sau să modifice o propunere de orientare sau de recomandare sau un apel la acțiune.

(31) De asemenea, CERT-UE ar trebui 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) instituită în temeiul articolului 15 din directiva respectivă. În plus, în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei ([6]), CERT-UE ar trebui 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 din statele membre. CERT-UE ar trebui, de asemenea, să colaboreze cu alți omologi din sectorul public și privat, inclusiv din cadrul Organizației Tratatului Atlanticului de Nord, sub rezerva aprobării prealabile de către IICB.

(32) În sprijinirea securității cibernetice operaționale, CERT-UE ar trebui să utilizeze expertiza de care dispune ENISA prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881. 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 ar trebui să coopereze cu ENISA în ceea ce privește analiza amenințărilor cibernetice și să îi transmită în mod regulat raportul său privind situația amenințărilor.

(33) CERT-UE ar trebui să poată coopera și face schimb de informații cu comunitățile relevante de securitate cibernetică din Uniune și din statele sale membre pentru a încuraja cooperarea operațională și pentru a permite rețelelor existente să își valorifice pe deplin potențialul de protejare a Uniunii.

(34) Întrucât serviciile și sarcinile CERT-UE sunt în interesul 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.

([5]) Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului din 29 februarie 1968 de stabilire a Statutului funcționarilor Comunităților Europene, precum și a Regimului aplicabil celorlalți agenți ai acestor comunități și de instituire a unor măsuri speciale tranzitorii aplicabile funcționarilor Comisiei (JO L 56, 4.3.1968, p. 1).

([6]) 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).

(35) 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 și capacitatea de recuperare în urma incidentelor, entitățile Uniunii ar trebui să poată informa CERT-UE cu privire la incidente, amenințări cibernetice, vulnerabilități și incidente evitate la limită și să facă schimb de detalii tehnice adecvate care să permită detectarea sau atenuarea, precum și răspunsul în urma unor incidente, amenințări cibernetice, vulnerabilități și incidente evitate la limită similare în alte entități ale Uniunii. Urmând aceeași abordare ca în Directiva (UE) 2022/2555, entitățile Uniunii ar trebui să transmită CERT-UE o avertizare timpurie în termen de 24 de ore de la identificarea unui incident semnificativ. 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 entităților Uniunii și ale omologilor entităților Uniunii împotriva unor incidente similare.

(36) 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 de incidente semnificative și le permite entităților Uniunii să solicite asistență și, pe de altă parte, raportarea aprofundată care permite extragerea unor învățăminte valoroase din incidentele individuale și îmbunătățește în timp reziliența cibernetică a diverselor entități ale Uniunii și contribuie la ameliorarea situației lor generale de securitate cibernetică. În această privință, prezentul regulament ar trebui să includă raportarea incidentelor care, pe baza unei evaluări inițiale efectuate de entitatea Uniunii în cauză, ar putea cauza perturbări operaționale grave ale funcționării entității Uniunii sau pierderi financiare pentru entitatea Uniunii în cauză sau ar putea afecta alte persoane fizice sau juridice, cauzând 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 entității Uniunii, gravitatea și caracteristicile tehnice ale unei amenințări cibernetice și orice vulnerabilități subiacente care sunt exploatate, precum și experiența entității Uniunii în ceea ce privește incidente similare. Indicatori precum măsura în care este afectată funcționarea entității Uniunii, durata unui incident sau numărul de persoane fizice sau juridice afectate ar putea juca un rol important în identificarea nivelului de gravitate a perturbării operaționale.

(37) Întrucât infrastructura, rețelele și sistemele informatice ale entității Uniunii relevante și ale statului membru în care este situată entitatea Uniunii sunt interconectate, este esențial ca statul membru respectiv să fie informat fără întârzieri nejustificate cu privire la un incident semnificativ în cadrul entității Uniunii respective. În acest scop, entitatea Uniunii afectată ar trebui să informeze orice omologi relevanți din statele membre desemnați sau stabiliți în temeiul articolelor 8 și 10 din Directiva (UE) 2022/2555 despre apariția unui incident semnificativ pe care îl raportează către CERT-UE. În cazul în care CERT-UE ia cunoștință de un incident semnificativ care survine într-un stat membru, acesta ar trebui să notifice omologul statului membru respectiv.

(38) Ar trebui pus în aplicare un mecanism care să asigure eficacitatea schimbului de informații, a coordonării și a cooperării entităților Uniunii în cazul unor incidente majore, inclusiv o identificare clară a rolurilor și a responsabilităților entităților Uniunii implicate. Reprezentantul Comisiei în cadrul IICB ar trebui, sub rezerva planului de gestionare a crizelor cibernetice, să fie punctul de contact pentru a facilita schimbul de informații relevante între IICB și Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), ca o contribuție la conștientizarea comună a situației. Rolul reprezentantului Comisiei în cadrul IICB ca punct de contact nu ar trebui să aducă atingere rolului separat și distinct al Comisiei în cadrul EU-CyCLONe în temeiul articolului 16 alineatul (2) din Directiva (UE) 2022/2555.

(39) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([7]) se aplică prelucrărilor de date cu caracter personal efectuate în temeiul prezentului regulament. Prelucrarea datelor cu caracter personal ar putea avea loc în legătură cu măsurile adoptate în contextul gestionării riscurilor de securitate cibernetică, al gestionării vulnerabilității și a incidentelor, al schimbului de informații cu privire la incidente, amenințări cibernetice și vulnerabilități, precum și al coordonării și cooperării în ceea ce privește răspunsul la incidente. Aceste măsuri ar putea necesita prelucrarea anumitor categorii de date cu caracter personal, cum ar fi adresele IP, localizatoarele

([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).

uniforme de resurse (URL-uri), numele de domenii, adresele de e-mail, rolurile organizaționale ale persoanei vizate, mărcile temporale, subiectele de e-mail sau numele fișierelor. Toate măsurile luate în temeiul prezentului regulament ar trebui să respecte cadrul de protecție a datelor și a vieții private, iar entitățile Uniunii, CERT-UE și, după caz, IICB ar trebui să ia toate măsurile tehnice și organizatorice relevante pentru a garanta respectarea acestui cadru în mod responsabil.

(40) Prezentul regulament stabilește temeiul juridic pentru prelucrarea datelor cu caracter personal de către entitățile Uniunii, CERT-UE și, după caz, IICB, în scopul îndeplinirii sarcinilor și obligațiilor care le revin în temeiul prezentului regulament, în conformitate cu articolul 5 alineatul (1) litera (b) din Regulamentul (UE) 2018/1725. CERT-UE poate acționa în calitate de operator sau de persoană împuternicită de operator, în funcție de sarcina pe care o îndeplinește în temeiul Regulamentului (UE) 2018/1725.

(41) În anumite cazuri, în scopul respectării obligațiilor care le revin în temeiul prezentului regulament pentru a asigura un nivel ridicat de securitate cibernetică și, în special, în contextul gestionării vulnerabilității și a incidentelor, poate fi necesar ca entitățile Uniunii și CERT-UE să prelucreze categorii speciale de date cu caracter personal, astfel cum se menționează la articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725. Prezentul regulament stabilește temeiul juridic pentru prelucrarea categoriilor speciale de date cu caracter personal de către entitățile Uniunii și CERT-UE în conformitate cu articolul 10 alineatul (2) litera (g) din Regulamentul (UE) 2018/1725. Prelucrarea categoriilor speciale de date cu caracter personal în temeiul prezentului regulament ar trebui să fie strict proporțională cu obiectivul urmărit. Sub rezerva condițiilor prevăzute la articolul 10 alineatul (2) litera (g) din regulamentul respectiv, entitățile Uniunii și CERT-UE ar trebui să poată prelucra astfel de date numai în măsura în care este necesar și atunci când acest lucru este prevăzut în mod explicit în prezentul regulament. Atunci când prelucrează categorii speciale de date cu caracter personal, entitățile Uniunii și CERT-UE ar trebui să respecte esența dreptului la protecția datelor și să prevadă măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanelor vizate.

