REKOMENDACIJOS

KOMISIJOS REKOMENDACIJA (ES) 2017/1584

2017 m. rugsėjo 13 d.

dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 292 straipsnį,

kadangi:

(1) informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo esminiais aspektais visuose ekonominės veiklos sektoriuose, nes mūsų įmonės ir piliečiai skirtinguose sektoriuose ir skirtingose valstybėse labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, nei bet kada anksčiau. Kibernetinio saugumo incidentas, paveikiantis organizacijas daugiau kaip vienoje valstybėje narėje ar net visoje Sąjungoje ir galintis stipriai sutrikdyti vidaus rinką ir plačiau – tinklus ir informacines sistemas, kuriomis remiasi Sąjungos ekonomika, demokratija ir visuomenė, yra scenarijus, kuriam valstybės narės ir ES institucijos turi būti gerai pasirengusios;

(2) kibernetinio saugumo incidentas gali būti laikomas Sąjungos lygmens krize, kai dėl incidento kilęs sutrikdymas yra per didelio masto, kad jį galėtų pašalinti pati paveikta valstybė narė, arba kai jis paveikia dvi arba daugiau valstybių narių ir jo poveikis yra toks platus ir techniškai arba politiškai svarbus, kad būtina laiku koordinuoti veiksmus ir reaguoti Sąjungos politiniu lygmeniu;

(3) kibernetinio saugumo incidentai gali sukelti platesnę krizę ir paveikti sektorius, kurių veikla neapsiriboja tinklais ir informacinėmis sistemomis ar ryšių tinklais; bet koks tinkamas reagavimas turi būti grindžiamas ir kibernetinėmis, ir nekibernetinėmis poveikio mažinimo priemonėmis;

(4) kibernetinio saugumo incidentai yra nenuspėjami, dažnai įvyksta ir išsiplėtoja per labai trumpą laiką, todėl paveikti subjektai ir tie, kurių pareigos yra susijusios su reagavimu į incidentą ir jo poveikio mažinimu, privalo reaguoti greitai ir koordinuotai. Be to, kibernetinio saugumo incidentai dažnai neapsiriboja konkrečia geografine teritorija ir gali įvykti arba staiga išplisti tuo pačiu metu daugelyje šalių;

(5) norint veiksmingai reaguoti į didelio masto kibernetinio saugumo incidentus ir krizes ES lygmeniu, būtinas greitas ir veiksmingas visų atitinkamų suinteresuotųjų subjektų bendradarbiavimas ir toks reagavimas priklauso nuo atskirų valstybių narių pasirengimo ir galimybių, taip pat nuo Sąjungos remiamų koordinuotų bendrų veiksmų. Taigi reagavimas į incidentus laiku ir veiksmingai priklauso nuo to, ar egzistuoja iš anksto nustatytos ir, kiek tai įmanoma, gerai išbandytos bendradarbiavimo procedūros ir mechanizmai ir ar yra nacionaliniu ir Sąjungos lygmeniu aiškiai nustatytos pagrindinių dalyvių funkcijos ir pareigos;

(6) savo 2011 m. gegužės 27 d. išvadose ([1]) dėl ypatingos svarbos informacinės infrastruktūros apsaugos Taryba paragino ES valstybes nares „Stiprinti valstybių narių bendradarbiavimą ir, remiantis nacionaline krizių valdymo patirtimi ir rezultatais, taip pat bendradarbiaujant su ENISA, prisidėti prie Europos bendradarbiavimo kibernetinių incidentų atveju mechanizmų, kurie būtų patikrinti kitų 2012 m. įvyksiančių *Cyber Europe* pratybų metu, kūrimo“.

(7) 2016 m. komunikate „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“ ([2]) valstybės narės raginamos kuo labiau pasinaudoti Tinklų ir informacijos saugumo direktyvos ([3]) bendradarbiavimo mechanizmais ir plėtoti tarpvalstybinį bendradarbiavimą,

([1]) Tarybos išvados dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“, dokumentas 10299/11, Briuselis, 2011 m. gegužės 27 d.

([2]) COM(2016) 410 *final*, 2016 m. liepos 5 d.

([3]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

susijusį su pasirengimu didelio masto kibernetinio saugumo incidentui. Jame pridurta, kad nustačius koordinuotą bendradarbiavimo krizės atveju metodą, apimantį įvairius kibernetinės ekosistemos elementus, kuris būtų išdėstytas plane, būtų užtikrinta geresnė parengtis ir kad toks planas turėtų taip pat užtikrinti sinergiją ir derėjimą su esamais krizių valdymo mechanizmais;

(8) Tarybos išvadose ([1]) dėl pirmiau minėto komunikato valstybės narės paragino Komisiją pateikti tokį planą svarstyti įstaigoms ir kitiems atitinkamiems suinteresuotiesiems subjektams. Tačiau Tinklų ir informacijos saugumo direktyvoje Sąjungos bendradarbiavimo didelio masto kibernetinio saugumo incidentų ir krizių atveju sistema nenumatyta;

