COMISIA
EUROPEANĂ

Bruxelles, 4.10.2017
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Valorificarea la maximum a NIS – către punerea în aplicare eficace a Directivei (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune

Introducere

Directiva (UE) 2016/1148 privind securitatea rețelelor și a sistemelor informatice în Uniune[1] (denumită în continuare „Directiva NIS" sau „directiva"), adoptată la 6 iulie 2016, este primul act legislativ orizontal al UE care abordează provocările în materie de securitate cibernetică și constituie un punct de cotitură în ceea ce privește reziliența cibernetică și cooperarea în Europa.

Directiva are trei obiective principale:

- îmbunătățirea capacităților naționale în domeniul securității cibernetice;
- consolidarea cooperării la nivelul UE și
- promovarea unei culturi a gestionării riscurilor și a raportării incidentelor în rândul principalilor actori economici, în special operatorii care furnizează servicii esențiale pentru menținerea activităților economice și societale și furnizorii de servicii digitale.

Directiva NIS reprezintă piatra de temelie a răspunsului UE la amenințările cibernetice tot mai mari și la provocările care însoțesc procesul de digitalizare a vieții noastre economice și societale și, prin urmare, punerea sa în aplicare constituie o componentă importantă a pachetului din domeniul securității cibernetice prezentat la 13 septembrie 2017. Eficacitatea răspunsului UE este obstrucționată atât timp cât Directiva NIS nu este transpusă pe deplin în toate statele membre ale UE. Acest lucru a fost recunoscut, de asemenea, ca fiind un punct esențial în Comunicarea Comisiei din 2016 privind „Consolidarea sistemului de reziliență cibernetică al Europei"[2].

Noutatea Directivei NIS și necesitatea urgentă de a aborda peisajul amenințărilor cibernetice care evoluează rapid impun acordarea unei atenții speciale provocărilor cu care se confruntă toți actorii în ceea ce privește asigurarea transpunerii la timp și cu succes a directivei. Având în vedere termenul de transpunere, și anume 9 mai 2018, și termenul de identificare a operatorilor de servicii esențiale, și anume 9 noiembrie 2018, Comisia a sprijinit procesul de transpunere al statelor membre și activitatea desfășurată de acestea în cadrul Grupului de cooperare.

Prezenta comunicare și anexa la aceasta se bazează pe activitatea pregătitoare a Comisiei și pe analiza sa referitoare la punerea în aplicare până în prezent a Directivei NIS, pe contribuția Agenției Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și pe discuțiile purtate cu statele membre în etapa de transpunere a directivei, în special în cadrul Grupului de cooperare[3]. Prezenta comunicare vine în completarea eforturilor considerabile întreprinse până în prezent, în special prin:

[1] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Directiva a intrat în vigoare la 8 august 2016.
[2] COM(2016) 410 final.
[3] Un mecanism de cooperare strategică între statele membre prevăzut la articolul 11 din Directiva NIS.

- activitatea intensă a Grupului de cooperare, care a convenit asupra unui plan de lucru care vizează cu precădere transpunerea Directivei NIS și, în special, identificarea operatorilor de servicii esențiale și a obligațiilor care le revin acestora în materie de cerințe de securitate și de notificare a incidentelor. Deși directiva prevede o marjă de apreciere în ceea ce privește transpunerea dispozițiilor referitoare la operatorii de servicii esențiale, statele membre au recunoscut importanța unei abordări armonizate în această privință[4];
- instituirea și intrarea rapidă în funcțiune a rețelei formate din echipe de intervenție în caz de incidente de securitate informatică (CSIRT), în conformitate cu articolul 12 alineatul (1) din directivă. De atunci, această rețea a început să pună bazele pentru o cooperare operațională structurată la nivel european.

Atât pentru nivelul politic, cât și pentru nivelul operațional, reprezentat de aceste structuri, angajamentul deplin al tuturor statelor membre este esențial pentru îndeplinirea obiectivului de asigurare a unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

Prezenta comunicare şi anexa la aceasta vor consolida eforturile prin reunirea și compararea bunelor practici din statele membre care sunt relevante pentru punerea în aplicare a directivei, prin emiterea de orientări suplimentare cu privire la modul în care directiva ar trebui să fie pusă în aplicare și prin furnizarea de explicații mai detaliate referitoare la dispoziții specifice. Obiectivul global este de a sprijini statele membre să realizeze o punere în aplicare eficace și armonizată a Directivei NIS în întreaga UE.