(42) În temeiul articolului 33 din Regulamentul (UE) 2018/1725, entitățile Uniunii și CERT-UE ar trebui, ținând seama de stadiul actual al tehnologiei, de costurile punerii în aplicare și de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel adecvat de securitate a datelor cu caracter personal, cum ar fi acordarea unor drepturi de acces restricționate pe baza principiului necesității de a cunoaște, aplicarea principiilor pistei de audit, adoptarea lanțului de custodie, stocarea datelor în repaus într-un mediu controlat și auditabil, proceduri operaționale standardizate și măsuri de protecție a vieții private, cum ar fi pseudonimizarea sau criptarea. Măsurile respective nu ar trebui să fie puse în aplicare într-un mod care să afecteze obiectivul gestionării incidentelor și al integrității probelor. În cazul în care o entitate a Uniunii sau CERT-UE transferă date cu caracter personal legate de un incident, inclusiv categorii speciale de date cu caracter personal, către un omolog sau un partener în înțelesul prezentului regulament, astfel de transferuri ar trebui să respecte Regulamentul (UE) 2018/1725. În cazul în care categorii speciale de date cu caracter personal sunt transferate unei părți terțe, entitățile Uniunii și CERT-UE ar trebui să se asigure că partea terță aplică măsuri privind protecția datelor cu caracter personal la un nivel echivalent cu Regulamentul (UE) 2018/1725.

(43) Datele cu caracter personal prelucrate în înțelesul prezentului regulament ar trebui păstrate numai atât timp cât este necesar, în conformitate cu Regulamentul (UE) 2018/1725. Entitățile Uniunii și, după caz, CERT-UE, care acționează în calitate de operator, ar trebui să stabilească perioade de păstrare care să se limiteze la ceea ce este necesar pentru atingerea scopurilor specificate. În special în ceea ce privește datele cu caracter personal colectate pentru gestionarea incidentelor, entitățile Uniunii și CERT-UE ar trebui să facă distincție între datele cu caracter personal colectate pentru detectarea unei amenințări cibernetice în mediile lor TIC pentru a preveni un incident și datele cu caracter personal care sunt colectate pentru atenuarea unui incident, pentru răspunsul la acesta și pentru recuperarea în urma sa. Pentru detectarea unei amenințări cibernetice, este important să se țină seama de intervalul în care un actor care generează amenințări poate rămâne nedetectat într-un sistem. Pentru atenuarea unui incident, pentru răspunsul la acesta și pentru recuperarea în urma sa, este important să se analizeze dacă datele cu caracter personal sunt necesare pentru a urmări și a gestiona un incident recurent sau un incident de natură similară pentru care ar putea fi demonstrată o corelație.

(44) Gestionarea informațiilor de către entitățile Uniunii și CERT-UE ar trebui să respecte normele aplicabile privind securitatea informațiilor. Includerea securității resurselor umane ca măsură de gestionare a riscurilor de securitate cibernetică ar trebui, de asemenea, să respecte normele aplicabile.

(45) În scopul schimbului de informații, se utilizează marcaje vizibile pentru a indica faptul că destinatarii informațiilor trebuie să aplice limite de partajare pe baza, în special, a unor acorduri de nedivulgare sau a unor acorduri informale de nedivulgare cum ar fi protocolul TLP („Traffic Light Protocol") sau alte indicații clare din partea sursei. Protocolul TLP trebuie înțeles drept mijloc de a furniza informații despre orice limitări în ceea ce privește răspândirea ulterioară a informațiilor. Este utilizat în aproape toate CSIRT și în unele centre de analiză și schimb de informații.

(46) Prezentul regulament ar trebui să fie evaluat periodic în lumina viitoarelor negocieri privind cadrele financiare multianuale, permițând luarea unor decizii suplimentare în ceea ce privește funcționarea și rolul instituțional al CERT-UE, inclusiv posibila instituire a CERT-UE ca oficiu al Uniunii.

(47) IICB, cu sprijinul CERT-UE, ar trebui să revizuiască și să evalueze punerea în aplicare a prezentului regulament și ar trebui să raporteze constatările sale Comisiei. Pe baza acestei contribuții, Comisiei îi revine sarcina de a raporta Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor. Raportul respectiv, cu contribuția IICB, ar trebui să evalueze oportunitatea includerii rețelelor și a sistemelor informatice care gestionează IUEC în domeniul de aplicare al prezentului regulament, în special în absența unor norme comune în materie de securitate a informațiilor pentru entitățile Uniunii.

(48) În conformitate cu principiul proporționalității, este necesar și oportun, în vederea realizării obiectivului fundamental de a atinge un nivel comun ridicat de securitate cibernetică în cadrul entităților Uniunii, să se reglementeze securitatea cibernetică pentru entitățile Uniunii. Prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului urmărit, în conformitate cu articolul 5 alineatul (4) din Tratatul privind Uniunea Europeană.

(49) Prezentul regulament reflectă faptul că entitățile Uniunii diferă în ceea ce privește dimensiunea și capacitatea, inclusiv în ceea ce privește resursele financiare și umane.

(50) 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 ([8]),

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 ceea ce privește:

(a) instituirea de către fiecare entitate a Uniunii a unui cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică în temeiul articolului 6;

(b) gestionarea riscurilor de securitate cibernetică, raportarea și schimbul de informații;

(c) organizarea, funcționarea și operarea Consiliului interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10, precum și organizarea, funcționarea și operarea Serviciului de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii (CERT-UE);

(d) monitorizarea punerii în aplicare a prezentului regulament.

([8]) JO C 258, 5.7.2022, p. 10.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică entităților Uniunii, Consiliului interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10 și CERT-UE.

(2) Prezentul regulament se aplică fără a aduce atingere autonomiei instituționale în temeiul tratatelor.

(3) Cu excepția articolului 13 alineatul (8), prezentul regulament nu se aplică rețelelor și sistemelor informatice care gestionează informații UE clasificate (IUEC).

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 (TFUE) 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 un organ de coordonare și supraveghere responsabil cu funcționarea unei entități a Uniunii, la cel mai înalt nivel administrativ, având mandatul de a adopta sau de a autoriza decizii în conformitate cu mecanismele de guvernanță la nivel înalt ale acestei entități a Uniunii, fără a aduce atingere responsabilităților oficiale ale altor niveluri de conducere în ceea ce privește conformitatea și gestionarea riscurilor de securitate cibernetică în domeniile lor de responsabilitate respective;

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

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

8. „incident major” înseamnă un incident care cauzează un nivel de perturbare ce depășește capacitatea unei entități a Uniunii și a CERT-UE de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două entități ale Uniunii;

9. „incident de securitate cibernetică de mare amploare” înseamnă un incident de securitate cibernetică de mare amploare astfel cum este definit la articolul 6 punctul 7 din Directiva (UE) 2022/2555;

10. „gestionarea incidentului” înseamnă gestionarea incidentului astfel cum este definită la articolul 6 punctul 8 din Directiva (UE) 2022/2555;

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

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

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

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

15. „serviciu de cloud computing” înseamnă un serviciu de cloud computing astfel cum este definit la articolul 6 punctul 30 din Directiva (UE) 2022/2555.

Articolul 4

Prelucrarea datelor cu caracter personal

(1) Prelucrarea datelor cu caracter personal în temeiul prezentului regulament de către CERT-UE, Consiliul interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10 și entitățile Uniunii se efectuează în conformitate cu Regulamentul (UE) 2018/1725.

(2) Atunci când îndeplinesc sarcini sau obligații în temeiul prezentului regulament, CERT-UE, Consiliul interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10 și entitățile Uniunii prelucrează și fac schimb de date cu caracter personal numai în măsura în care este necesar și exclusiv în scopul îndeplinirii sarcinilor sau obligațiilor respective.

(3) Prelucrarea categoriilor speciale de date cu caracter personal menționate la articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725 este considerată necesară din motive de interes public major în temeiul articolului 10 alineatul (2) litera (g) din regulamentul respectiv. Aceste date pot fi prelucrate numai în măsura necesară pentru punerea în aplicare a măsurilor de gestionare a riscurilor de securitate cibernetică menționate la articolele 6 și 8, pentru furnizarea de servicii de către CERT-UE în temeiul articolului 13, pentru schimbul de informații referitoare la incidente în temeiul articolului 17 alineatul (3) și al articolului 18 alineatul (3), pentru schimbul de informații în temeiul articolului 20, pentru obligațiile de raportare în temeiul articolului 21, pentru coordonarea și cooperarea în ceea ce privește răspunsul la incidente în temeiul articolului 22 și pentru gestionarea incidentelor majore în temeiul articolului 23 din prezentul regulament. Atunci când acționează în calitate de operatori de date, Entitățile Uniunii și CERT-UE aplică măsuri tehnice pentru a preveni prelucrarea categoriilor speciale de date cu caracter personal în alte scopuri și prevăd măsuri adecvate și specifice pentru a proteja drepturile fundamentale și interesele persoanelor vizate.

