COMISIA
EUROPEANĂ

Bruxelles, 15.6.2023
C(2023) 4049 final

COMUNICARE A COMISIEI

Punerea în aplicare a setului de instrumente pentru securitatea cibernetică a rețelelor 5G

COMUNICARE A COMISIEI

Punerea în aplicare a setului de instrumente pentru securitatea cibernetică a rețelelor 5G

Securitatea rețelelor 5G este o prioritate majoră pentru Comisia Europeană. Aceste rețele constituie o infrastructură centrală care oferă baza pentru o gamă largă de servicii esențiale pentru funcționarea pieței interne și pentru întreținerea și exploatarea unor funcții societale și economice vitale. Pentru a proteja rețelele 5G, statele membre, cu sprijinul Comisiei și al Agenției UE pentru Securitate Cibernetică (ENISA), au identificat și evaluat în comun[1] amenințările și riscurile cibernetice și, pe această bază, au fost identificate o serie de măsuri cuprinzătoare pentru atenuarea acestor riscuri, sub forma setului de instrumente al UE pentru securitatea cibernetică a rețelelor 5G[2], adoptat în 2020 de Grupul de cooperare NIS și aprobat de Consiliul European și de Comisie.

În martie 2022, la Versailles, șefii de stat sau de guvern au decis să își asume o mai mare responsabilitate pentru securitatea noastră și să ia noi măsuri decisive în direcția consolidării suveranității noastre europene și a reducerii dependențelor noastre, inclusiv prin consolidarea rezilienței noastre cibernetice și prin protejarea infrastructurii – în special a infrastructurii noastre critice[3]. Punerea în aplicare a setului de instrumente al UE reprezintă o componentă vitală a Strategiei UE privind uniunea securității[4] și sprijină cadrul mai larg de politici europene în materie de autonomie strategică și reziliență sporită, precum și cadrul specific pentru protecția rețelelor de comunicații electronice și a altor infrastructuri critice[5], în special punerea în aplicare a articolului 40 din Codul european al comunicațiilor electronice, care prevede că „*operatorii trebuie să ia măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona în mod corespunzător riscurile la adresa securității rețelelor și serviciilor*”[6].

În cadrul setului de instrumente al UE, având în vedere obiectivul final de a asigura securitatea și reziliența rețelelor 5G și durabilitatea acestora, statele membre au convenit asupra necesității de a se evalua profilul de risc al furnizorilor individuali și, în consecință, de a se aplica restricții relevante pentru furnizorii care se consideră că prezintă un risc ridicat, inclusiv excluderi necesare pentru a se atenua efectiv riscurile, pentru activele-cheie, astfel cum se indică în setul de instrumente.

În conformitate cu evaluarea coordonată la nivelul UE a riscurilor, profilul de risc al furnizorilor individuali poate fi evaluat pe baza mai multor factori. Probabilitatea ca furnizorul să facă obiectul unei imixtiuni din partea unei țări din afara UE este prezentată ca unul dintre aspectele-cheie în

[1] Raportul privind o evaluare coordonată la nivelul UE a riscurilor în materie de securitate a rețelelor 5G, Grupul de cooperare NIS.
[2] Setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G, Grupul de cooperare NIS, 29 ianuarie 2020. Setul de instrumente al UE a fost adoptat de autoritățile naționale din domeniul securității cibernetice din statele membre și aprobat de Consiliul European și de Comisie.
[3] Reuniunea informală a șefilor de stat sau de guvern, Declarația de la Versailles, 10-11 martie 2022.
[4] Strategia UE privind uniunea securității, COM(2020) 605 final
[5] Setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G, Grupul de cooperare NIS, 29 ianuarie 2020. Setul de instrumente al UE a fost adoptat de autoritățile naționale din domeniul securității cibernetice din statele membre și aprobat de Consiliul European și de Comisie.
[6] Începând din octombrie 2024, această dispoziție se înlocuiește cu articolul 21 alineatul (1) din Directiva NIS2.

evaluarea vulnerabilităților fără caracter tehnic legate de rețelele 5G, aceasta putând fi facilitată de mai mulți factori, în special legătura dintre un furnizor și guvernul unei anumite țări terțe, legislația țării terțe și caracteristicile proprietății corporative a furnizorului.

Comisia ia act de adoptarea celui de Al doilea raport privind progresele înregistrate în ceea ce privește punerea în aplicare a setului de instrumente al UE de către Grupul de cooperare NIS și salută adoptarea acestuia.

În lumina acestui raport, Comisia își exprimă îngrijorarea profundă față de riscurile pe care anumiți furnizori de echipamente de comunicații prin rețele mobile le prezintă pentru securitatea Uniunii, astfel cum se reflectă și în deciziile luate de unele state membre. Raportul NIS subliniază „riscul clar de dependență persistentă de furnizori cu grad ridicat de risc pe piața internă, cu un potențial impact negativ grav asupra securității pentru utilizatorii și întreprinderile din întreaga UE și pentru infrastructura critică a UE".

Astfel cum se menționează în Raportul privind progresele înregistrate în domeniul NIS și într-un raport anterior al Curții de Conturi Europene[7], este evident că există diferențe clare între caracteristicile furnizorilor de tehnologie 5G, în special în ceea ce privește probabilitatea ca aceștia să fie influențați de anumite țări terțe în care există legi în materie de securitate și guvernanță corporativă ce reprezintă un risc potențial pentru securitatea Uniunii. Raportul NISA indică, de asemenea, că Huawei și ZTE au făcut obiectul unor decizii și recomandări publice în anumite state membre[8], ca urmare a preocupărilor legate de securitatea națională, inclusiv a evaluărilor efectuate de serviciile de informații ale statelor membre în cauză. În alte state membre, deciziile de restricționare sau de excludere a anumitor furnizori din rețelele lor 5G s-au luat în mod confidențial, pe baza evaluării acestora. Constatările acestor state membre sunt similare cu analiza autorităților competente din anumite țări terțe[9].

