Parlamentul European
2019-2024

Comisia pentru afaceri constituționale

2022/0085(COD)

31.1.2023

AVIZ

al Comisiei pentru afaceri constituționale

destinat Comisiei pentru industrie, cercetare și energie

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

Raportoare pentru aviz: Markéta Gregorová

PA_Legam

JUSTIFICARE SUCCINTĂ

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

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

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

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

AMENDAMENTELE

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

Amendamentul 1

Propunere de regulament
Considerentul 1

Textul propus de Comisie	*Amendamentul*
(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații transparente, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale	(1) În era digitală, tehnologia informației și comunicațiilor este o piatră de temelie a unei administrații transparente, eficiente și independente a Uniunii. Evoluția tehnologiei și creșterea gradului de complexitate și de interconectare a sistemelor digitale

amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și proteja datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.	amplifică riscurile de securitate cibernetică, făcând administrația Uniunii mai vulnerabilă la amenințările și incidentele cibernetice, care reprezintă, în cele din urmă, amenințări la adresa continuității activității administrației și a capacității acesteia de a-și proteja datele. Deși utilizarea sporită a serviciilor de tip cloud computing, utilizarea ubicuă a tehnologiei informației ***și comunicațiilor (TIC)***, nivelul ridicat de digitalizare, munca la distanță și evoluția tehnologiei și a conectivității sunt, în prezent, caracteristici esențiale ale tuturor activităților entităților administrative ale Uniunii, reziliența digitală nu este încă suficient integrată.

Justificare

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

Amendamentul 2

Propunere de regulament
Considerentul 2

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

și exploatând rapid vulnerabilitățile.

Amendamentul 3

Propunere de regulament
Considerentul 3

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

Amendamentul 4
Propunere de regulament
Considerentul 4

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

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

instituțiile, organele***, oficiile*** și agențiile Uniunii să atingă un nivel comun ridicat de securitate cibernetică printr-un „nivel de referință în materie de securitate cibernetică” (un set de norme ***comune*** minime în materie de securitate cibernetică pe care rețelele și sistemele informatice, precum și operatorii și utilizatorii acestora trebuie să le respecte pentru a ***limita*** riscurile de securitate cibernetică), ***printr-un schimb*** de informații și ***o colaborare periodică și eficace*** în acest domeniu***, precum și prin formarea în materie de securitate cibernetică***.

Amendamentul 5

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) Diferențele dintre instituțiile, organele și agențiile Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică ***nu*** ar trebui să ***includă nicio obligație care să interfereze în mod direct cu*** exercitarea misiunilor instituțiilor, organelor și agențiilor Uniunii ***sau*** să ***aducă atingere autonomiei*** lor ***instituționale***. Astfel, aceste instituții, organe și agenții ***trebuie*** să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică.	(7) Diferențele dintre instituțiile, organele***, oficiile*** și agențiile Uniunii necesită o anumită flexibilitate în ceea ce privește punerea în aplicare, deoarece nu există o abordare universală. Măsurile pentru un nivel comun ridicat de securitate cibernetică ar trebui să ***sprijine*** exercitarea misiunilor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii ***și*** să ***țină seama de autonomia*** lor ***instituțională***. Astfel, aceste instituții, organe***, oficii*** și agenții ***ar trebui*** să își stabilească propriile cadre pentru gestionarea, guvernanța și controlul riscurilor de securitate cibernetică și să adopte propriile planuri de referință și de securitate cibernetică***, ținând seama de coerența și interoperabilitatea cadrelor lor respective și pe baza cadrului comun stabilit de prezentul regulament***.