(9) Komisija su valstybėmis narėmis konsultavosi dviejuose konsultaciniuose seminaruose, surengtuose Briuselyje 2017 m. balandžio 5 ir liepos 4 d. su valstybių narių reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) atstovais, pagal Tinklų ir informacijos saugumo direktyvą sukurta bendradarbiavimo grupe ir Tarybos Kibernetinių klausimų horizontaliąja darbo grupe, taip pat Europos išorės veiksmų tarnybos, Europos Sąjungos tinklų ir informacijos apsaugos agentūros (ENISA), Europos kovos su elektroniniu nusikalstamumu centro (Europol/EC3) ir Tarybos Generalinio sekretoriato atstovais;

(10) prie šios rekomendacijos pridedamas koordinuoto reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes Sąjungos lygmeniu planas parengtas pagal minėtų konsultacijų rezultatus ir papildo komunikatą „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“;

(11) plane apibūdinami ir nustatomi valstybių narių, ES institucijų, įstaigų, organų ir agentūrų (toliau – ES institucijų) bendradarbiavimo reaguojant į didelio masto kibernetinio saugumo incidentus ir krizes tikslai ir būdai ir kaip esamuose krizių valdymo mechanizmuose galima panaudoti visus esamus ES lygmens kibernetinio saugumo subjektus;

(12) reaguojant į kibernetinio saugumo krizę, kaip apibūdinta 2 konstatuojamojoje dalyje, atsakui koordinuoti politiniu Sąjungos lygmeniu Taryboje bus naudojamas ES integruotas politinio atsako į krizes mechanizmas (IPCR) ([2]); Komisija panaudos ARGUS ([3]) aukšto lygio tarpsektorinio krizės koordinavimo procesą. Jei krizė susijusi su svarbiais išorės arba bendros saugumo ir gynybos politikos (BSGP) aspektais, bus panaudotas Europos išorės veiksmų tarnybos reagavimo į krizę mechanizmas ([3]);

(13) tam tikrose srityse ES lygmens sektorių krizių valdymo mechanizmuose numatytas bendradarbiavimas kibernetinio saugumo incidentų ir krizių atveju. Pavyzdžiui, kalbant apie pasaulinę palydovinės navigacijos sistemą (GNSS), Tarybos sprendime 2014/496/BUSP ([4]) jau nustatytos atitinkamos Tarybos, vyriausiojo įgaliotinio, Komisijos, Europos GNSS agentūros ir valstybių narių funkcijos operatyvinių pareigų grandinėje, sukurtoje siekiant reaguoti į grėsmę Sąjungai, valstybėms narėms ar GNSS, taip pat ir kibernetinių atakų atveju. Todėl ši rekomendacija turėtų būti taikoma nedarant poveikio tokiems mechanizmams;

(14) pagrindinė atsakomybė reaguoti į didelio masto kibernetinio saugumo incidentus ir krizes tenka jų paveiktoms valstybėms narėms. Tačiau, vadovaujantis Sąjungos teisės aktais ir atsižvelgiant į tai, kad kibernetinio saugumo incidentai ir krizės gali paveikti visas ekonominės veiklos sritis bendrojoje rinkoje, Sąjungos saugumą ir tarptautinius santykius, taip pat pačias institucijas, svarbus vaidmuo tenka Komisijai, vyriausiajam įgaliotiniui ir kitoms ES institucijoms ir tarnyboms;

(15) Sąjungos lygmeniu svarbiausi atsako į kibernetinio saugumo krizes dalyviai, be kitų, yra naujos pagal Tinklų ir informacijos saugumo direktyvą sukurtos struktūros ir mechanizmai, būtent reagavimo į kompiuterių saugumo incidentus tarnybų tinklas, taip pat atitinkamos agentūros ir įstaigos, būtent ENISA, Europol/EC3, ES žvalgybos analizės centras (INTCEN), ES karinio štabo žvalgybos skyrius (EUMS INT) ir ES situacijų kabinetas (SITROOM), bendradarbiaujantys Bendrame žvalgybinės informacijos analizės centre (SIAC), ES hibridinių grėsmių analizės ir informavimo centras (įsikūręs INTCEN), Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnyba (CERT-ES) ir Europos Komisijos Reagavimo į nelaimes koordinavimo centras;

(16) reaguojant į kibernetinio saugumo incidentus valstybių narių bendradarbiavimas techniniu lygmeniu vykdomas per Tinklų ir informacijos saugumo direktyva sukurtą CSIRT tinklą. ENISA užtikrina tinklo sekretoriato funkciją