CAPITOLUL II

MĂSURI PENTRU UN NIVEL COMUN RIDICAT DE SECURITATE CIBERNETICĂ

Articolul 5

Punerea în aplicare a măsurilor

(1) Până la 8 septembrie 2024, Consiliul interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10, după consultarea Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) și după primirea de orientări din partea CERT-UE, emite orientări pentru entitățile Uniunii în scopul efectuării unei analize inițiale a securității cibernetice și al instituirii unui cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică în temeiul articolului 6, al efectuării unor evaluări ale maturității în materie de securitate cibernetică în temeiul articolului 7, al luării unor măsuri de gestionare a riscurilor de securitate cibernetică în temeiul articolului 8, precum și al adoptării planului de securitate cibernetică în temeiul articolului 9.

(2) La punerea în aplicare a articolelor 6-9, entitățile Uniunii țin seama de orientările menționate la alineatul (1) de la prezentul articol, precum și de orientările și recomandările relevante adoptate în temeiul articolelor 11 și 14.

Articolul 6

Cadrul de gestionare, guvernanță și control al riscurilor de securitate cibernetică

(1) Până la 8 aprilie 2025, fiecare entitate a Uniunii, după efectuarea unei analize inițiale a securității cibernetice, cum ar fi un audit, instituie un cadru intern de gestionare, guvernanță și control al riscurilor de securitate cibernetică (denumit în continuare „cadrul”). Instituirea cadrului se află sub supravegherea și responsabilitatea celui mai înalt nivel de conducere al entității Uniunii.

(2) Cadrul acoperă întregul mediu TIC neclasificat al entității Uniunii în cauză, inclusiv orice mediu TIC de la fața locului, rețea tehnologică operațională, 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 aceste medii (mediul TIC). Cadrul se bazează pe o abordare care ia în considerare toate riscurile.

(3) Cadrul asigură un nivel ridicat de securitate cibernetică. Cadrul stabilește politici interne de securitate cibernetică, inclusiv obiective și priorități, pentru securitatea rețelelor și a sistemelor informatice, precum și rolurile și responsabilitățile personalului entității Uniunii însărcinat cu asigurarea punerii în aplicare eficace a prezentului regulament. Cadrul include, de asemenea, mecanisme de măsurare a eficacității punerii în aplicare.

(4) Cadrul este revizuit periodic, având în vedere evoluția riscurilor de securitate cibernetică, și cel puțin o dată la patru ani. După caz și în urma unei cereri din partea Consiliului interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10, cadrul unei entități a Uniunii poate fi actualizat pe baza orientărilor CERT-UE privind incidentele identificate sau posibilele lacune observate în punerea în aplicare a prezentului regulament.

(5) Cel mai înalt nivel de conducere al fiecărei entități a Uniunii este responsabil cu punerea în aplicare a prezentului regulament și supraveghează respectarea de către organizația sa a obligațiilor legate de cadru.

(6) După caz și fără a aduce atingere responsabilității sale pentru punerea în aplicare a prezentului regulament, cel mai înalt nivel de conducere al fiecărei entități a Uniunii poate delega obligații specifice în temeiul prezentului regulament personalului cu funcții superioare de conducere în sensul articolului 29 alineatul (2) din Statutul funcționarilor sau altor funcționari de nivel echivalent, din entitatea Uniunii în cauză. Indiferent de astfel de delegări, cel mai înalt nivel de conducere poate fi tras la răspundere pentru încălcarea prezentului regulament de către entitatea Uniunii în cauză.

(7) 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. La stabilirea acestui procent se ține seama în mod corespunzător de cadru.

(8) 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. Responsabilul local cu securitatea cibernetică facilitează punerea în aplicare a prezentului regulament și raportează periodic în mod direct celui mai înalt nivel de conducere cu privire la stadiul punerii în aplicare. Fără a aduce atingere faptului că responsabilul local cu securitatea cibernetică este punctul unic de contact în fiecare entitate a Uniunii, o entitate a Uniunii poate delega CERT-UE anumite sarcini ale responsabilului local cu securitatea cibernetică în ceea ce privește punerea în aplicare a prezentului regulament, pe baza unui acord privind nivelul serviciilor încheiat între entitatea Uniunii respectivă și CERT-UE, sau sarcinile respective pot fi partajate de mai multe entități ale Uniunii. În cazul în care aceste sarcini sunt delegate CERT-UE, Consiliul interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10 decide dacă furnizarea serviciului respectiv urmează să facă parte dintre serviciile de referință ale CERT-UE, ținând seama de resursele umane și financiare ale entității Uniunii în cauză. Fiecare entitate a Uniunii comunică CERT-UE, fără întârzieri nejustificate, responsabilii locali cu securitatea cibernetică numiți și orice modificare ulterioară a numirilor.

CERT-UE întocmește și menține actualizată o listă a responsabililor locali cu securitatea cibernetică numiți.

(9) Personalul cu funcții superioare de conducere în sensul articolului 29 alineatul (2) din Statutul funcționarilor sau alți funcționari de nivel echivalent din fiecare entitate a Uniunii, precum și toți membrii relevanți ai personalului însărcinați cu punerea în aplicare a măsurilor de gestionare a riscurilor de securitate cibernetică și cu îndeplinirea obligațiilor prevăzute în prezentul regulament urmează periodic cursuri de formare specifice în vederea dobândirii unor cunoștințe și competențe suficiente pentru a înțelege și a evalua riscul în materie de securitate cibernetică și practicile de gestionare a securității cibernetice, precum și impactul acestora asupra operațiunilor entității Uniunii.

Articolul 7

Evaluări ale maturității în materie de securitate cibernetică

(1) Până la 8 iulie 2025 și, ulterior, cel puțin o dată la doi ani, fiecare entitate a Uniunii efectuează o evaluare a maturității în materie de securitate cibernetică încorporând toate elementele mediului său TIC.

(2) Evaluările maturității în materie de securitate cibernetică se efectuează, după caz, cu asistența unei părți terțe specializate.

(3) Entitățile Uniunii cu structuri similare pot coopera la efectuarea evaluărilor maturității în materie de securitate cibernetică pentru entitățile lor respective.

(4) Pe baza unei cereri din partea Consiliului interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10 și cu consimțământul explicit al entității Uniunii în cauză, rezultatele unei evaluări a maturității în materie de securitate cibernetică pot fi discutate în Consiliul respectiv sau în grupul informal de responsabili locali cu securitatea cibernetică, cu scopul de a învăța din experiență și de a face schimb de bune practici.

Articolul 8

Măsuri de gestionare a riscurilor de securitate cibernetică

(1) Fără întârzieri nejustificate și, în orice caz, până la 8 septembrie 2025, fiecare entitate a Uniunii, sub supravegherea celui mai înalt nivel de conducere, ia măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile de securitate cibernetică identificate în temeiul cadrului și pentru a preveni sau a reduce la minimum impactul incidentelor. Ținând seama de stadiul actual al tehnologiei și, după caz, de standardele europene și internaționale relevante, măsurile respective asigură un nivel de securitate a rețelelor și a sistemelor informatice în întregul mediu TIC proporțional cu riscurile de securitate cibernetică existente. Atunci când se evaluează proporționalitatea măsurilor respective, se ține seama în mod corespunzător de gradul de expunere a entității Uniunii la riscuri de securitate cibernetică, de dimensiunea sa, de probabilitatea producerii unor incidente și de gravitatea acestora, inclusiv de impactul lor societal, economic și interinstituțional.

(2) Entitățile Uniunii abordează 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 6 și la alineatul (3) de la prezentul articol;

(b) politicile privind analiza riscurilor de securitate cibernetică și securitatea sistemelor informatice;

(c) obiectivele de politică privind utilizarea serviciilor de cloud computing;

(d) auditul de securitate cibernetică, după caz, care poate include o evaluare a riscurilor de securitate cibernetică, a vulnerabilității și a amenințărilor cibernetice, precum și teste de penetrare efectuate periodic de un furnizor privat de încredere;

(e) punerea în aplicare a recomandărilor rezultate în urma auditurilor de securitate cibernetică menționate la litera (d) prin intermediul actualizărilor securității cibernetice și ale politicilor;

(f) organizarea securității cibernetice, inclusiv stabilirea rolurilor și a responsabilităților;

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

(h) securitatea resurselor umane și controlul accesului;

(i) securitatea operațiunilor;

(j) securitatea comunicațiilor;

(k) achiziționarea, dezvoltarea și întreținerea de sisteme, inclusiv politicile privind gestionarea și divulgarea vulnerabilităților;

(l) acolo unde este posibil, politicile privind transparența codului-sursă;

(m) securitatea lanțului de aprovizionare, inclusiv aspectele legate de securitate referitoare la relațiile dintre fiecare entitate a Uniunii și furnizorii sau prestatorii de servicii direcți ai acesteia;

(n) gestionarea incidentelor și cooperarea cu CERT-UE, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate;

(o) gestionarea continuității activității, de exemplu gestionarea copiilor de rezervă și recuperarea în caz de dezastru, precum și gestionarea crizelor; precum și

(p) promovarea și dezvoltarea unor programe de educație, competențe, sensibilizare, exerciții și formare în materie de securitate cibernetică.