Amendamentul 6
Propunere de regulament
Considerentul 8

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

Amendamentul 7

Propunere de regulament
Considerentul 9

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

Amendamentul 8

Propunere de regulament
Considerentul 10

Textul propus de Comisie	*Amendamentul*
(10) Instituțiile, organele și agențiile Uniunii ***trebuie*** să evalueze riscurile legate de relațiile cu furnizorii și prestatorii de servicii, inclusiv cu prestatorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate, și să ia măsurile adecvate pentru a combate astfel de riscuri. Aceste măsuri ***trebuie*** să facă parte din nivelul de referință în materie de securitate cibernetică și să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor ***trebuie*** să se țină seama în mod corespunzător de legislația și politicile relevante ale UE, inclusiv de evaluările riscurilor și de recomandările emise de Grupul de cooperare privind securitatea rețelelor și a informațiilor, cum ar fi evaluarea coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G. În plus, ar ***putea fi necesară*** certificarea produselor, a serviciilor și a proceselor TIC relevante, în cadrul sistemelor europene specifice de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.	(10) Instituțiile, organele***, oficiile*** și agențiile Uniunii ***ar trebui*** să evalueze riscurile legate de relațiile cu furnizorii și prestatorii de servicii, inclusiv cu prestatorii de servicii de stocare și prelucrare a datelor sau de servicii de securitate gestionate, și să ia măsurile adecvate pentru a combate astfel de riscuri. ***Acești furnizori și prestatori de servicii ar trebui să fie verificați cu atenție, ținându-se seama de întregul lanț de aprovizionare și de mediul economic și politic în care își desfășoară activitatea. În cazul în care relațiile cu astfel de furnizori și prestatori de servicii reprezintă un risc pentru integritatea proceselor democratice din Uniune, ar trebui să înceteze fără întârzieri nejustificate.*** Aceste măsuri ***ar trebui*** să facă parte din nivelul de referință în materie de securitate cibernetică și să fie detaliate în documentele de orientare sau în recomandările emise de CERT-UE. La definirea măsurilor și a orientărilor ***ar trebui*** să se țină seama în mod corespunzător de legislația și politicile relevante ale UE, inclusiv de evaluările riscurilor și de recomandările emise de Grupul de cooperare privind securitatea rețelelor și a informațiilor, cum ar fi evaluarea coordonată la nivelul UE a riscurilor de securitate cibernetică aferente rețelelor 5G și setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G. În plus, ***având în vedere peisajul amenințărilor și importanța consolidării rezilienței,*** ar ***trebui să se solicite*** certificarea produselor, a serviciilor și a proceselor TIC relevante ***utilizate în instituțiile, organele, oficiile și agențiile Uniunii***, în cadrul sistemelor europene

specifice de certificare a securității cibernetice adoptate în temeiul articolului 49 din Regulamentul (UE) 2019/881.

Amendamentul 9

Propunere de regulament
Considerentul 13

Textul propus de Comisie	*Amendamentul*
(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de instituții, organe și agenții ale Uniunii sau comunități de interes care includ instituții, organe și agenții ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare, instituțiile, organele și agențiile Uniunii ***trebuie*** să informeze CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative și să facă schimb de detalii tehnice adecvate care să permită detectarea sau atenuarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor similare în alte instituții, organe și agenții ale Uniunii, precum și răspunsul la astfel de amenințări, vulnerabilități și incidente. Urmând aceeași abordare precum cea prevăzută în Directiva [propunerea NIS 2], în cazul în care iau cunoștință de un incident semnificativ, entitățile ar trebui să transmită CERT-UE o ***notificare inițială*** în ***termen*** de 24 de ore. Acest schimb de informații ***trebuie*** să permită CERT-UE să disemineze informațiile către alte instituții, organe și agenții ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor ***informatice*** ale Uniunii și ale omologilor Uniunii împotriva unor incidente, amenințări și vulnerabilități similare.	(13) Multe atacuri cibernetice fac parte din campanii mai ample care vizează grupuri de instituții, organe***, oficii*** și agenții ale Uniunii sau comunități de interes care includ instituții, organe***, oficii*** și agenții ale Uniunii. Pentru a permite detectarea proactivă, răspunsul la incidente sau măsurile de atenuare, instituțiile, organele***, oficiile*** și agențiile Uniunii ***ar trebui*** să informeze CERT-UE cu privire la amenințările cibernetice semnificative, vulnerabilitățile semnificative și incidentele semnificative și să facă schimb de detalii tehnice adecvate care să permită detectarea sau atenuarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor similare în alte instituții, organe***, oficii*** și agenții ale Uniunii, precum și răspunsul la astfel de amenințări, vulnerabilități și incidente. Urmând aceeași abordare precum cea prevăzută în Directiva [propunerea NIS 2], în cazul în care iau cunoștință de un incident semnificativ, entitățile ar trebui să transmită CERT-UE o ***avertizare timpurie fără întârzieri nejustificate și,*** în ***orice caz, nu mai târziu*** de 24 de ore. ***Instituțiilor, organelor, oficiilor și agențiilor Uniunii ar trebui să li se aloce resurse suficiente pentru a-și îndeplini obligațiile de raportare în mod rapid și eficient, astfel încât să se asigure funcționarea corectă a sistemului conceput.*** Acest schimb de informații ***ar trebui*** să permită CERT-UE să disemineze informațiile către alte instituții, organe***,***

