RECOMANDĂRI

RECOMANDAREA (UE) 2017/1584 A COMISIEI

din 13 septembrie 2017

privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare

COMISIA EUROPEANĂ,

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

întrucât:

(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale în toate sectoarele de activitate economică, întrucât întreprinderile și cetățenii sunt astăzi mai interconectați și mai interdependenți decât oricând, dincolo de sectoare și de frontiere. Statele membre și instituțiile UE trebuie să fie bine pregătite pentru eventualitatea unui incident de securitate cibernetică ce ar afecta organizațiile din mai multe state membre sau chiar din întreaga Uniune, cu perturbări potențial grave ale pieței interne și, într-un sens mai larg, ale rețelelor și sistemelor informatice pe care se bazează economia, democrația și societatea din Uniune.

(2) Un incident de securitate cibernetică poate fi considerat o criză la nivelul Uniunii dacă perturbarea cauzată de incidentul respectiv este prea extinsă pentru ca un stat membru afectat să o gestioneze singur sau dacă incidentul afectează două sau mai multe state membre și are un impact tehnic sau politic atât de mare încât să necesite o coordonare și un răspuns prompte la nivel politic din partea Uniunii.

(3) Dat fiind că incidentele de securitate cibernetică pot declanșa o criză mai extinsă, cu impact și asupra altor sectoare de activitate decât rețelele și sistemele informatice și rețelele de comunicare, un răspuns adecvat trebuie să cuprindă măsuri de atenuare nu numai de natură cibernetică, ci și de natură mai amplă.

(4) Incidentele de securitate cibernetică sunt imprevizibile, adesea apar și evoluează în intervale foarte scurte de timp și, prin urmare, entitățile afectate și toți cei cu responsabilități în ceea ce privește răspunsul la incident și atenuarea efectelor acestuia trebuie să se coordoneze rapid. În plus, adesea incidentele de securitate cibernetică nu sunt limitate la o zonă geografică specifică și pot să apară simultan sau să se extindă instantaneu la mai multe țări.

(5) Un răspuns eficace la incidentele și crizele de securitate cibernetică de mare amploare la nivelul UE necesită o cooperare promptă și eficace între toate părțile interesate și depinde atât de nivelul de pregătire și de capacitățile fiecărui stat membru, cât și de luarea de măsuri coordonate bazate de capacitățile Uniunii. Prin urmare, pentru a răspunde prompt și eficace la astfel de incidente sunt necesare proceduri și mecanisme de cooperare care să fie instituite în prealabil și, în măsura posibilului, să facă obiectul unor exerciții adecvate, cu definirea clară a rolurilor și responsabilităților actorilorcheie la nivel național și la nivelul Uniunii.

(6) În concluziile ([1]) sale din 27 mai 2011 privind protecția infrastructurilor critice de informație, Consiliul a invitat statele membre ale UE să „consolideze cooperarea dintre statele membre și să contribuie, pe baza experiențelor și a rezultatelor naționale în domeniul gestionării crizelor și în cooperare cu ENISA, la dezvoltarea unor mecanisme europene de cooperare în caz de incidente informatice care urmează să fie testate în cadrul următorului exercițiu informatic european în 2012”.

(7) Comunicarea din 2016 privind consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator ([2]) a invitat statele membre să utilizeze cât mai mult mecanismele de cooperare instituite de Directiva privind securitatea rețelelor și a informațiilor ([3]) și să

([1]) Concluziile Consiliului privind protecția infrastructurilor critice de informație „Realizări și etape următoare: către un context global de securitate cibernetică”, documentul 10299/11, Bruxelles, 27 mai 2011.
([2]) COM(2016) 410 final, 5 iulie 2016.
([3]) 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).

consolideze cooperarea transfrontalieră legată de pregătirea pentru un incident de securitate cibernetică de mare amploare. De asemenea, comunicarea a arătat că un „plan de acțiune" care să instituie o abordare coordonată privind cooperarea în situații de criză între diferitele elemente ale ecosistemului cibernetic ar spori gradul de pregătire și ar asigura totodată sinergiile și coerența cu mecanismele existente de gestionare a crizelor.

(8) În Concluziile Consiliului ([1]) privind comunicarea menționată anterior, statele membre au cerut Comisiei să prezinte un astfel de plan de acțiune, pentru a fi examinat de organismele relevante și de celelalte părți interesate. Directiva privind securitatea rețelelor și a sistemelor informatice nu prevede însă un cadru de cooperare la nivelul Uniunii în cazul unor incidente și crize de securitate cibernetică de mare amploare.

(9) La 5 aprilie și la 4 iulie 2017, Comisia a organizat la Bruxelles două ateliere de consultare a statelor membre, la care au participat reprezentanți ai statelor membre din echipele de intervenție în caz de incidente de securitate informatică (CSIRT), din grupul de cooperare instituit prin Directiva privind securitatea rețelelor și a sistemelor informatice și din Grupul de lucru orizontal pentru chestiuni cibernetice al Consiliului, precum și reprezentanți ai Serviciului European de Acțiune Externă (SEAE), ai ENISA, ai Europol/EC3 și ai Secretariatului General al Consiliului (SGC).

(10) Planul de acțiune privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare la nivelul Uniunii, anexat la prezenta recomandare, este rezultatul consultărilor menționate mai sus și completează Comunicarea privind consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator.

(11) Planul de acțiune descrie și stabilește obiectivele și modalitățile de cooperare între statele membre și instituțiile, organele, oficiile și agențiile UE (denumite în continuare „instituțiile UE") în vederea răspunsului la incidentele și crizele de securitate cibernetică de mare amploare, precum și modul în care mecanismele existente de gestionare a crizelor pot valorifica la maximum resursele entităților din domeniul securității cibernetice instituite la nivelul UE.

(12) Pentru a răspunde unei crize de securitate cibernetică în sensul considerentului 2, coordonarea răspunsului la nivel politic al Uniunii în cadrul Consiliului va utiliza mecanismul integrat pentru un răspuns politic la crize (IPCR) ([2]); Comisia va utiliza procesul ARGUS ([3]) de coordonare transsectorială la nivel înalt în situații de criză. În cazul în care criza are o importantă dimensiune externă sau de politică de securitate și apărare comună (PSAC), se activează mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă ([3]) (SEAE).

(13) În anumite domenii, mecanismele sectoriale de gestionare a crizelor la nivelul UE prevăd modalități de cooperare în cazul unor incidente sau crize de securitate cibernetică. De exemplu, în contextul Sistemului Global de Navigație prin Satelit European (GNSS), Decizia 2014/496/PESC a Consiliului ([4]) a definit deja rolurile care revin Consiliului, Înaltului Reprezentant, Comisiei, Agenției GNSS European și statelor membre în cadrul lanțului de responsabilități operaționale instituit pentru a reacționa la o amenințare la adresa Uniunii, a statelor membre sau a GNSS, inclusiv în caz de atacuri cibernetice. Prin urmare, prezenta recomandare ar trebui să nu aducă atingere acestor mecanisme.

(14) Statele membre răspund în principal de răspunsul la incidentele sau crizele de securitate cibernetică de mare amploare care le afectează. Comisia, Înaltul Reprezentant și alte instituții sau servicii ale UE au totuși un rol important, care decurge din dreptul Uniunii sau din faptul că incidentele și crizele de securitate cibernetică pot avea un impact asupra tuturor sectoarelor de activitate economică ale pieței unice, asupra securității și a relațiilor internaționale ale Uniunii, precum și asupra instituțiilor UE.

(15) La nivelul Uniunii, principalele entități implicate în răspunsul la crizele de securitate cibernetică sunt structurile și mecanismele nou instituite prin Directiva privind securitatea rețelelor și a sistemelor informatice, și anume rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT), precum și agențiile și organismele relevante, și anume Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), Centrul european de combatere a criminalității informatice (Europol/EC3), Centrul de analiză a informațiilor al UE (INTCEN), Divizia de informații a Statului-Major al UE (EUMS INT) și Celula de supraveghere (SITROOM), care cooperează în cadrul SIAC (Capacitatea unică de analiză a informațiilor), al Celulei de fuziune a UE împotriva amenințărilor hibride (care funcționează în cadrul INTCEN), al Centrului de răspuns la incidente de securitate cibernetică pentru instituțiile și agențiile UE (CERT-UE) și în cadrul Centrului de coordonare a răspunsului la situații de urgență al Comisiei Europene.

(16) Cooperarea la nivel tehnic dintre statele membre în ceea ce privește răspunsul la incidentele de securitate cibernetică este asigurată de rețeaua CSIRT instituită prin Directiva privind securitatea rețelelor și a sistemelor

([1]) Documentul 14540/16, 15 noiembrie 2016.
([2]) Informații suplimentare pot fi găsite în secțiunea 3.1 din apendicele privind gestionarea crizei, mecanismele de cooperare și actorii la nivelul UE.
([3]) Ibid.
([4]) Decizia 2014/496/PESC a Consiliului din 22 iulie 2014 privind aspecte ale desfășurării, funcționării și utilizării Sistemului Global de Navigație prin Satelit European care afectează securitatea Uniunii Europene și de abrogare a Acțiunii comune 2004/552/PESC (JO L 219, 25.7.2014, p. 53)

informatice. ENISA asigură secretariatul rețelei și sprijină activ cooperarea dintre echipele CSIRT. Echipele naționale CSIRT și CERT-UE cooperează și fac schimb de informații în mod voluntar, inclusiv, atunci când este necesar, pentru a răspunde la incidente de securitate cibernetică ce afectează unul sau mai multe state membre. La cererea reprezentantului unei echipe CSIRT dintr-un stat membru, acestea pot discuta și, dacă este posibil, identifica un răspuns coordonat la un incident care a fost identificat în jurisdicția respectivului stat membru. Procedurile aplicabile vor fi definite în Procedurile standard de operare (PSO) ale rețelei CSIRT ([1]).

(17) Rețeaua CSIRT are, de asemenea, sarcina de a discuta, a examina și a identifica noi forme de cooperare operațională, inclusiv în ceea ce privește categoriile de riscuri și incidente, alertele timpurii, asistența reciprocă și principiile și modalitățile de coordonare, în contextul răspunsului statelor membre la riscuri și incidente transfrontaliere.

(18) Grupul de cooperare instituit în temeiul articolului 11 din Directiva privind securitatea rețelelor și a sistemelor informatice are sarcina de a elabora orientări strategice pentru activitățile rețelei CSIRT și de a discuta capacitățile și nivelul de pregătire ale statelor membre, precum și, pe bază de voluntariat, de a evalua strategiile naționale privind securitatea rețelelor și a sistemelor informatice și eficacitatea echipelor CSIRT, identificând cele mai bune practici.

(19) În cadrul grupului de cooperare, o linie specifică de activitate este reprezentată de pregătirea de orientări privind notificarea incidentelor, în temeiul articolului 14 alineatul (7) din Directiva privind securitatea rețelelor și a sistemelor informatice, în ceea ce privește circumstanțele în care operatorii de servicii esențiale sunt obligați să notifice incidente în temeiul articolului 14 alineatul (3) și formatul și procedurile pentru aceste notificări ([2]).

(20) Pentru a lua decizii bine fundamentate, este indispensabil să se asigure, prin intermediul rapoartelor, al evaluărilor, al cercetării, al anchetelor și al analizei, o cunoaștere și o înțelegere în timp real a situației, a poziției de risc și a amenințărilor. Această cunoaștere a situației de către toate părțile interesate este esențială pentru un răspuns coordonat eficace. Cunoașterea situației include aspectele privind cauzele, precum și impactul și originea incidentului. Este recunoscut faptul că aceasta depinde de schimbul și de partajarea informațiilor între părțile relevante într-un format adecvat, conform unei taxonomii comune pentru descrierea incidentului și într-un mod suficient de securizat.

