DEPARTAMENTUL DE STUDII PARLAMENTARE ŞI POLITICI UE

DIRECŢIA STUDII ŞI DOCUMENTARE LEGISLATIVĂ

LEGISLAȚIA ÎN DOMENIUL SECURITĂȚII CIBERNETICE ȘI INSTITUȚIILE DE RĂSPUNS LA INCIDENTELE DE SECURITATE CIBERNETICĂ ÎN UNIUNEA EUROPEANĂ – ASPECTE COMPARATIVE

septembrie 2024

Documentare și sinteză: Aurora Trănescu
consilier parlamentar, Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

CUPRINS

INTRODUCERE

Un centru de operațiuni de securitate (**Security Operation Center** - **SOC**) poate fi definit ca o structură care furnizează un serviciu de detectare a incidentelor prin observarea evenimentelor tehnice din rețele și sisteme informatice și poate fi, de asemenea, responsabil de reacția la incidente și de gestionarea acestora. În organizațiile mari, SOC-urile se concentrează, uneori, doar pe serviciile de monitorizare și de detectare după care predau gestionarea incidentelor unei echipe CSIRT[1] separate. În organizațiile și entitățile mai mici mai mici, CSIRT-urile și SOC-urile sunt adesea considerate cvasi-sinonime.

De obicei, echipele SOC operează în locații specifice, unde analiștii stau la stațiile de lucru în fața unui display video care proiectează un rezumat al situației curente (riscuri, amenințări etc). Echipele SOC au evoluat, de obicei, din echipele de securitate din domeniul tehnologiei informației (IT) care își automatizează activitatea prin utilizarea SIEM (Security Information and Event Management) și a altor tehnologii de automatizare și orchestrare a securității pentru monitorizarea securității. De obicei, echipele SOC își concentrează indicatorii-cheie de performanță (KPI) în jurul indicatorilor de calitate - viteza de detectare, amploarea detecției, acoperirea, ratele fals-pozitive - precum și al incidentelor gestionate, raportul alerte/evenimente/incidente, numărul de escaladări și volumul de muncă per incident.

Pe lângă funcționarea fizică, SOC-urile pot fi formate din personal virtual și externalizat sau dintr-un model hibrid de personal intern și externalizat. Este o practică obișnuită ca, de-a lungul timpului, SOC-urile să alterneze între operațiunile externalizate și cele interne.

Termenul **CSIRT** (**Computer Security Incident Response Team**) sau echipă de răspuns la incidente de securitate cibernetică, a fost stabilit în anii 1990. CSIRT-urile sunt cunoscute și sub numele de CIRT-uri (Computer Incident Response Teams), CERT-uri (Computer Emergency Response Teams), SIRT (Security Incident Response Teams) etc. Echipele naționale pot fi denumite și Centre naționale de securitate cibernetică (NCSC), cărora, prin lege, li se atribuie de regulă rolul unui CSIRT, precum și furnizarea de servicii suplimentare pentru națiune (de exemplu, gestionarea sistemelor de clasificare a informațiilor unei țări). Fiecare echipă își alege numele în funcție de preferința organizației.

CSIRT a devenit un nume generic pentru o echipă care furnizează un set de servicii cu un caracter aparte, și anume: informații și gestionarea incidentelor de securitate cibernetică (ca serviciu de bază), monitorizarea securității, gestionarea vulnerabilităților, conștientizarea situației și gestionarea cunoștințelor de securitate cibernetică.

În termeni simpli, un CSIRT este o echipă însărcinată cu gestionarea incidentelor de securitate informatică (denumită adesea, securitate cibernetică). Adesea, aceasta include responsabilități suplimentare, de la detectare la analiza și chiar repararea practică, precum și diferite activități de cunoaștere a situației, de transfer de cunoștințe și activități de

[1] Echipă de răspuns la incidente de securitate cibernetică în engleză: *computer security incident response team* (CSIRT)

gestionare a vulnerabilităților. De-a lungul anilor, rolul CSIRT[2] a evoluat de la furnizarea de servicii de monitorizare și gestionare a incidentelor la coordonarea și comunicare cu diferite părți interesate, țări și sectoare specifice.

În noiembrie 1988, un incident de securitate informatică cunoscut sub numele de „viermele internetului" a afectat părți importante ale internetului. Reacția la acest incident a fost izolată și necoordonată, ceea ce a dus la dublarea multor eforturi și la soluții contradictorii. Câteva săptămâni mai târziu, a fost înființat Centrul de coordonare CERT[3]. La scurt timp după aceea, Departamentul pentru Energie al Statelor Unite a înființat echipa denumită Computer Incident Advisory Capability (CIAC) pentru a-și deservi clienții.

În următorii doi ani, numărul echipelor de răspuns la incidente a continuat să crească, fiecare având propriul său scop, finanțare, cerințe de raportare și grup de interese. Interacțiunea dintre aceste echipe a întâmpinat dificultăți din cauza diferențelor de limbă, fus orar și standarde sau convenții internaționale. În octombrie 1989, un incident major numit „viermele Wank" a evidențiat necesitatea unei mai bune comunicări și coordonări între echipe.

Forumul echipelor de răspuns la incidente și de securitate (Forum of Incident Response and Security Teams FIRST) a fost creat în 1990 ca răspuns la această problemă. De atunci, acesta a continuat să crească și să evolueze ca răspuns la nevoile în schimbare ale echipelor de securitate și de răspuns la incidente și ale grupurilor lor de interese.

Până în 2002, internetul a crescut de la 60 000 de sisteme informatice gazdă la 150 de milioane (în aproape toate țările lumii). Multe întreprinderi se bazează în prezent pe internet în tranzacțiile lor zilnice. Membrii FIRST sunt echipe dintr-o mare varietate de organizații, inclusiv organizații educaționale, comerciale, furnizori, guvernamentale și militare. FIRST coagulează comunitatea globală de răspuns la incidente, având mai mult de 700 de membri, răspândiți în Africa, America, Asia, Europa și Oceania.

---

[2] Un CSIRT se poate concentra pe soluționarea incidentelor, cum ar fi încălcări ale securității datelor și atacuri de tip denial-of-service, precum și furnizarea de alerte și orientări privind gestionarea incidentelor. De asemenea, CERT desfășoară în permanență campanii de sensibilizare a publicului și se implică în activități de cercetare menite să îmbunătățirea sistemelor de securitate. Indiferent dacă sunt denumite CERT, CSIRT, CIRT sau orice alt acronim similar, rolul tuturor echipelor de intervenție în caz de urgență informatică este destul de comparabil. Toate aceste organizații încearcă să atingă aceleași obiective legate de răspunsul la incidente, de a răspunde la de securitate informatică, în vederea redobândirii controlului și a minimizării pagubelor. În acest scop, ele pot furniza sau asista la un răspuns eficient la incidente și la recuperare și la prevenirea repetării incidentelor de securitate informatică. În general, o echipă de răspuns la incidente este responsabilă de protejarea organizației împotriva problemelor legate de securitatea informatică, de rețea sau cibernetică care pot amenința organizația și informațiile acesteia. Un model universal pentru răspunsul la incidente, care este utilizat de mult timp, este modelul „protejează, detectează și răspunde".

[3] CERT este un departament al Carnegie Mellon University The CERT Division | Software Engineering Institute (cmu.edu)

Serviciul Trusted-Introducer (TI) a fost înființat în Europa în anul 2000 pentru a facilita colaborarea între de echipe de răspuns și, prin urmare, pentru a crește nivelul de securitate prin răspunsul mai rapid la atacurile în desfășurare și a amenințărilor de tip nou. TI asigură o bază de încredere, cu servicii adiţionale specializate pentru toate echipele de răspuns la incidente de securitate. De asemenea, serviciul TI menține baza de date europeană a echipelor de securitate cibernetică, inclusiv CSIRT-uri, CERT-uri, SOC-uri, PCSIRT-uri, ISAC-uri etc. Echipele din directorul TI sunt cunoscute sub denumirea de echipe „listate". Echipele listate au fost aprobate de acele echipe care - pe lângă faptul că au fost listate - au fost acreditate și/sau certificate. Echipele acreditate și certificate sunt un subset al echipelor listate și îndeplinesc cerințele acreditării formale TI. Acesta este mecanismul de acreditare și certificare bazat pe cele mai bune practici dezvoltate și testate de-a lungul timpului în cadrul aceleiași comunități de echipe TI și oferă o imagine de ansamblu actualizată asupra nivelului lor demonstrat de maturitate și abilitate.

Instituționalizarea capacităților cibernetice este o caracteristică bine cunoscută de zeci de ani încoace. Odată cu implementarea instituționalizării, este nevoie și de un cadru de reglementare care să contureze și să modeleze organizarea și mandatul acestora, precum și rolul lor în cadrul mecanismelor naționale de gestionare a crizelor. Capacitățile tehnice sunt de obicei organizate în echipe CERT/CSIRT, care au evoluat ca un standard pentru răspunsul la incidente, cu proceduri și standarde stabilite, urmate la nivel cvasi-global. Echipele de tip CERT/CSIRT au devenit o parte obișnuită a cadrelor naționale de securitate.

Necesitatea de a proteja infrastructura informatică critică și de a crea capacitățile naționale corespunzătoare a fost subliniată atât de NATO, cât și de UE timp de mulți ani. În timp ce „securitate cibernetică" și „incident cibernetic" sunt termeni acceptați, în ceea ce privește infrastructura critică și infrastructura informatică critică, nu există o astfel de definiție echivalentă la nivelul NATO. Termenul și conținutul său au rămas astfel în sfera de competență a națiunilor individuale.

Pentru țările membre UE, situația a fost clarificată în 2016 prin adoptarea Directivei (EU) 2016/1148 privind securitatea rețelelor și a sistemelor informatice, așa-numita directivă NIS. Deși evită termenii „infrastructură critică" și „infrastructură informatică critică", directiva a furnizat o listă de bază a sectoarelor și serviciilor care trebuie protejate, a subliniat funcțiile pe care un stat ar trebui să le garanteze și structurile pe care trebuie să le pună în aplicare pentru a asigura o astfel de protecție.

Printre alte aspecte, directiva NIS a obligat țările să instituie cel puțin o autoritate competentă și cel puțin o echipă de tip CSIRT pentru a acoperi serviciile reglementate, precum și elaborarea unei strategii naționale de securitate cibernetică.

Directiva totuși nu a prescris un model specific de guvernanță. Chiar și acele țări din UE care, până atunci, au întârziat în construirea structurilor lor naționale de guvernanță în domeniul securității cibernetice, au trebuit acum să se conformeze directivei NIS. Țările candidate la UE au încercat, de asemenea, să își alinieze cadrele legislative și instituționale legislative și instituționale.

Revizuirea din 2022 a directivei a extins obligațiile legate de guvernanță și capacitate pentru a acoperi și mai multe servicii și entități și a conferit autorităților competente puteri sporite de supraveghere și punere în aplicare. Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în UE, cunoscută sub numele de NIS 2, stabilește un cadru comun de reglementare cu scopul de a spori nivelul de securitate cibernetică în UE. Directiva se aplică în principal entităților mijlocii și mari care își desfășoară activitatea în sectoare cu o importanță critică ridicată (esențiale) definite in anexa I și entităților importante, definite în anexa II.

