RĂSPUNSURILE COMISIEI EUROPENE

LA RAPORTUL SPECIAL AL CURȚII DE CONTURI EUROPENE

Securitatea cibernetică a instituțiilor, organelor și agențiilor UE: nivelul general de pregătire nu este proporțional cu amenințările

Cuprins

I. RĂSPUNSURILE COMISIEI PE SCURT 2

a) Introducere generală 2

b) Poziția Comisiei cu privire la principalele observații și recomandări ale CCE 2

c) Cele mai recente evoluții relevante și etapele următoare 3

II. RĂSPUNSURILE COMISIEI LA PRINCIPALELE OBSERVAȚII ALE CCE 3

1. Nivelurile de maturitate în materie de securitate cibernetică ale IOAUE 3

2. Mecanismele de cooperare ale IOAUE 4

3. Schimbul de informații cu privire la incidentele sau vulnerabilitățile semnificative 5

III. RĂSPUNSURILE COMISIEI LA CONCLUZIILE ȘI RECOMANDĂRILE CCE 5

Recomandarea 1 – Îmbunătățirea nivelului de pregătire în materie de securitate cibernetică al tuturor IOAUE prin norme comune obligatorii și resurse sporite pentru CERT-UE 5

Recomandarea 2 – Promovarea unor sinergii suplimentare între IOAUE în anumite domenii 6

Recomandarea 3 – Intensificarea accentului pus de CERT-UE și de ENISA pe acele IOAUE mai puțin avansate în domeniul securității cibernetice 6

În conformitate cu articolul 259 din Regulamentul financiar, prezentul document cuprinde răspunsurile Comisiei Europene la observațiile dintr-un raport special al Curții de Conturi Europene și urmează să fie publicat concomitent cu raportul special.

I. RĂSPUNSURILE COMISIEI PE SCURT

a) Introducere generală

Securitatea cibernetică a devenit o prioritate politică și operațională majoră a Comisiei Europene. Criza provocată de pandemia de COVID-19 a accentuat dependența noastră de serviciile digitale (cloud computing, dispozitive mobile, inteligență artificială). În ultimii doi ani, am putut constata o trecere masivă către munca la domiciliu. Prin urmare, sfera de acțiune atât a criminalității cibernetice, cât și a spionajului cibernetic, principalele amenințări la adresa instituțiilor, a organismele și a agențiilor Uniunii Europene (IOAUE), s-a mutat, de asemenea, preponderent în mediul online. Comisia recunoaște această tendință și s-a impus în mod consecvent și decisiv ca un lider în materie de securitate cibernetică. Regulamentul privind securitatea cibernetică a intrat în vigoare în 2019 și, printre altele, a extins mandatul ENISA și i-a conferit acesteia statut permanent. Acest regulament a stabilit, de asemenea, o relație de cooperare formală între ENISA și CERT-UE (Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE). În 2020, Comisia a propus consolidarea Directivei privind securitatea rețelelor și a sistemelor informatice (Directiva NIS), iar documentul respectiv este pe cale să fie aprobat de către colegiuitori.

Strategia de securitate cibernetică din 2020 prevede, de asemenea, trei acțiuni care au un impact asupra securității cibernetice a IOAUE. Strategia a anunțat un regulament privind securitatea informațiilor în instituțiile și organele și agențiile UE, un regulament privind normele comune de securitate cibernetică pentru instituțiile, organele și agențiile UE și intenția de a oferi un nou temei juridic pentru CERT-UE pentru a consolida mandatul și finanțarea acestui centru, astfel încât să dispună de resurse adecvate în fața amenințărilor, riscurilor și incidentelor emergente din domeniu.

S-au realizat progrese în ceea ce privește redactarea acestor propuneri, care nu au fost încă adoptate de colegiu, dar se preconizează că vor fi adoptate în primul trimestru al anului 2022. Printre aspectele importante discutate între instituții în această etapă pregătitoare se numără temeiul juridic al propunerii, precum și capacitatea bugetară a tuturor IOAUE de a îndeplini cerințele impuse legate de finanțarea propriilor nevoi în materie de securitate cibernetică și de identificarea resurselor necesare pentru a sprijini CERT-UE, bugetul său și, în special, posturile sale.