Având în vedere aceste riscuri ridicate și pe baza unei evaluări a criteriilor stabilite în setul de instrumente pentru identificarea „furnizorilor cu risc ridicat", Comisia consideră că deciziile adoptate de statele membre pentru a restricționa sau a exclude Huawei și ZTE sunt justificate și conforme cu setul de instrumente 5G. Fără a aduce atingere competențelor statelor membre în materie de securitate națională, Comisia a aplicat, de asemenea, criteriile din setul de instrumente pentru a evalua nevoile și vulnerabilitățile sistemelor de comunicații corporative proprii și ale celorlalte instituții, organisme și agenții europene, precum și punerea în aplicare a programelor de finanțare ale Uniunii din perspectiva obiectivelor generale de politică ale Uniunii.

În acest context, în conformitate cu aplicarea de către anumite state membre a setului de instrumente 5G, Comisia consideră că Huawei și ZTE prezintă, de fapt, riscuri semnificativ mai mari decât alți furnizori de 5G. Având în vedere criteriile din setul de instrumente, această evaluare efectuată de Comisie se bazează pe informațiile disponibile cu privire la:

1) evaluările naționale ale statelor membre ale UE și ale țărilor terțe în ceea ce privește riscurile prezentate de furnizori

[7] Raport special: securitatea rețelelor 5G (europa.eu)
[8] Al doilea raport privind progresele înregistrate în ceea ce privește punerea în aplicare a setului de instrumente al UE privind securitatea cibernetică a rețelelor 5G, 15 iunie 2023
[9] Huawei Designated Vendor Direction (publishing.service.gov.uk)

2) textele legislative și de reglementare relevante ale statelor membre ale UE și ale țărilor terțe referitoare la măsurile de abordare a riscurilor generate de furnizori;
3) raportul relevant al Curții de Conturi Europene;
4) probabilitatea unei ingerințe din partea guvernului unei țări din afara UE fără constrângeri juridice sau judiciare adecvate;
5) nivelul activităților răuvoitoare care afectează securitatea cibernetică a instituțiilor UE;
6) riscurile unei potențiale perturbări care să afecteze lanțul de aprovizionare cu echipamente 5G în contextul geopolitic actual;
7) prezența semnificativă a acestor furnizori în rețelele 5G ale UE.

Zece state membre și-au exercitat competențele pentru a impune obligații de restricționare sau de excludere a furnizorilor cu grad ridicat de risc din rețelele lor 5G. Având în vedere caracterul interconectat al rețelelor, Comisia îndeamnă statele membre care nu au pus încă în aplicare setul de instrumente să adopte de urgență măsuri relevante, astfel cum se recomandă în setul de instrumente al UE, pentru a aborda în mod eficace și rapid riscurile, ținând seama de ceea ce alte state membre au făcut deja în conformitate cu setul de instrumente, precum și de această evaluare.

Acestea trebuie să acționeze, de asemenea, ținând seama de riscurile legate de perturbările potențiale care afectează lanțul de aprovizionare al echipamentelor 5G, având în vedere contextul geopolitic actual și prezența semnificativă a acestor furnizori în rețelele 5G ale UE, care creează vulnerabilități puternice și o dependență pentru Uniune în ansamblu.

Comisia îndeamnă statele membre ca, atunci când pun în aplicare aceste măsuri, să țină seama cât de mult posibil și de recomandările din raportul NIS, în special în ceea ce privește domeniul de aplicare a restricțiilor, care ar trebui să acopere activele critice și extrem de sensibile identificate în evaluarea coordonată la nivelul UE a riscurilor, inclusiv rețeaua de acces radio, precum și în ceea ce privește utilizarea perioadelor de tranziție, care vor fi definite pentru a se garanta eliminarea echipamentelor existente în cel mai scurt timp posibil.

Comisia poate lua inițiative suplimentare pentru a sprijini punerea în aplicare cuprinzătoare a setului de instrumente 5G.

În plus, după cum s-a menționat anterior, Comisia este, de asemenea, preocupată de securitatea și confidențialitatea comunicărilor instituționale ale Comisiei și ale altor instituții, organisme și agenții ale UE. Comisia va lua măsuri pentru a evita expunerea comunicațiilor sale corporative la rețelele mobile ale căror furnizori sunt Huawei și ZTE, ca parte a politicii sale de securitate cibernetică corporativă și aplicând setului de instrumente pentru securitatea cibernetică a rețelelor 5G. Aceste măsuri vor include neachiziționarea de noi servicii de conectivitate care se bazează pe echipamente de la furnizorii respectivi, cu aplicarea condițiilor de securitate relevante. Comisia va colabora cu statele membre și cu operatorii de telecomunicații pentru a se asigura că furnizorii respectivi sunt eliminați treptat din serviciile de conectivitate existente ale site-urilor Comisiei.

Acest lucru se va aplica tuturor sediilor Comisiei, inclusiv sediilor principale, reprezentanțelor și birourilor sale din toate statele membre[10]. Comisia va încuraja alte instituții, organisme și agenții ale

[10] Inclusiv agențiile sale executive.

UE să ia măsuri similare. Comisia va lua măsurile necesare pentru a pune rapid în aplicare aceste decizii.

De asemenea, în conformitate cu competențele care îi revin în temeiul normelor de guvernanță respective, Comisia intenționează să reflecte această decizie în toate programele și instrumentele de finanțare relevante ale UE.

COPIE LEGALIZATĂ
Pentru Secretarul General

Martine DEPREZ
Director
Procesul decizional și colegialitatea
COMISIA EUROPEANA