Directiva instituie o rețea a echipelor naționale CSIRT[4] și un grup de cooperare pentru a sprijini și a facilita cooperarea strategică și schimbul de informații. Grupul este compus din reprezentanți ai statelor membre, ai Comisiei și ai ENISA[5]. După caz, Grupul de cooperare poate invita să participe la lucrările sale Parlamentul European și reprezentanți ai părților interesate relevante.

Directiva trebuie să fie transpusă în legislația națională până la 17 octombrie 2024 (însă este foarte probil ca termenul să fie prelungit). Normele ar trebui să se aplice de la 18 octombrie 2024. Statele membre trebuie să întocmească o **listă a entităților esențiale** și **importante**, precum și a entităților care furnizează servicii de înregistrare a numelor de domenii, până la **17 aprilie 2025**. De menționat că până la momentul prezent, doar Belgia și Croația au transpus Directive NIS2 în legislația națională.

Modelele naționale alese de statele membre variază, reflectând configurațiile constituționale și tradițiile administrative respective. **Astfel, unele țări au optat pentru o abordare mai centralizată[6] și au o autoritate competentă și un CERT/CSIRT care se ocupă de sectoarele identificate în directiva NIS, inclusiv guvernul și administrația publică, în timp ce altele au ales o abordare sectorială și au desemnat o autoritate competentă și un CERT/CSIRT pentru sectoare individuale sau grupuri ale acestora, sau chiar pentru infrastructura din cadrul unității administrative teritoriale a unei țări[7]. Există, de asemenea, țări în care un CERT/CSIRT național este responsabil pentru serviciile esențiale în temeiul directivei NIS, în timp ce un altul se ocupă de administrația publică/ infrastructura guvernamentală**.[8]

[4] Rețeaua este gestionată de ENISA.
[5] Agenția Uniunii Europene pentru Cibersecuritate
[6] Franța (https://www.cert.ssi.gouv.fr/a-propos) sau Republica Cehă (Sectiunea 20 of a Legii 181/2014 privind cyber securitatea, https://www.nukib.cz/en/cyber-security/regulation-and-audit/legislation/).
[7] Germania (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/CyberSicherheitslage/Reaktion/CERT-Bund/Nationale-und-internationale-Zusammenarbeit/nationale-undinternationale-zusammenarbeit_node.html), Slovacia (Sectiunea 9 și Anexa 1 din Legea 69/2018 privind cibersecuritatea și modificări ale unor acte
[8] Slovenia, (Sectiunea 1 a Legii 2018-01-1350, privind Informarea și Securitatea, https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2018-01-1350?sop=2018-01-1350).

Deseori structurile de securitate cibernetică au existat, la origine, în cadrul instituțiilor de securitate ale unei țări, fie în cadrul armatei, fie în cadrul structurilor serviciilor interne. Datorită dezvoltărilor tehnologice și a riscurilor aferente, serviciile de tehnologia informației au început în anii 1990-2000 să se specializeze in ciber-securitate și să se dezvolte ca departamente specializate, conform strategiilor de securitate naționale ale statelor. Așadar, la momentul apariției Directivei NIS pre-existau în numeroase țări structuri de acest fel, existau rețelele și comunitățile profesionale organizate în jurul FIRST sau Trusted Introducer.

Structuri – sau cel puțin nuclee – de cibersecuritate au fost dezvoltate și în alte domenii precum administrație, financiar-bancar, sănătate, educație-cercetare, telecomunicații, furnizori de servicii și in special furnizori de servicii de internet, companii aeriene, conglomerate comerciale etc.

Deși sectorul energiei este esențial pentru societate și considerat critic, echipele de urgențe de ciber-securitate din acest domeniu sunt mai puțin numeroase decât ar fi de așteptat. În niciuna dintre țările studiate nu există, în cadrul administrației publice, departamente sau servicii dedicate exclusiv ciber-securității în sectorul energiei. Totuși, legile din unele țări precum Polonia și Spania lasă deschisă opțiunea de a avea entități coordonatoare pe domenii de activitate. În Austria exista, anterior Directivei NIS, echipa specializată denumită Austrian Energy CERT specializată în răspunsuri la incidente de securitate cibernetică, finanțată în comun de către 20 de operatori din industria energiei. În alte țări precum Polonia, Franța, Portugalia, Ungaria companiile majore din industria energiei dețin propriile echipe de cibersecuritate, echipe care fac parte din rețelele CSIRT naționale sau internaționale.

ASPECTE COMPARATIVE

AUSTRIA

Odată cu punerea în aplicare a primei directive NIS a UE prin Legea federală pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice (NISG), GovCERT a primit un temei juridic clar în 2018. Secțiunile 14 și 15 stabilesc sarcinile și cerințele pentru echipele de urgență informatică, așa cum sunt denumite CERT-urile în lege. Odată cu intrarea în vigoare a Legii privind securitatea rețelelor și a sistemelor informatice (NISG) în 2018, funcționarea GovCERT Austria a fost definită legal ca o sarcină a Cancelarului federal. GovCERT Austria este responsabilă de primirea rapoartelor privind riscurile, incidentele și incidentele de securitate la nivelul instituțiilor administrației publice la nivel federal, la nivel de stat și local.

GovCERT Austria este echipa guvernamentală de intervenție în caz de urgență informatică pentru administrația publică din Austria. Din aprilie 2008, Cancelaria Federală operează și această facilitate, prin *Departamentul I/8*, în cooperare cu CERT.at. De atunci, Cancelaria Federală îndeplinește sarcinile GovCERT Austria – mai precis partea strategică a GovCERT Austria – și utilizează resursele tehnice și calificările tehnice ale CERT.at adică partea tehnică/operațională a GovCERT Austria, pentru a aborda și preveni incidentele de securitate în domeniul tehnologiilor informației și comunicațiilor (TIC) în administrația publică. GovCERT Austria promovează, de asemenea, dezvoltarea unor echipe de intervenție în caz de urgență informatică specifice fiecărui sector. În cazul atacurilor asupra calculatoarelor la nivel național, CERT.at coordonează și informează operatorii de rețea respectivi și echipele locale de securitate responsabile.

Așadar, Cancelaria Federală austriacă se ocupă de coordonarea strategică în domeniul cibernetic, care include atât coordonarea națională, cât și relația cu securitatea europeană în domeniu. În cadrul Cancelariei Federale, *Departamentul I/8 Securitatea cibernetică și Centrul de calcul al crizelor* este responsabil de domeniul securității cibernetice. Biroul pentru securitatea strategică a rețelelor și a sistemelor informatice face parte din Departamentul I/8 și răspunde pentru de punerea în aplicare a obligațiilor legale care decurg din Directiva NIS (UE) 2016/1148 în Austria și din Legea privind securitatea rețelelor și a sistemelor informatice (Legea NISG). În plus, autoritatea operațională NIS din cadrul Ministerului Federal de Interne îndeplinește sarcini operaționale.

Documentul GovCERT Austria RFC 2350 descrie structura, interfețele și serviciile GovCERT Austria într-o formă standardizată. Scopul principal este de a comunica altor echipe de securitate ce pot aștepta de la GovCERT Austria.

Centrul Național de Coordonare pentru Securitate Cibernetică (NCC-AT) face parte din rețeaua de centre naționale de coordonare la nivelul UE și, împreună cu Centrul European de Competență pentru Securitate Cibernetică (ECCC), formează noul cadru european pentru sprijinirea inovării și a politicii industriale în domeniul securității cibernetice. În Austria, Cancelaria federală operează, de asemenea, NCC-AT cu sprijinul Agenției austriece pentru promovarea cercetării (FFG), îndeplinind astfel mandatul Regulamentului (UE) 2021/887 de stabilire a Centrului european de competențe industriale, tehnologice și de cercetare în domeniul securității cibernetice și a Rețelei de centre naționale de coordonare.

Inițial, a existat „Strategia austriacă pentru securitate cibernetică” (ÖSCS) elaborată în 2013. Ca parte a acestei strategii, a fost definit pentru prima dată în Austria un concept proactiv de protecție a spațiului cibernetic și a persoanelor din spațiul virtual, garantând în același timp respectarea drepturilor omului. O componentă a acestui concept a fost extinderea și consolidarea rolului GovCERT Austria, gestionat de Cancelaria Federală (BKA). Provocările legate de dezvoltarea dinamică a spațiului cibernetic au făcut necesară actualizarea ÖSCS.

Odată cu noua Strategie austriacă de securitate cibernetică, guvernul a adoptat în 2021 un concept reînnoit, cuprinzător și proactiv pentru protecția spațiului cibernetic și a persoanelor din spațiul virtual. ÖSCS 2021 formează cadrul strategic pentru politica națională de securitate cibernetică, precum și pentru crearea pe termen lung a unui spațiu cibernetic sigur, ca o contribuție la creșterea rezilienței Austriei și a Uniunii Europene printr-o abordare la nivelul întregii administrații.

Regulamentul de procedură al GovCERT Austria specifică în esență participarea la schimbul activ de informații și participarea la reuniunile GovCERT Austria: obiectivul explicit al GovCERT Austria este de a promova înființarea de echipe de răspuns la incidentele de Securitate cibernetică (CSIRT) în toate sectoarele.

Austria are 10 echipe de răspuns la incidente de cibersecuritate înregistrate formal.

Austrian Energy CERT (AEC), una dintre acestea, este deținută de industria energiei din Austria. Rolul său este să întărească securitatea IT și competențele din acest domeniu. În mod curent, AEC gestionează incidentele de securitate, procesând mesajele și solicitările de informații, oferă instruire, participă la crearea de concept e Securitate pentru industria energiei electrice și a gazului natural. Totodată, AEC are rolul de punct unic de contact petru incidentele de cibersecuritate din domeniul energiei, ceea ce implică o coordonare a experților IT din industrie. AEC este prima echipă de intervenție în caz de urgență informatică (CERT) specifică industriei din Europa pentru întregul sector energetic și funcționează în conformitate cu cerințele Directivei NIS publicată în 2016. AEC coordonează grupul de lucru ARGE E-CERT format din companii din industria energetică austriacă care a fost constituit la sfârșitul lunii octombrie 2015.

Consorțiul ARGE E-CERT cuprinde 20 de parteneri care reprezintă toate companiile din industria energetică austriacă din sectorul energetic (electricitate și gaze). Consorțiul este alcătuit din:

13 companii mari din industria energiei electrice: producția și distribuția de energie electrică, precum și gaz, operatorul sistemului austriac de transport al energiei electrice, cei patru mari operatori de rețele de gaze (operatorii sistemelor de transport și distribuție, TSO și DSO) cel mai mare producător și comerciant de energie electrică din Austria precum și un grup care include toate întreprinderile mici.