([1]) Dokumentas 14540/16, 2016 m. lapkričio 15 d.
([2]) Daugiau informacijos galima rasti priedėlio dėl ES lygmens krizių valdymo, bendradarbiavimo mechanizmų ir dalyvių 3.1 skirsnyje.
([3]) Ten pat.
([4]) 2014 m. liepos 22 d. Tarybos sprendimas 2014/496/BUSP dėl Europos globalios navigacijos palydovinės sistemos diegimo, veikimo ir naudojimo aspektų, turinčių įtakos Europos Sąjungos saugumui, kuriuo panaikinami Bendrieji veiksmai 2004/552/BUSP (OL L 219, 2014 7 25, p. 53).

ir aktyviai remia CSIRT tarpusavio bendradarbiavimą. Nacionalinės CSIRT ir CERT-ES bendradarbiauja ir keičiasi informacija savanoriškai, įskaitant, kai reikia, reaguodamos į kibernetinio saugumo incidentus, paveikiančius vieną arba daugiau valstybių narių. Jei paprašo valstybės narės CSIRT atstovas, jos gali aptarti ir, kai įmanoma, apibrėžti koordinuoto reagavimo į tos valstybės narės jurisdikcijoje nustatytą incidentą veiksmus. Atitinkama tvarka bus nustatyta CSIRT tinklo standartinėse veiklos procedūrose ([1]);

(17) CSIRT tinklui taip pat pavesta aptarti, išnagrinėti ir nustatyti kitas operatyvinio bendradarbiavimo, įskaitant susijusio su rizikos ir incidentų kategorijomis, išankstiniais perspėjimais, tarpusavio pagalba, koordinavimo principais ir būdais, kai valstybės narės reaguoja į tarpvalstybinę riziką ir incidentus, formas;

(18) pagal Tinklų ir informacijos saugumo direktyvos 11 straipsnį sukurtai bendradarbiavimo grupei pavesta užduotis teikti strategines rekomendacijas dėl CSIRT tinklo veiklos, aptarti valstybių narių galimybes bei pasirengimą ir savanoriškai vertinti nacionalines tinklų ir informacijos sistemų saugumo strategijas ir CSIRT veiksmingumą ir nustatyti geriausią praktiką;

(19) speciali bendradarbiavimo grupės darbo grupė pagal Tinklų ir informacijos saugumo direktyvos 14 straipsnio 7 dalį rengia pranešimo apie incidentus gaires dėl aplinkybių, kuriomis esminių paslaugų operatoriai pagal 14 straipsnio 3 dalį privalo pranešti apie incidentus, ir tokių pranešimų formatą bei teikimo procedūrą ([2]);

(20) norint sudaryti sąlygas priimti informacija pagrįstus sprendimus, labai svarbus tikralaikės padėties, rizikos situacijos ir grėsmės žinojimas ir suvokimas, įgytas iš ataskaitų teikimo, vertinimo, mokslinių tyrimų, tyrimo ir analizės. Norint užtikrinti veiksmingą ir koordinuotą reagavimą, labai svarbus visų atitinkamų suinteresuotųjų subjektų informuotumas apie padėtį. Informuotumas apie padėtį apima elementus, susijusius su incidento priežastimis, taip pat jo poveikiu ir kilme. Suprantama, kad tai priklauso nuo atitinkamų šalių keitimosi informacija tinkamu formatu, naudojant bendrą incidentų apibūdinimo sistemą ir atitinkamai saugiu būdu;

(21) priklausomai nuo kibernetinio saugumo incidento, reagavimas į jį gali būti įvairių formų, nuo techninių priemonių nustatymo, kai du ar daugiau subjektų kartu tiria technines incidento priežastis (pvz., atlieka kenkimo programinės įrangos analizę) arba nustato būdus, kaip organizacijos gali įvertinti, ar jos buvo paveiktos (pvz., nustato užvaldymo rodiklius), iki operatyvinių sprendimų taikyti tokias priemones ir, politiniu lygmeniu, sprendimo naudoti kitas priemones, pvz., bendro reagavimo į kibernetinio kenkimo veiklą sistemą ([3]) ar ES operatyvinių veiksmų protokolą dėl kovos su hibridinėmis grėsmėmis ([4]);

(22) skaitmeninės bendrosios rinkos klestėjimui labai svarbus Europos piliečių ir įmonių pasitikėjimas skaitmeninėmis paslaugomis. Todėl informavimas apie krizę yra labai svarbus siekiant sumažinti neigiamą kibernetinio saugumo incidentų ir krizių poveikį. Pranešimai pasinaudojant bendro diplomatinio atsako sistema gali būti panaudojami ir kaip priemonė trečiosiose šalyse veikiančių (potencialių) agresorių elgesiui paveikti. Siekiant užtikrinti politinio atsako veiksmingumą, labai svarbu, kad viešieji pranešimai, kuriais siekiama sumažinti neigiamą kibernetinio saugumo incidentų ir krizių poveikį, ir viešieji pranešimai, kuriais siekiama paveikti agresorių, būtų suderinti;

(23) visuomenės informavimas, kaip naudotojai ir organizacijos gali sumažinti incidento poveikį (pvz., įdiegdami programinės įrangos pataisą ar imdamiesi papildomų veiksmų, kad išvengtų grėsmės ir t. t.), gali būti veiksminga didelio masto kibernetinio saugumo incidento arba krizės poveikio mažinimo priemonė;