(21) Răspunsul la incidentele de securitate cibernetică poate lua mai multe forme, în funcție de tipul de incident, de la identificarea unor măsuri tehnice care pot implica investigarea în comun de către două sau mai multe entități a cauzelor tehnice ale incidentelor (de exemplu, analiza programelor *malware*) sau identificarea unor metode prin care organizațiile pot evalua dacă au fost afectate (de exemplu, indicatori de compromis), la decizii operaționale privind aplicarea acestor măsuri și, la nivel politic, decizii privind utilizarea altor instrumente, precum Cadrul pentru un răspuns comun la activitățile cibernetice răuvoitoare ([3]) sau protocolul operațional al UE pentru combaterea amenințărilor hibride ([4]).

(22) Încrederea cetățenilor și a întreprinderilor din UE în serviciile digitale este esențială pentru ca piața unică digitală să prospere. Prin urmare, comunicarea în situații de criză joacă un rol deosebit de important în atenuarea efectelor negative ale incidentelor și crizelor de securitate cibernetică. Comunicarea poate fi, de asemenea, utilizată în contextul Cadrului pentru un răspuns diplomatic comun, pentru a influența comportamentul agresorilor (potențiali) care acționează din țări terțe. Pentru un răspuns politic eficace, este esențială o armonizare a comunicării publice care vizează atenuarea efectelor negative ale incidentelor și crizelor de securitate cibernetică, precum și a comunicării publice care urmărește să influențeze un agresor.

(23) Informarea publicului în legătură cu modul în care utilizatorii și organizațiile pot atenua efectele unui incident (de exemplu prin aplicarea unui *patch* sau prin acțiuni complementare pentru a evita amenințarea) ar putea fi o măsură eficace de atenuare a unui incident sau a unei crize cibernetice de mare amploare.

(24) Comisia, prin intermediul infrastructurii de servicii digitale pentru securitatea cibernetică a Mecanismului pentru interconectarea Europei (MIE), dezvoltă în prezent un mecanism de cooperare, sub forma unei platforme centrale de servicii (MeliCERTes), între CSIRT ale statelor membre participante, cu scopul de a îmbunătăți nivelul de pregătire, cooperarea și răspunsul la amenințările și incidentele cibernetice emergente. Comisia, prin intermediul unor cereri competitive de propuneri pentru acordarea de granturi în cadrul MIE, cofinanțează CSIRT din statele membre în vederea îmbunătățirii capacităților operaționale ale acestora la nivel național.

([1]) În curs de elaborare; se preconizează că vor fi adoptate până la sfârșitul anului 2017.
([2]) Orientările sunt planificate să fie finalizate până la sfârșitul anului 2017.
([3]) Concluziile Consiliului referitoare la un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică"), doc. 9916/17.
([4]) Documentul de lucru al serviciilor Comisiei privind protocolul operațional al UE pentru combaterea amenințărilor hibride, SWD(2016) 227 final din 5 iulie 2016.

(25) Exercițiile de securitate cibernetică la nivelul UE sunt esențiale pentru a stimula și a îmbunătăți cooperarea dintre statele membre și sectorul privat. În acest scop, începând din 2010, ENISA organizează periodic exerciții de securitate cibernetică paneuropene („Cyber Europe").

(26) În Concluziile Consiliului ([1]) privind punerea în aplicare a Declarației comune a președintelui Consiliului European, președintelui Comisiei Europene și secretarului general al Organizației Tratatului Atlanticului de Nord se subliniază necesitatea de a consolida cooperarea în materie de exerciții de securitate cibernetică prin participarea reciprocă a personalului la exercițiile în cauză, inclusiv, în special, la exercițiile Cyber Coalition și Cyber Europe.

(27) Evoluția continuă a naturii amenințărilor, precum și incidentele recente de securitate cibernetică sunt un indiciu al riscului tot mai mare cu care se confruntă Uniunea, iar statele membre ar trebui să dea curs prezentei recomandări fără întârziere și, în orice caz, până la sfârșitul anului 2018,

ADOPTĂ PREZENTA RECOMANDARE:

(1) Statele membre și instituțiile UE ar trebui să instituie un cadru al UE de răspuns la crizele de securitate cibernetică, în care să integreze obiectivele și modalitățile de cooperare prezentate în planul de acțiune, conform principiilor directoare descrise în acesta.

(2) Cadrul UE de răspuns la crizele de securitate cibernetică ar trebui, în special, să identifice actorii, instituțiile UE și autoritățile naționale relevante, la toate nivelurile necesare – tehnic, operațional, strategic/politic – și să instituie, după caz, proceduri standard de operare care să definească modalitățile de cooperare în cadrul mecanismelor UE de gestionare a crizelor. Ar trebui să se pună accentul pe posibilitatea schimbului de informații fără întârzieri nejustificate și pe coordonarea răspunsului în situații de incidente și crize de securitate cibernetică de mare amploare.

(3) În acest scop, autoritățile competente ale statelor membre ar trebui să colaboreze pentru a detalia suplimentar protocoalele privind schimbul de informații și cooperarea. Grupul de cooperare și instituțiile relevante ale UE ar trebui să facă schimb de experiență cu privire la aceste chestiuni.

(4) Statele membre ar trebui să se asigure că mecanismele lor naționale de gestionare a crizelor abordează în mod adecvat răspunsul la incidentele de securitate cibernetică și stabilesc procedurile necesare pentru cooperarea în contextul cadrului UE.

(5) În ceea ce privește mecanismele existente de gestionare a crizelor ale UE, statele membre, în colaborare cu serviciile Comisiei și cu SEAE, ar trebui să stabilească, în conformitate cu planul de acțiune, orientări practice de punere în aplicare în ceea ce privește integrarea entităților și a procedurilor în materie de gestionare a crizelor și de securitate cibernetică în mecanismele de gestionare existente la nivelul UE, și anume IPCR și mecanismul de răspuns în caz de criză al SEAE. În special, statele membre ar trebui să asigure instituirea structurilor adecvate pentru a permite un flux eficient de informații între autoritățile lor naționale de gestionare a crizelor și reprezentanții acestora la nivelul UE, în contextul mecanismelor UE de gestionare a crizelor.

(6) Statele membre ar trebui să utilizeze pe deplin oportunitățile oferite de programul Mecanismului pentru interconectarea Europei (MIE) referitor la infrastructurile de servicii digitale pentru securitatea cibernetică și să coopereze cu Comisia pentru a se asigura că mecanismul de cooperare sub forma platformei centrale de servicii, care este în curs de elaborare, oferă funcționalitățile necesare și îndeplinește cerințele lor de cooperare, inclusiv în cazul crizelor de securitate cibernetică.

(7) Statele membre, cu sprijinul ENISA și utilizând experiența din activitățile anterioare în acest domeniu, ar trebui să coopereze pentru a dezvolta și a adopta o taxonomie și un model comune pentru rapoartele situaționale, în vederea descrierii cauzelor tehnice și a impacturilor incidentelor de securitate cibernetică, precum și a îmbunătățirii în continuare a cooperării lor tehnice și operaționale în situații de criză. În această privință, statele membre ar trebui să ia în considerare lucrările actuale desfășurate de grupul de cooperare pentru a elabora orientări privind notificarea incidentelor, în special în legătură cu formatul notificărilor naționale.

(8) Procedurile stabilite de cadru ar trebui testate și, atunci când este necesar, revizuite, pentru a se ține cont de învățămintele desprinse în urma participării statelor membre la exerciții de securitate cibernetică naționale, regionale și la nivelul Uniunii, precum și la exerciții privind diplomația cibernetică și la exerciții organizate de NATO. În special, acestea ar trebui testate în contextul exercițiilor CyberEurope organizate de ENISA. CyberEurope 2018 reprezintă prima oportunitate de acest fel.

([1]) ST 15283/16, 6 decembrie 2016.

(9) Statele membre și instituțiile UE ar trebui să organizeze periodic exerciții pentru a-și îmbunătăți răspunsul, inclusiv la nivel politic dacă este necesar, în situații de incidente și crize de securitate cibernetică de mare amploare la nivel european, cu implicarea, după caz, a entităților din sectorul privat.

Adoptată la Bruxelles, 13 septembrie 2017.

Pentru Comisie

Mariya GABRIEL

Membru al Comisiei

ANEXĂ

Plan de acțiune privind răspunsul coordonat la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare

INTRODUCERE

Prezentul plan de acțiune se aplică incidentelor de securitate cibernetică care afectează statul membru vizat într-o măsură prea mare pentru a gestiona situația pe cont propriu sau care afectează două sau mai multe state membre ori instituții ale UE, consecințele tehnice sau politice fiind atât de ample și de importante încât trebuie să se asigure rapid coordonarea politicilor și răspunsul la nivelul politic al Uniunii.

Aceste incidente de securitate cibernetică de mare amploare sunt considerate o „criză" de securitate cibernetică.

În cazul unei crize la nivelul UE cu impact asupra securității cibernetice, Consiliul asigură coordonarea răspunsului la nivelul politic al Uniunii, prin intermediul mecanismului integrat pentru un răspuns politic la crize (IPCR).

În cadrul Comisiei, coordonarea se va asigura în conformitate cu ARGUS, sistemul de alertă rapidă.

În cazul în care criza are o importantă dimensiune externă sau de politică de securitate și apărare comună (PSAC), se activează mecanismul de răspuns în caz de criză al SEAE.

Planul de acțiune descrie modul în care aceste mecanisme precise de gestionare a crizelor ar trebui să recurgă pe deplin la entitățile din domeniul securității cibernetice instituite la nivelul UE, precum și la mecanismele de cooperare dintre statele membre.

Astfel, planul de acțiune ține seama de o serie de principii directoare (principiul proporționalității, al subsidiarității, al complementarității și al confidențialității informațiilor), prezintă principalele obiective ale cooperării (răspuns eficace, conștientizare comună a situației, mesaje de comunicare publice) la trei niveluri (strategic/politic, operațional și tehnic), mecanismele și actorii implicați, precum și activitățile în vederea îndeplinirii obiectivelor principale menționate anterior.

Planul de acțiune nu acoperă întregul ciclul de gestionare a crizelor (prevenire/atenuare, pregătire, răspuns, redresare), ci se concentrează asupra răspunsului. Cu toate acestea, se abordează anumite activități, în special cele legate de conștientizarea comună a situației.

Trebuie, de asemenea, subliniat faptul că incidentele de securitate cibernetică pot fi la originea unei crize mai ample sau pot fi o componentă a acestei crize mai ample, cu consecințe și asupra altor sectoare. În contextul în care se estimează că majoritatea crizelor de securitate cibernetică vor avea consecințe asupra lumii fizice, un răspuns adecvat trebuie să includă activități de atenuare atât cu caracter cibernetic, cât și fără caracter cibernetic. Activitățile de răspuns în caz de criză de securitate cibernetică ar trebui să fie coordonate cu alte mecanisme de gestionare a crizelor de la nivelul UE, de la nivel național sau sectorial.

În fine, planul de acțiune nu înlocuiește și nu ar trebui să aducă atingere mecanismelor, sistemelor sau instrumentelor sectoriale sau de politică existente, precum cele instituite în cazul Programului pentru Sistemul Global de Navigație prin Satelit European (GNSS) ([1]).