În sensul primului paragraf litera (m), entitățile Uniunii iau în considerare vulnerabilitățile specifice fiecărui furnizor și prestator de servicii direct, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale furnizorilor și prestatorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare.

(3) Entitățile Uniunii iau cel puțin următoarele măsuri specifice de gestionare a riscurilor de securitate cibernetică:

(a) măsuri tehnice pentru a permite și a susține telemunca;

(b) măsuri concrete pentru trecerea la principiile de încredere zero;

(c) utilizarea autentificării multifactor ca normă pentru toate rețelele și sistemele informatice;

(d) utilizarea criptografiei și a criptării, în special a criptării de la un capăt la altul, precum și a semnăturilor digitale securizate;

(e) după caz, comunicații securizate de voce, video și text, precum și sisteme securizate de comunicații de urgență în entitatea Uniunii;

(f) măsuri proactive pentru detectarea și eliminarea programelor malware și spyware;

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

(h) 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 pentru membrii personalului entității Uniunii însărcinați cu asigurarea punerii în aplicare eficace a prezentului regulament;

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

(j) după caz, participarea la analizele de risc privind interconectivitatea între entitățile Uniunii;

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

(i) eliminarea barierelor contractuale care limitează partajarea informațiilor de către furnizorii de servicii TIC cu CERT-UE despre incidente, vulnerabilități și amenințări cibernetice;

(ii) obligațiile contractuale de a raporta incidentele, vulnerabilitățile și amenințările cibernetice, precum și de a institui mecanisme adecvate de răspuns la incidente și de monitorizare a acestora.

Articolul 9

Planuri de securitate cibernetică

(1) În urma încheierii evaluării maturității în materie de securitate cibernetică efectuate în temeiul articolului 7 și ținând seama de activele și riscurile de securitate cibernetică identificate în cadru, precum și de măsurile de gestionare a riscurilor de securitate cibernetică luate în temeiul articolului 8, cel mai înalt nivel de conducere al fiecărei entități a Uniunii aprobă un plan de securitate cibernetică fără întârzieri nejustificate și, în orice caz, până la 8 ianuarie 2026. Planul de securitate cibernetică vizează creșterea gradului de securitate cibernetică în ansamblu a entității Uniunii și contribuie, astfel, la îmbunătățirea unui nivel comun ridicat de securitate cibernetică în entitățile Uniunii. Planul de securitate cibernetică include cel puțin măsurile de gestionare a riscurilor de securitate cibernetică luate în temeiul articolului 8. Planul de securitate cibernetică se revizuiește o dată la doi ani, sau mai des dacă este necesar, în urma evaluărilor maturității în materie de securitate cibernetică efectuate în temeiul articolului 7 sau a oricărei revizuiri substanțiale a cadrului.

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

(3) Entitatea Uniunii transmite planul de securitate cibernetică finalizat Consiliului interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10.

CAPITOLUL III

CONSILIUL INTERINSTITUȚIONAL PENTRU SECURITATE CIBERNETICĂ

Articolul 10

Consiliul interinstituțional pentru securitate cibernetică

(1) Se instituie Consiliul interinstituțional pentru securitate cibernetică (IICB).

(2) IICB este responsabil cu:

(a) monitorizarea și sprijinirea punerii în aplicare a prezentului regulament de către entitățile Uniunii;

(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) un reprezentant desemnat de fiecare dintre următoarele instituții:

(i) Parlamentul European;

(ii) Consiliul European;

(iii) Consiliul Uniunii Europene;

(iv) Comisie;

(v) Curtea de Justiție a Uniunii Europene;

(vi) Banca Centrală Europeană;

(vii) Curtea de Conturi;

(viii) Serviciul European de Acțiune Externă;

(ix) Comitetul Economic și Social European;

(x) Comitetul European al Regiunilor;

(xi) Banca Europeană de Investiții;

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

(xiii) ENISA;

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

(xv) Agenția Uniunii Europene pentru Programul Spațial;

(b) trei reprezentanți desemnați de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta interesele organelor, oficiilor și agențiilor Uniunii care își gestionează propriul mediu TIC, altele decât cele menționate la litera (a).

Entitățile Uniunii reprezentate în IICB urmăresc să asigure echilibrul de gen în rândul reprezentanților desemnați.

(4) Membrii IICB pot fi asistați de un supleant. Alți reprezentanți ai entităților Uniunii menționate la alineatul (3) sau ai altor entități ale Uniunii pot fi invitați de președinte să participe la reuniunile IICB, fără drept de vot.

(5) Șeful CERT-UE și președinții Grupului de cooperare, ai rețelei CSIRT și ai EU-CyCLONe instituite în temeiul articolelor 14, 15 și, respectiv, 16 din Directiva (UE) 2022/2555, sau supleanții acestora pot participa la reuniunile IICB în calitate de observatori. În cazuri excepționale, IICB poate, în conformitate cu regulamentul său intern de procedură să decidă altfel.

(6) IICB își stabilește regulamentul intern de procedură.

(7) IICB numește un președinte din rândul membrilor săi, în conformitate cu regulamentul intern de procedură, pentru o perioadă de trei ani. Supleantul președintelui devine membru titular al IICB pentru aceeași durată.

(8) IICB se reunește de cel puțin trei ori pe an la inițiativa președintelui său, la solicitarea CERT-UE sau la solicitarea oricăruia dintre membrii săi.

(9) 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 IICB votează doar în caz de egalitate de voturi, situație în care poate exprima un vot decisiv.

(10) IICB poate acționa printr-o procedură scrisă simplificată inițiată în conformitate cu regulamentul său 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.

(11) Secretariatul IICB este asigurat de Comisie și răspunde în fața președintelui IICB.

(12) Reprezentantul numit de EUAN informează membrii EUAN cu privire la deciziile adoptate de IICB. Orice membru al EUAN are dreptul să supună atenției acelor reprezentanți și președintelui IICB orice chestiune care, în opinia sa, ar trebui adusă în atenția IICB.

(13) IICB poate înființa 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.

(14) Până la 8 ianuarie 2025 și, ulterior, în fiecare an, IICB prezintă Parlamentului European și Consiliului un raport care detaliază progresele înregistrate în ceea ce privește punerea în aplicare a prezentului regulament și care specifică, în special, gradul de cooperare a CERT-UE cu omologii săi naționali în fiecare dintre statele membre. Raportul reprezintă o contribuție la raportul bienal privind situația în materie de securitate cibernetică în Uniune, adoptat în temeiul articolului 18 din Directiva (UE) 2022/2555.