Părțile contractante formează un consorțiu sub forma juridică a unui parteneriat de drept civil, adică fără personalitate juridică proprie, care funcționează sub denumirea ARGE „Stabilirea și funcționarea unei echipe de intervenție în caz de urgență informatică pentru industria energetică austriacă” sau, pe scurt, ARGE E-CERT. Conducerea ARGE este formată din două persoane, fiecare dintre acestea fiind numită de adunarea generală pentru un an și putând fi demisă în orice moment.

Coordonarea cu autoritățile are loc prin intermediul consiliului consultativ.

BELGIA

Belgia este una dintre cele două țări, alături de Croația, care și-a actualizat legislația în domeniu. Legea din 26 aprilie 2024 de instituire a unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice de interes general pentru siguranța publică (Legea NIS2) transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 (Directiva NIS2) în Belgia. Aceasta va intra în vigoare la 18 octombrie 2024.

Legea NIS2 actualizează cadrul juridic belgian privind securitatea cibernetică prin înlocuirea vechii Legi din 7 aprilie 2019 de instituire a unui cadru pentru securitatea rețelelor și sistemelor informatice de interes general pentru securitatea publică (legea NIS1). Noul text este însoțit de Decretul regal din 9 iunie 2024 care pune în aplicare dispozițiile sale, de exemplu prin desemnarea Centrului pentru Securitate Cibernetică din Belgia (CCB) ca autoritate națională de securitate cibernetică.

Scopul legii este acela de a consolida măsurile de securitate cibernetică, gestionarea incidentelor și supravegherea entităților care furnizează servicii esențiale pentru menținerea activităților societale sau economice critice. De asemenea, legea vizează îmbunătățirea coordonării politicilor publice în domeniul securității cibernetice.

Pentru a fi acoperită de legea belgiană NIS2, o organizație trebuie: să furnizeze un serviciu enumerat în anexele I și II ale legii NIS2 în Uniunea Europeană; să depășească pragurile de mărime ale unei întreprinderi mijlocii stabilite prin Recomandarea 2003/361/CE, și anume să aibă o forță de muncă de cel puțin 50 de lucrători cu normă întreagă sau o cifră de afaceri anuală sau un bilanț total care depășește 10 milioane de euro; și să aibă sediul în Belgia.

Este important, în primul rând, de remarcat faptul că Legea NIS2 se aplică automat tuturor entităților identificate ca operatori de infrastructuri critice în sensul Legii din 1 iulie 2011 privind securitatea și protecția infrastructurilor critice, indiferent de mărimea acestora. În temeiul legii NIS2, acești operatori sunt entități esențiale.

În al doilea rând, entitățile identificate ca operatori de servicii esențiale (OES) sau furnizori de servicii digitale (DSP) în temeiul legii NIS1 intră, în principiu, și sub incidența legii NIS2 dacă depășesc pragurile de mărime necesare. Motivul este simplu: domeniul de aplicare al directivei NIS2 este o extindere a domeniului de aplicare al directivei NIS1.

Pentru a intra în domeniul de aplicare al legii NIS2, o organizație trebuie să aibă o anumită dimensiune. În principiu, o organizație trebuie să fie cel puțin o întreprindere mijlocie, calculată utilizând anexa la Recomandarea 2003/361/CE a Comisiei, dar există anumite excepții.

Tipuri de entități ce intră în domeniul de aplicare al legii NIS2 (indiferent de mărimea lor):

- prestatorii de servicii fiduciare calificați (esențial);
- furnizori de servicii fiduciare necalificate (important în cazul microîntreprinderilor, întreprinderilor mici sau mijlocii și esențial în cazul întreprinderilor mari);
- furnizori de servicii DNS (esențial);
- registre de nume TLD (esențial);
- servicii de înregistrare a numelor de domeniu (numai pentru obligația de înregistrare);
- furnizori de rețele publice de comunicații electronice (esențial);
- furnizorii de servicii de comunicații electronice accesibile publicului (esențial);
- entități identificate ca operatori de infrastructură critică (esențial);
- entitățile administrației publice care depind de statul federal (esențial).

Independent de aceste norme, autoritatea națională de securitate cibernetică (CCB) va putea, de asemenea, să identifice în mod specific entitățile calsificate ca fiind „esențiale" sau „importante", de exemplu atunci când acestea sunt singurul furnizor al unui serviciu sau atunci când întreruperea serviciului furnizat ar putea avea un impact semnificativ asupra securității publice, siguranței publice sau sănătății publice.

Dincolo de plafonul de mărime, condiția privind serviciile impune unei organizații să analizeze pe deplin fiecare dintre serviciile sale furnizate terților, pe sectoare și subsectoare. Acest lucru este important, având în vedere că chiar și cel mai auxiliar serviciu furnizat poate face ca o organizație în ansamblu să intre în domeniul de aplicare al legii NIS2, cu excepția cazului în care se prevede altfel în definiția serviciului respectiv.

Toate serviciile care intră sub incidența legii NIS2 sunt detaliate în anexele I și II (sau în definiții) la Lege. În cazul în care o organizație furnizează unul dintre serviciile menționate acolo și îndeplinește criteriul de mărime corespunzător, atunci aceasta intră în domeniul de aplicare al legii NIS2 dacă are legătură cu Belgia. Diferitele servicii sunt grupate pe sectoare și subsectoare[9].

În principiu, legea belgiană NIS2 se aplică numai entităților stabilite în Belgia care își furnizează serviciile sau își desfășoară activitățile în UE. Două concepte sunt importante aici:

[9] Există 2 anexe. Anexa I listează Sectoare extrem de critice: energie, energie electrică, încălzire și răcire urbană, petrol, gaz, hidrogen, transport (aer, feroviar, pe apă, rutier), sectorul bancar, infrastructura pieței financiare, sănătate, apă potabilă, apă reziduală, infrastructură digitală, gestionarea serviciilor TIC (B2B), administrație publică, spațiu.
Anexa II enumeră "alte servicii critice: servicii poștale și de curierat, gestionarea deșeurilor, fabricarea, producerea și distribuția de produse chimice, Producția, prelucrarea și distribuția de produse alimentare, industria prelucrătoare, fabricarea dispozitivelor medicale și a dispozitivelor medicale de diagnostic in vitro, fabricarea produselor informatice, electronice și optice, fabricarea de echipamente electrice, fabricarea de mașini și echipamente n.c.a., fabricarea autovehiculelor, remorcilor și semiremorcilor, fabricarea altor echipamente de transport, furnizori de servicii digitale, cercetare.

- Conceptul de „stabilire” - implică exercitarea efectivă a unei activități prin intermediul unei instalații permanente, indiferent de forma juridică adoptată, fie că este vorba de sediul social, de o sucursală simplă sau de o filială cu personalitate juridică.
- Noțiunea de „entitate”, cum este definită la articolul 8 punctul 37 din legea NIS2 - ca o persoană fizică sau juridică creată și recunoscută ca atare în temeiul legislației naționale a locului său de stabilire și care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații.

Legea NIS2 definește „incidentul” ca fiind un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora.

Un incident „semnificativ” este orice incident care are un impact semnificativ asupra furnizării de servicii în sectoarele sau subsectoarele enumerate în anexele la legea NIS2 și care a cauzat sau este susceptibil de a cauza perturbări grave în funcționarea oricăruia dintre serviciile din sectoarele sau subsectoarele enumerate în anexele I și II sau pierderi financiare pentru entitatea în cauză; sau a cauzat sau este posibil să cauzeze daune materiale, personale sau morale semnificative altor persoane fizice sau juridice.

În cazul în care incidentul în cauză se încadrează în această definiție, notificarea se face către un CSIRT național (CCB). Pe lângă notificarea către CSIRT-ul național, după caz, entitățile în cauză informează destinatarii serviciilor lor cu privire la incidentele semnificative care pot afecta furnizarea serviciilor din anexele I și II care le sunt furnizate. De asemenea, entitățile informează destinatarii serviciilor lor care pot fi afectați de o amenințare cibernetică semnificativă cu privire la amenințarea respectivă și la toate măsurile și corecțiile care pot fi luate pentru a răspunde la aceasta.

În cadrul ENISA sunt înregistrate (pentru Belgia) 11 echipe de răspuns la incidente de securitate cibernetică (CSIRT). Acestea își desfășoară activitatea în domeniul public, militar, educație-cercetare, trafic aerian, comercial și al furnizorilor de internet.

GERMANIA

Proiectul de lege NIS2UmsuCG va transpune în legislația germană cerințele minime ale UE privind securitatea cibernetică din Directiva UE NIS2, le va extinde în funcție de particularitățile de reglementare germane și va intra în vigoare la sfârșitul anului 2024. Proiectul de lege al Cabinetului datează din iulie 2024 și mai are de parcurs etapele procesului legislativ până în octombrie 2024. În plus față de NIS2, legea-cadru KRITIS va reglementa operatorii critici cu reziliență, iar EU DORA sectorul financiar.

În sprijinul implementării NIS2, a legii-cadru KRITIS, precum și aplicării legii privind securitatea informatică și a cadrului european pentru operatorii de infrastructuri critice, a fost creată platforma OpenKRITIS.

Au fost inițiate mai multe proiecte de lege, aflate în diferite stadii de finalizare, pentru implementarea NIS2; actualul proiect de lege este elaborat de Ministerul Federal de Interne (BMI).

Entitățile vor fi reglementate de Agenția Federală pentru Securitate Cibernetică (BSI). Foaia de parcurs pentru noile proiecte, datele oficiale de publicare și termenul de începere sunt în prezent neclare.

În ceea ce privește transpunerea prevederilor NIS2, în legislația germană vor exista mai multe particularități:

- metoda germană existentă pentru identificarea infrastructurilor critice, KRITIS, va rămâne în NIS2;
- operatorii germani KRITIS pe infrastructuri critice vor fi transferați în NIS2 ca operatori de infrastructuri critice de tipul celei de-a treia entități;
- entitățile esențiale și importante din NIS2 vor fi denumite *entități foarte importante* și *importante*;
- sectoarele NIS2 din anexele I și II sunt definite ușor diferit - gestionarea serviciilor TIC și infrastructura digitală sunt incluse în sectorul german IT/Telco;
- sectoarele KRITIS existente vor rămâne ca set separat pentru operatorii critici;
- sectorul administrației publice este definit diferit în Germania și va include (în cea mai mare parte) numai entități ale administrației federale.[10]

În sectorul energetic, operatorii reglementați și instalațiile furnizează publicului larg patru servicii esențiale - furnizarea de energie electrică, gaze, combustibil și păcură și încălzire urbană. Aceste servicii trebuie protejate prin obligații de securitate cibernetică în conformitate cu NIS2 și KRITIS. Operatorii KRITIS furnizează aceste servicii critice în propriile lor instalații și devin KRITIS dacă depășesc valorile-prag.[11]

Autoritatea federală în domeniul securității cibernetice este BSI (*Bundesamt für Sicherheit in der Informationstechnik*). În cadrul BSI funcționează Centrul Național Operațional IT (*Cyber-Abwehr für Deutschland - CAD*). Stațiile de lucru din centrul operațional au fost suplimentate și a fost instalată cea mai recentă tehnologie media pentru a putea evalua permanent starea securității cibernetice a Germaniei, într-un serviciu de informare 24/7. Un concept de cameră multifuncțională sprijină experții în întreaga gamă de sarcini care apar - de la operațiunile de zi cu zi, la incidentele IT.