Principii directoare

În demersurile întreprinse în vederea realizării obiectivelor, pentru a identifica activitățile necesare și a atribui rolurile și responsabilitățile actorilor sau ale mecanismelor respective s-au aplicat următoarele principii directoare, care trebuie respectate, de asemenea, atunci când se pregătesc viitoarele orientări de punere în aplicare.

Proporționalitatea: marea majoritate a incidentelor de securitate cibernetică care afectează statele membre nu pot fi considerate nici pe departe o „criză" națională, și cu atât mai puțin una europeană. Cooperarea între statele membre în ceea ce privește răspunsul la astfel de incidente este asigurată de rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) instituită prin Directiva privind securitatea rețelelor și a informațiilor ([2]). Echipele CSIRT naționale cooperează și fac schimb de informații zilnic și în mod voluntar, inclusiv, atunci când este necesar, pentru a răspunde la incidentele de securitate cibernetică care afectează unul sau mai multe state membre, respectând procedurile standard de operare (PSO) ale rețelei CSIRT. Prin urmare, planul de acțiune ar trebui să utilizeze pe deplin aceste PSO, iar orice alte sarcini specifice crizelor de securitate cibernetică ar trebui să se regăsească în planul de acțiune.

([1]) Decizia 2014/496/PESC.
([2]) Directiva (UE) 2016/1148.

Subsidiaritate: principiul subsidiarității este un principiu esențial. Statele membre răspund în principal de răspunsul la incidentele sau crizele de securitate cibernetică de mare amploare care le afectează. Cu toate acestea, Comisia, Serviciul European de Acțiune Externă și celelalte instituții, organe, oficii și agenții ale UE au un rol important. Acest rol este definit în mod clar în mecanismele IPCR și derivă, de asemenea, din dreptul Uniunii sau din simplul fapt că incidentele și crizele de securitate cibernetică pot avea un impact asupra tuturor sectoarelor de activitate economică ale pieței unice, asupra securității și a relațiilor internaționale ale Uniunii, precum și asupra instituțiilor UE.

Complementaritate: planul de acțiune ține seama pe deplin de mecanismele de gestionare a crizelor existente la nivelul UE, în principal mecanismul integrat pentru un răspuns politic la crize (IPCR), ARGUS și mecanismul de răspuns în caz de criză al SEAE, integrează în PSO noile structuri și mecanisme prevăzute de Directiva privind securitatea rețelelor și a informațiilor, în principal rețeaua CSIRT, precum și agențiile și organismele relevante, în principal Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), Centrul european de combatere a criminalității informatice din cadrul Europol (Europol/EC3), Centrul de analiză a informațiilor al UE (INTCEN), Direcția de informații a Statului-Major al UE (EUMS INT) și Celula de supraveghere (SITROOM) din cadrul INTCEN care lucrează împreună ca SIAC (Capacitatea unică de analiză a informațiilor); celula de fuziune a UE împotriva amenințărilor hibride (din cadrul INTCEN) și Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE). Astfel, planul de acțiune ar trebui să asigure, de asemenea, că interacțiunea și cooperarea între acestea asigură un grad maxim de complementaritate, concomitent cu un grad minim de suprapuneri.

Confidențialitatea informațiilor: toate schimburile de informații în contextul planului de acțiune trebuie să respecte normele în materie de securitate aplicabile ([1]), cele privind protecția datelor cu caracter personal și protocolul de schimb de informații *Traffic Light Protocol* ([2]). În ceea ce privește schimbul de informații clasificate, indiferent de sistemul de clasificare aplicat, trebuie folosite instrumentele acreditate disponibile ([3]). În ceea ce privește prelucrarea datelor cu caracter personal, se vor respecta normele UE aplicabile, în special Regulamentul general privind protecția datelor ([4]), Directiva asupra confidențialității și comunicațiilor electronice ([5]), precum și regulamentul ([6])„privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date".

Obiective principale

Cooperarea în cadrul planului de acțiune are loc la cele trei niveluri menționate mai sus, și anume la nivel politic, operațional și tehnic. La fiecare nivel, cooperarea poate implica schimb de informații și acțiuni comune, cu obiectivul de a atinge următoarele obiective principale.

— Facilitarea unui răspuns eficace: răspunsul poate lua mai multe forme, în funcție de tipul de incident, de la identificarea unor măsuri tehnice care pot implica investigarea în comun de către două sau mai multe entități a cauzelor tehnice ale incidentelor (de exemplu, analiza programelor malware) sau identificarea unor metode prin care organizațiile pot evalua dacă au fost afectate (de exemplu, indicatori de compromis), la decizii operaționale privind aplicarea acestor măsuri tehnice și, la nivel politic, decizii privind recurgerea la alte instrumente, precum răspunsul diplomatic al UE la activități informatice răuvoitoare („Setul de instrumente pentru diplomația cibernetică") sau protocolul operațional al UE pentru combaterea amenințărilor hibride.

— Conștientizarea comună a situației: pentru a asigura un răspuns coordonat, este esențial ca, pe măsură ce evenimentele se desfășoară, toate părțile interesate relevante să înțeleagă suficient de bine evenimentele la cele trei niveluri (tehnic, operațional, politic). Conștientizarea situației poate include elementele tehnologice privind cauzele, precum și impactul și originea incidentului. Întrucât incidentele de securitate cibernetică pot afecta o gamă largă de sectoare (finanțe, energie, transport, asistență medicală etc.), trebuie ca informațiile corespunzătoare, în formatul adecvat, să ajungă la toate părțile interesate relevante în timp util.

([1]) Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41) și Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53); Decizia Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate din 19 aprilie 2013 privind normele de securitate pentru Serviciul European de Acțiune Externă (JO C 190, 29.6.2013, p. 1); Decizia 2013/488/UE a Consiliului din 23 septembrie 2013 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 274, 15.10.2013, p. 1).

([2]) https://www.first.org/tlp/

([3]) În iunie 2016, aceste canale de transmitere a informațiilor erau: CIMS (Sistemul de gestionare al informațiilor clasificate), ACID (algoritmul de criptare), RUE (sistemul securizat pentru crearea, comunicarea și arhivarea documentelor RESTREINT UE/EU RESTRICTED) și SOLAN. Alte modalități, de exemplu, pentru transmiterea informațiilor clasificate sunt PGP sau S/MIME.

([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([5]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

([6]) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1) – în revizuire.

— Convenirea asupra principalelor mesaje de comunicare publică ([1]): în situații de criză, comunicarea îndeplinește un rol important în atenuarea efectelor negative ale crizelor și incidentelor de securitate cibernetică și poate fi, de asemenea, utilizată ca mijloc de influențare a comportamentului agresorilor (potențiali). Un mesaj adecvat poate fi, de asemenea, utilizat pentru a semnala în mod clar eventualele consecințe ale unui răspuns diplomatic, astfel încât să se influențeze comportamentul agresorilor. Pentru un răspuns politic eficace, este esențială o armonizare a comunicării publice care vizează atenuarea efectelor negative ale incidentelor și crizelor de securitate cibernetică, precum și a comunicării publice care vizează să influențeze un agresor. În securitatea cibernetică este deosebit de important să se difuzeze informații precise și exacte privind modalitățile prin care publicul poate atenua efectele unui incident (de exemplu, aplicarea unui *patch*, luarea de acțiuni complementare pentru a evita amenințarea etc.).

COOPERAREA LA NIVEL TEHNIC, OPERAȚIONAL ȘI STRATEGIC/POLITIC ÎNTRE STATELE MEMBRE ȘI ÎNTRE STATELE MEMBRE ȘI ACTORII UE

Răspunsul eficace la incidentele sau crizele de securitate cibernetică de mare amploare la nivelul UE depinde de eficacitatea cooperării tehnice, operaționale și strategice/politice.

La fiecare nivel, actorii implicați ar trebui să efectueze activități specifice în ceea ce privește atingerea celor trei obiective principale:

— răspunsul coordonat;

— conștientizarea comună a situației;

— comunicațiile publice.

Pe durata incidentului sau a crizei, nivelurile inferioare ale structurii de cooperare vor alerta, informa și sprijini nivelurile superioare, iar nivelurile superioare vor oferi orientări ([2]) și decizii nivelurilor inferioare, după caz.

Cooperarea la nivelul tehnic

Sfera activităților:

— administrarea incidentelor ([3]) în cursul unei crize de securitate cibernetică

— monitorizarea și supravegherea incidentului, inclusiv analiza continuă a amenințărilor și a riscurilor.

Actori potențiali

La nivel tehnic, mecanismul central de cooperare în cadrul planului de acțiune este rețeaua CSIRT, prezidată de președinție, ENISA asigurând secretariatul.

— Statele membre:

  — autoritățile competente și punctele unice de contact instituite prin Directiva privind securitatea rețelelor și a informațiilor

  — CSIRT

— Organele/birourile/agențiile UE:

  — ENISA

  — Europol/EC3

  — CERT-UE

([1]) Trebuie precizat că prin comunicare publică se poate înțelege atât comunicarea cu publicul larg cu privire la incident, cât și comunicarea de informații cu caracter mai degrabă tehnic sau operațional cu sectoare critice și/sau cu cei afectați. Pentru aceasta ar putea fi necesar să se utilizeze canale de difuzare confidențiale și instrumente/platforme tehnice specifice. În orice caz, comunicarea cu operatorii și cu publicul larg în orice stat membru este prerogativa fiecărui stat membru și ține de responsabilitatea fiecărui stat membru. Așadar, în conformitate cu principiul subsidiarității prezentat mai sus, statele membre și CSIRT naționale au responsabilitatea finală pentru informațiile pe care le difuzează pe teritoriul lor și persoanelor pe care le reprezintă.

([2]) „Permisiunea de a acționa” – în caz de criză de securitate cibernetică, timpul de reacție scurt este esențial pentru stabilirea acțiunilor de atenuare adecvate. Pentru a asigura acest timp de reacție scurt, un stat membru poate acorda unui alt stat membru „permisiunea de a acționa” voluntară, astfel încât statul membru are permisiunea de a acționa imediat, fără a mai fi necesar să consulte nivelurile superioare sau instituțiile UE și să treacă prin toate canalele oficiale, prevăzute în mod normal, dacă acest lucru nu este impus într-un anumit incident (de exemplu, CSIRT nu ar trebui să consulte nivelurile superioare pentru a transmite informații importante CSIRT din alt stat membru).

([3]) „Administrarea incidentului” înseamnă toate procedurile utilizate pentru detectarea, analiza și limitarea unui incident și răspunsul la acesta;

— Comisia Europeană:

  — ERCC (serviciu operațional 24/7, cu sediul în cadrul DG ECHO) și serviciul coordonator desemnat (DG CNECT sau DG HOME în funcție de natura incidentului), Secretariatul General (secretariatul ARGUS), DG HR (Direcția Securitate), DG DIGIT (operațiuni de securitate IT);

  — în cazul altor agenții ale UE ([1]), DG-ul din cadrul Comisiei de care aparțin sau SEAE (primul punct de contact).

— SEAE:

  — SIAC (Capacitatea unică de analiză a informațiilor): INTCEN UE și EUMS INT;

  — Celula de supraveghere a UE și serviciul geografic sau tematic desemnat;

  — Celula de fuziune a UE împotriva amenințărilor hibride (din cadrul INTCEN UE – securitatea cibernetică în context hibrid).

