

Bruxelles, 2 decembrie 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	2 decembrie 2020
Destinatar:	Delegațiile

Subiect:	Concluziile Consiliului privind securitatea cibernetică a dispozitivelor conectate
	- Concluziile Consiliului aprobate prin procedură scrisă

În anexă, se pun la dispoziția delegațiilor concluziile Consiliului privind securitatea cibernetică a dispozitivelor conectate, astfel cum au fost aprobate de Consiliu la 2 decembrie 2020, prin intermediul unei proceduri scrise.

Concluziile Consiliului privind securitatea cibernetică a dispozitivelor conectate

Consiliul Uniunii Europene,

REAMINTIND

- Concluziile Consiliului privind comunicarea comună către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetică puternice pentru UE”,
- Concluziile Consiliului privind consolidarea capacităților și a capabilităților în domeniul securității cibernetică în UE,
- Concluziile Consiliului privind importanța tehnologiei 5G pentru economia europeană și necesitatea de a atenua riscurile pentru securitate legate de tehnologia 5G,
- Concluziile Consiliului privind viitorul unei Europe cu un grad ridicat de digitalizare după 2020: „Stimularea competitivității digitale și economice în întreaga Uniune și a coeziunii digitale”,
- Concluziile Consiliului privind conturarea viitorului digital al Europei,
- Concluziile Consiliului European privind COVID-19, piața unică, politica industrială, dimensiunea digitală și relațiile externe,
- Comunicarea Comisiei Europene privind conturarea viitorului digital al Europei.

1. **SUBLINIAZĂ** că Uniunea Europeană și statele sale membre trebuie să își asigure suveranitatea digitală și autonomia strategică, menținând concomitent o economie deschisă. Acest lucru include o sporire a capacității de a face alegeri tehnologice autonome și, ca unul dintre pilonii principali, infrastructuri, produse și servicii reziliente și sigure pentru a consolida încrederea în piața unică digitală și în societatea europeană. Valorile fundamentale ale Uniunii Europene susțin în mod special viața privată, securitatea, egalitatea, demnitatea umană, statul de drept și internetul deschis drept condiții prealabile pentru realizarea unei societăți, a unei economii și a unei industrii centrate pe factorul uman și având drept vector domeniul digital.

2. RECUNOAȘTE importanța crescândă a dispozitivelor conectate și a securității acestora, inclusiv a echipamentelor, senzorilor și rețelelor care alcătuiesc internetul obiectelor. Dispozitivele conectate vor juca un rol-cheie în conturarea în continuare a viitorului digital al Europei, atât din punct de vedere industrial și comercial, cât și în viața de zi cu zi a consumatorilor unei noi generații de tehnologie. Pe lângă tehnologia 5G, inteligența artificială, informatica cuantică, calculul de înaltă performanță, cloud computing, tehnologiile registrelor distribuite, precum blockchain și orice alte noi aplicații, oportunitățile aflate în slujba unei creșteri economice durabile și a unui nivel mai ridicat de digitalizare a societății noastre pot fi accesate numai prin dispozitive conectate, securizate din punct de vedere cibernetic.
3. CONSTATĂ că utilizarea sporită a produselor de consum și a dispozitivelor industriale conectate la internet va genera totodată noi riscuri pentru protejarea vieții private, securitatea informațiilor și securitatea cibernetică, inclusiv un impact potențial tot mai mare asupra integrității și disponibilității produselor și datelor, care poate afecta în mod direct siguranța. Este esențial ca aceste riscuri să fie reduse cât mai mult posibil pentru a proteja consumatorii, a consolida reziliența cibernetică globală a Europei și a spori încrederea cetățenilor în soluțiile și tehnologiile digitale. Acest lucru va stimula, de asemenea, competitivitatea și capacitățile de inovare ale furnizorilor europeni de dispozitive de acest tip. Securitatea cibernetică și protejarea vieții private ar trebui recunoscute drept cerințe esențiale în procesele de inovare, producție și dezvoltare a produselor, inclusiv în faza de proiectare (securitatea de la stadiul conceperii), și ar trebui să fie asigurate pe parcursul întregului ciclu de viață al unui produs și de-a lungul întregului său lanț de aprovizionare.
4. EVIDENȚIAZĂ că, pe lângă asigurarea unui nivel ridicat de securitate a dispozitivelor conectate, este la fel de important să crească gradul de sensibilizare a consumatorilor cu privire la riscurile potențiale prezentate de acestea la adresa vieții private și a securității. Acest lucru ar contribui la reducerea la minimum a amenințărilor care decurg din utilizarea sporită a dispozitivelor conectate, ar spori încrederea în piața unică digitală și ar valorifica la maximum beneficiile economice și societale pe care le oferă tehnologiile dispozitivelor conectate.

