RECOMANDĂRI

RECOMANDAREA (UE) 2019/553 A COMISIEI

din 3 aprilie 2019

privind securitatea cibernetică în sectorul energetic

[notificată cu numărul C(2019) 2400]

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 292,

întrucât:

(1) Sectorul energetic european trece printr-o tranziție importantă către o economie decarbonizată, asigurând în același timp securitatea aprovizionării și competitivitatea. Ca parte a acestei tranziții energetice și a descentralizării aferente a producției de energie din surse regenerabile, progresul tehnologic, cuplarea sectorială și digitalizarea transformă rețeaua electrică a Europei într-o „rețea inteligentă". În același timp, acest lucru generează noi riscuri, pe măsură ce digitalizarea expune din ce în ce mai mult sistemul energetic la atacuri cibernetice și la incidente care pot pune în pericol securitatea aprovizionării cu energie.

(2) Adoptarea tuturor celor opt propuneri legislative ([1]) ale pachetului „Energie curată pentru toți europenii", care include Regulamentul privind guvernanța uniunii energetice ca piatră de temelie, permite crearea unui mediu favorabil transformării digitale a sectorului energetic. De asemenea, prin aceasta se recunoaște importanța securității cibernetice în sectorul energetic. În special, reformarea Regulamentului privind piața internă a energiei electrice ([2]) prevede adoptarea unor norme tehnice pentru energia electrică, cum ar fi un cod de rețea privind normele sectoriale pentru aspectele de securitate cibernetică a fluxurilor transfrontaliere de energie electrică, cerințele minime comune, planificarea, monitorizarea, raportarea și gestionarea crizelor. Regulamentul privind nivelul de pregătire pentru riscuri în domeniul energiei electrice ([3]) urmează, în linii mari, abordarea aleasă în Regulamentul privind securitatea aprovizionării cu gaze naturale ([4]); el subliniază necesitatea de a evalua în mod corespunzător toate riscurile, inclusiv cele legate de securitatea cibernetică, și propune adoptarea de măsuri de prevenire și de atenuare a riscurilor identificate.

(3) Atunci când a adoptat Strategia de securitate cibernetică a UE ([5]) în 2013, Comisia a identificat consolidarea rezilienței cibernetice a Uniunii ca o prioritate. Unul dintre principalele rezultate ale strategiei este Directiva privind securitatea rețelelor și a sistemelor informatice ([6]) (denumită în continuare „Directiva NIS"), care a fost adoptată în iulie 2016. În calitate de prim act legislativ orizontal al UE privind securitatea cibernetică, Directiva NIS sporește nivelul global al securității cibernetice în Uniune prin dezvoltarea capacităților naționale în materie de securitate cibernetică, intensificarea cooperării la nivelul UE și introducerea unor obligații de raportare în materie de securitate și incidente pentru societăți, denumite „operatori de servicii esențiale". Raportarea incidentelor este obligatorie în sectoare-cheie, inclusiv în sectorul energetic.

([1]) Directiva (UE) 2018/2001 a Parlamentului European și a Consiliului din 11 decembrie 2018 privind promovarea utilizării energiei din surse regenerabile (JO L 328, 21.12.2018, p. 82); Directiva (UE) 2018/2002 a Parlamentului European și a Consiliului din 11 decembrie 2018 de modificare a Directivei 2012/27/UE privind eficiența energetică (JO L 328, 21.12.2018, p. 210); Regulamentul (UE) 2018/1999 al Parlamentului European și al Consiliului din 11 decembrie 2018 privind guvernanța uniunii energetice și a acțiunilor climatice, de modificare a Regulamentelor (CE) nr. 663/2009 și (CE) nr. 715/2009 ale Parlamentului European și ale Consiliului, a Directivelor 94/22/CE, 98/70/CE, 2009/31/CE, 2009/73/CE, 2010/31/UE, 2012/27/UE și 2013/30/UE ale Parlamentului European și ale Consiliului, a Directivelor 2009/119/CE și (UE) 2015/652 ale Consiliului și de abrogare a Regulamentului (UE) nr. 525/2013 al Parlamentului European și al Consiliului (JO L 328, 21.12.2018, p. 1); Directiva (UE) 2018/844 a Parlamentului European și a Consiliului din 30 mai 2018 de modificare a Directivei 2010/31/UE privind performanța energetică a clădirilor și a Directivei 2012/27/UE privind eficiența energetică (JO L 156, 19.6.2018, p. 75). În cadrul sesiunii plenare din martie 2019, Parlamentul European a confirmat acordurile politice la care s-a ajuns cu Consiliul cu privire la propunerile de organizare a pieței energiei electrice [Regulamentul privind pregătirea pentru riscuri, Regulamentul de instituire a Agenției pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (ACER), Directiva privind energia electrică și Regulamentul privind energia electrică]. Adoptarea oficială de către Consiliu este prevăzută pentru luna aprilie; textul juridic va fi publicat ulterior în JO.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Regulamentul (UE) 2017/1938 al Parlamentului European și al Consiliului din 25 octombrie 2017 privind măsurile de garantare a siguranței furnizării de gaze și de abrogare a Regulamentului (UE) nr. 994/2010 (JO L 280, 28.10.2017, p. 1).