Conștientizarea comună a situației

— Ca parte a cooperării periodice la nivel tehnic pentru a sprijini conștientizarea de către Uniune a situației, ENISA ar trebui să pregătească periodic Raportul asupra situației tehnice a incidentelor și amenințărilor de securitate cibernetică în UE, pe baza informațiilor disponibile în mod public, a propriei analize și a rapoartelor care i-au fost transmise de CSIRT ale statelor membre (în mod voluntar) sau de punctele unice de contact instituite prin Directiva privind securitatea rețelelor și a informațiilor, de Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol și CERT-UE și, după caz, de Centrul de analiză a informațiilor al Uniunii Europene (INTCEN) din cadrul Serviciului European de Acțiune Externă (SEAE). Raportul ar trebui să fie pus la dispoziția structurilor relevante ale Consiliului, Comisiei, ÎR/VP și ale rețelei CSIRT.

— În caz de incident major, președintele rețelei CSIRT, asistat de ENISA, pregătește un raport asupra situației incidentelor de securitate cibernetică din UE ([2]) care este prezentat Președinției, Comisiei și ÎR/VP prin intermediul CSIRT al președinției prin rotație.

— *Toate celelalte agenții ale UE* raportează către direcțiile generale de care aparțin, care, la rândul lor, raportează serviciului coordonator al Comisiei.

— *CERT-UE* transmite rapoarte tehnice rețelei CSIRT, instituțiilor și agențiilor UE (după caz) și ARGUS (dacă este activat).

— *Europol/EC3* ([3]) *și CERT-UE* pun la dispoziția rețelei CSIRT analiză criminalistică de specialitate pentru elementele tehnice, precum și alte informații cu caracter tehnic.

— SIAC a SEAE: în numele INTCEN, celula de fuziune a UE împotriva amenințărilor hibride raportează departamentelor SEAE relevante.

Răspuns

— *Rețeaua CSIRT* face schimb de detalii tehnice și analize cu privire la incident, precum adresele IP, indicatorii de compromitere ([4]) etc. Aceste informații ar trebui furnizate ENISA fără întârzieri nejustificate și în termen de cel mult 24 de ore de la identificarea incidentului.

— În conformitate cu procedurile standard de operare ale rețelei CSIRT, membrii acesteia cooperează în eforturile lor de analizare a elementelor tehnice disponibile și a altor informații cu caracter tehnic legate de incident, cu scopul de a determina cauza incidentului și eventualele măsuri de atenuare tehnice.

— ENISA asistă CSIRT în activitățile sale tehnice, în conformitate cu experiența și mandatul său ([5]).

([1]) În funcție de natura și de impactul incidentului asupra diferitelor sectoare de activitate (finanțe, transport, energie, asistență medicală etc.), agențiile sau organele relevante ale UE vor fi implicate.

([2]) Raportul asupra situației incidentelor de securitate cibernetică din UE este o agregare de rapoarte naționale furnizate de CSIRT naționale. Formatul raportului ar trebui să fie descris în procedurile standard de operare ale rețelei CSIRT.

([3]) În conformitate cu condițiile și procedurile stabilite în cadrul juridic al EC3.

([4]) Indicatorul de compromitere – în criminalistica informatică este un element observat pe o rețea sau într-un sistem de operare care indică cu un grad ridicat de încredere o intruziune informatică. Printre indicatorii de compromitere obișnuiți se numără semnăturile de viruși, adresele IP, codurile hash MD5 ale fișierelor malware, URL-urile sau numele de domeniu ale serverelor de comandă și control ale botnetului.

([5]) Propunere de regulament privind ENISA, Agenția europeană de securitate cibernetică, abrogarea Regulamentului (UE) nr. 526/2013 și certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Actul privind securitatea cibernetică”), 13 septembrie 2017.

— CSIRT ale statelor membre își coordonează activitățile de răspuns tehnic cu asistența acordată de ENISA și Comisie.

— SIAC a SEAE: În numele INTCEN, celula de fuziune a UE împotriva amenințărilor hibride lansează procesul de colectare a dovezilor inițiale.

Comunicații publice

— CSIRT emite informări tehnice ([1]) și alerte de vulnerabilitate ([2]) și le difuzează comunităților din sfera lor de competență și publicului, urmând procedurile de autorizare aplicabile în fiecare caz.

— ENISA facilitează elaborarea și difuzarea comunicărilor rețelei CSIRT comune.

— ENISA își coordonează activitățile de comunicare publică cu rețeaua CSIRT și cu serviciului purtătorului de cuvânt al Comisiei.

— ENISA și EC3 își coordonează activitățile de comunicare publică pe baza unei poziții asupra căreia au convenit statele membre cu privire la conștientizarea comună a situației. Acestea își coordonează activitățile de comunicare publică cu serviciul purtătorului de cuvânt al Comisiei.

— În cazul în care criza are o dimensiune externă sau de politică de securitate și apărare comună (PSAC), comunicarea publică ar trebui să fie coordonată de SEAE și de serviciul purtătorului de cuvânt al ÎR/VP.

Cooperarea la nivelul operațional

Sfera activităților

— Pregătirea procesului decizional la nivel politic

— Coordonarea gestionării crizelor de securitate cibernetică (după caz)

— Evaluarea consecințelor și a impactului la nivelul UE și propunerea eventualelor măsuri de atenuare

Actori potențiali

— Statele membre:

  — autoritățile competente și punctele unice de contact instituite prin Directiva privind securitatea rețelelor și a informațiilor

  — CSIRT, agențiile de securitate cibernetică

  — Alte autorități sectoriale de la nivel național (în cazul incidentelor sau crizelor multisectoriale)

— Organele/birourile/agențiile UE:

  — ENISA

  — Europol/EC3

  — CERT-UE

— Comisia Europeană:

  — secretar general (adjunct) al SG (sistemul ARGUS)

  — DG CNECT/DG HOME

  — Autoritatea de securitate a Comisiei

  — Alte DG-uri (în cazul incidentelor sau crizelor multisectoriale)

([1]) Informare de natură tehnică în ceea ce privește cauzele incidentului și eventuale măsuri de atenuare.
([2]) Informații cu privire la vulnerabilitatea tehnică care este exploatată pentru a crea efecte negative asupra sistemelor informatice.

— SEAE:

  — secretarul general (adjunct) pentru răspunsul în caz de criză și SIAC (INTCEN UE și EUMS INT)

  — Celula de fuziune a UE împotriva amenințărilor hibride

— Consiliul:

  — Președinția [președintele Grupului de lucru orizontal pentru chestiuni cibernetice sau Coreper ([1])], sprijinită de SGC sau de COPS ([2]) și – dacă este activat – de mecanismul IPCR;

Conștientizarea situației

— Sprijinirea elaborării de rapoarte asupra situației politice/strategice (de exemplu, ISAA în cazul activării IPCR);

— *Grupul de lucru orizontal pentru chestiuni cibernetice al Consiliului* pregătește reuniunea Coreper sau COPS, după caz

— Dacă se activează mecanismul IPCR,

  — Președinția poate convoca mese rotunde, în vedere pregătirii reuniunilor Coreper sau COPS, la care participă părțile interesate relevante din statele membre, instituțiile, agențiile și părțile terțe, precum țările din afara UE și organizațiile internaționale. Acestea sunt reuniuni de criză care au scopul de a identifica blocajele și de a elabora propuneri de acțiune pentru chestiunile transversale.

  — *Serviciul coordonator al Comisiei sau SEAE* ca serviciu coordonator al ISAA pregătește raportul ISAA pe baza contribuțiilor primite de la ENISA, rețeaua CSIRT, Europol/EC3, EUMS INT, INTCEN și toți ceilalți actori relevanți. Raportul ISAA reprezintă o evaluare la nivelul UE pe baza corelației dintre incidentele tehnice și evaluarea crizei (analiza amenințărilor, evaluarea riscurilor, consecințele și efectele fără caracter tehnic, aspectele incidentului sau crizei care nu țin de securitatea cibernetică etc.) care sunt adaptate nevoilor de la nivelul operațional și politic.

— Dacă se activează sistemul ARGUS,

  — CERT-UE și EC3 ([3]) contribuie în mod direct la schimbul de informații în cadrul Comisiei.

— În cazul în care se activează mecanismul de răspuns în caz de criză al SEAE:

  — SIAC va intensifica colectarea informațiilor și agregarea informațiilor din toate sursele și va pregăti o analiză și o evaluare cu privire la incident.

Răspuns (la cererea formulată de la nivel politic)

— Cooperarea transfrontalieră cu punctul unic de contact și autoritățile naționale competente (Directiva privind securitatea rețelelor și a informațiilor), pentru a atenua consecințele și efectele.

— Activarea tuturor măsurilor de atenuare tehnice și coordonarea capacităților tehnice necesare pentru stoparea sau reducerea impactului atacurilor asupra sistemelor informatice vizate.

— Cooperarea și, dacă se ia o decizie în acest sens, coordonarea capacităților tehnice în vederea unui răspuns comun sau colaborativ, în conformitate cu ***PSO ale rețelei CSIRT***.

— Evaluarea necesității de a coopera cu părțile terțe relevante.

— Proces decizional în cadrul sistemului ARGUS (dacă s-a activat).

— Pregătirea deciziilor și coordonare în cadrul mecanismului IPCR (dacă s-a activat).

— Sprijinirea procesului decizional al SEAE în cadrul mecanismului de răspuns în caz de criză al SEAE (dacă s-a activat), inclusiv în ceea ce privește contactele cu țările terțe și organizațiile internaționale, precum și orice măsură care are scopul de a proteja misiunile și operațiile PSAC și delegațiile UE.

([1]) Comitetul Reprezentanților Permanenți sau Coreper (articolul 240 din Tratatul privind funcționarea Uniunii Europene – TFUE) răspunde de pregătirea activității Consiliului Uniunii Europene.

([2]) Comitetul politic și de securitate este un comitet al Consiliului Uniunii Europene care se ocupă de politica externă și de securitate comună (PESC) menționată la articolul 38 din Tratatul privind Uniunea Europeană.

([3]) În conformitate cu condițiile și procedurile stabilite în cadrul juridic al EC3.

Comunicații publice

— Acord asupra mesajelor publice legate de incident.

— În cazul în care criza are o dimensiune externă sau de politică de securitate și apărare comună (PSAC), comunicarea publică ar trebui să fie coordonată de SEAE și de serviciul purtătorului de cuvânt al ÎR/VP.

Cooperarea la nivel strategic/politic

Actori potențiali

— În cazul statelor membre, miniștrii responsabili de securitatea cibernetică.

— În cazul Consiliului European, președintele.

— În cazul Consiliului, președinția prin rotație.

— Atunci când se iau măsuri în cadrul „Setului de instrumente pentru diplomația cibernetică", COPS și Grupul de lucru orizontal.

— În cazul Comisiei Europene, președintele sau vicepreședintele/comisarul delegat.

— Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate/Vicepreședinte al Comisiei.

Sfera activităților: gestionarea strategică și politică a aspectelor crizei cu caracter cibernetic, precum și a celor fără caracter cibernetic, inclusiv măsuri în temeiul Cadrului privind un răspuns diplomatic comun al UE la activitățile informatice răuvoitoare.

Conștientizarea comună a situației

— Identificarea efectelor pe care perturbările cauzate de criză le au asupra funcționării Uniunii.

Răspuns

— Activarea mecanismelor/instrumentelor adiționale de gestionare a crizelor în funcție de natura și impactul incidentului. Printre acestea se poate număra, de exemplu, mecanismul de protecție civilă.