Articolul 11

Sarcinile IICB

Când își exercită responsabilitățile, IICB, în special:

(a) oferă orientări șefului CERT-UE;

(b) monitorizează și supraveghează efectiv punerea în aplicare a prezentului regulament și sprijină entitățile Uniunii în consolidarea securității lor cibernetice, inclusiv, după caz, solicitând rapoarte ad-hoc din partea entităților Uniunii și a CERT-UE;

(c) în urma unei discuții strategice, adoptă o strategie multianuală privind creșterea nivelului de securitate cibernetică în entitățile Uniunii, o evaluează periodic și, în orice caz, o dată la cinci ani, dacă este necesar, o modifică;

(d) stabilește metodologia și aspectele organizatorice pentru efectuarea evaluărilor inter pares voluntare de către entitățile Uniunii, cu scopul de a învăța din experiențele comune, de a consolida încrederea reciprocă, de a atinge un nivel comun ridicat de securitate cibernetică, precum și de a consolida capacitățile în materie de securitate cibernetică ale entităților Uniunii, asigurându-se că astfel de evaluări inter pares sunt efectuate de experți în materie de securitate cibernetică desemnați de o entitate a Uniunii diferită de entitatea Uniunii care este analizată și că metodologia se bazează pe articolul 19 din Directiva (UE) 2022/2555 și, după caz, este adaptată entităților Uniunii;

(e) aprobă, pe baza unei propuneri din partea șefului CERT-UE, programul anual de lucru al CERT-UE și monitorizează implementarea acestuia;

(f) aprobă, pe baza unei propuneri din partea șefului CERT-UE, catalogul de servicii al CERT-UE și orice actualizări ulterioare ale acestuia;

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

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

(i) examinează și aprobă raportul anual întocmit de șeful CERT-UE, care acoperă activitățile și gestionarea fondurilor de către CERT-UE;

(j) aprobă și monitorizează indicatorii cheie de performanță (KPI) pentru CERT-UE, stabiliți pe baza unei propuneri din partea șefului CERT-UE;

(k) aprobă acordurile de cooperare, acordurile privind nivelul serviciilor sau contractele dintre CERT-UE și alte entități în temeiul articolului 18;

(l) adoptă orientări și recomandări pe baza unei propuneri din partea CERT-UE în conformitate cu articolul 14 și încredințează CERT-UE sarcina să emită, să retragă sau să modifice o propunere de orientări sau recomandări sau un apel la acțiune;

(m) instituie grupuri consultative tehnice cu sarcini specifice pentru a sprijini activitatea IICB, le aprobă mandatul și desemnează președinții acestor grupuri;

(n) primește și evaluează documentele și rapoartele prezentate de entitățile Uniunii în temeiul prezentului regulament, cum ar fi evaluări ale nivelului de maturitate al securității cibernetice;

(o) facilitează instituirea unui grup informal care să reunească responsabilii locali cu securitatea cibernetică ai entităților Uniunii, sprijinit de ENISA, în scopul de a face schimb de bune practici și de informații în legătură cu punerea în aplicare a prezentului regulament;

(p) ținând cont de informațiile privind riscurile identificate în materie de securitate cibernetică și de lecțiile învățate oferite de CERT-UE, monitorizează caracterul adecvat al acordurilor de interconectivitate între mediile TIC ale entităților Uniunii și oferă consiliere cu privire la posibile îmbunătățiri;

(q) stabilește un plan de gestionare a crizelor cibernetice pentru a sprijini, la nivel operațional, gestionarea coordonată a incidentelor majore care afectează entitățile Uniunii și pentru a contribui la schimbul periodic de informații relevante, în special în ceea ce privește impactul, gravitatea și posibilele modalități de atenuare a efectelor incidentelor majore;

(r) coordonează adoptarea planurilor individuale de gestionare a crizelor cibernetice ale entităților Uniunii menționate la articolul 9 alineatul (2);

(s) adoptă recomandări legate de securitatea lanțurilor de aprovizionare menționate la articolul 8 alineatul (2) primul paragraf litera (m), ținând cont de rezultatele evaluărilor coordonate la nivelul Uniunii ale riscurilor lanțurilor de aprovizionare critice menționate la articolul 22 din Directiva (UE) 2022/2555, pentru a sprijini entitățile Uniunii în adoptarea unor măsuri de securitate cibernetică eficace și proporționale de gestionare a riscurilor de securitate cibernetică.

Articolul 12

Respectarea dispozițiilor

(1) În conformitate cu articolul 10 alineatul (2) și cu articolul 11, IICB monitorizează în mod eficace punerea în aplicare de către entitățile Uniunii a prezentului regulament și a orientărilor, a recomandărilor și a apelurilor la acțiune adoptate. IICB poate solicita entităților Uniunii informațiile sau documentele necesare în acest scop. În scopul adoptării unor măsuri de asigurare a conformității în temeiul prezentului articol, atunci când entitatea Uniunii în cauză este reprezentată direct în IICB, aceasta nu are drept de vot.

(2) În cazul în care constată că o entitate a Uniunii nu a pus în aplicare în mod efectiv prezentul regulament sau orientările, recomandările sau apelurile la acțiune emise în temeiul acestuia, IICB poate, fără a aduce atingere procedurilor interne ale entității Uniunii în cauză și după ce îi oferă entității Uniunii în cauză ocazia de a-și prezenta observațiile:

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

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

(c) să emită un avertisment în vederea remedierii deficiențelor identificate într-o perioadă specificată, inclusiv recomandări de modificare a măsurilor adoptate de entitatea Uniunii în cauză în temeiul prezentului regulament;

(d) să emită o notificare motivată către entitatea Uniunii în cauză, în cazul în care deficiențele identificate într-un avertisment emis în temeiul literei (c) nu au fost abordate suficient în termenul specificat;

(e) să emită:

(i) o recomandare de efectuare a unui audit; sau

(ii) o cerere privind efectuarea unui audit de către un serviciu de audit terț;

(f) dacă este cazul, să informeze Curtea de Conturi, în limitele mandatului său, cu privire la presupusa neconformitate;

(g) să emită o recomandare pentru toate statele membre și entitățile Uniunii de a implementa o suspendare temporară a fluxurilor de date către entitatea Uniunii în cauză.

În sensul primului paragraf litera (c), audiența unui avertisment este restricționată în mod corespunzător, dacă este necesar, având în vedere riscul în materie de securitate cibernetică.

Avertismentele și recomandările emise în temeiul primului paragraf se adresează celui mai înalt nivel de conducere al entității Uniunii în cauză.

(3) În cazul în care IICB a adoptat măsuri în temeiul alineatului (2) primul paragraf literele (a)-(g), entitatea Uniunii în cauză oferă detalii ale măsurilor și acțiunilor întreprinse pentru a remedia presupusele deficiențe identificate de IICB. Entitatea Uniunii transmite aceste detalii într-un termen rezonabil care urmează să fie convenit cu IICB.

(4) În cazul în care consideră că există o încălcare persistentă a dispozițiilor prezentului regulament de către o entitate a Uniunii, care rezultă direct din acțiunile sau omisiunile unui funcționar sau ale unui alt agent al Uniunii, inclusiv la cel mai înalt nivel de conducere, IICB solicită entității Uniunii în cauză să ia măsurile corespunzătoare, solicitându-i inclusiv să adopte măsuri de natură disciplinară, în conformitate cu normele și procedurile prevăzute în Statutul funcționarilor Uniunii Europene și cu orice altă norme și proceduri aplicabile. În acest scop, IICB transferă informațiile necesare către entitatea Uniunii în cauză.

(5) În cazul în care entitățile Uniunii notifică faptul că nu sunt în măsură să respecte termenele-limită stabilite la articolul 6 alineatul (1) și la articolul 8 alineatul (1), IICB poate, în cazuri justificate în mod corespunzător, ținând cont de dimensiunea entității Uniunii, să autorizeze prelungirea acestor termene-limită.

CAPITOLUL IV

CERT-UE

Articolul 13

Misiunea și sarcinile CERT-UE

(1) Misiunea CERT-UE este de a contribui la securitatea mediului TIC neclasificat al entităților Uniunii, oferindu-le consiliere cu privire la securitatea cibernetică, oferindu-le asistență pentru prevenirea, detectarea, gestionarea și atenuarea incidentelor, răspunsul la acestea și redresarea în urma lor și acționând ca centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.

(2) CERT-UE colectează, gestionează, analizează și face schimb de informații cu entitățile Uniunii cu privire la amenințări cibernetice, vulnerabilități și incidente legate de infrastructura TIC neclasificată. Acesta coordonează răspunsurile la incidente la nivel interinstituțional și la nivelul entităților Uniunii, inclusiv prin furnizarea de asistență operațională specializată sau prin coordonarea acesteia.

(3) CERT-UE îndeplinește următoarele sarcini pentru a asista entitățile Uniunii:

(a) le oferă sprijin la punerea în aplicare a prezentului regulament și contribuie la coordonarea punerii în aplicare a prezentului regulament prin intermediul măsurilor enumerate la articolul 14 alineatul (1) sau al rapoartelor ad-hoc solicitate de IICB;

(b) oferă servicii CSIRT standard pentru entitățile Uniunii printr-un pachet de servicii de securitate cibernetică descrise în catalogul său de servicii (servicii de referință);

(c) menține o rețea de omologi și parteneri pentru a sprijini serviciile, astfel cum se prevede la articolele 17 și 18;

(d) aduce în atenția IICB orice problemă legată de punerea în aplicare a prezentului regulament și a orientărilor, recomandărilor și apelurilor la acțiune;

(e) pe baza informațiilor menționate la alineatul (2), contribuie la conștientizarea situației amenințărilor la adresa securității cibernetice în Uniune în strânsă cooperare cu ENISA;

(f) coordonează gestionarea incidentelor majore;

(g) îndeplinește pentru entitățile Uniunii un rol echivalent celui de coordonator desemnat în scopul divulgării coordonate a vulnerabilităților în temeiul articolului 12 alineatul (1) din Directiva (UE) 2022/2555;

(h) furnizează, la cererea unei entități a Uniunii, scanarea proactivă și neintruzivă a rețelelor și a sistemelor informatice accesibile publicului respectivei entități a Uniunii.