([5]) JOIN(2013) 1.

([6]) 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 (JO L 194, 19.7.2016, p. 1).

(4) La punerea în aplicare a măsurilor de pregătire în domeniul securității cibernetice, părțile interesate relevante, inclusiv operatorii de servicii esențiale din domeniul energetic, astfel cum sunt identificați în temeiul Directivei NIS, ar trebui să țină seama de orientările orizontale emise de Grupul de cooperare privind NIS, instituit în temeiul articolului 11 din Directiva NIS. Acest grup de cooperare, format din reprezentanți ai statelor membre, ai Agenției europene pentru Securitate Cibernetică (denumită în continuare „ENISA") și ai Comisiei, a adoptat documente de orientare privind măsurile de securitate și privind notificarea incidentelor. În iunie 2018, acest grup a creat un flux de lucru specific privind energia.

(5) Comunicarea comună din 2017 privind securitatea cibernetică ([7]) recunoaște importanța considerentelor și a cerințelor specifice sectorului la nivelul UE, inclusiv a celor din sectorul energetic. Securitatea cibernetică și posibilele implicații în materie de politică au făcut obiectul unor ample runde de discuții în Uniune în ultimii ani. Prin urmare, în prezent, este tot mai evident faptul că anumite sectoare economice se confruntă cu probleme de securitate cibernetică specifice și, prin urmare, trebuie să își dezvolte propriile abordări sectoriale în contextul mai larg al strategiilor generale de securitate cibernetică.

(6) Schimbul de informații și încrederea reprezintă elemente esențiale în securitatea cibernetică. Comisia își propune să intensifice schimbul de informații între părțile interesate relevante prin organizarea de evenimente specifice (cum ar fi, de exemplu, masa rotundă la nivel înalt privind securitatea cibernetică în domeniul energiei, organizată la Roma în martie 2017, și conferința la nivel înalt privind securitatea cibernetică în domeniul energiei, organizată la Bruxelles în octombrie 2018). De asemenea, Comisia dorește să consolideze cooperarea dintre părțile interesate relevante și entități specializate, cum ar fi Centrul european de schimb de informații și de analiză în domeniul energiei.

(7) Regulamentul privind ENISA („Agenția UE pentru Securitate Cibernetică") și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Regulamentul privind securitatea cibernetică" ([8])) consolidează mandatul Agenției UE pentru Securitate Cibernetică, astfel încât aceasta să sprijine mai eficient statele membre în combaterea amenințărilor și atacurilor cibernetice. Regulamentul creează, de asemenea, un cadru european în materie de securitate cibernetică pentru certificarea produselor, proceselor și serviciilor, care va fi valabil în întreaga Uniune și care prezintă un interes deosebit pentru sectorul energetic.

(8) Comisia a prezentat o recomandare ([9]) privind riscurile în materie de securitate cibernetică privind tehnologiile de rețea de a 5-a generație (5G) prin stabilirea unor orientări privind analiza de risc și măsuri de gestionare adecvate la nivel național, privind elaborarea unei analize de risc coordonate la nivel european și privind stabilirea unui proces de elaborare a unui set comun de măsuri de gestionare a riscurilor. Odată desfășurate, rețelele 5G vor constitui coloana vertebrală a unei game largi de servicii esențiale pentru funcționarea pieței interne și pentru funcții societale și economice vitale, cum ar fi furnizarea de energie.