— Luarea de măsuri în temeiul Cadrului privind un răspuns diplomatic comun al UE la activitățile informatice răuvoitoare.

— Punerea la dispoziția statelor membre afectate a sprijinului de urgență, de exemplu prin activarea Fondului de intervenție de urgență în materie de securitate cibernetică ([1]), de îndată ce se va aplica.

— Cooperarea și coordonarea cu organizațiile internaționale, după caz, de exemplu cu Organizația Națiunilor Unite (ONU), Organizația pentru Securitate și Cooperare în Europa (OSCE) și, în special, cu NATO.

— Evaluarea implicațiilor de securitate și de apărare de la nivel național.

Comunicații publice

Luarea unei decizii cu privire la o strategie comună de comunicare cu publicul.

RĂSPUNSUL COORDONAT CU STATELE MEMBRE LA NIVELUL UE ÎN CADRUL MECANISMELOR IPCR

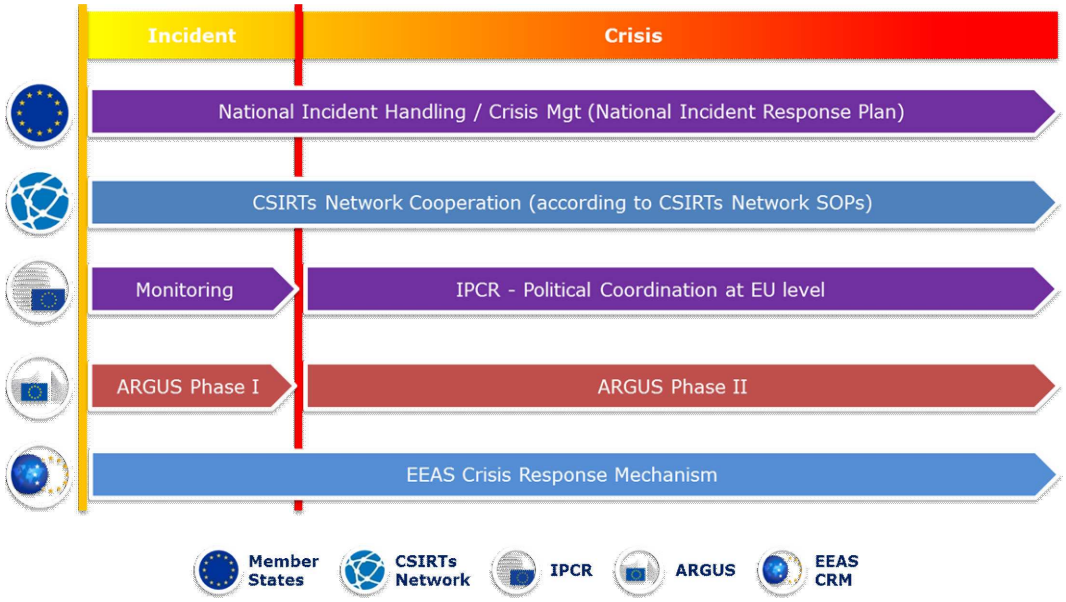
Având în vedere principiul complementarității la nivelul UE, această secțiune prezintă și pune accentul pe obiectivul principal și pe responsabilitățile și activitățile autorităților din statele membre, ale rețelei CSIRT, ENISA, CERT-UE, Europol/EC3, INTCEN, ale celulei de fuziune a UE împotriva amenințărilor hibride și ale Grupului de lucru orizontal pentru chestiuni cibernetice al Consiliului în contextul procesului IPCR. Se pleacă de la premisa că actorii acționează în conformitate cu procedurile stabilite la nivelul UE sau la nivel național.

Trebuie precizat faptul că, după cum reiese din figura 1, indiferent dacă se activează mecanismele UE de gestionare a crizelor, activitățile la nivel național, precum și cooperarea în cadrul rețelei CSIRT (dacă este necesar) se derulează pe durata incidentului/crizei conform principiilor subsidiarității și proporționalității.

([1]) Fondul de intervenție de urgență în materie de securitate cibernetică este o acțiune propusă în temeiul Comunicării comune: „Reziliență, descurajare și apărare: asigurarea unei securități cibernetice solide pentru UE", JOIN(2017) 450/1.

Figura 1

Răspunsul la nivelul UE la incidentele/crizele de securitate cibernetică



Toate activitățile descrise mai jos se vor desfășura în conformitate cu procedurile/normele standard de operare ale mecanismelor implicate și cu respectarea acestor proceduri/norme și în conformitate cu mandatele și competențele definite ale diferiților actori și ale diferitelor instituții. Pentru a asigura cooperarea optimă și răspunsul eficace la incidentele și crizele de securitate cibernetică de mare amploare, ar putea fi necesară completarea sau modificarea acestor proceduri/norme.

S-ar putea, ca în cazul unui incident anume, să nu fie necesară intervenția tuturor actorilor prezentați mai jos. Cu toate acestea, planul de acțiune și procedurile standard de operare relevante ale mecanismelor de cooperare ar trebui să prevadă implicarea potențială a acestora.

Având în vedere gradul diferit al impactului pe care un incident sau o criză de securitate cibernetică îl poate avea asupra societății, gradul ridicat de flexibilitate în ceea ce privește implicarea actorilor sectoriali de la toate nivelurile și răspunsurile adecvate vor depinde atât de activitățile de atenuare cu caracter cibernetic, cât și de activitățile de atenuare fără caracter cibernetic.

Gestionarea crizelor de securitate cibernetică – Integrarea aspectelor legate de securitatea cibernetică în procesul IPCR

Mecanismul IPCR, descris în PSO ([1]) ale IPCR, respectă ordinea etapelor descrise în continuare (efectuarea unora dintre aceste etape va depinde de situație).

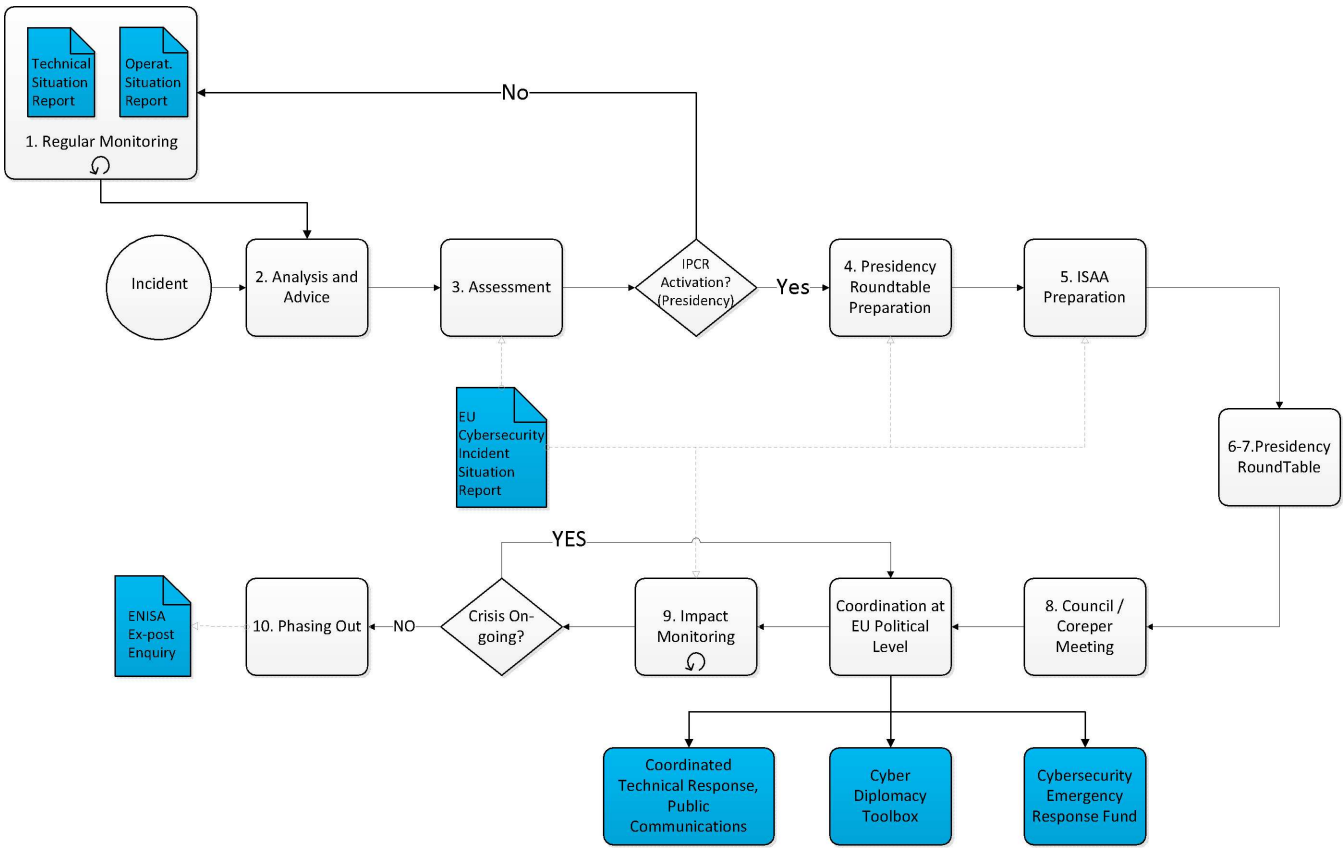
Pentru fiecare etapă se precizează activitățile și actorii implicați în securitatea cibernetică. Din considerente ce țin de facilitarea lecturii, pentru fiecare etapă se prezintă textul PSO ale IPCR, urmat de activitățile specifice planului de acțiune. Această abordare în etape permite, de asemenea, identificarea clară a **lacunelor** existente în ceea ce privește capacitățile și procedurile necesare care împiedică răspunsul eficace la crizele de securitate cibernetică.

Figura 2 [de mai jos ([2])] este o reprezentare grafică a procesului IPCR, noile elemente care se introduc fiind evidențiate în albastru.

([1]) Din documentul 12607/15 „Procedurile standard de operare ale IPCR”, convenite de Grupul „Prietenii Președinției”, de care Coreper a luat act în octombrie 2015.
([2]) În apendice este inclusă o versiune mai mare a figurii.

Figura 2

Elemente specifice securității cibernetice în cadrul IPCR



Notă: dat fiind caracterul amenințărilor hibride în domeniul cibernetic ce nu vor atinge nivelul unei crize care va fi recunoscută, UE trebuie să ia măsuri de prevenire și de pregătire. Celula de fuziune a UE împotriva amenințărilor hibride are sarcina de a analiza rapid incidentele relevante și de a informa structurile de coordonare corespunzătoare. Rapoartele periodice ale celulei de fuziune împotriva amenințărilor hibride poate contribui la informarea procesului de formulare a politicilor sectoriale, cu scopul de a consolida pregătirea.

— **Etapa 1 – Monitorizarea sectorială periodică și alerte**: rapoartele sectoriale asupra situației, prezentate periodic și alertele existente oferă Președinției Consiliului indicații cu privire la apariția unei crize și la eventuala evoluție a acesteia.

  — **Lacună identificată**: în prezent, la nivelul UE nu există rapoarte asupra situației în materie de securitate cibernetică care se prezintă în mod periodic și coordonat și nici alerte în ceea ce privește incidentele (și amenințările) de securitate cibernetică.