[10] https://www.openkritis.de/eu/eu-nis-2-germany.html
[11] https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html

În timpul orelor de program, CAD este sprijinit de experții BSI pentru infrastructuri critice (KRITIS) și de echipa federală de intervenție în caz de urgență informatică (CERT-Bund), precum și de ofițerii de securitate a informațiilor din cadrul Comandamentului pentru spațiul informatic și informațional (KdoCIR). În afara orelor de program, CERT-Bund și KRITIS sunt de gardă, iar cooperarea cu KdoCIR are loc prin intermediul interfețelor stabilite între cele două autorități. CAD, în calitate de birou central de raportare al BSI, reunește, de asemenea, diverse puncte de raportare legale și voluntare, astfel încât grupurile țintă afectate să poată fi identificate rapid, iar punctele comune și amenințările similare să poată fi recunoscute și prelucrate. Centrele de raportare sunt completate de monitorizarea activă a situației (monitorizarea mass-media, cercetarea în aproximativ 400 de surse publice și senzori proprii etc.).

În cazul unui incident de securitate IT, BSI poate să sprijine organizațiile afectate în determinarea și evaluarea situației. În acest scop, pot fi organizate întâlniri cu experți și specialiști. Pentru administrația federală și infrastructurile critice, expertiza suplimentară a BSI în domeniul analizei programelor malware, al expertizei criminalistice digitale sau al analizei datelor de log poate fi, de asemenea, utilizată în gestionarea incidentului. În cazuri excepționale, BSI poate trimite o echipă mobilă de răspuns la incidente (MIRT) pentru a oferi asistență la fața locului. Acest serviciu este disponibil în principal pentru administrația federală și pentru entitățile critice.

Constatările BSI privind incidentele de securitate IT deja cunoscute pot furniza indicatori tehnici pentru detectarea atacurilor și clarificarea incidentului și pot fi definite în mod specific pentru incident la finalizarea analizei. Cu consimțământul organizației în cauză, rezultatele pot fi transmise terților într-o formă adecvată pentru detectarea tiparelor de atac, în vederea detectării și prevenirii altor daune aduse altor organizații. În plus, BSI poate, de asemenea, să sprijine organizațiile în identificarea unor furnizori de servicii adecvați, care să le sprijine în gestionarea, detectarea sau analiza incidentelor.[12]

FRANȚA

Agenția Națională pentru Securitatea Sistemelor Informatice (ANSSI - Agence nationale de la sécurité des systèmes d'information), creată în 2009, este autoritatea națională pentru securitatea cibernetică. Aflată sub autoritatea prim-ministrului și subordonată Secretarului General pentru Apărare și Securitate Națională (SGDSN), aceasta este în măsură să implementeze o politică globală de securitate cibernetică și să o coordoneze la nivel interministerial. Această politică vizează apărarea celor mai critice infrastructuri digitale publice și private. ANSSI se adresează, de asemenea, tuturor actorilor implicați în

[12] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Vorfallunterstuetzung/vorfallsunterstuetzung_node.html

transformarea digitală a țării și favorizează condițiile unui dialog cu omologii săi la nivel european și internațional.

Decretul nr. 2009-834 din 7 iulie 2009 privind crearea Agenției Naționale de Securitate a Sistemelor Informatice (ANSI) a conferit acestei agenții, pe lângă asigurarea securității sistemelor informatice ale statului, misiunea de a consilia și sprijini administrațiile și operatorii de importanță vitală și de a contribui la securitatea societății informaționale, în special prin participarea la cercetarea și dezvoltarea tehnologiilor de securitate și la promovarea acestora.

În conformitate cu orientările stabilite în Carta albă privind apărarea și securitatea națională din 2013, ANSSI contribuie la orientarea cercetării naționale și europene în domeniul securității sistemelor informatice. Atunci când este necesar, ANSSI beneficiază de expertiza unui comitet strategic format din înalți funcționari guvernamentali. Rolul acestui comitet este de a propune strategia statului în acest domeniu.

ANSSI a înlocuit Direcția Centrală pentru Securitatea Sistemelor Informatice (DCSSI) din cadrul Secretariatului General pentru Apărare și Securitate Națională (SGDSN), consolidându-și în același timp competențele, personalul și resursele. În calitate de autoritate națională pentru securitatea și apărarea sistemelor informatice, ANSSI are expertiza pentru a asista departamentele guvernamentale și operatorii de importanță vitală. Totodată, este responsabilă de promovarea tehnologiilor, sistemelor și expertizei naționale. Centrul guvernamental de transmisiuni, plasat sub autoritatea SGDSN, asistă ANSSI prin punerea în aplicare a mijloacelor securizate de comandă și de legătură solicitate de președintele Republicii și de guvern.

Articolul 34 din Legea nr. 2018-607 privind programarea militară pentru perioada 2019-2025 completează, de asemenea, atribuțiile agenției. Acesta precizează punerea în aplicare a sistemelor de detectare în timpul evenimentelor care pot afecta securitatea sistemelor informatice ale statului, ale autorităților publice și ale operatorilor publici și privați, precum și colectarea de informații tehnice referitoare la aceste incidente și sprijinirea în reacția la acestea.

ANSSI este plasată sub autoritatea primului-ministru și atașată Secretariatului General pentru Apărare și Securitate Națională (SGDSN). Activitățile sale sunt axate pe protecția, securitatea și apărarea sistemelor informatice. Modelul francez de securitate și apărare cibernetică se bazează pe o separare clară, în cadrul statului, între misiunile defensive și cele ofensive. Acest model se concretizează în rolul de autoritate națională jucat de ANSSI, ale cărei misiuni acoperă întregul domeniu al apărării și protecției sistemelor informatice. În plus, ANSSI este interesată doar de securitatea rețelelor și nu de informațiile și conținutul pe care aceste rețele le conțin.

Poziționarea instituțională a agenției contribuie, de asemenea, la echilibrul modelului: fiind atașată SGDSN și aflată sub autoritatea prim-ministrului, agenția beneficiază de un statut interministerial care îi permite să lucreze cu toți interlocutorii săi. Statutul ANSSI și caracterul defensiv al misiunilor sale îi permit să își desfășoare acțiunile eficient, în legătură cu

partenerii săi ministeriali, cu entitățile victime, cu reprezentanții aleși, cu specialiștii în securitate cibernetică și cu furnizorii privați de servicii.

Conform organigramei ANSSI, in cadrul agenției funcționează 4 direcții[13]: Expertiză, Operațiuni, Resurse și Strategie.

Dintre acestea, rolul de echipă de răspuns la incidente de securitate cibernetică la nivel național, CERT-FR/SOC este în sarcina Direcției Operațiuni din cadrul Agenției Naționale pentru Securitatea Sistemelor Informatice (ANSSI).

Principalii beneficiari ai activităților desfășurate de CERT-FR sunt :

- organisme publice: ministere, instituții, instanțe, autorități independente, autorități locale;
- operatori de importanță vitală (OIV): operatori publici sau privați care utilizează echipamente și instalații esențiale pentru funcționarea și supraviețuirea națiunii franceze;
- operatori de servicii esențiale (OSE): operatori de rețele sau de sisteme informatice, care furnizează un serviciu esențial a cărui întrerupere ar avea un impact semnificativ asupra funcționării economiei sau a societății.

Deși furnizează informații accesibile tuturor prin intermediul site-ului propriu (lista vulnerabilităților, starea amenințării informatice etc.), CERT-FR nu intervine direct pe lângă persoanele fizice și IMM-uri. Sprijinul pentru aceste grupuri este oferit de site-ul guvernamental cybermalveillance.gouv.fr[14] .

In acest context, sarcinile CERT-FR sunt:

- să răspundă solicitărilor de asistență ca urmare a incidentelor de securitate în rețelele și sistemele informatice ale beneficiarilor săi. Aceasta implică primirea cererilor, analizarea simptomelor incidentului, identificarea posibilelor corelații cu alte incidente similare și definirea soluțiilor de recuperare în caz de incident;
- gestionarea alertelor și reacția la atacurile informatice. În acest scop, CERT-FR efectuează o analiză tehnică a atacurilor, participă la schimburi de informații cu alte CERT-uri și contribuie la studii tehnice specifice pe diverse teme de securitate cibernetică;
- detectarea atacurilor care vizează sistemele informatice guvernamentale. În acest scop, CERT-FR operează un serviciu permanent de supraveghere a securității (SOC) pentru departamentele guvernamentale;
- detectarea vulnerabilităților sistemelor, în special prin monitorizarea tehnologică a principalelor produse de pe piață;

[13] sau *sub-direcții* conform terminologiei franceze: sous-direction

[14] Misiunea Cybermalveillance.gouv.fr este de a ajuta persoanele fizice, întreprinderile, asociațiile, autoritățile locale și departamentele guvernamentale care au căzut victime atacurilor cibernetice și de a le informa cu privire la amenințările digitale și cum să se protejeze împotriva acestora.

- contribuția la prevenirea atacurilor informatice, prin difuzarea de informații privind măsurile de precauție care trebuie luate pentru a reduce riscul de incidente și a minimiza consecințele posibile ale acestora;
- coordonarea prevenirii incidentelor și a răspunsului cu entitățile partenere. Coordonarea operațiunilor înseamnă că CERT-urile naționale și internaționale, centrele de competențe în materie de rețele, operatorii și furnizorii de servicii internet pot fi mobilizați în funcție de necesități.

In Franța, transpunerea Directivei **(**EU) 2016/1148 NIS a avut loc printr-o serie de acte, dintre care menționăm Titlul I din LEGEA nr. 2018-133 din 26 februarie 2018 privind diverse dispoziții de adaptare la dreptul Uniunii Europene în domeniul securității **și** Decretul nr. 2018-384 din 23 mai 2018 privind securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale **.**

Franța dispune de o rețea bine dezvoltată de echipe de răspuns la incidente, în număr de 62 de CSIRT, care acoperă domenii diverse: public guvernamental, militar, furnizori de servicii de internet, educație și cercetare, sectorul financiar, servicii de importanță critică, firme comerciale etc.

Dintre acestea, TotalEnergies, companie globală integrată care produce și comercializează energie – petrol și biocombustibili, gaze naturale și gaze verzi, surse regenerabile și electricitate – dispune de echipa proprie de răspuns la incidente de securitatea cibernetică. Astfel, TotalEnergies CERT este echipa de intervenție în caz de urgență informatică responsabilă de coordonarea răspunsului la incidente și de evaluarea securității cibernetice în cadrul entităților TotalEnergies Company și al filialelor TotalEnergies Company**.**

IRLANDA

Irlanda continuă să lucreze la proiectul legislativ de transpunere a directivei NIS2, având în vedere data scadentă,17 octombrie 2024.

Centrul Național de Securitate Cibernetică (NCSC) a fost înființat în 2011 și este o componentă operațională a Departamentului pentru Mediu, Climă și Comunicații (DECC). NCSC este responsabil cu consilierea și informarea furnizorilor de IT guvernamentali și de infrastructură națională critică cu privire la amenințările și vulnerabilitățile actuale asociate cu securitatea informațiilor în rețea.