5. SUBLINIAZĂ că investițiile publice în cercetare și inovare, în special prin programele Orizont Europa și Europa digitală, precum și investițiile private, ar putea genera stimulente valoroase pentru producerea unor dispozitive conectate mai sigure și mai securizate, sporind în consecință reziliența rețelelor de comunicații inteligente. De asemenea, ar trebui să fie accelerate investițiile în infrastructura și tehnologia digitală necesare pentru implementarea celor mai recente tehnologii pentru dispozitivele conectate, pentru a conferi poziția de lider în sectorul industrial și digital și pentru a asigura autonomia strategică, menținând concomitent o economie deschisă.
6. SUBLINIAZĂ nevoia de a asigura un nivel ridicat de complementaritate și comparabilitate a funcționalităților de securitate ale sistemelor TIC și ale componentelor TIC, care sunt utilizate în numeroase sectoare diferite ale pieței unice digitale.
7. RECUNOAȘTE evoluțiile actuale de la nivelul Uniunii vizând creșterea nivelului de securitate cibernetică a dispozitivelor conectate, în special în ceea ce privește inițiativele recente ale Comisiei de a aborda, pe termen scurt aspectele legate de securitatea cibernetică în actele juridice relevante, de exemplu actele din noul cadru legislativ, în special Directiva 2014/53/UE (Directiva privind echipamentele radio). SUBLINIAZĂ că este important să fie evaluată necesitatea unei legislații orizontale, care să specifice totodată condițiile necesare pentru introducerea pe piață, pe termen lung pentru a aborda toate aspectele relevante ale securității cibernetice a dispozitivelor conectate, cum ar fi disponibilitatea, integritatea și confidențialitatea. SALUTĂ, în acest sens, o discuție pe tema analizării domeniului de aplicare al unei astfel de legislații și a legăturilor sale cu cadrul de certificare a securității cibernetice, astfel cum este definit în Regulamentul privind securitatea cibernetică, cu scopul de a spori nivelul de securitate în interiorul pieței unice digitale.
8. SUBLINIAZĂ că cerințele în materie de securitate cibernetică ar trebui definite în conformitate cu legislația relevantă a Uniunii, inclusiv Regulamentul privind securitatea cibernetică, noul cadru legislativ, Regulamentul privind standardizarea europeană și o posibilă legislație orizontală viitoare, pentru a evita fragmentarea și ambiguitatea în cadrul legislației.

9. RECUNOAȘTE rolul important al tuturor părților interesate, în special al producătorilor, în sporirea nivelului de securitate cibernetică a dispozitivelor conectate pe piața unică digitală și, prin urmare, SOLICITĂ coordonarea și cooperarea strânsă cu toate părțile interesate relevante din sectorul public și din cel privat, inclusiv în perspectiva unei posibile legislații orizontale viitoare.
- 9a. SALUTĂ lucrările în curs de desfășurare conduse de ENISA vizând elaborarea primelor sisteme de certificare a securității cibernetice ale UE, respectiv criteriile comune propuse ale Uniunii Europene și sistemele propuse aplicabile furnizorilor de servicii cloud. Aceste sisteme vor constitui bazele relevante pentru certificarea dispozitivelor conectate.
10. EVIDENȚIAZĂ faptul că orice sistem de certificare suplimentar vizând dispozitivele conectate și serviciile conexe, care ar urma să fie prevăzut în programul de activitate etapizat la nivelul Uniunii și definit în cadrul Regulamentului privind securitatea cibernetică ar trebui să specifice modul în care ar trebui să fie îndeplinite cerințele de securitate aplicabile la nivelul de asigurare relevant pe baza unor standarde specifice recunoscute la nivel european și internațional, indiferent de sectorul în care urmează să fie utilizat produsul și să precizeze specificațiile de testare, certificatele etc. care urmează să fie aplicate.
11. RECUNOAȘTE că certificarea dispozitivelor conectate ar necesita norme, standarde sau specificații tehnice relevante pentru evaluările securității cibernetice în conformitate cu Regulamentul privind securitatea cibernetică. Prin urmare, SUBLINIAZĂ necesitatea de a stabili norme, standarde sau specificații tehnice în materie de securitate cibernetică pentru dispozitive conectate și RECOMANDĂ intensificarea eforturilor depuse de organizațiile europene de standardizare în această privință. În același timp, IA ACT de standardul ETSI EN 303 645 în materie de securitate cibernetică pentru dispozitivele de internet al obiectelor destinate consumatorilor, ca un pas important în această direcție.