(24) Komisija per Europos infrastruktūros tinklų priemonės kibernetinio saugumo skaitmeninių paslaugų infrastruktūrą rengia pagrindinių paslaugų platformos dalyvaujančių valstybių narių CSIRT bendradarbiavimo mechanizmą, vadinamąjį *MeliCERTes*, kuriuo siekiama pagerinti jų pasirengimą kylančiai kibernetinei grėsmei ir incidentams, bendradarbiavimą ir atsaką į juos. Komisija, panaudodama kvietimus teikti konkurso pasiūlymus dėl dotacijų skyrimo pagal Europos infrastruktūros tinklų priemonę, bendrai finansuoja valstybių narių CSIRT, siekdama pagerinti jų veiklos galimybes nacionaliniu lygmeniu;

([1]) Rengiamos; numatyta priimti iki 2017 m. pabaigos.
([2]) Gaires ketinama parengti iki 2017 m. pabaigos.
([3]) Tarybos išvados dėl bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos („Kibernetinio saugumo diplomatijos priemonių rinkinio“), dokumentas 9916/17.
([4]) Bendras tarnybų darbinis dokumentas „ES operatyvinių veiksmų protokolas dėl kovos su hibridinėmis grėsmėmis (ES scenarijus)“, SWD(2016) 227 *final*, 2016 m. liepos 5 d.

(25) siekiant skatinti ir gerinti valstybių narių tarpusavio ir privačiojo sektoriaus bendradarbiavimą labai svarbios yra ES kibernetinio saugumo pratybos. Todėl nuo 2010 m. ENISA organizuoja reguliarias visos Europos kibernetinių incidentų pratybas („Cyber Europe“);

(26) Tarybos išvadose ([1]) dėl Europos Vadovų Tarybos pirmininko, Europos Komisijos pirmininko ir Šiaurės Atlanto sutarties organizacijos Generalinio sekretoriaus bendro pareiškimo įgyvendinimo raginama stiprinti bendradarbiavimą kibernetinių pratybų srityje skatinant abipusį darbuotojų dalyvavimą atitinkamose pratybose, įskaitant visų pirma pratybas „Kibernetinė koalicija“ ir „Cyber Europe“.

(27) nuolat kintanti grėsmės aplinka ir pastarieji kibernetinio saugumo incidentai rodo didėjančią riziką Sąjungai, todėl valstybės narės turėtų nedelsdamos ir būtinai iki 2018 m. pabaigos imtis veiksmų pagal šią rekomendaciją,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

(1) Valstybės narės ir ES institucijos, vadovaudamosi plane aprašytais principais, turėtų sukurti ES reagavimo į kibernetinio saugumo krizes sistemą, į kurią būtų integruoti plane nustatyti bendradarbiavimo tikslai ir būdai.

(2) ES reagavimo į kibernetinio saugumo krizes sistemoje visų pirma turėtų būti nustatyti atitinkami visų lygmenų – techninio, operatyvinio, strateginio ir politinio – dalyviai, ES institucijos ir valstybių narių valdžios institucijos ir prireikus parengtos standartinės veiklos procedūros, kuriomis nustatoma, kaip tie dalyviai bendradarbiauja taikant ES krizių valdymo mechanizmus. Daugiausia dėmesio turėtų būti skirta tam, kaip nedelsiant keistis informacija ir koordinuoti reagavimą didelio masto kibernetinio saugumo incidentų ir krizių metu.

(3) Todėl valstybių narių kompetentingos institucijos turėtų bendradarbiaudamos išsamiau nustatyti dalijimosi informacija ir bendradarbiavimo protokolus. Bendradarbiavimo grupė šia patirtimi turėtų dalytis su atitinkamomis ES institucijomis.

(4) Valstybės narės turėtų užtikrinti, kad jų nacionaliniuose krizių valdymo mechanizmuose būtų tinkamai sprendžiami reagavimo į kibernetinio saugumo incidentus klausimai ir numatytos būtinos bendradarbiavimo ES lygmeniu procedūros taikant ES sistemą.

(5) Kalbant apie esamus ES krizių valdymo mechanizmus, pagal planą valstybės narės turėtų kartu su Komisijos tarnybomis ir Europos išorės veiksmų tarnyba nustatyti praktinio įgyvendinimo gaires, susijusias su jų krizių valdymo ir kibernetinio saugumo nacionalinių subjektų ir procedūrų integravimu į esamus ES krizių valdymo mechanizmus, būtent IPCR ir Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmą. Visų pirma, valstybės narės turėtų užtikrinti, kad būtų sukurtos atitinkamos struktūros, kurios jų nacionalinėms krizių valdymo institucijoms ir jų ES lygmens atstovams užtikrintų galimybę efektyviai keistis informacija taikant ES krizių valdymo mechanizmus.