Informațiile menționate la primul paragraf litera (e) se comunică IICB, rețelei CSIRT și Centrului de situații și de analiză a informațiilor al Uniunii Europene (INTCEN UE), dacă este cazul și în funcție de situație și sub rezerva unor condiții de confidențialitate adecvate.

(4) CERT-UE poate, în conformitate cu articolul 17 sau 18, după caz, să coopereze cu comunitățile relevante în materie de securitate cibernetică din Uniune și din statele sale membre, 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 privind rețeaua CSIRT, inclusiv în ceea ce privește asistența reciprocă;

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

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

(5) În limitele competențelor sale, 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.

(6) CERT-UE poate furniza 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 (3), în temeiul unor acorduri privind nivelul serviciilor și sub rezerva resurselor disponibile, în special monitorizarea rețelelor cu spectru larg, inclusiv monitorizarea non-stop din prima linie pentru amenințările cibernetice grave;

(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) la cerere, o scanare proactivă a rețelei și a sistemelor informatice ale entității Uniunii în cauză pentru a detecta vulnerabilitățile cu un impact potențial semnificativ;

(d) servicii care sprijină securitatea mediului TIC furnizat 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, pe baza unor acorduri scrise și cu aprobarea prealabilă a IICB.

În ceea ce privește primul alineat litera (d), CERT-EU poate, cu titlu excepțional, să încheie acorduri privind nivelul serviciilor cu alte entități decât entitățile Uniunii, cu aprobarea prealabilă a IICB.

(7) CERT-UE organizează și poate participa la exerciții de securitate cibernetică sau poate recomanda participarea la exercițiile existente, dacă este cazul în strânsă cooperare cu ENISA, pentru a testa nivelul de securitate cibernetică al entităților Uniunii.

(8) CERT-UE poate oferi entităților Uniunii asistență privind incidentele din rețele și din sistemele de informații care procesează IUEC dacă entitățile Uniunii în cauză îi solicită acest lucru în mod expres în conformitate cu procedurile lor respective. Furnizarea de asistență din partea CERT-UE în temeiul prezentului alineat nu aduce atingere normelor aplicabile privind protecția informațiilor clasificate.

(9) CERT-UE informează entitățile Uniunii cu privire la procedurile și procesele sale de gestionare a incidentelor.

(10) CERT-UE contribuie, cu un nivel ridicat de confidențialitate și fiabilitate, prin intermediul mecanismelor de cooperare și al liniilor de raportare adecvate, cu informații relevante și anonimizate cu privire la incidentele majore și la modul în care acestea au fost gestionate. Informațiile respective sunt incluse în raportul menționat la articolul 10 alineatul (14).

(11) CERT-EU, în cooperare cu AEPD, sprijină entitățile Uniunii în cauză atunci când abordează incidente care duc la încălcarea securității datelor cu caracter personal, fără a aduce atingere competenței și sarcinilor AEPD în calitate de autoritate de supraveghere în temeiul Regulamentului (UE) 2018/1725.

(12) La solicitarea explicită a departamentelor tematice ale entităților Uniunii, CERT-UE poate oferi consultanță sau sprijin tehnic cu privire la aspecte de politică relevante.

Articolul 14

Orientări, 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 orientări, 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 ale Uniunii.

În ceea ce privește primul paragraf litera (a), entitatea Uniunii în cauză informează CERT-UE, fără întârzieri nejustificate după primirea apelului la acțiune, cu privire la modul în care au fost aplicate măsurile de securitate urgente.

(2) Orientările și recomandările pot include:

(a) metodologii comune și un model pentru evaluarea maturității în materie de securitate cibernetică a entităților Uniunii, inclusiv baremele sau indicatorii-cheie de performanță corespunzători, care să servească drept referință în sprijinul îmbunătățirii continue a securității cibernetice în toate entitățile Uniunii și să faciliteze stabilirea priorităților în domeniile și măsurile de securitate cibernetică, ținând cont de poziția entităților în materie de securitate cibernetică;

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

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

(d) după caz, utilizarea tehnologiei și a arhitecturii comune, din sursă deschisă, precum și a bunelor practici asociate în scopul realizării interoperabilității și a standardelor comune, inclusiv o abordare coordonată privind securitatea lanțului de aprovizionare;

(e) după caz, informații pentru a facilita utilizarea instrumentelor de achiziții publice comune pentru achiziționarea de servicii și produse de securitate cibernetică relevante de la furnizori terți;

(f) acorduri privind schimbul de informații în temeiul articolului 20.

Articolul 15

Șeful CERT-UE

(1) După obținerea aprobării cu o majoritate de două treimi din membrii IICB, Comisia numește șeful CERT-UE. IICB este consultat în toate etapele procedurii de numire, în special în ceea ce privește elaborarea anunțurilor privind posturile vacante, examinarea dosarelor de candidatură și desemnarea comitetelor de selecție pentru acest post. Procedura de selecție, inclusiv lista scurtă finală a candidaților de pe care urmează să fie selectat șeful CERT-UE, asigură o reprezentare echitabilă a fiecărui gen, ținând cont de candidaturile depuse.

(2) Șeful CERT-UE este responsabil pentru buna funcționare a CERT-UE și acționează în limitele competențelor sale și sub conducerea IICB. Șeful CERT-UE raportează în mod regulat președintelui IICB și prezintă rapoarte ad-hoc IICB, la solicitarea acestuia.

(3) Șeful CERT-UE acordă ordonatorului de credite delegat responsabil asistență la întocmirea raportului de activitate anual, care conține informații financiare și de gestiune, inclusiv rezultatele controalelor, redactate în conformitate cu articolul 74 alineatul (9) din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului ([9]), și îi raportează periodic acestuia cu privire la punerea în aplicare a măsurilor pentru care i-au fost subdelegate competențe șefului CERT-UE.

(4) Șeful CERT-UE elaborează anual o planificare financiară a veniturilor și cheltuielilor administrative pentru activitățile sale, o propunere de program de lucru anual, o propunere de catalog de servicii al CERT-UE, o propunere de revizuire a catalogului de servicii, o propunere de modalități pentru acordurile privind nivelul serviciilor și o propunere de indicatori-cheie de performanță pentru CERT-UE, care urmează să fie aprobate de IICB în conformitate cu articolul 11. Atunci când revizuiește lista serviciilor din catalogul de servicii al CERT-UE, șeful CERT-UE ține cont de resursele alocate CERT-UE.

(5) Șeful CERT-UE prezintă IICB și președintelui IICB rapoarte cel puțin o dată pe an cu privire la activitățile și performanțele CERT-UE în perioada de referință, inclusiv cu privire la execuția bugetului, la acordurile privind nivelul serviciilor și la acordurile scrise încheiate, la cooperarea cu omologii și partenerii și la misiunile efectuate de personal, inclusiv rapoartele menționate la articolul 11. Aceste rapoarte includ un program de lucru pentru perioada următoare, planificarea financiară a veniturilor și cheltuielilor, inclusiv personalul, actualizările planificate ale catalogului de servicii al CERT-UE și o evaluare a impactului preconizat pe care astfel de actualizări îl pot avea în ceea ce privește resursele financiare și umane.

Articolul 16

Aspecte financiare și de personal

(1) CERT-UE este integrat în structura administrativă a unei direcții generale a Comisiei pentru a beneficia de structurile de sprijin administrativ, financiar și contabil ale Comisiei, menținându-și în același timp statutul de furnizor interinstituțional autonom de servicii pentru toate entitățile Uniunii. Comisia informează IICB cu privire la amplasarea administrativă a CERT-UE și la eventuale modificări ale acesteia. Comisia revizuiește acordurile administrative referitoare la CERT-UE în mod regulat și, în orice caz, înainte de instituirea oricărui cadru financiar multianual în temeiul articolului 312 din TFUE, pentru a permite luarea de măsuri adecvate. Revizuirea include posibilitatea de a institui CERT-UE ca oficiu al Uniunii.