12. INVITĂ Comisia Europeană să analizeze posibilitatea de a impune [...] propunerea de sisteme de certificare a securității cibernetice pentru dispozitive conectate și servicii conexe pe baza programului de lucru etapizat al Uniunii aflat în curs de elaborare, ținând seama în cea mai mare măsură de sistemele europene orizontale de certificare a securității cibernetice în curs de elaborare. Pe bază voluntară, un astfel de sistem va permite producătorilor de astfel de produse să promoveze produse cu un nivel de asigurare evaluat.
13. INVITĂ la o discuție privind modul în care obiectivul securității cibernetice ar putea fi ancorat într-o legislație orizontală viitoare privind riscurile în materie de securitate cibernetică aferente dispozitivelor conectate și IA ACT totodată de nevoia de a analiza adaptarea cerințelor esențiale ale directivelor relevante din noul cadru legislativ, acolo unde este cazul.
14. ÎNCURAJEAZĂ Comisia să evalueze totodată, acolo unde este necesar, reglementările sectoriale complementare care ar trebui să definească nivelul de securitate cibernetică care ar trebui să fie îndeplinit de dispozitivul conectat pentru a garanta faptul că sunt instituite cerințe specifice în materie de securitate și de protejare a vieții private pentru astfel de dispozitive cu riscuri de securitate mai ridicate.
15. SUBLINIAZĂ necesitatea de a îmbunătăți calitatea vieții și bunăstarea cetățenilor europeni și de a stimula încrederea în piața unică digitală. Securitatea și protejarea vieții private în cadrul societăților noastre sunt esențiale pentru susținerea valorilor noastre fundamentale ale Uniunii. Prin urmare, SUBLINIAZĂ că este necesară valorificarea cadrului oferit de Regulamentul privind securitatea cibernetică pentru a armoniza cerințele în materie de securitate, în funcție de diferitele niveluri de asigurare, în toate sectoarele din noul cadru legislativ, pentru a evita fragmentarea și verificările multiple ale unor cerințe identice și oferă condiții de concurență echitabile în întreaga Uniune Europeană pentru concurență și inovare.

16. INVITĂ Comisia, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Comitetul pentru evaluarea conformității și supravegherea pieței telecomunicațiilor și Grupul european pentru certificarea securității cibernetice (ECCG) să participe activ la această inițiativă de consolidare a pieței unice digitale și de sporire a încrederii în produsele, serviciile și procesele TIC pentru dispozitivele conectate prin asigurarea protejării vieții private și a securității cibernetice și să faciliteze creșterea competitivității la nivel mondial a industriei internetului obiectelor din Uniune prin asigurarea celor mai înalte standarde de reziliență, siguranță și securitate.
17. EVIDENȚIAZĂ, în acest context, necesitatea de a sprijini IMM-urile ca element esențial al ecosistemului european de securitate cibernetică și ÎNCURAJEAZĂ IMM-urile să participe la toate consultările publice lansate, precum și la activitățile de standardizare, pentru a se ține seama de contribuția valoroasă și importantă a acestora în ceea ce privește transformarea securității cibernetice într-un obiectiv accesibil, precum și într-un avantaj competitiv pe piața europeană.
18. CONSTATĂ că obligația de a asigura securitatea cibernetică și protejarea vieții private pe parcursul întregului ciclu de viață al unui produs și de-a lungul lanțului său de aprovizionare ar putea avea un impact pozitiv asupra amprentei ecologice a sectorului tehnologic, determinând producătorii să se orienteze către procese de dezvoltare și de producție inteligente și durabile, reducând astfel cantitatea de deșeuri electronice legate de eliminarea dispozitivelor conectate.
-