Există diferențe importante între IOAUE din punctul de vedere al maturității pregătirii lor în materie de securitate cibernetică. Unele IOAUE sunt într-adevăr bine pregătite din punctul de vedere al securității cibernetice și ar trebui să își asume în continuare un rol de lider, stimulând și inspirând realizarea de progrese și îmbunătățiri suplimentare la nivelul întregului peisaj al securității cibernetice. Pentru a realiza progrese măsurabile, este important să se recunoască faptul că există niveluri diferite de maturitate în rândul IOAUE și să se stabilească priorități prin canalizarea acțiunilor de îmbunătățire în primul rând către acele IOAUE în cazul cărora lacunele identificate sunt asociate cu nivelul cel mai ridicat de risc.

b) Poziția Comisiei cu privire la principalele observații și recomandări ale CCE

Comisia salută raportul CCE privind securitatea cibernetică a instituțiilor, organelor și agențiilor UE. Comisia ia act de faptul că raportul subliniază importanța existenței unor cadre juridice comune pentru toate IOAUE în materie de securitate a informațiilor și de securitate cibernetică pentru

îmbunătățirea nivelului general de securitate cibernetică. Comisia observă că principalele observații și recomandări ale CCE nu privesc securitatea cibernetică operațională propriu-zisă a Comisiei, ci rolul său la nivelul politicilor, în procesul de propunere a unor acte legislative care să consolideze maturitatea pregătirii în materie de securitate cibernetică a IOAUE.

Viitoarele regulamente privind „Securitatea informațiilor în instituțiile, organele și agențiile UE” și „Normele comune în materie de securitate cibernetică pentru instituțiile, organele și agențiile UE” vor stabili norme comune în vederea atingerii unui nivel ridicat de securitate a informațiilor și de securitate cibernetică, însă punerea lor în aplicare în contextul organizațional și operațional al fiecăreia dintre IOAUE (în special având în vedere profilurile lor de amenințare și de risc) va fi în continuare responsabilitatea autonomă a IOAUE. Propunerea de regulament privind securitatea cibernetică va prevedea mecanisme de asigurare a conformității care să fie adecvate și proporționale cu obiectivul și domeniul de aplicare al noilor norme, fără a aduce atingere autonomiei instituțiilor, organelor și agențiilor.

În prezent, Comisia deține (pentru perioada acestui mandat, care este în mod tipic de până la 2 ani) președinția prin rotație a subgrupului pentru securitate cibernetică din cadrul Comitetului interinstituțional privind transformarea digitală (ICDT). Se constată faptul că nu au fost alocate resurse specifice pentru activitatea subgrupului, toate acțiunile prevăzute urmând să se bazeze pe maxima diligență a participanților, care ar contribui în mod benevol.

Comisia este de acord cu ideea generală de a consolida resursele și mandatul CERT-UE.

În acest sens, Comisia este de acord cu principalele observații și recomandări ale raportului. Poziția noastră detaliată este explicată în observațiile suplimentare din secțiunea III. În ceea ce privește recomandările, Comisia acceptă recomandările 1a, 1b, 1c, 1d, 1e, 1f, 1g și recomandările 2a, 2b și 2c.

c) Cele mai recente evoluții relevante și etapele următoare

A fost finalizată o consultare formală la nivelul directorilor generali ai IOAUE cu privire la proiectele de texte consolidate pentru cele două regulamente (privind securitatea informațiilor și privind securitatea cibernetică), iar în prezent sunt evaluate contribuțiile primite, urmând ca pachetul legislativ să fie finalizat și adoptat de către colegiu în cursul primului trimestru al anului 2022.

II. RĂSPUNSURILE COMISIEI LA PRINCIPALELE OBSERVAȚII ALE CCE

1. Nivelurile de maturitate în materie de securitate cibernetică ale IOAUE

Comisia este de acord că, atunci când se analizează nivelul cheltuielilor efectuate de IOAUE pentru securitatea cibernetică, este important să se țină seama de amenințări și de riscuri.

Tot astfel, sub aspectul resurselor umane, stabilitatea resurselor umane ale IOAUE este influențată de o serie de factori. Piața pentru recrutarea de experți specializați în securitate cibernetică este din

ce în ce mai complexă. În multe cazuri, regulile privind resursele umane nu sunt adaptate profilurilor specializate (în materie de recrutare, dezvoltare a carierei sau formare). În plus, din cauza presiunii generalizate exercitate de autoritatea bugetară asupra nivelului efectivelor de personal ale IOAUE, în domenii emergente de înaltă prioritate, cum ar fi securitatea cibernetică, ocuparea posturilor este în continuare suboptimă, în special în serviciile operaționale interne.

Referirea la progresele realizate în materie de guvernanță și de gestionare a riscurilor ar trebui să țină seama de faptul că monitorizarea conformității trece în prezent din etapa-pilot în cea a implementării efective. Prin urmare, este normal ca gradul de acoperire să fie, deocamdată, destul de scăzut. Acest proiect de asigurare a conformității este următoarea etapă a unui proces de lungă durată ce vizează îmbunătățirea maturității cibernetice, proces care a început cu definirea unei metodologii comune de evaluare a riscurilor, cu construirea unor instrumente comune, cu implementarea gestionării vulnerabilității și cu monitorizarea, testarea și validarea inventarului activelor. În pofida complexității bazei de active a Comisiei, formată din peste 1 000 de sisteme informatice, gestionate de mai mult de 50 de direcții generale și agenții executive, a-au înregistrat progrese în acest proces de durată.