oficii și agenții ale Uniunii, precum și către omologii corespunzători, pentru a contribui la protejarea mediilor ***TIC*** ale Uniunii și ale omologilor Uniunii împotriva unor incidente, amenințări și vulnerabilități similare.

Amendamentul 10

Propunere de regulament
Considerentul 14

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

Amendamentul 11

Propunere de regulament
Considerentul 16

Textul propus de Comisie	*Amendamentul*
(16) IICB ar trebui să monitorizeze respectarea regulamentului, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adresate de CERT-UE. În ceea ce privește aspectele tehnice, IICB ***trebuie***	(16) IICB ar trebui să monitorizeze respectarea regulamentului, precum și punerea în aplicare a documentelor de orientare, a recomandărilor și a apelurilor la acțiune adresate de CERT-UE. În ceea ce privește aspectele tehnice, IICB ***ar***

să beneficieze de sprijin din partea grupurilor consultative tehnice ***a căror componență este decisă de IICB***, care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu instituțiile, organele și agențiile Uniunii și cu alte părți interesate, după caz. Dacă este necesar, IICB ***trebuie*** să emită avertismente ***fără caracter obligatoriu*** și ***să recomande*** audituri.

trebui să beneficieze de sprijin din partea grupurilor consultative tehnice, care ar trebui să lucreze în strânsă cooperare cu CERT-UE, cu instituțiile, organele***, oficiile*** și agențiile Uniunii și cu alte părți interesate, după caz. Dacă este necesar, IICB ***ar trebui*** să emită avertismente și ***recomandări pentru*** audituri.

Amendamentul 12

Propunere de regulament
Considerentul 17

Textul propus de Comisie	*Amendamentul*
(17) CERT-UE ***trebuie*** să aibă misiunea de a contribui la securitatea mediului ***informatic*** al tuturor instituțiilor, organelor și agențiilor Uniunii. CERT-UE ***trebuie*** să acționeze ca echivalent al coordonatorului desemnat pentru instituțiile, organele și agențiile Uniunii, în scopul divulgării coordonate a vulnerabilităților către registrul european al vulnerabilităților, astfel cum se menționează la articolul 6 din ***[propunerea de Directivă*** NIS 2].	(17) CERT-UE ***ar trebui*** să aibă misiunea de a contribui la securitatea mediului ***TIC*** al tuturor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii. CERT-UE ***ar trebui*** să acționeze ca echivalent al coordonatorului desemnat pentru instituțiile, organele***, oficiile*** și agențiile Uniunii, în scopul divulgării coordonate a vulnerabilităților către registrul european al vulnerabilităților, astfel cum se menționează la articolul 6 din ***Directiva [propunerea*** NIS 2].