(6) Valstybės narės turėtų pasinaudoti visomis Europos infrastruktūros tinklų priemonės kibernetinio saugumo skaitmeninių paslaugų infrastruktūrų programos galimybėmis ir bendradarbiauti su Komisija, siekdamos užtikrinti, kad šiuo metu rengiamame pagrindinių paslaugų platformos bendradarbiavimo mechanizme būtų numatytos būtinos funkcijos ir jis atitiktų jų reikalavimus dėl bendradarbiavimo ir kibernetinio saugumo krizių metu.

(7) Valstybės narės, padedamos ENISA ir pasinaudodamos šioje srityje atliktu darbu, turėtų bendradarbiauti, kad parengtų ir priimtų bendrą incidentų apibūdinimo sistemą ir padėties ataskaitų šabloną, kuriais naudojantis būtų galima apibūdinti kibernetinio saugumo incidentų technines priežastis ir poveikį ir taip dar labiau sustiprinti valstybių narių operatyvinį bendradarbiavimą krizių metu. Todėl valstybės narės turėtų atsižvelgti į bendradarbiavimo grupės darbą dėl pranešimo apie incidentus gairių, ypač į aspektus, susijusius su nacionalinių pranešimų forma.

(8) Sistemoje nustatyta tvarka turėtų būti išbandyta ir prireikus persvarstyta atsižvelgiant į valstybių narių dalyvavimo nacionalinėse, regioninėse ir Sąjungos, taip pat kibernetinės diplomatijos ir NATO, kibernetinio saugumo pratybose patirtį. Visų pirma ji turėtų būti išbandyta per ENISA organizuojamas „Cyber Europe“ pratybas. Pirma tokia galimybė bus per 2018 m. „Cyber Europe“ pratybas.

([1]) ST 15283/16, 2016 m. gruodžio 6 d.

(9) Valstybės narės ir ES institucijos turėtų reguliariai mokytis reaguoti į didelio masto kibernetinio saugumo incidentus ir krizes nacionaliniu ir Europos lygmeniu, įskaitant, kai reikia, politinį atsaką ir prireikus dalyvaujant privačiojo sektoriaus subjektams.

Priimta Briuselyje 2017 m. rugsėjo 13 d.

Komisijos vardu

Mariya GABRIEL

Komisijos narė

PRIEDAS

Koordinuoto atsako į didelio masto tarpvalstybinius kibernetinio saugumo incidentus ir krizes projektas

ĮVADAS

Šis projektas taikomas kibernetinio saugumo incidentams, kurių sukeliamų sutrikimų atitinkama valstybė narė negali pašalinti viena pati arba kurie dviem ar daugiau valstybių narių arba ES institucijų padaro tokio plataus masto ir tokios didelės techninės arba politinės reikšmės poveikį, kad būtina laiku koordinuoti politiką ir reaguoti Sąjungos politiniu lygmeniu.

Tokie didelio masto kibernetinio saugumo incidentai laikomi kibernetinio saugumo krize.

Kilus ES masto krizei, susijusiai su kibernetiniu saugumu, Sąjungos politinio lygmens atsaką koordinuoja Taryba, naudodamasi Integruoto politinio atsako į krizes (IPCR) mechanizmu.

Komisijoje atsakas koordinuojamas taikant skubaus įspėjimo sistemą ARGUS.

Jei krizei būdingas svarbus išorės arba bendros saugumo ir gynybos politikos (BSGP) aspektas, bus panaudotas Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmas.

Projekte parodoma, kaip šiems įtvirtintiems krizių valdymo mechanizmams turėtų būti visapusiškai panaudojami esami ES lygmens kibernetinio saugumo subjektai ir valstybių narių bendradarbiavimo mechanizmai.

Projekte atsižvelgiama į pagrindinius principus (proporcingumo, subsidiarumo, papildomumo ir informacijos konfidencialumo), pateikiami pagrindiniai trijų lygmenų (strateginio bei politinio, operatyvinio ir techninio) bendradarbiavimo tikslai (veiksmingas atsakas, bendras informuotumas apie padėtį, viešoji komunikacija), mechanizmai bei susiję subjektai ir veiksmai, kuriais siekiama minėtųjų pagrindinių tikslų.

Projektas neapima viso krizių valdymo ciklo (prevencijos ir (arba) poveikio mažinimo, pasirengimo, atsako ir atkūrimo), jame koncentruojamasi į atsaką. Tačiau jame aptariami ir kiti veiksmai, visų pirma susiję su bendru informuotumu apie padėtį.

Pažymėtina, kad kibernetinio saugumo incidentai gali būti pagrindinė arba viena iš platesnio masto krizės, veikiančios kitus sektorius, priežasčių. Turint omenyje tai, kad dauguma kibernetinio saugumo krizių daro poveikį materialiajam pasauliui, tinkamas atsakas turi būti grindžiamas ir kibernetinėmis, ir nekibernetinėmis poveikio mažinimo priemonėmis. Reagavimo į kibernetines krizes veiksmai turi būti derinami su kitais krizių valdymo mechanizmais ES, nacionaliniu ar sektorių lygmenimis.