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

([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 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).

(3) Sarcinile și activitățile CERT-UE, inclusiv serviciile furnizate de CERT-UE în temeiul articolului 13 alineatele (3), (4), (5) și (7) și al articolului 14 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 se bazează pe orientările oferite de IICB și convenite între fiecare entitate a Uniunii 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) din prezentul articol, ca venituri alocate interne, astfel cum se prevede la articolul 21 alineatul (3) litera (c) din Regulamentul (UE, Euratom) 2018/1046.

(5) Costurile aferente serviciilor furnizate la articolul 13 alineatul (6) se recuperează de la entitățile Uniunii beneficiare ale serviciilor furnizate de CERT-UE. Veniturile sunt alocate liniilor bugetare prin care se suportă costurile.

Articolul 17

Cooperarea CERT-UE cu omologii din statele membre

(1) CERT-UE, fără întârzieri nejustificate, cooperează și face schimb de informații cu omologii naționali din statele membre, in special CSIRT desemnate sau stabilite în conformitate cu articolul 10 din Directiva (UE) 2022/2555, sau, după caz, autoritățile competente și punctele unice de contact menționate la articolul 8 din directiva respectivă, cu privire la incidente, amenințări cibernetice, vulnerabilități, incidente evitate la limită, la posibile 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 stabilit în conformitate cu articolul 16 din Directiva (UE) 2022/2555 în ceea ce privește gestionarea coordonată a incidentelor și crizelor de securitate cibernetică de mare amploare.

(2) În cazul în care CERT-UE ia cunoștință de incidente semnificative care au loc pe teritoriul unui stat membru, acesta notifică fără întârziere omologilor relevanți din statul membru respectiv în conformitate cu alineatul (1).

(3) Cu condiția ca datele cu caracter personal să fie protejate în conformitate cu dreptul aplicabil al Uniunii privind protecția datelor, CERT-UE face schimb de informații relevante, fără întârzieri nejustificate, referitoare la incident cu omologii din statele membre pentru a facilita detectarea amenințărilor sau incidentelor cibernetice similare sau pentru a contribui la analiza unui incident, fără autorizarea entității Uniunii afectate. CERT-UE face schimb de informații referitoare la incidente care dezvăluie identitatea țintei incidentului numai în unul din următoarele cazuri:

(a) entitatea Uniunii afectată își dă consimțământul;

(b) entitatea Uniunii nu își dă consimțământul, astfel cum se prevede la litera (a), dar publicarea identității entității Uniunii afectate ar crește probabilitatea ca incidentele din altă parte să fie evitate sau atenuate;

(c) entitatea Uniunii afectată a făcut deja public faptul că a fost afectată.

Deciziile de a face schimb de informații specifice incidentului care dezvăluie identitatea țintei incidentului în temeiul primului paragraf litera (b) sunt aprobate de șeful CERT-UE. Înainte de a emite o astfel de decizie, CERT-UE contactează în scris entitatea Uniunii afectată, explicând în mod clar modul în care divulgarea identității sale ar contribui la evitarea sau atenuarea incidentelor în altă parte. Șeful CERT-UE furnizează explicația și solicită în mod explicit entității Uniunii să precizeze dacă își dă consimțământul într-un termen stabilit. Șeful CERT-UE informează, de asemenea, entitatea Uniunii că, având în vedere explicația oferită, își rezervă dreptul de a divulga informațiile chiar și în absența consimțământului. Entitatea Uniunii afectată este informată înainte de divulgarea informațiilor.

Articolul 18

Cooperarea CERT-UE cu alți omologi

(1) CERT-UE poate coopera cu omologi din Uniune alții decât cei menționați la articolul 17, care fac obiectul cerințelor privind securitatea cibernetică, 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 tip de cooperare cu astfel de omologi, CERT-UE solicită aprobarea prealabilă a IICB, de la caz la caz. În cazul în care CERT-UE stabilește o cooperare cu astfel de omologi, informează orice omologi relevanți din statele membre menționați la articolul 17 alineatul (1), în statul membru în care este situat omologul. Dacă este aplicabil și adecvat, o astfel de cooperare și condițiile aferente, inclusiv în ceea ce privește securitatea cibernetică, protecția datelor și gestionarea informațiilor, se stabilesc în acorduri de confidențialitate specifice, cum ar fi contractele sau acordurile administrative. Acordurile de confidențialitate nu necesită aprobarea prealabilă a IICB, însă trebuie să fie informat președintele IICB. În cazul unei nevoi urgente și iminente de a face schimb de informații în materie de securitate cibernetică în interesul entităților Uniunii sau al unei alte părți, CERT-UE poate face acest lucru cu o entitate a cărei competență, capacitate și expertiză specifice sunt necesare în mod justificat pentru a sprijini o astfel de nevoie urgentă și iminentă, chiar dacă CERT-UE nu a încheiat un acord de confidențialitate cu entitatea respectivă. În astfel de cazuri, CERT-UE informează imediat președintele IICB și raportează IICB prin intermediul unor rapoarte sau reuniuni periodice.

(2) CERT-UE poate coopera cu 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 extinsă cu astfel de parteneri, CERT-UE solicită aprobarea prealabilă a IICB, de la caz la caz.

(3) CERT-UE poate, cu acordul entității Uniunii afectate de un incident și cu condiția să existe un acord sau un contract de nedivulgare cu omologul sau partenerul relevant, să furnizeze informații referitoare la incidentul specific omologilor sau partenerilor menționați la alineatele (1) și (2) exclusiv în scopul de a contribui la analiza acestuia.

CAPITOLUL V

OBLIGAȚII DE COOPERARE ȘI DE RAPORTARE

Articolul 19

Gestionarea informațiilor

(1) Entitățile Uniunii și CERT-UE respectă obligația de a nu divulga informații care constituie secret profesional, în conformitate cu articolul 339 din TFUE sau cu cadrele echivalente aplicabile.

(2) Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului ([10]) 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 entități ale Uniunii sau, după caz, statele membre, ori de câte ori o cerere se referă la documentele lor.

(3) Entitățile Uniunii și CERT-UE gestionează informațiile în conformitate cu normele aplicabile privind securitatea informațiilor.

([10]) 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).

Articolul 20

Acorduri privind schimbul de informații în materie de securitate cibernetică

(1) Entitățile Uniunii pot, în mod voluntar, să aducă la cunoștința CERT-UE și să-i furnizeze informații privind incidentele, amenințările cibernetice, incidentele evitate la limită și vulnerabilitățile care le afectează. CERT-UE se asigură că sunt disponibile mijloace eficiente de comunicare, cu un nivel ridicat de trasabilitate, confidențialitate și fiabilitate, 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. Fără a aduce atingere articolului 12, notificarea voluntară nu impune entității Uniunii care transmite informația nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.

(2) Pentru a-și îndeplini misiunea și sarcinile încredințate în conformitate cu articolul 13, CERT-UE poate solicita entităților 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 Uniunii care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.

(3) CERT-UE poate face schimb de informații referitoare la incidente cu entitățile Uniunii care dezvăluie identitatea entității Uniunii afectate de incident, cu condiția ca entitatea respectivă a Uniunii să-și fi dat acordul. În cazul în care o entitate a Uniunii nu își dă consimțământul, aceasta furnizează CERT-UE motivele care justifică decizia respectivă.

(4) Entitățile Uniunii fac schimb, la cerere, de informații cu Parlamentul European și cu Consiliul cu privire la finalizarea planurilor de securitate cibernetică.

(5) IICB sau CERT-UE, după caz, fac schimb, la cerere, de orientări, recomandări și apeluri la acțiune cu Parlamentul European și cu Consiliul.

(6) Obligațiile de partajare prevăzute la prezentul articol nu se aplică:

(a) IUEC;

(b) informațiilor a căror distribuție ulterioară a fost exclusă prin intermediul unui marcaj vizibil, cu excepția cazului în care schimbul acestora cu CERT-UE a fost permis în mod explicit.