Amendamentul 13

Propunere de regulament
Considerentul 18

Textul propus de Comisie	*Amendamentul*
(18) În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate instituțiile, organele și agențiile Uniunii, cu o amploare și o profunzime adecvate, precum și o adaptare continuă la amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a	(18) În 2020, comitetul director al CERT-UE a stabilit un nou obiectiv strategic pentru CERT-UE de a garanta un nivel cuprinzător de apărare cibernetică pentru toate instituțiile, organele***, oficiile*** și agențiile Uniunii, cu o amploare și o profunzime adecvate, precum și o adaptare continuă la amenințările actuale sau iminente, inclusiv atacurile împotriva dispozitivelor mobile, a mediilor cloud și a

dispozitivelor conectate prin internetul obiectelor. Acest obiectiv strategic include, de asemenea, centre de operațiuni pentru securitate (SOC) cu spectru larg, care monitorizează rețelele, precum și monitorizarea permanentă a amenințărilor deosebit de grave. CERT-UE ***trebuie*** să ofere sprijin echipelor de securitate ***informatică*** ale instituțiilor, organelor și agențiilor mai mari ale Uniunii, inclusiv prin monitorizarea non-stop din prima linie. Pentru instituțiile, organele și agențiile mai mici și unele medii ale Uniunii, CERT-UE trebuie să furnizeze toată gama de servicii.	dispozitivelor conectate prin internetul obiectelor. Acest obiectiv strategic include, de asemenea, centre de operațiuni pentru securitate (SOC) cu spectru larg, care monitorizează rețelele, precum și monitorizarea permanentă a amenințărilor deosebit de grave. CERT-UE ***ar trebui*** să ofere sprijin echipelor de securitate ***TIC*** ale instituțiilor, organelor***, oficiilor*** și agențiilor mai mari ale Uniunii, inclusiv prin monitorizarea non-stop din prima linie. Pentru instituțiile, organele***, oficiile*** și agențiile mai mici și unele medii ale Uniunii, CERT-UE trebuie să furnizeze toată gama de servicii.

Amendamentul 14

Propunere de regulament
Considerentul 19 a (nou)

Textul propus de Comisie	*Amendamentul*
	(19a) Pentru a asigura o mai bună punere în aplicare a măsurilor și a orientărilor în materie de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii și pentru a consolida o cultură a securității cibernetice în cadrul acestora, CERT-UE ar trebui, de asemenea, să consolideze cooperarea cu Rețeaua și Centrul european de competențe în materie de securitate cibernetică.

Amendamentul 15

Propunere de regulament
Considerentul 20

Textul propus de Comisie	*Amendamentul*
(20) În sprijinirea cooperării operaționale în domeniul securității cibernetice, CERT-UE ***trebuie*** să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate Cibernetică	(20) În sprijinirea cooperării operaționale în domeniul securității cibernetice, CERT-UE ***ar trebui*** să utilizeze expertiza de care dispune Agenția Uniunii Europene pentru Securitate

prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[5]. ***Dacă este cazul,*** între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE ***trebuie*** să coopereze cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.

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

Cibernetică prin intermediul unei cooperări structurate, astfel cum se prevede în Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[5]. Între cele două entități ar trebui încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări și pentru a se evita suprapunerea activităților. CERT-UE ***ar trebui*** să coopereze cu Agenția Uniunii Europene pentru Securitate Cibernetică în ceea ce privește analiza amenințărilor și să transmită agenției în mod regulat raportul său privind situația amenințărilor.

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

Amendamentul 16
Propunere de regulament
Considerentul 24

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

Amendamentul 17

Propunere de regulament
Considerentul 25

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

Amendamentul 18

Propunere de regulament
Articolul 1 – alineatul 1 – litera a

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

Amendamentul 19

Propunere de regulament
Articolul 1 – alineatul 1 – litera c

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

Amendamentul 20

Propunere de regulament
Articolul 2 a (nou)

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

Amendamentul 21

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 2

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

Amendamentul 22

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 4

Textul propus de Comisie	*Amendamentul*
(4) „securitate cibernetică” înseamnă securitatea cibernetică ***în sensul articolului 4*** punctul ***3 din [propunerea de Directivă NIS 2]***;	(4) „securitate cibernetică” înseamnă securitatea cibernetică ***astfel cum este definită la articolul 2*** punctul ***1 din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului***[1a];
	[1a] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA

(Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

Amendamentul 23

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 5

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

Amendamentul 24

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 7

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

Amendamentul 25

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 11

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

Amendamentul 26

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 14

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

Amendamentul 27

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

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

Justificare

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

Amendamentul 28

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 15

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

Amendamentul 29
Propunere de regulament
Articolul 4 – alineatul 1

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

	cibernetică. Cadrul se instituie până cel târziu la …. [15 luni de la ***data intrării*** în vigoare a prezentului regulament].