(9) Prezenta recomandare ar trebui să ofere o orientare neexhaustivă pentru statele membre și părțile interesate relevante, în special pentru operatorii de rețea și furnizorii de tehnologie, pentru atingerea unui nivel mai ridicat de securitate cibernetică în sectorul energetic din punctul de vedere al cerințelor specifice în timp real, având în vedere cerințele specifice identificate pentru sectorul energetic, efectele în cascadă și combinația de tehnologii tradiționale cu cele de ultimă generație. Prezentele orientări își propun să ajute părțile interesate să țină seama de cerințele specifice ale sectorului energetic atunci când pun în aplicare standarde de securitate cibernetică recunoscute la nivel internațional ([10]).

(10) Comisia intenționează să revizuiască periodic prezenta recomandare, pe baza progreselor înregistrate în întreaga Uniune, în consultare cu statele membre și cu părțile interesate relevante. Comisia își va continua eforturile de consolidare a securității cibernetice în sectorul energetic, în special prin intermediul Grupului de cooperare privind NIS, care asigură cooperarea strategică și schimbul de informații între statele membre în domeniul securității cibernetice,

ADOPTĂ PREZENTA RECOMANDARE:

OBIECT

(1) Prezenta recomandare stabilește principalele aspecte legate de securitatea cibernetică în sectorul energetic, mai precis cerințele în timp real, efectele în cascadă și combinația de tehnologii vechi și de ultimă generație, și identifică principalele acțiuni pentru punerea în aplicare a măsurilor relevante de pregătire în materie de securitate cibernetică în sectorul energetic.

([7]) JOIN(2017) 450.

([8]) Legea privind securitatea cibernetică a fost adoptată de Parlamentul European în martie 2019. Adoptarea oficială de către Consiliu este prevăzută pentru luna aprilie; textul juridic va fi publicat ulterior în Jurnalul Oficial.

([9]) C(2019)2335.

([10]) Organizațiile internaționale de standardizare au publicat diverse standarde de securitate cibernetică (ISO/IEC 27000: Tehnologia informației) și de gestionare a riscurilor (ISO/IEC 31000: Implementarea managementului riscului). Un standard specific pentru sectorul energetic (ISO/IEC 27019: Controalele privind securitatea informațiilor pentru industria de utilități energetice) a fost publicat ca parte a seriei ISO/IEC 27000 în octombrie 2017.

(2) În aplicarea prezentei recomandări, statele membre ar trebui să încurajeze părțile interesate relevante să dezvolte cunoștințe și competențe legate de securitatea cibernetică în sectorul energetic. Dacă este cazul, statele membre ar trebui să includă aceste considerații și în cadrul lor național de securitate cibernetică, în special prin strategii, acte cu putere de lege, acte administrative și alte dispoziții administrative.

CERINȚE ÎN TIMP REAL PENTRU COMPONENTELE INFRASTRUCTURII ENERGETICE

(3) statele membre ar trebui să se asigure că părțile interesate relevante, în special operatorii de rețele de energie și furnizorii de tehnologie, în special operatorii de servicii esențiale identificați în temeiul Directivei NIS, pun în aplicare măsurile relevante de pregătire în materie de securitate cibernetică referitoare la cerințele în timp real din sectorul energetic. Unele elemente ale sistemului energetic trebuie să funcționeze în „timp real", adică să reacționeze la comenzi în câteva milisecunde, ceea ce face dificilă sau chiar imposibilă introducerea unor măsuri de securitate cibernetică, din lipsă de timp.

(4) În special, operatorii de rețele energetice ar trebui:

(a) să aplice cele mai recente standarde de securitate pentru instalațiile noi ori de câte ori este necesar și să ia în considerare măsuri complementare de securitate fizică în cazul în care baza instalată a instalațiilor vechi nu poate fi suficient protejată prin mecanismele de securitate cibernetică;

(b) să pună în aplicare standardele internaționale în materie de securitate cibernetică și standardele tehnice specifice adecvate pentru a asigura o comunicare securizată, în timp real, de îndată ce produsele respective devin disponibile pe piață;

(c) să ia în considerare constrângerile în timp real ale conceptului general de securitate pentru active, în special în ceea ce privește clasificarea activelor.