  — **Plan de acțiune: monitorizarea/raportarea situației privind securitatea cibernetică în UE**

    — **Un raport periodic la nivelul UE asupra situației tehnice în materie de securitate cibernetică** cu privire la incidentele și amenințările de securitate cibernetică va fi pregătit de ENISA, pe baza informațiilor disponibile în mod public, a propriei analize și a rapoartelor care i-au fost transmise de CSIRT ale statelor membre (în mod voluntar) sau de punctele unice de contact instituite prin Directiva privind securitatea rețelelor și a informațiilor, de Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol, de CERT-UE și de Centrul de analiză a informațiilor al Uniunii Europene (INTCEN) din cadrul Serviciului European de Acțiune Externă (SEAE). Raportul ar trebui să fie pus la dispoziția structurilor relevante ale Consiliului, Comisiei și ale rețelei CSIRT.

    — În numele SIAC, celula de fuziune a UE împotriva amenințărilor hibride ar trebui să compileze un **raport la nivelul UE asupra situației operaționale în materie de securitate cibernetică**. Raportul sprijină, de asemenea, Cadrul privind un răspuns diplomatic comun al UE la activitățile informatice răuvoitoare.

    — Ambele rapoarte sunt difuzate părților interesate de la nivelul UE și de la nivel național, pentru a contribui la conștientizarea situației de către acestea, pentru a sta la baza procesului decizional și a facilita cooperarea regională transfrontalieră.

După ce a fost detectat un incident

— **Etapa 2 – Analiză și consiliere**: pe baza sistemului de monitorizare și alertă disponibil, serviciile Comisiei, SEAE și SGC se informează reciproc cu privire la posibile evoluții, pentru a fi pregătite să ofere consiliere Președinției în ceea ce privește o posibilă activare (deplină sau în modul „partajare de informații") a IPCR;

— **Plan de acțiune**

— Pentru Comisie, DG CNECT, DG HOME, DG HR.DS și DG DIGIT, susținute de ENISA, EC3 și CERT-UE

— SEAE. Bazându-se pe activitatea Celulei de supraveghere a UE și pe sursele de informații, Celula de fuziune a UE împotriva amenințărilor hibride oferă o conștientizare a situației privind amenințările hibride reale și potențiale care afectează UE și partenerii săi, inclusiv amenințările cibernetice. Prin urmare, atunci când analiza și evaluarea efectuate de Celula de fuziune a UE împotriva amenințărilor hibride indică existența unor posibile amenințări îndreptate către un stat membru, către țări partenere sau către o organizație, INTCEN va informa (în primă instanță) nivelul operațional, în conformitate cu procedurile stabilite. Nivelul operațional va pregăti apoi recomandări pentru nivelul strategic politic, inclusiv posibila activare a mecanismelor de gestionare a crizelor în modul de monitorizare (de exemplu, mecanismul de răspuns în caz de criză al SEAE sau pagina de monitorizare a IPCR).

— Președintele rețelei CSIRT, asistat de ENISA, pregătește un Raport asupra situației incidentelor de securitate cibernetică din UE ([1]) care este prezentat Președinției, Comisiei și ÎR/VP prin intermediul CSIRT al statului membru care asigură Președinția prin rotație.

— **Etapa 3 – Evaluarea/Decizia privind activarea IPCR**: Președinția evaluează necesitatea coordonării politice, a schimbului de informații sau a procesului decizional la nivelul UE. În acest scop, Președinția poate convoca o masă rotundă informală. Președinția efectuează o identificare inițială a domeniilor care necesită implicarea Coreper sau a Consiliului. Aceasta va constitui baza orientărilor pentru redactarea rapoartelor privind analiza și conștientizarea integrată a situației (ISAA). Președinția va decide, având în vedere caracteristicile crizei, posibilele consecințe ale acesteia și necesitățile politice aferente, dacă este oportun să se convoace reuniunile Grupurilor de lucru relevante ale Consiliului și/sau ale Coreper și/sau ale COPS.

— **Plan de acțiune**

— Participanții la masa rotundă:

— Serviciile Comisiei și SEAE vor oferi consiliere Președinției în domeniile lor respective de competență.

— Reprezentanții statelor membre în Grupul de lucru orizontal pentru chestiuni cibernetice, asistați de experți din capitale (CSIRT, autoritățile competente în materie de securitate cibernetică, alții).

— Orientări politice/strategice pentru rapoartele ISAA pe baza celui mai recent Raport asupra situației incidentelor de securitate cibernetică din UE și informații suplimentare furnizate de participanții la masa rotundă.

— Grupuri de lucru și comitete relevante:

— Grupul de lucru orizontal pentru chestiuni cibernetice.

Comisia, SEAE și SGC, în deplin acord și în asociere cu Președinția, pot decide de asemenea să activeze IPCR în modul „partajare de informații" generând o pagină de criză, pentru a pregăti terenul în vederea unei posibile activări depline.

— **Etapa 4 – Activarea IPCR/Colectarea și schimbul de informații**: în momentul activării (fie în modul „partajare de informații", fie activare deplină), este generată o pagină de criză pe platforma web a IPCR, ce permite schimburi specifice de informații, cu accentul pe aspecte care vor contribui la ISAA și la pregătirea discuției la nivel politic. Serviciul responsabil cu coordonarea ISAA (unul dintre serviciile Comisiei sau SEAE) se va stabili în funcție de circumstanțele cazului.

— **Etapa 5 – Elaborarea rapoartelor ISAA**: va fi inițiată redactarea rapoartelor ISAA. Comisia/SEAE va emite rapoarte ISAA, astfel cum se menționează în PSO ale ISAA și poate încuraja ulterior schimbul de informații pe platforma web

([1]) Raportul asupra situației incidentelor de securitate cibernetică din UE este o agregare de rapoarte naționale furnizate de CSIRT naționale. Formatul raportului ar trebui să fie descris în procedurile standard de operare ale rețelei CSIRT.

a IPCR sau poate emite solicitări specifice de informații. Rapoartele ISAA vor fi adaptate nevoilor de la nivel politic (și anume Coreper sau Consiliul), astfel cum sunt definite de Președinție și prevăzute în orientările sale, permițând astfel o vedere de ansamblu strategică asupra situației și o dezbatere informată asupra punctelor de pe ordinea de zi definite de Președinție. În conformitate cu procedurile standard de operare ale ISAA, natura crizei de securitate cibernetică va determina dacă raportul ISAA este pregătit de unul dintre serviciile Comisiei (DG CNECT, DG HOME) sau de SEAE.

În urma activării IPCR, Președinția va prezenta domeniile specifice de interes pentru ISAA, pentru ca aceasta să sprijine coordonarea politică și/sau procesul decizional din cadrul Consiliului. De asemenea, Președinția va preciza calendarul raportului, în urma consultărilor cu serviciile Comisiei/SEAE;

— **Plan de acțiune**

— Raportul ISAA include contribuții din partea serviciilor relevante, inclusiv:

— Rețeaua CSIRT sub forma de Raportului asupra situației incidentelor de securitate cibernetică din UE;

— EC3, Celula de supraveghere a UE, Celula de fuziune a UE împotriva amenințărilor hibride, CERT-UE. Celula de fuziune a UE împotriva amenințărilor hibride va sprijini serviciul responsabil cu coordonarea ISAA și masa rotundă a IPCR și își va aduce contribuția sa, după caz.

— Agențiile și organismele sectoriale ale UE, în funcție de sectoarele afectate

— Autoritățile statelor membre (altele decât CSIRT).

— Colectarea contribuțiilor pentru ISAA ([1]):

— Comisia și agențiile UE: Sistemul informatic al ARGUS va constitui rețeaua internă de bază pentru ISAA. Agențiile UE își trimit contribuțiile către direcțiile generale responsabile respective, care la rândul lor vor furniza informațiile relevante către ARGUS. Serviciile Comisiei și agențiile vor colecta informații din rețelele sectoriale existente cu statele membre și organizațiile internaționale și din alte surse relevante.

— În ceea ce privește SEAE: Celula de supraveghere a UE, sprijinită de alte departamente relevante ale SEAE, va oferi rețeaua internă de bază și punctul unic de contact pentru ISAA. SEAE va colecta informații de la țările terțe și de la organizațiile internaționale relevante.

— **Etapa 6 – Pregătirea mesei rotunde informale organizate de Președinție**: Președinția, asistată de Secretariatul General al Consiliului, va defini calendarul, agenda, participanții și rezultatele preconizate (rezultatele posibile) ale mesei rotunde informale organizate de Președinție. SGC va transmite informații relevante pe platforma web a IPCR în numele Președinției și va emite în special avizul privind reuniunea.

— **Etapa 7 – Masa rotundă organizată de Președinție/măsuri pregătitoare pentru coordonarea politică/procesul decizional la nivelul UE**: Președinția va convoca o masă rotundă informală pentru a examina situația și pentru a pregăti și a analiza aspectele care urmează să fie aduse în atenția Coreper sau a Consiliului. Masa rotundă informală organizată de Președinție va reprezenta, de asemenea, forumul pentru dezvoltarea, analizarea și discutarea tuturor propunerilor de acțiune ce urmează a fi prezentate către Coreper/Consiliu.

— **Plan de acțiune**

— Grupul de lucru orizontal pentru chestiuni cibernetice al Consiliului ar trebui să pregătească COPS sau Coreper;

— **Etapa 8 – Coordonarea politică și procesul decizional în cadrul Coreper/Consiliului**: Rezultatele reuniunilor Coreper/Consiliului se referă la coordonarea activităților de răspuns la toate nivelurile, la deciziile privind măsurile excepționale, la declarațiile politice etc. Aceste decizii constituie, de asemenea, o orientare politică/strategică actualizată pentru elaborarea ulterioară a rapoartelor ISAA.

— **Plan de acțiune**

— Decizia politică de a coordona răspunsul la criza de securitate cibernetică este pusă în aplicare prin activitățile (efectuate de actorii corespunzători) descrise anterior în secțiunea 1 „Cooperarea la nivel strategic/politic, operațional și tehnic” în ceea ce privește **Răspunsul** și **Comunicarea publică**.

— Elaborarea de rapoarte ISAA se desfășoară pe baza cooperării la nivel tehnic, operațional și politic/strategic în ceea ce privește **conștientizarea situației**, descrisă, de asemenea, în secțiunea 1 de mai sus.

([1]) procedurile standard de operare ale ISAA

— **Etapa 9 – Monitorizarea impactului**: Serviciul responsabil cu coordonarea ISAA va oferi, cu sprijinul contribuitorilor la ISAA, informații cu privire la evoluția crizei și la impactul deciziilor politice adoptate. Acest circuit informațional bazat pe feedback va sprijini un proces evolutiv, precum și decizia Președinției de a continua implicarea nivelului politic al UE sau de a reduce treptat utilizarea IPCR.

— **Etapa 10 – Reducerea treptată a utilizării**: urmând aceeași procedură ca și în cazul activării, Președinția poate convoca o masă rotundă informală pentru a evalua caracterul oportun al menținerii IPCR activ sau nu. Președinția poate decide să închidă sau să reducă activarea.

— **Plan de acțiune**

— ENISA poate fi invitată să contribuie sau să efectueze o anchetă tehnică *ex post* a incidentului, în conformitate cu dispozițiile cuprinse în mandatul său.