Prezenta comunicare va fi completată în continuare de viitorul Regulament de punere în aplicare al Comisiei privind detalierea suplimentară a elementelor și a parametrilor referitori la cerințele de securitate și de notificare a incidentelor pe care trebuie să le respecte furnizorii de servicii digitale, în temeiul articolului 16 alineatul (8) din Directiva NIS. Regulamentul de punere în aplicare va facilita implementarea directivei în ceea ce privește obligațiile furnizorilor de servicii digitale[5].

Comunicarea prezintă principalele concluzii ale analizei aspectelor care sunt considerate drept puncte de referință importante și o potențială sursă de inspirație din perspectiva transpunerii în legislația națională. În acest caz, se acordă o atenție specială dispozițiilor referitoare la capacitățile și obligațiile statelor membre în ceea ce privește entitățile care intră în domeniul de aplicare al directivei. În anexă sunt analizate mai detaliat domeniile în care Comisia consideră că este cel mai util să furnizeze orientări practice de transpunere prin explicarea anumitor dispoziții ale directivei și prin prezentarea modului în care interpretează respectivele

[4] Grupul de cooperare lucrează în prezent la elaborarea unor documente de orientare de referință privind, printre altele: criteriile de definire a importanței vitale a unui operator în temeiul articolului 5 alineatul (2) din directivă, circumstanțele în care operatorii de servicii esențiale sunt obligați să notifice incidente în temeiul articolului 14 alineatul (7) din directivă și cerințele de securitate pentru operatorii de servicii esențiale, în conformitate cu articolul 14 alineatele (1) și (2).

[5] Proiectul de regulament de punere în aplicare este pus la dispoziția publicului pentru a formula observații la următoarea adresă: https://ec.europa.eu/info/law/better-regulation/have-your-say_ro

dispoziții, precum și prin prezentarea bunelor practici și a experienței acumulate până în prezent în ceea ce privește directiva.

Către punerea în aplicare eficace a Directivei NIS

Obiectivul Directivei NIS este de a realiza un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în UE. Acest lucru înseamnă îmbunătățirea securității internetului și a rețelelor private, precum și a sistemelor informatice pe care se bazează funcționarea societății și a economiei noastre. Primul element important în această privință este nivelul de pregătire al statelor membre care ar trebui să fie asigurat prin strategii naționale în domeniul securității cibernetice, astfel cum se menționează în directivă, prin activitatea CSIRTS și prin cea a autorităților naționale competente.

Caracterul cuprinzător al strategiilor naționale

Este important ca statele membre să valorifice oportunitatea oferită de transpunerea Directivei NIS pentru a-și revizui strategia națională de securitate cibernetică în lumina lacunelor, a bunelor practici și a noilor provocări abordate în anexă.

Deși, așa cum este de înțeles, directiva se concentrează asupra societăților și a serviciilor care sunt în mod special de importanță vitală, trebuie să se abordeze într-o manieră globală și coerentă securitatea cibernetică a economiei și a societății în ansamblul său, având în vedere dependența din ce în ce mai mare de TIC. În consecință, adoptarea unor strategii naționale cuprinzătoare care depășesc cerințele minime ale Directivei NIS (și anume, care acoperă mai multe sectoare și servicii decât cele enumerate în anexele II și III la directivă) ar spori nivelul general de securitate a rețelelor și a sistemelor informatice.

Întrucât securitatea cibernetică este încă un domeniu de politică publică relativ nou și care se extinde rapid, în majoritatea cazurilor sunt necesare investiții noi, chiar dacă situația globală a finanțelor publice impune reduceri și economii. Prin urmare, luarea de decizii ambițioase pentru a asigura resursele financiare și umane adecvate care sunt indispensabile în vederea unei puneri în aplicare eficace a strategiilor naționale, inclusiv punerea la dispoziția autorităților naționale competente și a CSIRT a unor resurse suficiente, este fundamentală pentru îndeplinirea obiectivelor directivei.