Articolul 21

Obligații de raportare

(1) Un incident este considerat a fi semnificativ dacă:

(a) a cauzat sau poate cauza perturbări operaționale grave în funcționarea entității Uniunii sau pierderi financiare pentru entitatea Uniunii în cauză;

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

(2) 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 în mai multe entități sau transfrontalier;

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

(c) la cererea CERT-UE, un raport intermediar privind actualizări relevante ale situației;

(d) un raport final, în termen de cel mult o lună de la transmiterea notificării cu privire la incident în temeiul literei (b), care să includă următoarele elemente:

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

(ii) tipul de amenințare sau de cauză principală care probabil a declanșat incidentul;

(iii) măsurile de atenuare aplicate și în curs;

(iv) după caz, impactul transfrontalier sau inter-entități al incidentului;

(e) în cazul unui incident în desfășurare la momentul prezentării raportului final menționat la litera (d), un raport privind progresele înregistrate și un raport final în termen de o lună de la gestionarea incidentului.

(3) O entitate a Uniunii informează, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care a luat cunoștință de un incident semnificativ, omologii relevanți din statele membre menționați la articolul 17 alineatul (1) din statul membru în care se află că s-a produs un incident semnificativ.

(4) Entitățile Uniunii notifică, printre altele, toate informațiile care permit CERT-UE să stabilească orice impact inter-entități, orice impact asupra statului membru gazdă sau orice impact transfrontalier în urma unui incident semnificativ. Fără a aduce atingere articolului 12, simpla notificare nu expune entitatea Uniunii la o răspundere sporită.

(5) După caz, entitățile Uniunii comunică, 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 și după caz, trebuie să ia măsuri de atenuare, orice măsuri sau măsuri corective pe care le pot lua ca răspuns la incidentul respectiv sau amenințarea respectivă. După caz, entitățile Uniunii informează utilizatorii respectivi despre amenințarea cibernetică semnificativă.

(6) 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 emite o alertă privind o amenințare cibernetică relevantă.

(7) 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 furniza detalii suplimentare privind tipurile de informații de care are nevoie pentru o cunoaștere detaliată a situației și pentru răspunsul la incidente.

(8) CERT-UE transmite IICB, ENISA, INTCEN UE și rețelei CSIRT, o dată la trei luni, un raport de sinteză care include date anonimizate și agregate privind incidentele semnificative, incidentele, amenințările cibernetice, incidentele evitate la limită și vulnerabilitățile în temeiul articolului 20 și incidentele semnificative notificate în temeiul alineatului (2) din prezentul articol. Raportul de sinteză reprezintă o contribuție la raportul bienal privind situația în materie de securitate cibernetică în Uniune, adoptat în temeiul articolului 18 din Directiva (UE) 2022/2555.

(9) Până la 8 iulie 2024, IICB emite orientări sau recomandări care aduc precizări suplimentare privind modalitățile și formatul și conținutul raportării în conformitate cu prezentul articol. Atunci când elaborează astfel de orientări sau recomandări, IICB ține seama de orice acte de punere în aplicare adoptate în temeiul articolului 23 alineatul (11) din Directiva (UE) 2022/2555 care precizează tipul de informații, formatul și procedura de notificare. CERT-UE difuzează detaliile tehnice adecvate pentru a permite detectarea proactivă, răspunsul la incidente sau adoptarea unor măsuri de atenuare de către entitățile Uniunii.

(10) Obligațiile de raportare prevăzute la prezentul articol nu se aplică:

(a) IUEC;

(b) informațiilor a căror distribuție ulterioară a fost exclusă prin intermediul unui marcaj vizibil, cu excepția cazului în care schimbul acestora cu CERT-UE a fost permis în mod explicit.

Articolul 22

Coordonarea răspunsului la incidente și cooperarea

(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 incidente, amenințările cibernetice, vulnerabilități și incidente evitate la limită, între:

(a) entitățile Uniunii;

(b) omologii menționați la articolele 17 și 18.

(2) CERT-UE, după caz în strânsă cooperare cu ENISA, facilitează coordonarea între entitățile Uniunii în ceea ce privește răspunsul la incidente, inclusiv prin:

(a) contribuția la o comunicare externă coerentă;

(b) sprijin reciproc, cum ar fi schimbul de informații relevante pentru entitățile Uniunii sau furnizarea de asistență, după caz, direct la fața locului;

(c) utilizarea optimă a resurselor operaționale;

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

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

(4) Până la 8 ianuarie 2025, pe baza unei propuneri din partea CERT-UE, IICB adoptă orientări sau recomandări 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, fără întârzieri nejustificate.

(5) În urma unei cereri specifice din partea unui stat membru și cu aprobarea entităților Uniunii în cauză, CERT-UE poate apela la experți de pe lista menționată la articolul 23 alineatul (4) pentru a contribui la răspunsul la un incident major care are un impact în statul membru respectiv sau la un incident de securitate cibernetică de mare amploare în conformitate cu articolul 15 alineatul (3) litera (g) din Directiva (UE) 2022/2555. Normele specifice privind accesul și folosirea experților tehnici din entitățile Uniunii sunt aprobate de IICB pe baza unei propuneri a CERT-UE.

Articolul 23

Gestionarea incidentelor majore

(1) Pentru a sprijini la nivel operațional gestionarea coordonată a incidentelor majore care afectează entitățile Uniunii și pentru a contribui la schimbul periodic de informații relevante între entitățile Uniunii și cu statele membre, IICB, în conformitate cu articolul 11 litera (q), stabilește un plan de gestionare a crizelor cibernetice pe baza activităților menționate la articolul 22 alineatul (2), în strânsă cooperare cu CERT-UE și ENISA. Planul de gestionare a crizelor cibernetice include cel puțin următoarele elemente:

(a) modalități cu privire la coordonarea și fluxul de informații între entitățile Uniunii pentru gestionarea incidentelor majore la nivel operațional;

(b) proceduri standard de operare (PSO) comune;

(c) o taxonomie comună a gravității incidentelor majore și a punctelor de declanșare a crizelor;

(d) exerciții periodice;

(e) canale de comunicare securizate care urmează să fie utilizate.

(2) Reprezentantul Comisiei în cadrul IICB, sub rezerva planului de gestionare a crizelor cibernetice instituit în temeiul alineatului (1) de la prezentul articol și fără a aduce atingere articolului 16 alineatul (2) primul paragraf din Directiva (UE) 2022/2555, este punctul de contact pentru schimbul de informații relevante în legătură cu incidentele majore cu EU-CyCLONe.

(3) CERT-UE coordonează, la nivelul entităților Uniunii, gestionarea incidentelor majore. CERT-UE menține un inventar al expertizei tehnice disponibile necesare pentru răspunsul la incidente în cazul unor incidente majore și sprijină IICB în coordonarea planurilor de gestionare a crizelor cibernetice ale entităților Uniunii pentru incidentele majore menționate la articolul 9 alineatul (2).

(4) 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.

CAPITOLUL VI

DISPOZIȚII FINALE

Articolul 24

Realocare bugetară inițială

Pentru a asigura funcționarea corectă și stabilă a CERT-UE, Comisia poate propune realocarea personalului și a resurselor financiare către bugetul Comisiei, pentru a fi utilizate în operațiunile CERT-UE. Realocarea produce efecte în același timp cu primul buget anual al Comisiei adoptat după intrarea în vigoare a prezentului regulament.

Articolul 25

Revizuire

(1) Până la 8 ianuarie 2025 și, ulterior, anual, IICB, cu sprijinul CERT-EU, prezintă un raport Comisiei cu privire la punerea în aplicare a prezentului regulament. IICB poate să facă recomandări Comisiei pentru a revizui prezentul regulament.

(2) Până la 8 ianuarie 2027 și, ulterior, o dată la doi ani, Comisia evaluează punerea în aplicare a prezentului regulament și experiența dobândită la nivel strategic și operațional și prezintă un raport Parlamentului European și Consiliului cu privire la aceasta.

Raportul menționat la primul paragraf de la prezentul alineat include revizuirea menționată la articolul 16 alineatul (1) privind posibilitatea instituirii CERT-UE ca oficiu al Uniunii.

(3) Până la 8 ianuarie 2029, Comisia evaluează funcționarea prezentului regulament și prezintă un raport Parlamentului European, Consiliului, Comitetului Economic și Social European și Comitetului Regiunilor. Comisia evaluează, de asemenea, oportunitatea includerii rețelelor și a sistemelor informatice care gestionează IUEC în domeniul de aplicare al prezentului regulament, ținând seama de alte acte legislative ale Uniunii aplicabile sistemelor respective. Raportul este însoțit, după caz, de o propunere legislativă.

Articolul 26

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 Strasbourg, 13 decembrie 2023.

Pentru Parlamentul European
Președinta
R. METSOLA

Pentru Consiliu
Președintele
P. NAVARRO RÍOS