APENDICE

1. GESTIONAREA CRIZEI, MECANISMELE DE COOPERARE ȘI ACTORII LA NIVELUL UE

Mecanisme de gestionare a crizei

Mecanismul integrat pentru un răspuns politic la crize (IPCR): Mecanismul integrat pentru un răspuns politic la crize (IPCR), aprobat de Consiliu la 25 iunie 2013 ([1]), este conceput pentru a facilita o coordonare și un răspuns în timp util la nivelul politic al UE în eventualitatea unei crize majore. IPCR sprijină, de asemenea, coordonarea la nivel politic a răspunsului la invocarea clauzei de solidaritate (articolul 222 din TFUE), astfel cum este definită în Decizia 2014/415/UE a Consiliului privind modalitățile de punere în aplicare de către Uniune a clauzei de solidaritate, adoptată la 24 iunie 2014. Procedurile standard de operare (PSO) ale IPCR ([2]) prevăd procesul de activare și acțiunile ulterioare care urmează să fie întreprinse.

ARGUS: Sistemul de coordonare a crizelor instituit de Comisia Europeană în 2005 pentru a oferi un proces specific de coordonare în cazul unei crize multisectoriale majore. Este sprijinit de un sistem general de alertă rapidă (instrument informatic) cu același nume. ARGUS prevede două etape, etapa II (în caz de criză multisectorială majoră) declanșând reuniuni ale Comitetului de coordonare a crizelor (JRC) sub autoritatea președintelui Comisiei sau a unui comisar căruia i-a fost atribuită responsabilitatea. JRC reunește reprezentanți ai direcțiilor generale relevante ale Comisiei, ai cabinetelor și ai altor servicii ale UE pentru a conduce și coordona răspunsul Comisiei la criză. Prezidat de secretarul general adjunct, JRC evaluează situația, analizează opțiunile, ia decizii concrete în ceea ce privește instrumentele UE care intră în responsabilitatea Comisiei și se asigură că deciziile sunt puse în aplicare ([3]) ([4]).

Mecanismul de răspuns în caz de criză al SEAE: Mecanismul de răspuns în caz de criză al SEAE este un sistem structurat care permite SEAE să răspundă la crize și situații de urgență cu un caracter extern sau cu o importantă dimensiune externă – inclusiv la amenințări hibride – care au un impact potențial sau efectiv asupra intereselor UE sau ale oricărui stat membru. Asigurând participarea serviciilor relevante ale Comisiei, precum și a funcționarilor Secretariatului Consiliului, la reuniunile sale, mecanismul de răspuns în caz de criză facilitează sinergia între eforturile diplomatice, de securitate și de apărare și instrumentele financiare, comerciale și de cooperare gestionate de Comisie. Celula de criză poate fi activată pe durata crizei.

Mecanismele de cooperare

Rețeaua CSIRT: Rețeaua echipelor de intervenție în caz de incidente de securitate informatică reunește toate echipele CSIRT naționale și guvernamentale, precum și CERT-UE. Obiectivul rețelei este de a permite și a consolida partajarea de informații între echipele CSIRT privind amenințările și incidentele de securitate cibernetică, precum și de a coopera pentru a răspunde la incidentele și crizele de securitate cibernetică.

Grupul de lucru orizontal pentru chestiuni cibernetice al Consiliului: Grupul de lucru a fost instituit în vederea asigurării coordonării strategice și orizontale a aspectelor legate de politica cibernetică în cadrul Consiliului și poate participa la activități atât legislative, cât și nelegislative.

Actori

ENISA: Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor a fost instituită în 2004. Agenția colaborează îndeaproape cu statele membre și cu sectorul privat pentru a oferi consultanță și soluții privind aspecte cum ar fi exercițiile paneuropene privind securitatea cibernetică, dezvoltarea strategiilor naționale de securitate cibernetică, cooperarea și consolidarea capacităților echipelor CSIRT. ENISA colaborează în mod direct cu echipele CSIRT în întreaga UE și asigură Secretariatul rețelei CSIRT.

ERCC: Centrul de coordonare a răspunsului la situații de urgență în cadrul Comisiei (sub tutela Direcției Generale Protecție Civilă și Operațiuni Umanitare Europene – DG ECHO) susține și coordonează o gamă largă de activități de prevenire, pregătire și răspuns, 24 de ore din 24, 7 zile din 7. Inaugurat în 2013, el are rolul de platformă a răspunsului Comisiei la situațiile de criză (asigurând legătura cu alte celule de criză ale UE), inclusiv rolul de punct de contact central al IPCR 24 de ore din 24, 7 zile din 7.

([1]) 10708/13 privind „Finalizarea procesului de revizuire a CCA: mecanismele referitoare la un răspuns integrat al UE la criza politică”, aprobat de Consiliu la 24 iunie 2013.
([2]) 12607/15 „Procedurile standard de operare ale IPCR”, convenite de Grupul „Prietenii Președinției”, de care Coreper a luat act în octombrie 2015.
([3]) Dispozițiile Comisiei de stabilire a sistemului general de alertă rapidă „ARGUS”, COM(2005) 662 final, 23 decembrie 2005.
([4]) Decizia 2006/25/CE, Euratom a Comisiei din 23 decembrie 2005 de modificare a regulamentului său de procedură (JO L 19, 24.1.2006, p. 20), de instituire a sistemului general de alertă rapidă „ARGUS”.

Europol/EC3: Centrul european de combatere a criminalității informatice (EC3), instituit în 2013 în cadrul Europol, sprijină răspunsul de asigurare a respectării legii la criminalitatea informatică în UE. EC3 oferă sprijin operațional și analitic pentru investigațiile statelor membre și are rolul de platformă centrală pentru informații și date operative privind criminalitatea, sprijinind operațiunile și investigațiile realizate de statele membre prin analize, coordonare și expertiză la nivel operațional, precum și oferind capacități de sprijin criminalistic la nivel tehnic și digital foarte specializate.

CERT-UE: Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE are mandatul de a îmbunătăți protecția instituțiilor, a organelor și a agențiilor UE împotriva amenințărilor cibernetice. Este membru al rețelei CSIRT. CERT-UE are acorduri tehnice privind partajarea de informații cu privire la amenințările cibernetice cu CIRC (capacitatea de răspuns la incidente cibernetice) a NATO, cu unele țări terțe și cu actori comerciali majori în domeniul securității cibernetice.

Comunitatea de Informații a UE cuprinde Centrul de analiză a informațiilor al UE (**INTCEN**) și direcția „informații" a Statului-Major al UE (EUMS INT) în cadrul acordului privind **Capacitatea unică de analiză a informațiilor** (SIAC). Misiunea SIAC este de a oferi Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate și Serviciului European de Acțiune Externă (SEAE) analize ale informațiilor, mecanisme de alertă timpurie și conștientizare a situației. SIAC își oferă serviciile diverselor organe de decizie ale UE în domeniul politicii externe și de securitate comună (PESC), al politicii de securitate și apărare comună (PSAC) și al combaterii terorismului (CT), precum și statelor membre. INTCEN UE și EUMS INT nu sunt agenții operaționale și nu dispun de capacitate de colectare. Nivelul operațional de informații este de competența statelor membre. SIAC se ocupă doar de analiza strategică.

Celula de fuziune a UE împotriva amenințărilor hibride: Comunicarea comună privind contracararea amenințărilor hibride din aprilie 2016 desemnează Celula de fuziune a UE împotriva amenințărilor hibride (HFC UE) ca punct focal pentru toate analizele privind sursele de amenințări hibride în UE: mandatul său a fost aprobat în decembrie 2016 de către Comisie printr-o consultare interservicii. Instituită în cadrul INTCEN, Celula de fuziune a UE împotriva amenințărilor hibride face parte din SIAC și, prin urmare, colaborează cu EUMS INT, printre membrii săi permanenți numărându-se un militar. Termenul „hibrid" se referă la utilizarea în mod deliberat de către un stat sau un actor nestatal a unei combinații de multiple instrumente și pârghii vizibile sau sub acoperire, militare sau civile, cum ar fi atacurile cibernetice, campaniile de dezinformare, spionajul, presiunile economice, utilizarea forțelor de substituție sau alte activități subversive. HFC UE colaborează cu o rețea extinsă de puncte de contact (PC), atât în cadrul Comisiei, cât și în cadrul statelor membre pentru a oferi răspunsul integrat necesar/abordarea la nivelul întregii administrații necesară pentru combaterea diverselor provocări.

Celula de supraveghere a UE: Celula de supraveghere a UE face parte din Centrul de analiză a informațiilor al UE (INTCEN UE) și oferă SEAE capacitatea operațională de a asigura un răspuns imediat și eficace la situațiile de criză. Acesta este un organism permanent civil și militar gata de intervenție care oferă monitorizare și conștientizare a situației la nivel mondial, având capacitatea de a fi operațional 24 de ore din 24, 7 zile din 7.

Instrumente relevante

Cadrul privind un răspuns diplomatic comun al UE la activitățile informatice răuvoitoare: cadrul, convenit în iunie 2017, face parte din abordarea UE în ceea ce privește diplomația cibernetică, care contribuie la prevenirea conflictelor, la atenuarea amenințărilor la adresa securității cibernetice și la o mai mare stabilitate în relațiile internaționale. Cadrul utilizează pe deplin măsurile în temeiul politicii externe și de securitate comună, inclusiv, dacă este necesar, măsurile restrictive. Utilizarea măsurilor în contextul cadrului ar trebui să încurajeze cooperarea, să faciliteze atenuarea amenințărilor imediate și pe termen lung și să influențeze comportamentul autorului responsabil și al agresorilor potențiali pe termen lung.

2. COORDONAREA GESTIONĂRII CRIZELOR DE SECURITATE CIBERNETICĂ ÎN CADRUL MECANISMULUI IPCR – COORDONARE LA NIVEL ORIZONTAL ȘI ACTIVAREA NIVELULUI POLITIC

Mecanismul IPCR poate fi (și a fost) utilizat pentru a aborda aspecte tehnice și operaționale, dar întotdeauna dintr-un punct de vedere politic/strategic.

În ceea ce privește activarea, IPCR poate fi utilizat în funcție de nivelul crizei, trecând de la modul „monitorizare" la modul „partajare de informații", care este primul nivel de activare a IPCR, până la „activarea deplină a IPCR".

Activarea deplină este o decizie a președinției prin rotație a Consiliului UE. Comisia, SEAE și SGC pot activa IPCR în modul „partajare de informații". Monitorizarea și partajarea de informații atrag după sine niveluri diferite de schimb de

informații, partajarea de informații activând cererea de elaborare a rapoartelor ISAA. Prin activarea deplină se adaugă la setul de instrumente reuniunile mesei rotunde ale IPCR, aducând la masa reuniunilor Președinția (de regulă președintele Coreper II sau un expert în domeniu la nivel de consilier al Reprezentanței Permanente, însă, în mod excepțional, au fost organizate mese rotunde la nivel ministerial).

Actori

Președinția rotativă (de regulă președintele Coreper) are rolul de coordonator;

Pentru Consiliul European, cabinetul președintelui;

Pentru Comisia Europeană, nivelul de secretar general adjunct/director general și/sau experți în domeniu;

Pentru SEAE, nivelul de secretar general adjunct/director executiv și/sau experți în domeniu;

Pentru SGC, cabinetul SG, echipa IPCR și direcțiile generale responsabile.

Sfera activităților: generarea unui tablou integrat comun al situației și sensibilizarea cu privire la blocaje sau deficiențe la fiecare dintre cele trei niveluri pentru a le aborda la nivel politic, generarea de decizii la masa reuniunilor dacă acestea țin de domeniul de competență al participanților sau generarea de propuneri de acțiune care să fie transmise Coreper II și ulterior Consiliului.