Eficacitatea punerii în aplicare a directivei și a asigurării respectării dispozițiilor acesteia

Necesitatea de a desemna autoritățile naționale competente și punctele unice de contact este subliniată la articolul 8 din directivă și este un element esențial pentru a se asigura o punere în aplicare eficace a Directivei NIS și cooperarea transfrontalieră. În această privință, în statele membre au apărut atât abordări mai centralizate, cât și mai descentralizate. Atunci când statele membre adoptă o abordare mai descentralizată în ceea ce privește desemnarea autorităților naționale competente, asigurarea unor acorduri de cooperare puternice între numeroasele autorități și punctul unic de contact s-a dovedit a fi esențială (*a se vedea tabelul 1 din secțiunea 3.2 din anexă*). Acest lucru ar spori eficacitatea punerii în aplicare a directivei și ar facilita asigurarea respectării dispozițiilor sale.

Valorificarea experienței anterioare în ceea ce privește protecția infrastructurilor critice de informații (CIIP) poate contribui la conceperea unui model optim de guvernanță pentru statele membre, asigurând atât punerea în aplicare sectorială eficace a Directivei NIS, cât și o abordare orizontală coerentă (*a se vedea secțiunea 3.1. din anexă*).

Consolidarea capacităților echipelor CSIRT naționale

Fără echipe CSIRT naționale eficace și care dispun de resurse adecvate în întreaga UE, astfel cum se prevede la articolul 9 din Directiva NIS, UE va rămâne prea vulnerabilă în fața amenințărilor cibernetice transfrontaliere. În consecință, statele membre ar putea lua în considerare extinderea sferei de acțiune a CSIRT și în alte sectoare și servicii decât cele care sunt incluse în domeniul de aplicare al directivei (*a se vedea secțiunea 3.3 din anexă*). Acest lucru ar permite echipelor CSIRT naționale să ofere sprijin operațional în cazul incidentelor cibernetice care au loc în întreprinderi și organizații care nu intră în domeniul de aplicare al directivei, dar care sunt, de asemenea, importante pentru societate și economie. În plus, statele membre ar putea să utilizeze pe deplin oportunitățile de finanțare suplimentară oferite de programul Mecanismului pentru interconectarea Europei (MIE) referitor la infrastructurile de servicii digitale (ISD) pentru securitatea cibernetică, menit să consolideze capacitățile echipelor CSIRT naționale și cooperarea dintre acestea (*a se vedea, de asemenea, capitolul 3.5 din anexă*).

Coerența procesului de identificare a operatorilor care furnizează servicii esențiale

În conformitate cu articolul 5 din Directiva NIS, statele membre au obligația de a identifica entitățile care vor fi considerate operatori de servicii esențiale până la data de 9 noiembrie 2018. În ceea ce privește această sarcină, statele membre ar putea lua în considerare utilizarea consecventă a definițiilor și a orientărilor incluse în prezenta comunicare pentru a se asigura că tipuri similare de entități care îndeplinesc un rol similar pe piața internă sunt identificate în mod coerent drept operatori de servicii esențiale în alte state membre. Statele membre ar putea, de asemenea, să ia în considerare extinderea domeniului de aplicare al Directivei NIS la administrațiile publice, având în vedere rolul pe care îl îndeplinesc acestea în societate și în economie în ansamblul său (*a se vedea secțiunile 2.1. și 4.1.3 din anexă*).

Alinierea abordărilor naționale cu privire la identificarea operatorilor de servicii esențiale în cea mai mare măsură posibilă, în special prin urmarea orientărilor elaborate de Grupul de cooperare (*a se vedea secțiunea 4.1.2 din anexă*) ar fi foarte utilă deoarece ar conduce la o aplicare mai uniformă a dispozițiilor directivei și ar reduce astfel riscul de fragmentare a pieței. În cazurile în care operatorii de servicii esențiale furnizează servicii esențiale în două sau mai multe state membre, este foarte important să se ajungă la un acord între statele membre în cadrul procesului de consultare prevăzut la articolul 5 alineatul (4) privind

identificarea coerentă a entităților (*a se vedea secțiunea 4.1.7 din anexă*), întrucât acest lucru ar permite evitarea unui tratament de reglementare diferit al aceleiași entități în diferitele jurisdicții ale statelor membre.