Rolurile principale ale NCSC sunt de a conduce gestionarea incidentelor majore de securitate cibernetică în întreaga guvernare, de a oferi îndrumări și consiliere cetățenilor și întreprinderilor cu privire la incidente majore de securitate cibernetică și de a dezvolta relații internaționale puternice în comunitatea globală de securitate cibernetică. Începând cu 2011,

unitatea și-a concentrat eforturile pe consolidarea capacității și stabilirea unei baze stabile pentru activitatea sa operațională.

În cadrul NCSC activează Echipa națională/guvernamentală de răspuns la incidente de securitate informatică (CSIRT-IE). CSIRT-IE reprezintă, de asemenea, punctul național de contact pentru partenerii internaționali care doresc să informeze entitățile din Irlanda cu privire la problemele de securitate cibernetică. Din 2017, CSIRT-IE a fost acreditat de serviciul *Trusted Introducer*[15] al TF-CSIRT.

In Irlanda mai activează HEAnet-CERT, centrul care deservește rețeaua irlandeză de educație și cercetare. Acesta este punctul unic de contact al rețelei HEAnet pentru clienții care se confruntă cu incidente de securitate informatică. În cazul în care un client suspectează o intruziune sau un atac, HEAnet-CERT oferă rapid sprijin, consiliere și expertiză.

HEAnet-CERT oferă următoarele servicii tuturor clienților rețelei HEAnet:

- asistență tehnică cu privire la ce trebuie să facă în cazul unui incident
- colectarea, analiza și raportarea de statistici privind incidentele
- notificări către site-uri cu privire la faptul că acestea ar putea fi sursa, intermediarul sau ținta unui atac, deoarece acestea pot fi adesea inconștiente.

HEAnet-CERT asistă, de asemenea, toți clienții HEAnet care doresc sprijin proactiv pentru probleme de securitate și vulnerabilități percepute.

In domeniul non-guvernamental există Serviciul irlandez de raportare și securitate a informațiilor (IRISS) care este o societate independentă fără scop lucrativ, cu răspundere limitată, înființată în 2008 pentru a oferi o serie de servicii gratuite întreprinderilor și consumatorilor irlandezi în legătură cu problemele de securitate a informațiilor, pentru a contribui la contracararea amenințărilor la adresa securității întreprinderilor irlandeze și a spațiului internet irlandez. Aceste servicii includ:

- furnizarea unui serviciu de alertă privind noile vulnerabilități și amenințări care pot compromite securitatea resurselor informatice și de comunicații pentru persoanele fizice, întreprinderile și organismele guvernamentale din Irlanda;
- furnizarea și alertarea cu privire la atacurile în curs de desfășurare asupra resurselor TIC din Irlanda pentru a permite altor entități să elaboreze și să pună în aplicare măsuri de protecție împotriva unor astfel de atacuri;
- furnizarea de statistici și rapoarte privind activitatea de criminalitate informatică din Irlanda pentru a ajuta organizațiile și persoanele fizice să își concentreze mai bine resursele asupra amenințărilor la adresa securității specifice Irlandei;
- oferă persoanelor și organizațiilor posibilitatea de a raporta incidentele de securitate;

[15] Grup de lucru care promovează colaborarea și coordonarea între CSIRT-urile din Europa și regiunile învecinate, menținând în același timp legătura cu organizațiile relevante la nivel global și în alte regiuni

- furnizează orientări și de tehnici de bune practici privind modul de prevenire a incidentelor de securitate și cel mai bun mod de a răspunde în cazul în care are loc un astfel de incident.

Gama de servicii de mai sus este asigurată de un nucleu de voluntari dedicați, experți în domeniul securității informațiilor, care își oferă gratuit serviciile comunității irlandeze de internet. IRISS este finanțat printr-o combinație de donații și sponsorizări corporative.

ITALIA

Autoritatea națională în domeniul securității cibernetice este ACN (*Agenzia per la Cybersicurezza Nazionale*), înființată prin Decretul Legislativ nr. 82 din 14 iunie 2021 care a redefinit arhitectura națională de securitate cibernetică, cu scopul de a raționaliza și simplifica sistemul de competențe existente la nivel național. ACN este responsabilă cu prevenirea și atenuarea atacurilor cibernetice și cu promovarea realizării autonomiei tehnologice.

Una dintre principalele sarcini ale Agenției este implementarea Strategiei Naționale de Securitate Cibernetică , adoptată de primul-ministru, în care sunt prevăzute obiectivele care urmează să fie atinse până în 2026.

CSIRT Italia este înființat în cadrul ACN și este structura tehnico-operațională și hub-ul național al notificărilor de incidente prevăzute de lege. Atribuțiile CSIRT sunt stabilite prin Decretul legislativ nr.65 din 18 mai 2018 și prin Decretul prim-ministrului 8 august 2019: monitorizarea incidentelor la nivel național; emiterea de avertismente timpurii, alerte, anunțuri și difuzarea de informații către părțile interesate cu privire la riscuri și incidente; intervenția în caz de incident; analiza dinamică a riscurilor și incidentelor; conștientizarea situației; participarea la rețeaua CSIRT.

ACN publică lunar un Raport privind starea amenințării cibernetice naționale, denumit „Rezumat operațional". Documentul conține cifre și indicatori legați de activitățile operaționale ale agenției desfășurate de CSIRT Italia. CSIRT Italia colectează, de asemenea, informații din surse deschise și comerciale, precum și de la alte entități omologe naționale și internaționale. Aceste informații, care constituie un larg unghi de vizibilitate asupra stării amenințării cibernetice, sunt studiate și exploatate de operatori și implică o serie de activități în funcție de actorii implicați și de tipul de eveniment analizat. Rezumatul operațional reprezintă un instrument funcțional util pentru înțelegerea fenomenelor și a evoluției lor în timp, vizând, de asemenea, consolidarea nivelului de prevenire pe baza cunoașterii evenimentelor care au avut loc.

CSIRT Italia stabilește relații de cooperare cu sectorul privat. Pentru a facilita cooperarea, CSIRT promovează adoptarea și utilizarea unor practici comune sau standardizate în domeniul procedurilor de gestionare a incidentelor și riscurilor și al sistemelor de clasificare a incidentelor, riscurilor și informațiilor. Profilul complet al CSIRT Italia este inclus în RFC 2350.[16]

Italia are 40 de echipe de răspuns la incidente de securitate cibernetică, așa cum apar centralizate de ENISA.

Dintre acestea, există 3 care activează în cadrul unor companii din domeniul energiei:

A2A este o firmă care distribuie energie electrică și gaze, apă potabilă și căldură prin sisteme de încălzire urbană. Asigură iluminare, conectare și proiectare pentu orașe și întreprinderi. Totodată găzduiește o echipă de răspuns la incidente, A2A-CERT, care oferă companiei servicii de gestionare a incidentelor de securitate cibernetică (ISIM), informații privind amenințările cibernetice (CTI), gestionarea platformei de securitate (SPM) și apărare activă (AD).

Enel Italia este o altă societate comercială în cadrul căreia există o echipă de răspuns la incidente de securitate cibernetică (care este acreditată cu Trusted Introducer).

De asemnea, în cadrul societății de transport a energiei electrice denumita Terna, funcționează TERNA-CERT, principalul punct de contact pentru colectarea, analiza și schimbul de informații privind amenințările informatice la care este expusă organizația. În plus, TERNA-CERT asigură servicii de asistență, formare, informare și cercetare și dezvoltare.

TERNA-CERT este format dintr-un grup de experți în securitate IT care lucrează împreună cu obiectivul comun de a proteja securitatea activelor Grupului Terna - inclusiv a activelor sale informatice - prin examinarea și monitorizarea naturii în continuă evoluție a amenințărilor cibernetice, desfășurarea de activități de prevenire, gestionarea situațiilor de urgență IT și coordonarea procedurilor de răspuns.

TERNA-CERT este membru al Forum of Incident Response (FIRST.org) și acreditat ca Trusted Introducer de TF-CSIRT și a fost autorizat de Universitatea Carnegie Mellon să utilizeze marca CERT. Colaborează cu alte organizații italiene și internaționale, pentru a promova interacțiunea și schimbul de informații cu privire la aspecte precum noile amenințări, atacurile informatice, noile tehnici de apărare și punctele slabe care pot fi exploatate, inclusiv prin utilizarea Threat Intelligence și a platformelor de schimb de informații.

[16] https://www.csirt.gov.it/chi-siamo

POLONIA

La 1 august 2018 Președintele Poloniei a semnat Legea nr. 1560/2018 privind sistemul național de securitate cibernetică, care transpune în sistemul juridic polonez Directiva (UE) privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în întreaga Uniune (Directiva 2016/1148), așa-numita Directivă NIS2.

Sistemul național de securitate cibernetică urmărește să asigure securitatea cibernetică la nivel național, în special pentru furnizarea neîntreruptă a serviciilor esențiale și a serviciilor digitale și atingerea unui nivel suficient de ridicat de securitate a sistemelor TIC prin care se furnizează aceste servicii.

Sistemul include operatori de servicii esențiale (în special din sectoarele **energiei**, transporturilor, sănătății și bancar), furnizori de servicii digitale, echipe CSIRT de răspuns la incidente la nivel național, echipe sectoriale și un punct unic de contact[17] pentru comunicare în cadrul cooperării în Uniunea Europeană în domeniul politicii de securitate cibernetică. Operatorii de servicii esențiale trebuie să pună în aplicare măsuri de protecție eficiente, să evalueze riscurile de securitate cibernetică, să comunice și să gestioneze incidentele majore în cooperare cu CSIRT-urile la nivel național. Operatorii de servicii esențiale trebuie, de asemenea, să numească o persoană responsabilă de securitatea cibernetică a serviciilor furnizate, de gestionarea și raportarea incidentelor și de schimbul de cunoștințe privind securitatea cibernetică.

Organele administrației publice și întreprinderile de telecomunicații sunt, de asemenea, incluse în sistemul național de securitate cibernetică - într-un mod armonizat cu reglementările existente în acest domeniu.

Furnizorii de servicii digitale, și anume piețele online, serviciile de cloud computing și motoarele de căutare, sunt, de asemenea, responsabili cerințele de securitate cibernetică. Datorită specificității internaționale a acestor entități, obligațiile furnizorilor de servicii digitale fac obiectul unui regim de reglementare armonizat la nivelul UE. Legea se referă aici la decizia de punere în aplicare a Comisiei Europene.

Există trei echipe principale de răspuns la nivel național în domeniul public. Acestea sunt CERT NASK, CSIRT GOV și CSIRT MON. Ale căror sarcini sunt definite in art. 26 din Legea 1560/2018.