Amendamentul 30

Propunere de regulament
Articolul 4 – alineatul 2

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

Amendamentul 31
Propunere de regulament
Articolul 4 – alineatul 4

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

Amendamentul 32

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

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

Amendamentul 33

Propunere de regulament
Articolul 5 – alineatul 1

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

aplicabile. Nivelul de referință în materie de securitate cibernetică se instituie până cel târziu la … [18 luni de la ***data intrării*** în vigoare a prezentului regulament] și abordează domeniile enumerate în anexa I și măsurile enumerate în anexa II.

Amendamentul 34

Propunere de regulament
Articolul 5 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Personalul de conducere de nivel superior din fiecare instituție, organ și agenție a Uniunii urmează periodic cursuri de formare specifice, pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor organizației.	2. Personalul de conducere de nivel superior din fiecare instituție, organ***, oficiu*** și agenție a Uniunii urmează periodic cursuri de formare specifice ***cu resurse adecvate***, pentru a dobândi cunoștințe și competențe suficiente care să le permită să înțeleagă și să evalueze practicile de gestionare a riscurilor de securitate cibernetică, precum și impactul acestora asupra operațiunilor organizației. ***În plus față de aceste cursuri de formare specifice și în scopul construirii și consolidării culturii securității cibernetice, în planul de securitate cibernetică se include o formare periodică a membrilor personalului în materie de securitate cibernetică, ce se actualizează cel puțin o dată la doi ani. Se asigură resurse suficiente pentru a asigura o formare de calitate.***

Amendamentul 35

Propunere de regulament
Articolul 6 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Fiecare instituție, organ și agenție a Uniunii efectuează o evaluare a nivelului de maturitate al securității cibernetice cel puțin o dată la ***trei*** ani, încorporând toate	Fiecare instituție, organ***, oficiu*** și agenție a Uniunii efectuează o evaluare a nivelului de maturitate al securității cibernetice ***până la ... [6 luni de la intrarea în vigoare a***

elementele mediului său ***informatic***, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în temeiul articolului 13.	***prezentului regulament] și, ulterior,*** cel puțin o dată la ***doi*** ani, încorporând toate elementele mediului său ***TIC***, astfel cum este descris la articolul 4, ținând seama de documentele de orientare și de recomandările relevante adoptate în temeiul articolului 13. ***Evaluarea maturității se bazează pe audituri de securitate cibernetică independente efectuate de prestatori verificați.***

Amendamentul 36

Propunere de regulament
Articolul 7 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În urma concluziilor desprinse din evaluarea nivelului de maturitate și luând în considerare activele și riscurile identificate în temeiul articolului 4, cel mai înalt nivel de conducere din fiecare instituție, organ și agenție a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului de gestionare, guvernanță și control al riscurilor și a nivelului de referință în materie de securitate cibernetică. Planul vizează creșterea gradului de securitate cibernetică în ansamblu a entității în cauză și contribuie, astfel, la atingerea sau îmbunătățirea unui nivel comun ridicat de securitate cibernetică în toate instituțiile, organele și agențiile Uniunii. Pentru a sprijini misiunea entității pe baza autonomiei sale instituționale, planul include cel puțin domeniile enumerate în anexa I, măsurile enumerate în anexa II, precum și măsuri legate de pregătirea pentru incidente, răspunsul la incidente și redresarea în urma incidentelor, cum ar fi monitorizarea și jurnalizarea evenimentelor de securitate. Planul se revizuiește cel puțin o dată la ***trei*** ani, în urma evaluărilor nivelului de maturitate, efectuate în temeiul	1. În urma concluziilor desprinse din evaluarea nivelului de maturitate și luând în considerare activele și riscurile identificate în temeiul articolului 4, cel mai înalt nivel de conducere din fiecare instituție, organ***, oficiu*** și agenție a Uniunii aprobă un plan de securitate cibernetică, fără întârzieri nejustificate, după instituirea cadrului de gestionare, guvernanță și control al riscurilor și a nivelului de referință în materie de securitate cibernetică. Planul vizează creșterea gradului de securitate cibernetică în ansamblu a entității în cauză și contribuie, astfel, la atingerea sau îmbunătățirea unui nivel comun ridicat de securitate cibernetică în toate instituțiile, organele***, oficiile*** și agențiile Uniunii. Pentru a sprijini misiunea entității pe baza autonomiei sale instituționale, planul include cel puțin domeniile enumerate în anexa I, măsurile enumerate în anexa II, precum și măsuri legate de pregătirea pentru incidente, răspunsul la incidente și redresarea în urma incidentelor, cum ar fi ***evaluarea securității prestatorilor și serviciilor,*** monitorizarea și jurnalizarea evenimentelor de securitate. Planul se revizuiește cel puțin o dată la ***doi*** ani, în urma evaluărilor nivelului de maturitate,