Galiausiai projektas nepakeičia esamų konkrečių sektorių ar konkrečios politikos mechanizmų, susitarimų ar priemonių, pavyzdžiui, nustatytų Europos pasaulinės palydovinės navigacijos sistemos (GNSS) programoje ([1]), ir neturėtų daryti jiems įtakos.

Pagrindiniai principai

Siekiant tikslų, nustatant būtinus veiksmus ir paskirstant funkcijas ir pareigas atitinkamiems subjektams arba mechanizmams, buvo laikomasi toliau nurodytų pagrindinių principų ir jų turi būti laikomasi vėliau rengiant įgyvendinimo gaires.

Proporcingumo principas. Didžioji dauguma valstybėse narėse įvykstančių kibernetinio saugumo incidentų toli gražu negali būti laikomi sukeliančiais nacionalinę ir juo labiau europinę krizę. Valstybių narių bendradarbiavimo reaguojant į tokius incidentus pagrindas yra reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklas, sukurtas pagal Tinklų ir informacijos saugumo direktyvą ([2]). Vadovaudamosi CSIRT tinklo standartinėmis veiklos procedūromis nacionalinės CSIRT savanoriškai bendradarbiauja ir kasdien keičiasi informacija, taip pat ir reaguodamos į kibernetinio saugumo incidentus, darančius poveikį vienai ar daugiau valstybių narių. Todėl šiame projekte turėtų būti visapusiškai pasinaudojama šiomis standartinėmis veiklos procedūromis, kuriose turėtų būti apžvelgiamos papildomos užduotys, vykdytinos kilus kibernetinio saugumo krizei.

([1]) Sprendimas 2014/496/BUSP.
([2]) Direktyva (ES) 2016/1148.

Subsidiarumo principas. Subsidiarumo principas yra esminis. Pagrindinė atsakomybė reaguoti į didelio masto kibernetinio saugumo incidentus ir krizes tenka jų paveiktoms valstybėms narėms. Tačiau svarbus vaidmuo tenka ir Komisijai, Europos išorės veiksmų tarnybai ir kitoms ES institucijoms, organams, agentūroms ir įstaigoms. Šis vaidmuo aiškiai nustatytas IPCR mechanizme, taip pat grindžiamas Sąjungos teisės aktais ir atsižvelgiant į tai, kad kibernetinio saugumo incidentai ir krizės gali paveikti visas bendrosios rinkos ekonominės veiklos sritis, Sąjungos saugumą ir tarptautinius santykius, taip pat pačias institucijas.

Papildomumo principas. Plane visapusiškai atsižvelgiama į esamus ES lygmens krizių valdymo mechanizmus, t. y. Integruotą politinio atsako į krizes (IPCR) mechanizmą, ARGUS ir Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmą, į jį įtrauktos pagal Tinklų ir informacijos saugumo direktyvą sukurtos naujos struktūros ir mechanizmai, t. y. CSIRT tinklas, taip pat atitinkamos agentūros ir įstaigos, t. y. Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA), Europolo Europos kovos su elektroniniu nusikalstamumu centras (EC3), ES žvalgybos analizės centras (INTCEN), ES karinio štabo žvalgybos skyrius (EUMS INT) ir ES situacijų kabinetas (SITROOM) (įsikūręs INTCEN), kartu vykdantys Bendro žvalgybinės informacijos analizės centro (SIAC) veiklą; ES hibridinių grėsmių analizės ir informavimo centras (įsikūręs INTCEN); Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnyba (CERT-ES). Projektas taip pat turėtų užtikrinti, kad sąveikaudami ir bendradarbiaudami jie kuo labiau papildytų vienas kitą ir jų veikla kuo mažiau dubliuotųsi.

Informacijos konfidencialumas. Visi informacijos mainai pagal šį projektą turi būti vykdomi laikantis galiojančių saugumo taisyklių ([1]), asmens duomenų apsaugos reikalavimų ir Srauto kontrolės protokolo ([2]). Įslaptintos informacijos mainams, nesvarbu, kuri klasifikavimo sistema taikoma, turi būti naudojamos turimos akredituotos priemonės ([3]). Tvarkant asmens duomenis bus laikomasi galiojančių ES taisyklių, visų pirma Bendrojo duomenų apsaugos reglamento ([4]), E. privatumo direktyvos ([5]), taip pat Reglamento dėl asmenų apsaugos Sąjungos institucijoms, įstaigoms, organams ir agentūroms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo ([6]).

Pagrindiniai tikslai

Kaip jau minėta, projekte numatytas trijų lygmenų – politinis, operatyvinis ir techninis – bendradarbiavimas. Bendradarbiaujant kiekvienu lygmeniu, gali būti keičiamasi informacija ir bendrais veiksmais siekiama toliau nurodytų pagrindinių tikslų.