Echipa CERT Polska funcționează în cadrul structurilor NASK - Institutul Național de Cercetare, unde desfășoară activități științifice, operează registrul național al domeniilor .pl și furnizează servicii TIC avansate. CERT Polska este prima echipă de răspuns la incidente înființată în Polonia. Datorită activității sale dinamice din 1996 în mediul echipelor de

[17] Punctul Național de Contact este in cadrul ministerului pentru digitalizare.

intervenție, aceasta a devenit o entitate recunoscută și experimentată în domeniul securității informatice.

De la începutul existenței echipei, nucleul activității acesteia a fost gestionarea incidentelor de securitate și cooperarea cu unități similare din întreaga lume, atât în activități operaționale, cât și în activități de cercetare și implementare. Din 1998, CERT Polska a fost membră a forumului internațional al echipelor de intervenție - FIRST, iar din 2000 a fost membră a grupului de lucru al echipelor europene de intervenție - TERENA TF-CSIRT și a organizației Trusted Introducer care funcționează în cadrul acestuia. În 2005, la inițiativa CERT Polska, a fost înființat Abuse FORUM, iar în 2010 CERT Polska s-a alăturat Grupului de lucru Anti-Phishing, o asociație care reunește companii și instituții care luptă activ împotriva criminalității online.

De la intrarea în vigoare a Legii din 5 iulie 2018 privind sistemul național de securitate cibernetică, echipa a îndeplinit unele dintre sarcinile CSIRT NASK, în conformitate cu articolul 26 din această lege.

CERT NASK gestionează incidente raportate de:

- unități ale administrației locale
- unități bugetare, instituții bugetare ale administrației locale
- agenții executive, instituții bugetare
- universități publice și Academia Poloneză de Științe
- Oficiul de inspecție tehnică, Agenția poloneză pentru servicii de navigație aeriană, Centrul polonez pentru acreditare
- Fondul național pentru protecția mediului și gestionarea apelor și fondurile provinciale pentru protecția mediului și gestionarea apelor
- societăți de drept comercial care îndeplinesc sarcini de utilitate publică care vizează satisfacerea continuă și neîntreruptă a colectivității
- cetățeni.

Echipa CSIRT GOV[18], condusă de șeful Agenției de Securitate Internă, acționează la nivel național fiind responsabilă de coordonarea răspunsului la incidentele informatice care au loc în domeniul amenințărilor la adresa securității, importante din punctul de vedere al continuității funcționării statului, a sistemelor TIC ale organismelor administrației publice sau a sistemului de rețele TIC acoperit de o listă uniformă de facilități, instalații, dispozitive și servicii incluse în infrastructura critică, precum și a sistemelor TIC ale proprietarilor și deținătorilor de facilități, instalații sau echipamente de infrastructură critică.

[18] Descrierea completă a echipei CERT Polska (în limba engleză) în conformitate cu RFC 2350 „Expectations for Computer Security Incident Response”. Documentul este semnat cu o cheie PGP CERT Polska https://cert.pl/uploads/misc/rfc2350.txt

CSIRT GOV gestionează incidente raportate de:

- autorități publice, inclusiv organe ale administrației publice, organe de control de stat și de aplicare a legii, instanțe și tribunale
- Banca Națională Poloneză, Bank Gospodarstwa Krajowego

CSIRT MON este echipa aflată in cadrul Ministerului Apărării Naționale și gestionează incidente raportate de:

- entități aflate în subordinea sau sub supravegherea ministrului apărării naționale, inclusiv entități ale căror sisteme TIC sau rețele TIC sunt incluse într-o listă uniformă de facilități, instalații, dispozitive și servicii incluse în infrastructura critică
- întreprinzători cu o importanță economică și de apărare deosebită, în legătură cu care ministrul apărării naționale este organismul care organizează și supraveghează îndeplinirea sarcinilor de apărare a statului

Legea din 5 iulie 2018 privind sistemul național de securitate cibernetică definește și **autoritățile competente** în materie de securitate cibernetică **responsabile cu supravegherea operatorilor de servicii esențiale** și servicii digitale. Operatorii de servicii esențiale vor trebui să pună în aplicare măsuri de protecție eficiente, să evalueze riscurile de securitate cibernetică și să raporteze și să gestioneze incidentele majore în cooperare cu CSIRT-urile la nivel național.

Autoritățile competente stabilite de Lege, conform art. 41, sunt:

- pentru **sectorul energetic** - **ministrul responsabil pentru energie**;
- pentru sectorul transporturilor, cu excepția subsectorului transportului pe apă - ministrul responsabil cu transporturile;
- pentru subsectorul transportului pe apă - ministrul responsabil de economia maritimă și ministrul responsabil de navigația interioară;
- pentru sectorul bancar și infrastructura pieței financiare - Autoritatea poloneză de supraveghere financiară;
- pentru sectorul sănătății, ministrul responsabil cu problemele de sănătate;
- pentru sectorul alimentării și distribuției cu apă potabilă - ministrul delegat pentru gospodărirea apelor
- pentru sectorul infrastructurii digitale, ministrul responsabil cu informatizarea;
- pentru sectorul infrastructurii digitale, ministrul apărării naționale;
- pentru furnizorii de servicii digitale ministrul responsabil cu informatizarea.

Sarcinile autorităților competente enumerate mai sus, sunt precizate in art. 42 din Lege, astfel că autoritățile competente:

- analizează continuu entitățile dintr-un anumit sector pentru recunoașterea/nerecunoașterea acestora ca operator de servicii și emite deciziile necesare;
- imediat după emiterea unei decizii privind recunoașterea ca operator de servicii esențiale sau a unei decizii privind expirarea deciziei privind recunoașterea ca operator de servicii esențiale, înaintează ministrului responsabil cu informatizarea cereri de înscriere în registrul operatorilor de servicii esențiale sau de radiere din acest registru
- elaborează, în cooperare cu CSIRT NASK, CSIRT GOV, CSIRT MON și echipele sectoriale de securitate cibernetică, recomandări privind acțiunile menite să consolideze securitatea cibernetică, inclusiv orientări sectoriale privind raportarea incidentelor;
- monitorizează aplicarea prevederilor Legii de către operatorii de servicii-cheie și furnizorii de servicii digitale;
- solicită, la cererea CSIRT NASK, CSIRT GOV sau CSIRT MON, operatorilor de servicii esențiale sau furnizorilor de servicii digitale să elimine, într-o perioadă determinată, vulnerabilitățile care au condus sau ar fi putut conduce la un incident grav, semnificativ sau critic;
- efectuează inspecții la operatorii de servicii esențiale și la furnizorii de servicii digitale;
- poate coopera cu autoritățile competente din statele membre ale Uniunii Europene prin intermediul Punctului unic de contact;
- prelucrează informații, inclusiv date cu caracter personal, referitoare la serviciile esențiale și serviciile digitale furnizate și la operatorii de servicii esențiale sau furnizorii de servicii digitale;
- participă la exerciții de securitate cibernetică organizate în Republica Polonă sau în Uniunea Europeană.

Legea prevede și faptul că autoritatea responsabilă pentru cibersecuritate poate stabili echipe sectoriale pentru anumite domenii de activitate, caz în care informează operatorii de servicii cheie despre existența și scopul echipei nou înființate.

În Polonia există în total 38 de echipe de răspuns la incidente de cibersecuritate. Dintre acestea, patru echipe sunt constituite în cadrul unor operatori de energie importanți.

Unul dintre acești mari operatori este Enea SA[19], cu sediul in Poznan. Misiunea CERT ENEA este de a sprijini companiile din Grupul Enea să se protejeze împotriva atacurilor

[19] Compania este furnizor de electricitate și a fost înființată ca urmare a transformării întreprinderii de stat Zakład Energetyczny Poznań în compania Energetyka Poznańska Spółka Akcyjna și fuziunea cu societățile: Energetyka Szczecińska SA, Zielonogórskie Zakłady Energetyczne SA, Zakład Energetyczny Gorzów SA, Zakład Energetyczny Bydgoszcz SA, prin preluarea activelor acestor societăți.

intenționate și rău intenționate care ar împiedica integritatea activelor lor IT și OT și ar dăuna intereselor Grupului Enea. Domeniul de aplicare al activităților CERT ENEA acoperă prevenirea, detectarea, răspunsul și recuperarea.

Alt operator care deține o echipă de răspuns la incidente este Energa SA cu sediul in Gdansk. Acesta este unul dintre furnizorii majori de energie electrică dar și de gaz și energie termică.

In cadrul operatorului GAZ-SYSTEM își desfășoară activitatea echipa GAZ-SYSTEM CERT care are misiunea de a răspunde activ și gestiona cuprinzător incidentele de securitate TIC la GAZ-SYSTEM S.A.

De asemenea, compania E.ON găzduiește E.ON CERT care sprijină în primul rând rezistența cibernetică a grupului E.ON SE și a filialelor în care E.ON este acționar majoritar și a societăților 50/50, la cererea societății. Componente sunt echipe de securitate a informațiilor.

PORTUGALIA

În Portugalia există mai multe act normative prin care s-a reglementat gradual domeniul securității cibernetice.

Prin Rezoluția Consiliului de Miniștri nr. 42/2012, din 13 aprilie, este creat comitetul de instalare, care are ca scop crearea, instalarea și funcționarea unui Centru Național de Securitate Cibernetică în Portugalia. La 6 octombrie 2014, prin Decretul-lege 69/2014 este creat Centrul Național de Cibersecuritate (referit atunci ca CNCSeg) în cadrul Oficiului Național de Securitate al țării. Centrul își dobândește denumirea actuală prin Decretul-lege nr. 136/2017. Odată cu publicarea Legii nr. 46/2018, care stabilește regimul juridic al securității spațiului cibernetic[20], CNCS primește competența de autoritate națională de securitate cibernetică în cadrul Oficiului Național de Securitate al Portugaliei, iar ca echipă de răspuns la incidentele de securitate cibernetică este desemnat CERT.PT[21] care exercită

[20] Această lege transpune Directiva (EU) 2016/1148 NIS2 în Portugalia.

[21] CERT.PT este un serviciu integral al CNSC care coordonează răspunsul la incidentele care implică entități ale administrației publice, operatori de infrastructuri critice, operatori de servicii esențiale și furnizori de servicii digitale dincolo de întregul spațiu cibernetic național, inclusiv orice dispozitiv care aparține unei rețele sau unui spațiu de adrese atribuit unui operator de comunicații electronice, unei instituții, unei persoane juridice sau fizice cu sediul pe teritoriul portughez sau situat fizic pe teritoriul portughez. CERT:PT exercită coordonarea operațională în materie de răspuns la incidente, în special în colaborare cu echipele sectoriale existente de răspuns la incidente de securitate IT
CERT.PT este membru al rețelei naționale CSIRT și reprezentant național în rețeaua europeană CSIRT, instituită prin Directiva NIS2.
CERT.PT este un *Trusted Introducer* acreditat și membru cu drepturi depline al Forum of Incident Response and Security Teams (FIRST).

coordonarea operațională în materie de răspuns la incidente, în special în colaborare cu echipele sectoriale de răspuns la incidente de securitate IT.

Regimul juridic al securității spațiului cibernetic se aplică entităților administrației publice, operatorilor de infrastructuri critice, operatorilor de servicii esențiale, furnizorilor de servicii digitale, precum și oricăror alte entități care utilizează rețele și sisteme informatice, respectiv în cadrul notificării voluntare a incidentelor.