Transmiterea către Comisie a informațiilor privind identificarea operatorilor care furnizează servicii esențiale

În conformitate cu articolul 5 alineatul (7), statele membre au obligația de a transmite Comisiei informații cu privire la măsurile naționale care permit identificarea operatorilor de servicii esențiale, lista de servicii esențiale, numărul de operatori de servicii esențiale identificați și relevanța acestora pentru sector. În plus, statele membre trebuie să furnizeze limitele, dacă acestea există, utilizate în procesul de identificare pentru determinarea nivelului relevant de furnizare sau importanța unui anumit operator pentru menținerea unui nivel suficient al furnizării. Statele membre ar putea lua în considerare, de asemenea, transmiterea către Comisie a listelor de operatori de servicii esențiale identificați, dacă este necesar cu titlu confidențial, deoarece acest lucru ar contribui la îmbunătățirea exactității și a calității evaluării efectuate de Comisie (*a se vedea secțiunile 4.1.5. și 4.1.6. din anexă*).

Abordări aliniate privind cerințele de securitate și de notificare a incidentelor pe care trebuie să le respecte operatorii de servicii esențiale

În ceea ce privește obligațiile referitoare la cerințele de securitate și de notificare a incidentelor pe care trebuie să le respecte operatorii de servicii esențiale [articolul 14 alineatele (1), (2) și (3)], o abordare aliniată privind cerințele de securitate și de notificare a incidentelor pentru a facilita conformitatea la nivel transfrontalier a operatorilor de servicii esențiale în statele membre ale UE ar promova în cea mai mare măsură posibilă un efect de piață unică. În acest domeniu, referința rămâne activitatea desfășurată în cadrului Grupului de cooperare privind elaborarea unui document de orientare (*a se vedea secțiunile 4.2. și 4.3. din anexă*).

În cazul unui atac informatic pe scară largă care afectează mai multe state membre, este foarte probabil ca notificarea obligatorie a incidentelor să fie transmisă de un operator de servicii esențiale sau de un furnizor de servicii digitale în temeiul articolului 14 alineatul (3) și al articolului 16 alineatul (3) sau de o altă entitate care nu intră în domeniul de aplicare al directivei, în mod voluntar, în temeiul articolului 20 alineatul (1). În conformitate cu Recomandarea Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare, statele membre ar putea lua în considerare alinierea abordărilor lor naționale, astfel încât să poată furniza în cel mai scurt timp posibil informații relevante pe baza acestor notificări către autoritățile competente sau CSIRT din alte state membre vizate. Informațiile fiabile și exacte ar fi esențiale pentru reducerea numărului de infectări sau abordarea vulnerabilităților înainte ca acestea să fie exploatate.

În spiritul parteneriatului pentru valorificarea la maximum a Directivei NIS, Comisia intenționează să extindă sprijinul acordat în cadrul Mecanismului pentru interconectarea Europei la toate părțile interesate relevante în temeiul acestui act legislativ. Dacă până acum s-a pus accentul pe consolidarea capacităților CSIRT și pe instituirea unei platforme pentru

cooperarea operațională rapidă și eficace, contribuind astfel la consolidarea rețelei CSIRT, acum Comisia va examina modul în care de finanțarea acordată în cadrul Mecanismului pentru interconectarea Europei pot să beneficieze, de asemenea, autoritățile naționale competente, precum și operatorii de servicii esențiale și furnizorii de servicii digitale.

Concluzie

Având în vedere termenul de transpunere a Directivei NIS în legislația națională, și anume 9 mai 2018, și având în vedere termenul de identificare a operatorilor de servicii esențiale, și anume 9 noiembrie 2018, statele membre ar trebui să ia măsurile corespunzătoare pentru a se asigura că dispozițiile și modelele de cooperare prevăzute în Directiva NIS pot oferi instrumentele cele mai bune posibil la nivelul UE pentru a realiza un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Comisia invită statele membre să țină seama, în cadrul acestui proces, de informațiile, orientările și recomandările relevante prevăzute în prezenta comunicare.

Prezenta comunicare poate fi completată în continuare prin alte acțiuni, inclusiv cele generate ca urmare a activității care este în curs de desfășurare în cadrul Grupului de cooperare.