(d) să examineze rețelele private pentru sisteme de teleprotecție, pentru a asigura nivelul de calitate a serviciilor necesar pentru constrângerile în timp real. Atunci când utilizează rețele publice de comunicații, operatorii ar trebui să aibă în vedere asigurarea unei alocări specifice a lărgimilor de bandă, a unor cerințe privind timpul de așteptare și a unor măsuri de securitate a comunicării.

(e) să divizeze sistemul global în zone logice și, în interiorul fiecărei zone, să definească constrângerile de timp și de proces pentru a permite aplicarea unor măsuri de securitate cibernetică adecvate sau să aibă în vedere metode de protecție alternative.

(5) Dacă este posibil, operatorii de rețele energetice ar trebui:

(a) să aleagă un protocol securizat de comunicare, având în vedere cerințele în timp real, de exemplu între o instalație și sistemele sale de gestionare (sistemul de gestionare a energiei – EMS/sistemul de gestionare a distribuției – DMS);

(b) să introducă un mecanism adecvat de autentificare pentru comunicarea dintre mașini, pentru a răspunde cerințelor în timp real.

EFECTE ÎN CASCADĂ

(6) Statele membre ar trebui să se asigure că părțile interesate relevante, în special operatorii de rețele de energie și furnizorii de tehnologie, în special operatorii de servicii esențiale identificați în temeiul Directivei NIS, pun în aplicare măsurile relevante de pregătire în materie de securitate cibernetică referitoare la efectele în cascadă din sectorul energetic. Rețelele de energie electrică și conductele de gaze sunt puternic interconectate în întreaga Europă, iar un atac cibernetic care ar provoca o întrerupere sau o perturbare într-o parte a sistemului energetic ar putea declanșa efecte în cascadă ample și în alte părți ale sistemului.

(7) În aplicarea prezentei recomandări, statele membre ar trebui să evalueze interdependențele și caracterul critic ale sistemelor de producere a energiei electrice și ale sistemelor de cerere flexibilă, ale substațiilor și liniilor de transport și de distribuție, precum și ale părților interesate asociate afectate (inclusiv situațiile transfrontaliere) în cazul unui atac cibernetic sau al unui incident cibernetic reușit. De asemenea, statele membre ar trebui să se asigure că operatorii de rețele energetice dispun de un cadru de comunicare cu toate părțile interesate cheie pentru a partaja semnalele de alertă timpurie și pentru a coopera în domeniul gestionării crizelor. Ar trebui să existe canale de comunicare structurate și formate convenite pentru schimbul de informații sensibile cu toate părțile interesate relevante, cu echipele de intervenție în caz de incidente de securitate cibernetică și cu autoritățile relevante.

(8) În special, operatorii de rețele energetice ar trebui:

(a) să se asigure că noile dispozitive, inclusiv dispozitivele care fac parte din internetul obiectelor, au și își vor menține un nivel de securitate cibernetică adaptat la caracterul critic al fiecărui sit;

(b) să ia în considerare în mod adecvat efectele ciber-fizice atunci când elaborează și revizuiesc periodic planurile de asigurare a continuității activității;

(c) să stabilească criterii de proiectare și o arhitectură pentru o rețea rezilientă, care ar putea fi realizate prin:

— punerea în aplicare a unor măsuri de apărare detaliate pentru fiecare sit, adaptate la caracterul critic al sitului;

— identificarea nodurilor critice, atât în ceea ce privește capacitatea de producție de energie, cât și în ceea ce privește impactul asupra clienților. Funcțiile critice ale unei rețele ar trebui să fie concepute pentru a reduce riscurile care pot provoca efecte în cascadă, prin luarea în considerare a redundanței, a rezistenței la variațiile de fază și a protecției împotriva întreruperilor de sarcină în cascadă;

— colaborarea cu alți operatori relevanți și cu furnizori de tehnologie pentru a preveni efectele în cascadă prin aplicarea de măsuri și servicii adecvate;

— proiectarea și construirea de rețele de comunicații și de control, cu scopul de a limita efectele eventualelor defecțiuni fizice și logice la anumite părți ale rețelelor și de a asigura măsuri de atenuare adecvate și rapide.