Legea 46/2018 instituie, în capitolul II, Structura națională pentru securitatea spațiului cibernetic, din care face parte Consiliul Superior pentru Securitatea Spațiului Cibernetic, ca organism specific de consultare a prim-ministrului cu privire la chestiuni legate de securitatea spațiului cibernetic. Tot în acest capitol, se instituie Centrul Național de Securitate Cibernetică ca autoritate națională de securitate cibernetică și „CERT.PT" ca echipă națională de răspuns la incidente de securitate informatică.

Capitolul III stabilește că entitățile cărora li se aplică regimul juridic privind securitatea spațiului cibernetic trebuie să adopte cerințe de securitate și să notifice Centrului Național de Securitate Cibernetică incidentele cu un impact relevant asupra securității rețelelor și sistemelor lor informatice. În sfârșit, capitolul IV consacră regimul de supraveghere și sancțiuni, iar capitolul V consacră dispozițiile finale, cu accent pe regimul de identificare a operatorilor de servicii esențiale și a furnizorilor de servicii digitale.

Decretul-lege nr. 65/2021, prevede aplicarea cerințelor de securitate și de notificare a incidentelor pentru toate entitățile din domeniu, cu excepția furnizorilor de servicii digitale cărora, în ceea ce privește cerințele de securitate și limitele pentru notificarea incidentelor, li se aplică Regulamentul de punere în aplicare (UE) 2018/151 al Comisiei. Obligațiile acestor entități includ, de asemenea:

- să desemneze și să comunice CNCS punctul de contact permanent respectiv și persoana responsabilă cu securitatea;
- să pregătească inventarul activelor și să transmită CNCS o listă a activelor;
- să elaboreze un plan de securitate;
- să elaboreze și să transmită CNCS raportul anual.

În calitate de coordonator operațional și de autoritate națională în materie de securitate cibernetică cu entitățile de stat, Centrul Național de Cibersecuritate își îndreaptă eforturile și către societate în general, alături de operatorii de infrastructuri critice naționale, operatorii de servicii esențiale și furnizorii de servicii digitale din Portugalia. CNCS dezvoltă un set de activități destinate cetățenilor și organizațiilor, cum ar fi:

- sensibilizarea și formarea pentru comportamente și atitudini (mai) sigure și responsabile în utilizarea tehnologiei și a spațiului cibernetic și formare specializată în diverse domenii ale securității cibernetice;
- elaborarea și difuzarea de alerte, orientări și bune practici pentru utilizarea (mai) sigură a tehnologiei de către cetățeni și organizații, precum și recomandări tehnice și elaborarea de reglementări și referințe destinate în special organizațiilor;

- producerea de cunoștințe privind starea securității cibernetice naționale în diferitele sale aspecte, inclusiv definirea nivelului național de alertă de securitate cibernetică;
- prin intermediul serviciului său CERT.PT, acreditat la nivel internațional și în coordonare cu celelalte entități competente, coordonează răspunsul la incidentele care afectează spațiul cibernetic de interes național; și
- în cadrul domeniului de aplicare al regimului juridic pentru securitatea spațiului cibernetic, care transpune directiva europeană privind securitatea rețelelor și a informațiilor, exercită competențe de reglementare și supraveghere pentru diferitele sectoare de activitate economică.

In rețeaua CSIRT, așa cum este actualizată de către ENISA în pagina CSIRTs by Country - Interactive Map — ENISA (europa.eu), pentru Portugalia sunt înregistrate 36 de echipe de răspuns la incidente de cibersecuritate. Acestea operează în diferite domenii: public, militar, financiar, comercial, educație/cercetare, utilități etc.

O singură echipă dintre acestea figurează in domeniul energiei, și anume CSIRT EDP, care activează în cadrul societății EDP[22]. Această societate are o activitate complexă, fiind furnizor de energie electrică, gaz dar și de servicii de curierat și de sănătate.

Dintre cele 36 de echipe CSIRT înregistrate in Portugalia, observăm că numai 6 sunt membre ale Forumului Echipelor de Răspuns la Incidentele de Securitate (FIRST).

SPANIA

În Spania, Directiva NIS este transpusă prin Decretul-lege regal 12/2018, din 7 septembrie, privind securitatea rețelelor și a sistemelor informatice. Decretul este aplicabil celor două categorii principale:

a) operatorilor de servicii esențiale stabiliți în Spania și operatorilor rezidenți sau domiciliați în alt stat care oferă servicii esențiale prin intermediul unui sediu permanent situat în Spania;

b) furnizorilor de servicii digitale care au sediul social în Spania și care își constituie sediul principal în Uniunea Europeană, precum și celor care, nefiind stabiliți în Uniunea Europeană, își desemnează reprezentantul în Uniune în Spania.

Autoritățile competente în domeniu sunt stabilite prin articolul 9 din Decret, iar acestea sunt:

- Pentru operatorii de servicii esențiale/critice: Ministerul de Interne, prin Centrul Național pentru Protecția Infrastructurii și Securitate Cibernetică (CNPIC);

[22] Natural Gas, Electricity and Energy Services | EDP

- Pentru operatorii de servicii care nu sunt critice: autoritatea sectorială corespunzătoare, astfel cum se stabilește prin reglementări;
- Pentru furnizorii de servicii digitale: secretarul de stat pentru agenda digitală, din cadrul Ministerului Economiei și Mediului de Afaceri;
- Pentru operatorii de servicii esențiale și furnizorii de servicii digitale care nu sunt operatori critici: Ministerul Apărării, prin Centrul Criptologic Național (CCN);
- Consiliul Național de Securitate, prin comisia sa specializată în securitate cibernetică, stabilește mecanismele necesare pentru coordonarea acțiunilor autorităților competente.

Decretul definește și așa numitele *echipe de răspuns la incidente de securitate informatică (CSIRT) de referință* (art. 11):

a) În ceea ce privește relațiile cu operatorii de servicii esențiale:

- CCN-CERT, al Centrului Criptologic Național;
- INCIBE-CERT, al Institutului Național de Securitate Cibernetică din Spania;
- ESPDEF-CERT, din cadrul Ministerului Apărării.

b) În ceea ce privește relațiile cu furnizorii de servicii digitale:

- INCIBE-CERT este de asemenea, o echipă de referință de răspuns la incidente pentru cetățeni, entități de drept privat și alte entități.

CSIRT-urile de referință se coordonează între ele și cu restul CSIRT-urilor naționale și internaționale de răspuns la incidente și de gestionare a riscurilor de securitate care le corespund.

În Spania, acțiunile necesare pentru optimizarea securității infrastructurilor critice sunt în principal încadrate în domeniul protecției împotriva agresiunilor deliberate și, în special, împotriva atacurilor teroriste și, prin urmare, sunt conduse de Ministerul de Interne. Legislația spaniolă stabilește necesitatea de a garanta furnizarea adecvată a serviciilor esențiale, sarcină încredințată Centrului Național pentru Protecția Infrastructurilor Critice (CNPIC), care îl asistă pe secretarul de stat pentru securitate în funcțiile sale. CNPIC a fost înființat în 2007 ca organismul Ministerului de Interne responsabil cu coordonarea și supravegherea tuturor activităților încredințate Secretariatului de Stat pentru securitate în legătură cu protecția infrastructurilor critice de pe teritoriul național.

Atunci când activitățile pe care le desfășoară pot afecta în orice fel un operator critic, CSIRT-urile de referință se coordonează cu Ministerul de Interne, prin intermediul Biroului de coordonare cibernetică al CNPIC, în modul stabilit prin reglementări.

Sistemul PIC[23], inclus în titlul II din Legea 8/2011 pentru protecția infrastructurilor critice, constă într-un set de agenți, din sectorul public și privat, cu competențe și responsabilități

[23] Protecție a infrastructurilor critice

bine definite, astfel încât infrastructurile critice ale statului să furnizeze servicii esențiale pentru societate cu garanții suficiente și fără întreruperi, creând un sistem preventiv care poate anticipa situațiile de criză. Sistemul PIC spaniol este alcătuit din 12 departamente ministeriale și 10 agenții ale administrației centrale și autonome, precum și din peste 250 de operatori critici - publici și privați - sub autoritatea secretarului de stat pentru securitate. Toate acestea implică gestionarea de către CNPIC a unei rețele de peste 300 de entități și a aproximativ 1 200 de planuri de securitate, atât la nivel strategic, cât și operațional.

Centrul Criptologic Național (CCN) este organismul însărcinat cu coordonarea acțiunilor diferitelor organisme ale administrației care utilizează mijloace sau proceduri de criptare, cu garantarea securității tehnologiilor informației în acest domeniu, cu raportarea privind achiziționarea coordonată de material criptologic și cu formarea personalului administrației specializat în acest domeniu.
CCN a fost creat în 2004[24], atașat Centrului Național de Informații (CNI). De fapt, Legea 11/2002, care reglementează CNI, încredințează Centrului exercitarea funcțiilor legate de securitatea tehnologiilor informației și de protecția informațiilor clasificate, conferindu-i secretarului de stat director responsabilitatea de a conduce CCN. Din acest motiv, CCN împarte cu CNI mijloace, proceduri, reglementări și resurse.

În cadrul CCN funcționează CCN-CERT care este echipa de răspuns la incidentele de securitate cibernetică. Acest serviciu a fost creat în 2006 în cadrul guvernului național spaniol, iar funcțiile sale sunt stabilite în Legea 11/2002 de reglementare a Centrului național de informații, în Decretul regal 421/2004 de reglementare a CCN și în Decretul regal 311/2022 din 3 mai, care reglementează sistemul de securitate națională. La început, CCN-CERT și-a concentrat activitatea asupra sistemelor diferitelor administrații (generale, regionale și locale) și, ulterior, a extins această responsabilitate la atacurile cibernetice asupra sistemelor întreprinderilor din sectoarele de interes strategic pentru securitatea națională și pentru economia țării în ansamblu.

Misiunea sa este de a contribui la îmbunătățirea securității cibernetice spaniole, fiind centrul național de alertă și răspuns care cooperează și ajută la un răspuns rapid și eficient la atacurile, inclusiv coordonarea la nivelul statului a diferitelor echipe de răspuns la incidente sau centre de operațiuni de securitate cibernetică existente. În cazurile de gravitate deosebită care sunt stabilite prin reglementări și care necesită un nivel de coordonare mai ridicat decât cel necesar în situații obișnuite, CCN-CERT exercita coordonarea națională a răspunsului tehnic al CSIRT-urilor.

În conformitate cu aceste reglementări, CCN-CERT este responsabil de gestionarea incidentelor informatice care afectează orice organism sau întreprindere publică. În cazul operatorilor critici din sectorul public, gestionarea incidentelor cibernetice va fi realizată de CCN-CERT în coordonare cu (CNPIC).

[24] prin Decretul regal 421/2004

În același mod, Strategia națională de securitate cibernetică acordă CCN-CERT un rol central în linia de acțiune Securitatea sistemelor informatice și de telecomunicații susținute de administrațiile publice, prin consolidarea capacităților de informații, detectare, analiză și răspuns ale CCN-CERT și ale sistemelor sale de detectare și avertizare rapidă.