2. Mecanismele de cooperare ale IOAUE

CERT-UE este o poveste de succes extraordinară prin faptul că promovează cooperarea nu numai între IOAUE, ci și la nivel european, prin participarea sa în calitate de membru cu drepturi depline al rețelei CSIRT instituite în temeiul Directivei NIS. CERT-UE este, astfel, un model exemplar pentru modul în care pot fi consolidate cooperarea și serviciile de securitate cibernetică. Observațiile Curții cu privire la CERT-UE ilustrează foarte clar rolul inestimabil al CERT-UE în contextul unui peisaj al amenințărilor cibernetice din ce în ce mai ostil și al lipsei cronice de resurse.

În temeiul Acordului interinstituțional (AII) în vigoare, agențiile descentralizate ale UE și întreprinderile comune sunt reprezentate oficial de ENISA în cadrul comitetului director al CERT-UE. În plus, opiniile acestora sunt exprimate în cadrul reuniunilor comitetului director de către un reprezentant al Comitetului consultativ TIC (ICTAC), care are dreptul să participe la acestea pentru a asista ENISA în rolul său de reprezentare a agențiilor, dar nu are un loc și nici un vot oficial în cadrul acestui comitet. Chestiunea reprezentării adecvate a agențiilor în cadrul comitetului director al CERT-UE va fi abordată în propunerea de regulament prin completarea componenței comitetului director cu până la trei reprezentanți desemnați de Rețeaua agențiilor Uniunii Europene (EUAN), la propunerea Comitetului consultativ TIC.

Participarea la subgrupul pentru securitate cibernetică al ICDT se desfășoară pe baza principiului maximei diligențe, la nivelul de implicare stabilit de fiecare IOAUE. Îmbunătățirile legate de schimbul de informații privind achizițiile publice, care sunt un subiect important pentru grupul operativ 2 din cadrul subgrupului pentru securitate cibernetică, sunt abordate în contextul elaborării noului contract-cadru privind securitatea cibernetică.

În ceea ce privește instrumentele comune pentru servicii precum cele de mesagerie electronică și de videoconferință, există deja posibilitatea de a utiliza în toate IOAUE, pentru e-mailurile criptate, sistemul SECEM-2 implementat de Comisie, care se bazează pe o gestionare eficace a cheilor și a certificatelor de criptare. În plus, este în curs de dezvoltare un instrument care va permite criptarea e-mailurilor dintre instituții (SECABC), intenția fiind aceea de a oferi acces la acest instrument tuturor IOAUE interesate începând din 2022. Serviciile de videoconferință securizată sunt deja disponibile pentru schimbul de informații sensibile neclasificate și pot fi extinse și la alte IOAUE pe bază ad-hoc, prin gestionarea identităților participanților la reuniuni. Schimbul de informații sensibile va face, de asemenea, obiectul propunerii de regulament privind securitatea informațiilor (și anume, prin folosirea de etichete și marcaje comune).

3. Schimbul de informații cu privire la incidentele sau vulnerabilitățile semnificative

Faptul că nu toate IOAUE notifică CERT-UE cu privire la incidentele sau vulnerabilitățile semnificative este abordat în propunerea de regulament privind securitatea cibernetică, în conformitate cu propunerea Comisiei din Directiva NIS-2[1]. Nivelul de punere în aplicare va depinde de resursele suplimentare alocate în acest scop de către IOAUE autonome. Posibilitatea asigurării transmiterii acestor notificări rămâne limitată, inclusiv conform dispozițiilor propunerii de regulament, în forma lor actuală, din cauza autonomiei instituționale a IOAUE. Propunerea de regulament privind securitatea cibernetică va prevedea mecanisme de asigurare a conformității care să fie adecvate și proporționale cu obiectivul și domeniul de aplicare al noilor norme, fără a aduce atingere autonomiei instituțiilor, organelor și agențiilor.

III. RĂSPUNSURILE COMISIEI LA CONCLUZIILE ȘI RECOMANDĂRILE CCE

Recomandarea 1 – Îmbunătățirea nivelului de pregătire în materie de securitate cibernetică al tuturor IOAUE prin norme comune obligatorii și resurse sporite pentru CERT-UE

Textul propunerii de regulament va include măsuri specifice menite să sporească și mai mult nivelul comun de securitate cibernetică. Aceste măsuri vor fi transpuse în planuri de securitate cibernetică, definite și puse în aplicare la nivelul IOAUE prin cadrul acestora de guvernanță în materie de securitate cibernetică.