articolului 6.	efectuate în temeiul articolului 6.

Amendamentul 37

Propunere de regulament
Articolul 7 – alineatul 2

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

Amendamentul 38

Propunere de regulament
Articolul 7 – alineatul 3

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

Amendamentul 39

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

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

Amendamentul 40

Propunere de regulament
Articolul 9 – alineatul 2 – litera a

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

Amendamentul 41

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

Textul propus de Comisie	*Amendamentul*
IICB este format din trei reprezentanți numiți de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta interesele agențiilor și organelor care își gestionează propriul mediu ***informatic*** și câte un reprezentant numit de fiecare dintre următoarele entități:	IICB este format din trei reprezentanți numiți de Rețeaua agențiilor UE (EUAN), la propunerea Comitetului său consultativ pentru tehnologia informației și comunicațiilor, pentru a reprezenta interesele ***oficiilor,*** agențiilor și organelor care își gestionează propriul mediu ***TIC*** și câte un reprezentant numit de fiecare dintre următoarele entități:

Amendamentul 42

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

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

Amendamentul 43

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

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

Amendamentul 44

Propunere de regulament
Articolul 11 – alineatul 1 – litera a

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

Amendamentul 45

Propunere de regulament
Articolul 11 – alineatul 1 – litera b

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

Amendamentul 46

Propunere de regulament
Articolul 12 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Misiunea CERT-UE, a Centrului autonom de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE, este de a contribui	1. Misiunea CERT-UE, a Centrului autonom de răspuns la incidente de securitate cibernetică pentru instituțiile, organele***, oficiile*** și agențiile UE, este de a

la securitatea mediului ***informatic*** neclasificat al tuturor instituțiilor, organelor și agențiilor Uniunii, oferindu-le consiliere în materie de securitate cibernetică, ajutându-le să prevină, să detecteze, să atenueze și să răspundă la incidente și acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.	contribui la securitatea mediului ***TIC*** neclasificat al tuturor instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, oferindu-le consiliere în materie de securitate cibernetică, ajutându-le să prevină, să detecteze, să atenueze și să răspundă la incidente și acționând în calitate de centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru aceste entități.

Amendamentul 47

Propunere de regulament
Articolul 12 – alineatul 2 – litera d

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

Amendamentul 48

Propunere de regulament
Articolul 12 – alineatul 4

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

Amendamentul 49

Propunere de regulament
Articolul 12 – alineatul 5 – partea introductivă

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

Amendamentul 50

Propunere de regulament
Articolul 12 – alineatul 5 – litera a

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

Amendamentul 51

Propunere de regulament
Articolul 12 – alineatul 5 – litera b

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

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

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

Amendamentul 53

Propunere de regulament
Articolul 12 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. CERT-UE poate organiza exerciții de securitate cibernetică sau poate recomanda participarea la exercițiile existente, în strânsă cooperare cu Agenția Uniunii Europene pentru Securitate Cibernetică, dacă este cazul, pentru a testa nivelul de securitate cibernetică al instituțiilor, organelor și agențiilor Uniunii.	6. CERT-UE poate organiza exerciții de securitate cibernetică sau poate recomanda participarea la exercițiile existente, în strânsă cooperare cu Agenția Uniunii Europene pentru Securitate Cibernetică, dacă este cazul, pentru a testa ***periodic*** nivelul de securitate cibernetică al instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii. ***În plus, prin intermediul cooperării consolidate și al programelor comune cu Rețeaua și Centrul european de competențe în materie de securitate cibernetică (ECCC), CERT-UE poate sprijini cercetarea și inovarea și poate contribui la consolidarea capacităților în materie de securitate cibernetică ale instituțiilor, organelor, oficiilor și agențiilor Uniunii.***