— Sudaryti sąlygas veiksmingam atsakui: priklausomai nuo kibernetinio saugumo incidento, atsakas į jį gali būti įvairių formų: nuo techninių priemonių nustatymo, kai du ar daugiau subjektų kartu tiria technines incidento priežastis (pvz., atlieka kenkimo programinės įrangos analizę) arba nustato būdus, kaip organizacijos gali įvertinti, ar jos buvo paveiktos (pvz., nustato užvaldymo rodiklius), iki operatyvinių sprendimų taikyti tokias technines priemones ir politinio lygmens sprendimo naudoti kitas priemones, pvz., ES diplomatinį atsaką į kibernetinę kenkimo veiklą (Kibernetinio saugumo diplomatijos priemonių rinkinį) ar ES operatyvinių veiksmų protokolą dėl kovos su hibridinėmis grėsmėmis.

— Būti visiems kartu informuotiems apie padėtį: atsakui koordinuoti būtina, kad visi minėtais trimis (techniniu, operatyviniu ir politiniu) lygmenimis veikiantys suinteresuotieji subjektai gerai suprastų vykstančius įvykius. Informuotumas apie padėtį gali apimti technines incidento priežastis, taip pat jo poveikį ir kilmę. Kibernetinio saugumo incidentų gali įvykti labai įvairiuose sektoriuose (finansų, energetikos, transporto, sveikatos priežiūros ir kt.), todėl būtina, kad reikalinga ir tinkamo formato informacija laiku pasiektų visus suinteresuotuosius subjektus.

([1]) 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl saugumo Komisijoje (OL L 72, 2015 3 17, p. 41) ir 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/444 dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 72, 2015 3 17, p. 53); 2013 m. balandžio 19 d. Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimas dėl Europos išorės veiksmų tarnybos saugumo taisyklių (OL C 190, 2013 6 29, p.1); 2013 m. rugsėjo 23 d. Tarybos sprendimas 2013/488/ES dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių (OL L 274, 2013 10 15, p. 1).

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

([3]) 2016 m. birželio mėn. tokie informacijos perdavimo kanalai buvo CIMS (įslaptintos informacijos valdymo sistema), ACID (šifravimo algoritmas), RUE (saugi slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėtų dokumentų kūrimo, mainų ir saugojimo sistema) ir SOLAN. Kitos priemonės, kuriomis perduodama įslaptinta informacija, yra PGP arba S/MIME.

([4]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([5]) 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).

([6]) 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1) (persvarstomas).

— Susitarti dėl pagrindinių viešosios komunikacijos pranešimų ([1]): kilus krizei, komunikacija labai svarbi siekiant sumažinti neigiamą kibernetinio saugumo incidentų ir krizių poveikį, tačiau gali būti naudojama ir (potencialių) agresorių elgesiui paveikti. Tinkamas pranešimas gali būti aiškus tikėtinų diplomatinio atsako padarinių signalas, kuriuo siekiama paveikti agresorių elgesį. Siekiant užtikrinti politinio atsako veiksmingumą, labai svarbu, kad viešasis komunikavimas siekiant sumažinti neigiamą kibernetinio saugumo incidentų ir krizių poveikį ir viešasis komunikavimas siekiant paveikti agresorių būtų suderinti. Ypač svarbu skleisti tikslią ir paveikią informaciją visuomenei apie tai, kaip galima sumažinti incidento padarinius (pvz., įdiegiant programinės įrangos pataisą ar imantis papildomų veiksmų grėsmei išvengti ir t. t.).

VALSTYBIŲ NARIŲ TARPUSAVIO IR VALSTYBIŲ NARIŲ BEI ES SUBJEKTŲ TECHNINIS, OPERATYVINIS IR STRATEGINIS BEI POLITINIS BENDRADARBIAVIMAS

Veiksmingas atsakas į didelio masto kibernetinio saugumo incidentus ar krizes ES lygmeniu priklauso nuo veiksmingo techninio, operatyvinio ir strateginio bei politinio bendradarbiavimo.

Susiję subjektai kiekvienu lygmeniu turėtų vykdydami tam tikrą veiklą siekti trijų pagrindinių tikslų:

— koordinuoto atsako,

— bendro informuotumo apie padėtį,

— viešosios komunikacijos.

Įvykus incidentui ar kilus krizei, žemesnioji bendradarbiavimo grandis įspės, informuos ir parems aukštesniąją grandį, o aukštesnioji grandis prireikus savo ruožtu pateiks žemesniajai grandžiai rekomendacijų ([2]) ir priims sprendimus.

Techninis bendradarbiavimas

Veiklos apimtis

— Incidentų valdymas ([3]) kilus kibernetinio saugumo krizei.

— Incidentų stebėjimas ir kontrolė įskaitant nenutrūkstamą grėsmių ir rizikos analizę.