Comisia acceptă această recomandare. În ceea ce privește subrecomandările specifice, Comisia remarcă următoarele:

a) Comisia acceptă recomandarea 1a. Proiectul de regulament va include dispoziții privind cadre de guvernanță și control instituite la cel mai înalt nivel de conducere executivă pentru fiecare IOAUE, pentru a asigura o gestionare eficace și prudentă a tuturor riscurilor în materie de securitate cibernetică.
b) Comisia acceptă recomandarea 1b. Proiectul de regulament va consolida abordarea bazată pe riscuri în ceea ce privește gestionarea securității cibernetice, clarificând faptul că acțiunile, planurile de securitate informatică și desfășurarea efectivă a controalelor esențiale ar trebui să reflecte concluziile evaluărilor.
c) Comisia acceptă recomandarea 1c. Programele de educație, sensibilizare și formare în materie de securitate cibernetică vor fi incluse în scenariul de referință în materie de securitate cibernetică prezentat în proiectul de regulament.
d) Comisia acceptă recomandarea 1d. Din experiența de până acum, deși auditurile și testele periodice sunt esențiale, ele nu sunt suficiente pentru a garanta realizarea de progrese. Prin

[1] Propunere de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148, COM(2020) 823 final.

urmare, este necesar să se realizeze raportări periodice și să se asigure transparența ca parte a cadrului de guvernanță în materie de securitate cibernetică prevăzute la litera a).

e) Comisia acceptă recomandarea 1e. Proiectul de regulament va include dispoziții referitoare la transmiterea de notificări de către IOAUE către CERT-UE cu privire la amenințările, vulnerabilitățile și incidentele cibernetice semnificative.

f) Comisia acceptă recomandarea 1f. Comisia susține necesitatea consolidării resurselor CERT-UE. Dispozițiile privind personalul și contribuțiile financiare din partea IOAUE vor fi incluse în textul proiectului de regulament.

g) Comisia acceptă recomandarea 1g. Regulamentul propus va prevedea mecanisme de asigurare a conformității proporționale cu obiectivul și domeniul de aplicare al dispozițiilor, cu respectarea autonomiei instituționale a IOAUE. Conținutul viitorului regulament depinde de rezultatul procedurii legislative și va fi rezultatul unei decizii luate de organul legislativ al UE cu privire la propunerea prezentată de Comisie.

Recomandarea 2 – Promovarea unor sinergii suplimentare între IOAUE în anumite domenii

Comisia, care deține în prezent președinția subgrupului pentru securitate cibernetică din cadrul Comitetului interinstituțional privind transformarea digitală (ICDT), este de acord cu recomandările referitoare la promovarea soluțiilor pentru schimbul coerent și securizat de informații sensibile, schimbul sistematic de informații cu privire la proiectele de securitate cibernetică și cadrele comune de achiziții și contractele care vizează servicii de securitate cibernetică.

Comisia acceptă această recomandare. În ceea ce privește subrecomandările specifice, Comisia remarcă următoarele:

a) Comisia acceptă recomandarea 2a. Comisia propune subgrupului pentru securitate cibernetică al ICDT inițiative și servicii tehnice care să promoveze și să sprijine utilizarea unor instrumente comune pentru schimbul de informații sensibile, în cadrul unor servicii precum cele de mesagerie electronică și de videoconferință. De asemenea, observăm că subiectul marcajelor comune și al normelor comune de tratare a informațiilor sensibile neclasificate va fi abordat în propunerea de regulament privind securitatea informațiilor.

b) Comisia acceptă recomandarea 2b. Grupurile operative existente din cadrul subgrupului pentru securitate cibernetică al ICDT discută cu privire la acest aspect, care va aprofundat în continuare. Îmbunătățirile în ceea ce privește schimbul de informații privind achizițiile publice sunt abordate în contextul elaborării noului contract-cadru privind securitatea cibernetică.

c) Comisia acceptă recomandarea 2c. IOAUE au deja acces la contracte-cadru interinstituționale în domeniul tehnologiilor informației și comunicațiilor gestionate de Comisie. Elaborarea noului contract-cadru privind securitatea cibernetică va fi coordonată împreună cu subgrupul pentru securitate cibernetică al ICDT.

Recomandarea 3 – Intensificarea accentului pus de CERT-UE și de ENISA pe acele IOAUE mai puțin avansate în domeniul securității cibernetice

Această recomandare se adresează CERT-UE și ENISA.