Amendamentul 54

Propunere de regulament
Articolul 12 – alineatul 7

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

Amendamentul 55

Propunere de regulament
Articolul 14 – paragraful 1

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

Amendamentul 56

Propunere de regulament
Articolul 16 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, inclusiv CERT, centrele naționale de securitate cibernetică, CSIRT și punctele unice de contact menționate la articolul 8 din ***[propunerea de Directivă*** NIS 2], cu privire la amenințările cibernetice, la vulnerabilități	1. CERT-UE cooperează și face schimb de informații cu omologii naționali din statele membre, inclusiv CERT, centrele naționale de securitate cibernetică, CSIRT și punctele unice de contact menționate la articolul 8 din ***Directiva [propunerea*** NIS 2], cu privire la amenințările cibernetice, la vulnerabilități

și incidente, la posibilele contramăsuri și la toate aspectele relevante pentru îmbunătățirea protecției mediilor ***informatice*** ale instituțiilor, organelor și agențiilor Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul 13 din ***[propunerea de Directivă*** NIS 2].	și incidente, la posibilele contramăsuri și la toate aspectele relevante pentru îmbunătățirea protecției mediilor ***TIC*** ale instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii, inclusiv prin intermediul rețelei CSIRT menționate la articolul 13 din ***Directiva [propunerea*** NIS 2].

Amendamentul 57

Propunere de regulament
Articolul 16 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. CERT-UE poate face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare fără consimțământul ***entității*** afectate. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul de securitate cibernetică numai cu consimțământul ***entității*** afectate.	2. CERT-UE poate face schimb de informații referitoare la incidente cu omologii naționali din statele membre pentru a facilita detectarea amenințărilor sau a incidentelor cibernetice similare fără consimțământul ***instituțiilor, organelor, oficiilor sau agențiilor Uniunii*** afectate***, atât timp cât prelucrarea datelor cu caracter personal respectă dispozițiile aplicabile din Regulamentul (UE) 2018/1725***. CERT-UE poate face schimb de informații referitoare la incidente care dezvăluie identitatea persoanei vizate de incidentul de securitate cibernetică numai cu consimțământul ***instituțiilor, organelor, oficiilor sau agențiilor Uniunii*** afectate.

Amendamentul 58

Propunere de regulament
Articolul 17 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. CERT-UE poate coopera cu omologii din statele terțe, inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice formă de	1. CERT-UE poate coopera cu omologii din statele terțe, inclusiv cu omologii din cadrul sectorului, cu privire la instrumente și metode, cum ar fi tehnici, tactici, proceduri și bune practici, precum și cu privire la amenințări cibernetice și vulnerabilități. Pentru orice formă de

cooperare cu astfel de omologi, inclusiv într-un cadru în care omologii din afara UE cooperează cu omologii naționali din statele membre, CERT-UE solicită aprobarea prealabilă a IICB.	cooperare cu astfel de omologi, inclusiv într-un cadru în care omologii din afara UE cooperează cu omologii naționali din statele membre, CERT-UE solicită aprobarea prealabilă a IICB. ***Orice astfel de cooperare respectă integritatea democratică a UE.***