Începând cu 28 octombrie 2014, Institutul Național de Tehnologii de Comunicații, S.A. (INTECO) a fost redenumit Institutul Național de Securitate Cibernetică din Spania M.P., S.A. (INCIBE), în conformitate cu hotărârea adoptată în cadrul Adunării Generale din 27 octombrie 2014. Prin această schimbare de nume și de imagine, INCIBE a căpătat o identitate în conformitate cu orientarea strategică și poziționarea sa ca centru național de referință în domeniul securității cibernetice.

Institutul Național de Securitate Cibernetică din Spania M.P., S.A. (INCIBE) este o companie aflată în subordinea Ministerului pentru Transformare Digitală și Funcție Publică prin intermediul Secretarului de Stat pentru Digitalizare și Inteligență Artificială și este entitatea de referință pentru dezvoltarea securității cibernetice și a încrederii digitale a cetățenilor, a rețelei academice și de cercetare spaniole (RedIRIS) și a companiilor, în special pentru sectoarele strategice. Ca centru de excelență, INCIBE este un instrument al guvernului pentru dezvoltarea securității cibernetice. În acest scop, cu o activitate bazată pe cercetare, furnizarea de servicii și coordonarea cu agenți cu competențe în domeniu, INCIBE coordonează diferite acțiuni pentru securitatea cibernetică la nivel național și internațional.

INCIBE-CERT este centrul de referință de răspuns la incidente de securitate pentru cetățeni și entități de drept privat din Spania, gestionat de Institutul Național de Securitate Cibernetică. În cazul gestionării incidentelor care afectează operatorii critici din sectorul privat, INCIBE-CERT este operat în comun de INCIBE și OCC, Biroul de coordonare a securității cibernetice al Ministerului de Interne. INCIBE-CERT este una dintre echipele de răspuns la incidente de referință care se coordonează cu restul echipelor naționale și internaționale pentru a îmbunătăți eficiența în lupta împotriva infracțiunilor care implică rețele și sisteme informatice.

UNGARIA

În 2013, luând în considerare Strategia de securitate a Ungariei, Strategia națională de securitate cibernetică a Ungariei și Strategia de securitate cibernetică a Uniunii Europene, Parlamentul maghiar a adoptat Legea L din 2013 privind securitatea informațiilor electronice ale organismelor de stat și ale administrațiilor locale (IBTV)[25], care a intrat în vigoare la 1 iulie 2013.

[25] https://nki.gov.hu/en/ncsc/contents/legislation/

IBTV stabilește ca obiectiv consolidarea activelor naționale de date electronice și securitatea sistemelor informatice electronice ale organismelor guvernamentale de stat și locale, precum și a sistemelor informatice vitale și a componentelor sistemului; declară că organismul de stat care operează și exploatează sistemele informatice electronice este responsabil pentru securitate.

În plus, legea a stabilit sistemul organizațional maghiar de apărare cibernetică, al cărui scop de bază este de a sprijini și de a controla îndeplinirea sarcinilor de securitate a informațiilor de către organismele de stat cu servicii de securitate și de a dezvolta conștiința de securitate cu privire la întregul sistem organizațional de stat.

Elementul de nivel strategic al sistemului organizațional este Consiliul Național de Coordonare Cibernetică, a cărui sarcină este de a facilita coordonarea activităților strategice ale guvernului și de a monitoriza punerea în aplicare, precum și Forumul de Securitate Cibernetică, înființat pentru a canaliza opinia profesională a sectorului privat în procesul decizional al guvernului.

Elementele operaționale ale sistemului de organizare sunt:

- autoritatea de securitate a informațiilor responsabilă de verificarea și aplicarea cerințelor legale;
- un centru de gestionare a incidentelor care abordează direct atacurile și amenințările din spațiul cibernetic și
- organismul responsabil de identificarea punctelor slabe ale sistemelor informatice și de testarea capacităților de protecție a sistemului (evaluarea vulnerabilității).

Ca urmare a modificării IBTV în 2015*, Serviciul Special pentru Securitate Națională (SSNS)* a fost desemnat să opereze sarcinile operaționale de mai sus cu privire la sistemele informatice ale organizațiilor guvernamentale de stat și locale. Iar în cadrul acestei organizații a fost înființat Centrul Național pentru Securitate Cibernetică (NKI) la 1 octombrie 2015. Centrul Național de Securitate Cibernetică pentru Ungaria a fost înființat prin unificarea GovCERT-Ungaria, a Autorității Naționale pentru Securitatea Informațiilor Electronice (NEISA) și a Autorității de Management a Apărării Cibernetice (CDMA). Astfel, Centrul este mai coordonat, iar punerea în aplicare a sarcinilor sunt mai eficiente în această organizație unificată. Datorită acestor măsuri, Centrul Național de Securitate Cibernetică poate urmări și ajuta întregul ciclu de viață al securității informatice a sistemelor informatice electronice, de la evoluție, faza de planificare, reglementare, până la control și gestionarea incidentelor.

Ca urmare a modificărilor legislative care au intrat în vigoare la 1 ianuarie 2019, Centrul Național pentru Securitate Cibernetică îndeplinește sarcinile de gestionare a evenimentelor din sistemele informatice critice și componentele sistemelor, precum și gestionează evenimentele și supraveghează oficial furnizorii de servicii care trebuie notificate, conform Legii CVIII din 2001 privind anumite aspecte ale serviciilor de comerț electronic și ale serviciilor societății informaționale, cum ar fi piețele online, serviciile de căutare pe internet și serviciile cloud.

Sarcinile legale ale Centrului Național pentru Securitate Cibernetică includ, de asemenea, funcționarea așa-numitului Punct național de contact (SPOC), care este responsabil pentru coordonarea în Ungaria a incidentelor cibernetice cu impact ridicat în cadrul Uniunii Europene, primirea și trimiterea rapoartelor privind incidentele către organizațiile partenere internaționale.

In anul 2020 a fost emis Decretul guvernamental 374/2020 (VII.30.) privind identificarea, desemnarea și protecția sistemelor și instalațiilor critice din sectorul energetic. Decretul stabilește autoritățile sectoriale pentru definirea infrastructurilor critice din sectorul energetic. Acestea sunt:

- Autoritatea de reglementare în domeniul energiei și al serviciilor publice pentru sistemul de energie electrică, sistemul de gaze naturale și sectorul încălzirii urbane;
- Autoritatea minieră în ceea ce privește industria petrolieră și producția de gaze naturale;
- Primăria Capitalei și birourile guvernamentale / județene în calitatea lor decizională pentru chestiuni metrologice și tehnice pentru prelucrarea petrolului și depozitarea produselor petroliere.

Prin decret sunt definite criteriile sectoriale pentru infrastructura critică europeană, pentru infrastructura critică națională, efectul perturbator semnificativ în sectorul energetic, praguri pentru serviciile de bază în sectorul energetic, cerințele de calificare pentru ofițerul de contact în materie de securitate, norme sectoriale detaliate pentru evenimentele extraordinare și alte norme tehnice.

In Ungaria există 3 echipe de răspuns la incidentele de securitate cibernetică, iar dintre acestea, Centrul Național de Securitate Cibernetică acoperă și domeniul energiei.

Webografie

https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-ReadinessTeam#:~:text=A%20Computer%20Emergency%20Response%20Team,to%20an%20organization's%20cybersecurity%20incidents

National CERT/CSIRT – Mandate and Organisation, NATO National_CERT-CSIRT_Mandate_and_Organisation_final_.pdf (ccdcoe.org)

Trusted introducer: Trusted Introducer : Services: Overview of TI Services: TI Overview: Romanian (trusted-introducer.org)

Ghid How to set up a CSIRT and SOC

Germania:

- Legea privind furnizarea de gaze și electricitate, https://www.gesetze-im-internet.de/enwg_2005/BJNR197010005.html
- Legea energiei termice și electrice combinate, https://www.gesetze-im-internet.de/kwkg_2016/BJNR249810015.html
- Legea privind extinderea energiilor regenerabile, https://www.gesetze-im-internet.de/eeg_2014/BJNR106610014.html
- Catalogul de securitate IT pentru rețelele de electricitate și gaz, https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/Anlagenbetreiber/start.html
- Securitatea aprovizionării cu electricitate și gaze, https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/start.html
- Politica federală de securitate energetică, https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html
- Protecția infrastructurilor critice (energie, apă, transport), https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-artikel.html;jsessionid=D2DAA23068A124EAEB2A81DFFDE68C57.live861
- Oficiul federal pentru protecție civilă și intervenție în caz de dezastre (BBK), https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html
- Agenția federală pentru rețele (BNetzA), https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/start.html

Măsuri în cazul unui incident informatic, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/Massnahmenkatalog/massnahmenkatalog_node.html

Irlanda:

- Strategia națională de securitate cibernetică 2019-2024, https://www.ncsc.gov.ie/strategy/
- Noi obligații impuse de Directiva NIS2, https://www.mccannfitzgerald.com/knowledge/data-privacy-and-cyber-risk/impending-cybersecurity-obligations-are-you-subject-to-nis-2
- Raportarea incidentelor, https://www.ncsc.gov.ie/incidentreporting/

Italia

- Rezumat al proiectului de lege care va implementa NIS2, https://www.agendadigitale.eu/sicurezza/litalia-si-allinea-alla-nis-2-ecco-le-nuove-norme-per-la-sicurezza-informatica/
- Planul de implementare a NIS2, https://www.enisa.europa.eu/events/enisapolicyconference-v2_pub.pdf
- Centrele de operațiuni de securitate (SOC), https://www.agendadigitale.eu/sicurezza/security-operations-center-quale-soc-scegliere-in-azienda-ibrido-tiered-o-interno-come-orientarsi/
- Securitatea cibernetică a sectorului energie, https://www.agendadigitale.eu/sicurezza/cybersecurity-settore-energetico-sotto-attacco-come-rispondono-ue-e-italia/
- Departamentul de informații pentru securitate, https://www.sicurezzanazionale.gov.it/chi-siamo/organizzazione/dis
- Agenția de informații și securitate externă, https://www.sicurezzanazionale.gov.it/chi-siamo/organizzazione/aise
- Cybersecurity in Italy, 2019, https://www.esteri.it/mae/resource/doc/2019/09/esteri_cibersecurity_web.pdf

Polonia:

Legal acts - Ministry of Digital Affairs - Portal Gov.pl (www.gov.pl)

Spania:

Legea 8/2011, din 28 aprilie, de stabilire a măsurilor de protecție a infrastructurilor critice

Decretul regal 704/2011, din 20 mai, de aprobare a Regulamentului pentru protecția infrastructurilor critice

Decretul-lege regal 12/2018, din 7 septembrie, privind securitatea rețelelor și a sistemelor informatice

Decretul regal 43/2021, din 26 ianuarie, care dezvoltă Decretul-lege regal 12/2018, din 7 septembrie, privind securitatea rețelelor și a sistemelor informatice