Conștientizarea comună a situației

(inactiv): pot fi generate pagini de monitorizare a IPCR pentru a urmări evoluția situațiilor care ar putea degenera într-o criză cu implicații la nivelul UE;

(partajarea de informații a IPCR): rapoartele ISAA vor fi redactate de către coordonatorul ISAA pe baza contribuțiilor din partea serviciilor Comisiei, a SEAE și a statelor membre (prin intermediul chestionarelor IPCR);

(activarea deplină a IPCR): pe lângă rapoartele ISAA, mesele rotunde informale ale IPCR reunesc diferiți actori interesați din statele membre, Comisia, SEAE, agențiile relevante etc. pentru a discuta deficiențele și blocajele.

Cooperare și răspuns

Activarea/sincronizarea mecanismelor/instrumentelor adiționale de gestionare a crizelor în funcție de natura și impactul incidentului. Acestea pot include, de exemplu, mecanismul de protecție civilă, Cadrul privind un răspuns diplomatic comun al UE la activitățile informatice răuvoitoare sau „Cadrul comun privind contracararea amenințărilor hibride”.

Comunicarea în situații de criză

Rețeaua IPCR a comunicatorilor care intervin în situații de criză poate fi activată de către Președinție, după consultarea cu serviciile relevante din cadrul Comisiei, SGC și SEAE, pentru a sprijini crearea unor mesaje comune sau pentru a elabora cele mai eficiente instrumente de comunicare.

3. GESTIONAREA CRIZELOR DE SECURITATE CIBERNETICĂ ÎN ARGUS – PARTAJAREA DE INFORMAȚII ÎN CADRUL COMISIEI EUROPENE

Fiind confruntată cu crize neprevăzute pentru care a fost necesară o acțiune la nivel european, de exemplu, atacurile teroriste de la Madrid (martie 2004), tsunamiul din Asia de Sud-Est (decembrie 2004) și atacurile teroriste de la Londra (iulie 2005), Comisia a instituit în 2005 sistemul de coordonare ARGUS, sprijinit de un sistem general de alertă rapidă cu același nume ([1]) ([2]). Obiectivul său este de a asigura un **proces** specific **de coordonare în caz de criză** în situația unei crize multisectoriale majore, de a permite schimbul de informații cu privire la criză în timp real și de a asigura un proces decizional rapid.

ARGUS definește două etape, în funcție de gravitatea evenimentului:

Etapa I: este utilizată pentru „partajarea de informații” cu privire la o criză de o amploare limitată

([1]) Comisia Comunităților Europene din 23 decembrie 2005, Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Dispozițiile Comisiei privind sistemul general de alertă rapidă „ARGUS”, COM(2005) 662 final.

([2]) Decizia 2006/25/CE, Euratom.

Printre exemplele recente de evenimente raportate în etapa I se numără incendiile forestiere din Portugalia și Israel, atacul de la Berlin din 2016, inundațiile din Albania, uraganul Matthew în Haiti și seceta din Bolivia. Orice DG poate deschide un eveniment de tipul „etapa I" atunci când consideră că o situație din domeniul său de competență este suficient de gravă pentru a justifica sau a beneficia de pe urma partajării de informații. De exemplu, DG CNECT sau DG HOME poate deschide un eveniment de tipul „etapa I" atunci când consideră că o situație cibernetică din domeniul lor de competență este suficient de gravă pentru a justifica sau a beneficia de pe urma partajării de informații.

Etapa II: este activată în cazul unei crize multisectoriale majore sau al unei amenințări previzibile sau iminente la adresa Uniunii

Etapa II declanșează un proces de coordonare specific care îi permite Comisiei să ia decizii și să gestioneze un răspuns rapid, coordonat și coerent, la cel mai înalt nivel în domeniul său de competență și în cooperare cu alte instituții. Etapa II este destinată situațiilor de criză multisectorială majoră sau de amenințare previzibilă sau iminentă. Printre exemple din viața reală de evenimente de tipul „etapa II" se numără criza migrației/refugiaților (2015 până în prezent), tripla catastrofă de la Fukushima (2011) și erupția vulcanului *Eyjafjallajökull* în Islanda (2010).

Etapa II este activată de președinte din proprie inițiativă sau la cererea unui membru al Comisiei. Președintele poate atribui responsabilitatea politică pentru răspunsul Comisiei unui comisar responsabil de serviciul cel mai afectat de criză sau poate decide să își asume el însuși această responsabilitate.

Etapa II prevede reuniuni de urgență ale Comitetului de coordonare a crizelor (JRC), convocate sub autoritatea președintelui sau a unui comisar căruia i-a fost atribuită responsabilitatea. Reuniunile sunt convocate de Secretariatul General prin intermediul instrumentului informatic ARGUS. JRC este o structură operațională specifică de gestionare a crizelor constituită în scopul de a conduce și a coordona răspunsul Comisiei la criză, reunind reprezentanți ai direcțiilor generale ale Comisiei, ai cabinetelor și ai altor servicii ale UE relevante. Prezidat de secretarul general adjunct, **JRC evaluează situația, analizează opțiunile și ia decizii, garantând punerea în aplicare a deciziilor și a acțiunilor** și, în același timp, coerența și consecvența răspunsului. SG oferă sprijin pentru JRC.

4. MECANISMUL DE RĂSPUNS ÎN CAZ DE CRIZĂ AL SEAE

Mecanismul de răspuns în caz de criză al SEAE (MRC) este activat în cazul unei situații grave sau al unei urgențe care se referă la dimensiunea externă a UE sau care implică în orice mod această dimensiune. MRC este activat de către Secretarul General adjunct pentru răspunsul în caz de criză, după consultarea cu ÎR/VP sau cu Secretarul General. De asemenea, ÎR/VP sau SG sau un alt secretar general adjunct sau director executiv pot solicita Secretarului General adjunct pentru răspunsul în caz de criză să inițieze mecanismul de răspuns în caz de criză.

MRC contribuie la coerența la nivelul UE a răspunsului în caz de criză în cadrul strategiei în materie de securitate. În special, MRC facilitează sinergia între eforturile diplomatice, de securitate și de apărare și instrumentele financiare, comerciale și de cooperare gestionate de Comisie.

MRC este legat de sistemul general de răspuns în caz de urgență al Comisiei (ARGUS) și de mecanismul integrat pentru un răspuns politic la crize (IPCR) al UE pentru a exploata sinergiile în cazul unei activări simultane. Celula de supraveghere din cadrul SEAE acționează ca platformă de comunicare între SEAE și sistemele de răspuns în caz de urgență din cadrul Consiliului și al Comisiei.

În mod normal, prima acțiune legată de punerea în aplicare a MRC este convocarea unei **reuniuni de criză** între cadrele de conducere de nivel superior ale SEAE, ale Comisiei și ale Consiliului direct afectate de criza în cauză. Reuniunea de criză evaluează efectele pe termen scurt ale crizei și poate conveni asupra adoptării unor acțiuni imediate sau asupra activării celulei de criză sau asupra convocării unei platforme de criză. Aceste acțiuni pot fi puse în aplicare în orice succesiune temporală.

Celula de criză este un centru operațional la scară redusă, în care reprezentanții serviciilor SEAE, Comisiei și Consiliului implicați în răspunsul la criză se reunesc pentru a monitoriza în permanență situația pentru a oferi sprijin factorilor de decizie din sediul central al SEAE. Atunci când este activată, celula de criză este operațională 24 de ore din 24, 7 zile din 7.

Platforma de criză reunește servicii relevante ale SEAE, Comisiei și Consiliului pentru a evalua efectele pe termen mediu și lung ale crizelor și pentru a conveni asupra măsurilor care trebuie luate. Este prezidată de către ÎR/VP sau de către Secretarul General sau de către Secretarul General adjunct pentru răspunsul în caz de criză. Platforma de criză evaluează eficacitatea acțiunii UE în țara sau în regiunea aflată în situație de criză, decide cu privire la modificarea măsurilor suplimentare și discută propuneri pentru acțiunea Consiliului. Platforma de criză este o reuniune ad-hoc; prin urmare, nu este activată în mod permanent.

Grupul operativ este alcătuit din reprezentanți ai serviciilor implicate în răspuns și poate fi activat pentru a monitoriza și a facilita punerea în aplicare a răspunsului UE. El evaluează impactul acțiunii UE, pregătește documentele de politică și documentele privind opțiunile, contribuie la pregătirea cadrului politic de abordare a crizelor, contribuie la strategia de comunicare și adoptă orice alte mecanisme care pot facilita punerea în aplicare a răspunsului UE.

5. DOCUMENTE DE REFERINȚĂ

Mai jos este prezentată o listă a documentelor de referință care au fost luate în considerare pentru pregătirea planului de acțiune:

— Cadrul de cooperare europeană pentru situații de criză cibernetică, versiunea 1, 17 octombrie 2012.

— „Report on Cyber Crisis Cooperation and Management", ENISA, 2014

— „Actionable Information for Security Incident Response", ENISA, 2014

— „Common practices of EU-level crisis management and applicability to cyber crises", ENISA, 2015

— „Strategies for Incident Response and Cyber Crisis Cooperation", ENISA, 2016

— „EU Cyber Standard Operating Procedures", ENISA, 2016

— „A good practice guide of using taxonomies in incident prevention and detection", ENISA, 2017

— Comunicarea privind „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator", COM(2016) 410 final din 5 iulie 2016

— Concluziile Consiliului privind „Consolidarea sistemului de reziliență cibernetică al Europei și promovarea unui sector al securității cibernetice competitiv și inovator" (15 noiembrie 2016), 14540/16

— Decizia 2014/415/UE a Consiliului din 24 iunie 2014 privind modalitățile de punere în aplicare de către Uniune a clauzei de solidaritate (JO L 192, 1.7.2014, p. 53)

— „Finalizarea procesului de revizuire a CCA: mecanismele referitoare la un răspuns integrat al UE la criza politică (IPCR)", 10708/13, 7 iunie 2013

— Integrated Situational Awareness and Analysis (ISAA) – Standard Operating Procedures, DS 1570/15, 22 octombrie 2015

— Dispozițiile Comisiei de stabilire a sistemului general de alertă rapidă „ARGUS", COM(2005) 662 final din 23 decembrie 2005

— Decizia 2006/25/CE, Euratom a Comisiei din 23 decembrie 2005 de modificare a regulamentului său de procedură (JO L 19, 24.1.2006, p. 20)

— ARGUS Modus Operandi, Comisia Europeană, 23 octombrie 2013

— Concluziile Consiliului referitoare la un Cadru privind un răspuns diplomatic comun al UE la activitățile informatice răuvoitoare („Setul de instrumente pentru diplomația cibernetică"), doc. 9916/17

— Protocolul operațional al UE pentru combaterea amenințărilor hibride („EU Playbook"), SWD(2016) 227

— Mecanismul de răspuns în caz de criză al SEAE, 8 noiembrie 2016 [Ares(2017)880661]. Document de lucru comun al serviciilor Comisiei privind protocolul operațional al UE pentru combaterea amenințărilor hibride, „EU Playbook", SWD(2016) 227 final din 5 iulie 2016

— Comunicare comună către Parlamentul European și Consiliu: Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene, JOIN/2016/018 final din 6 aprilie 2016

— EEAS(2016) 1674 – Document de lucru al Serviciului European de Acțiune Externă „EU Hybrid Fusion Cell – Terms of Reference"

6. ELEMENTELE SPECIFICE PRIVIND SECURITATEA CIBERNETICĂ ÎN PROCESUL IPCR