TEHNOLOGIA TRADIȚIONALĂ ȘI CEA DE ULTIMĂ GENERAȚIE

(9) Statele membre ar trebui să se asigure că părțile interesate relevante, în special operatorii de rețele de energie și furnizorii de tehnologie, dar mai ales operatorii de servicii esențiale identificați în temeiul Directivei NIS, pun în aplicare măsurile relevante de pregătire în materie de securitate cibernetică legate de combinația de tehnologii tradiționale și de ultimă generație din sectorul energetic. Într-adevăr, în sistemul energetic actual coexistă două tipuri de tehnologii: o tehnologie mai veche, cu o durată de viață de 30-60 de ani, concepută înainte de apariția considerațiilor legate de securitatea cibernetică, și echipamente moderne, care reflectă digitalizarea și dispozitivele inteligente de ultimă oră.

(10) În aplicarea prezentei recomandări, statele membre ar trebui să încurajeze operatorii de rețele energetice și furnizorii de tehnologii să respecte, ori de câte ori este posibil, standardele relevante acceptate la nivel internațional în materie de securitate cibernetică. Între timp, părțile interesate și clienții ar trebui să adopte o abordare orientată către securitatea cibernetică în momentul conectării dispozitivelor la rețea.

(11) În special, furnizorii de tehnologie ar trebui să ofere în mod gratuit soluții testate pentru problemele de securitate legate de tehnologiile existente sau de cele noi, de îndată ce o problemă de securitate relevantă devine cunoscută.

(12) În special, operatorii de rețele energetice ar trebui:

(a) să analizeze riscurile legate de conectarea tehnologiei tradiționale cu cea a internetului obiectelor și să fie conștienți de interfețele interne și externe și de vulnerabilitățile acestora.

(b) să ia măsuri adecvate împotriva atacurilor care provin de la un număr mare de dispozitive sau aplicații ale consumatorilor aflate sub control rău intenționat;

(c) să instituie o capacitate automată de monitorizare și de analiză pentru evenimentele legate de securitate în mediul tradițional și în cel al internetului obiectelor, cum ar fi încercările nereușite de conectare, alarmele de semnalizare a deschiderii ușilor cabinetelor etc.

(d) să efectueze periodic o analiză a riscurilor specifice în materie de securitate cibernetică pentru toate instalațiile tradiționale, în special atunci când conectează tehnologii vechi și noi; întrucât instalațiile tradiționale reprezintă adesea un număr foarte mare de elemente, analiza riscurilor ar putea fi efectuată pe clase de elemente;

(e) să actualizeze la versiunea cea mai recentă elementele software și hardware ale sistemelor tradiționale și ale internetului obiectelor, ori de câte ori acest lucru este adecvat; în acest sens, operatorii de rețele energetice ar trebui să aibă în vedere măsuri complementare, cum ar fi segregarea sistemului sau adăugarea de bariere de securitate externe în cazul în care corectarea sau actualizarea ar fi adecvate, dar nu sunt posibile, de exemplu, pentru produsele care nu beneficiază de suport;

(f) să prezinte oferte care să ia în considerare securitatea cibernetică (și anume, să solicite informații cu privire la elementele de securitate și respectarea standardelor de securitate cibernetică existente, să se asigure că se propun în permanență măsuri de alertă, de corectare și de atenuare în cazul descoperirii de vulnerabilități și să clarifice răspunderea vânzătorului în caz de atacuri cibernetice sau incidente);

(g) să colaboreze cu furnizorii de tehnologie pentru a înlocui sistemele tradiționale ori de câte ori acest lucru este benefic din motive de securitate, dar să ia în considerare funcționalitățile critice ale sistemului.

MONITORIZARE

(13) Statele membre ar trebui să comunice Comisiei, în termen de 12 luni de la adoptarea prezentei recomandări și, ulterior, din doi în doi ani, informații detaliate privind stadiul punerii în aplicare a prezentei recomandări prin intermediul Grupului de cooperare privind NIS.

REVIZUIRE

(14) Pe baza informațiilor prezentate de statele membre, Comisia va revizui punerea în aplicare a prezentei recomandări și va evalua dacă sunt necesare măsuri suplimentare, după caz, în consultare cu statele membre și cu părțile interesate relevante.

DESTINATARI

(15) Prezenta recomandare se adresează statelor membre.

Adoptată la Bruxelles, 3 aprilie 2019.

Pentru Comisie
Miguel ARIAS CAÑETE
Membru al Comisiei