Amendamentul 59

Propunere de regulament
Articolul 17 – alineatul 2

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

Amendamentul 60

Propunere de regulament
Articolul 17 – alineatul 3

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

Amendamentul 61

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

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

Amendamentul 62

Propunere de regulament
Articolul 19 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Pentru ***a coordona gestionarea vulnerabilităților și răspunsul*** la ***incidente***, CERT-UE ***le*** poate solicita instituțiilor, organelor și agențiilor Uniunii să îi furnizeze informații din inventarele lor de sisteme ***informatice care sunt relevante pentru sprijinul CERT-UE. Instituția***, ***organul sau agenția*** care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.	1. Pentru ***a-și îndeplini misiunea și sarcinile astfel cum sunt definite*** la ***articolul 12***, CERT-UE poate solicita instituțiilor, organelor***, oficiilor*** și agențiilor Uniunii să îi furnizeze informații din inventarele lor de sisteme ***TIC, inclusiv informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, indicatori de compromitere***, ***alerte de securitate cibernetică și recomandări privind configurarea instrumentelor de securitate cibernetică pentru detectarea incidentelor cibernetice. Entitatea*** care primește o astfel de solicitare transmite informațiile solicitate și orice modificare ulterioară a acestora, fără întârzieri nejustificate.

Amendamentul 63

Propunere de regulament
Articolul 19 – alineatul 2

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

Amendamentul 64
Propunere de regulament
Articolul 20 – titlu

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

Amendamentul 65

Propunere de regulament
Articolul 20 – alineatul 1 – paragraful 1

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

Amendamentul 66

Propunere de regulament
Articolul 20 – alineatul 1 – paragraful 2

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

Amendamentul 67

Propunere de regulament
Articolul 20 – alineatul 2 – partea introductivă

Textul propus de Comisie	*Amendamentul*
2. Instituțiile, organele și agențiile Uniunii transmit apoi către CERT-UE, fără întârzieri nejustificate, detalii tehnice adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea, răspunsul la incidente sau adoptarea unor măsuri de atenuare. Notificarea include, dacă sunt disponibili:	2. Instituțiile, organele***, oficiile*** și agențiile Uniunii transmit apoi ***o notificare*** către CERT-UE, fără întârzieri nejustificate ***și***, ***în orice caz, în termen de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ, actualizează avertizarea timpurie și furnizează o evaluare inițială a incidentului semnificativ, a gravității și a impactului acestuia, cu*** detalii tehnice adecvate privind amenințările cibernetice, vulnerabilitățile și incidentele care permit detectarea, răspunsul la incidente sau adoptarea unor măsuri de atenuare. Notificarea include, dacă sunt disponibili:

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

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

Amendamentul 69

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

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

Amendamentul 70

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

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

Amendamentul 71

Propunere de regulament
Articolul 20 – alineatul 3

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

Amendamentul 72

Propunere de regulament
Articolul 20 – alineatul 4

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

Amendamentul 73

Propunere de regulament
Articolul 20 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Obligațiile de notificare nu se aplică în cazul informațiilor IUEC și al informațiilor pe care o instituție, un organ	***eliminat***

sau o agenție a Uniunii le-a primit de la un serviciu de securitate sau de informații al unui stat membru sau de la o autoritate de aplicare a legii cu condiția explicită ca acestea să nu fie comunicate CERT-UE.

Amendamentul 74

Propunere de regulament
Articolul 24 – alineatul 2

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

Amendamentul 75

Propunere de regulament
Articolul 24 – alineatul 3

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

Amendamentul 76

Propunere de regulament
Anexa I – paragraful 1 – partea introductivă

Textul propus de Comisie	*Amendamentul*
Domeniile următoare trebuie abordate în	***Cel puțin*** domeniile următoare trebuie

cadrul nivelului de referință în materie de securitate cibernetică:	abordate în cadrul nivelului de referință în materie de securitate cibernetică:

Amendamentul 77

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

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

Amendamentul 78

Propunere de regulament
Anexa I – paragraful 1 – punctul 3

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

Amendamentul 79

Propunere de regulament
Anexa I – paragraful 1 – punctul 7

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

Amendamentul 80

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

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

cibernetică;

Amendamentul 81

Propunere de regulament
Anexa I – paragraful 1 – punctul 9

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

Amendamentul 82

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

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

Amendamentul 83

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

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

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

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

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA SESIZATĂ PENTRU AVIZ

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

0	-

0	0

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