Potencialūs veikiantys subjektai

Pagrindinis šiame projekte numatytas techninio bendradarbiavimo mechanizmas – CSIRT tinklas, kuriam pirmininkauja Tarybai pirmininkaujanti valstybė narė, o sekretoriato funkciją atlieka ENISA.

— Valstybės narės

  — Kompetentingos institucijos ir bendrieji informaciniai centrai, įsteigti pagal Tinklų ir informacijos saugumo direktyvą

  — CSIRT

— ES įstaigos, organai ir agentūros

  — ENISA

  — Europolo EC3

  — CERT-ES

([1]) Pažymėtina, kad viešoji komunikacija gali reikšti tiek visos visuomenės informavimą apie incidentą, tiek labiau techninio ar operatyvinio pobūdžio informacijos teikimą svarbiems sektoriams ir (arba) per incidentą nukentėjusiems asmenims. Tam gali prireikti konfidencialios informacijos sklaidos kanalų ir specialių techninių priemonių ir (arba) platformų. Bet kuriuo atveju komunikavimas su operatoriais ir plačiąja visuomene valstybėje narėje yra tos valstybės narės prerogatyva ir pareiga. Todėl laikantis pirmiau minėto subsidiarumo principo valstybės narės ir nacionalinės CSIRT yra visiškai atsakingos už informacijos sklaidą savo teritorijoje ir savo tikslinėms grupėms.

([2]) Leidimas veikti: kilus kibernetinio saugumo krizei, gyvybiškai svarbu greitai reaguoti, kad būtų imtasi reikiamų poveikio mažinimo veiksmų. Kad būtų įmanoma greitai sureaguoti, valstybės narės viena kitai gali suteikti leidimus veikti, tada jos gali veikti nedelsdamos ir neprivalėdamos konsultuotis su aukštesne instancija arba ES institucijomis visais įprastai reikalaujamais oficialiais kanalais, nebent to reikia dėl konkretaus incidento (pvz., CSIRT nereikėtų konsultuotis su aukštesne grandimi dėl vertingos informacijos persiuntimo kitos valstybės narės CSIRT).

([3]) Incidentų valdymas – visos procedūros, padedančios nustatyti, ištirti bei suvaldyti incidentą ir į jį reaguoti.

— Europos Komisija

  — Reagavimo į nelaimes koordinavimo centras (visą parą septynias dienas per savaitę veikianti operatyvinė tarnyba, įsikūrusi Europos civilinės saugos ir humanitarinės pagalbos operacijų generaliniame direktorate) ir paskirta vadovaujančioji tarnyba (tai gali būti Ryšių tinklų, turinio ir technologijų GD arba Migracijos ir vidaus reikalų GD, nelygu incidento pobūdis), Generalinis sekretoriatas (ARGUS sekretoriatas), Žmogiškųjų išteklių ir saugumo GD (Saugumo direktoratas), Informatikos GD (IT saugumo operacijos)

  — Kitų ES agentūrų ([1]) – atitinkamas pagrindinis Komisijos generalinis direktoratas arba Europos išorės veiksmų tarnyba (kreipiamasi pirmiausia)

— Europos išorės veiksmų tarnyba

  — SIAC (Bendras žvalgybinės informacijos analizės centras: ES INTCEN ir EUMS INT)

  — ES situacijų kabinetas ir pagal geografinę vietą ar tematiką paskirta tarnyba

  — ES hibridinių grėsmių analizės ir informavimo centras (ES INTCEN veiklos dalis, apimanti kibernetinį saugumą, susijusį su hibridinėmis grėsmėmis)

Bendras informuotumas apie padėtį

— Reguliaraus techninio bendradarbiavimo, padedančio būti geriau informuotiems apie padėtį Sąjungoje, dalis turėtų būti ENISA'os reguliariai rengiama ES kibernetinio saugumo techninės padėties ataskaita, kurioje apžvelgiami incidentai ir grėsmės ir kuri grindžiama viešai prieinama informacija, pačios agentūros atliekama analize ir ataskaitomis, kurias agentūrai pateikia valstybių narių CSIRT (savanoriškai) arba pagal Tinklų ir informacijos saugumo direktyvą įsteigti bendrieji informaciniai centrai, Europolo Europos kovos su elektroniniu nusikalstamumu centras (EC3) bei CERT-ES ir prireikus Europos išorės veiksmų tarnybai priklausantis ES žvalgybos analizės centras (INTCEN). Ataskaita turėtų būti pateikti atitinkamoms Tarybos instancijoms, Komisijai, vyriausiajam įgaliotiniui ir CSIRT tinklui.

— Įvykus dideliam incidentui, CSIRT tinklo pirmininkas, kuriam padeda ENISA, parengia ES kibernetinio saugumo incidento padėties ataskaitą ([2]), kurią per Tarybai rotacijos tvarka pirmininkaujančios valstybės narės CSIRT pateikia pirmininkaujančiai valstybei narei, Komisijai ir vyriausiajam įgaliotiniui.

— *Visos kitos ES agentūros* ataskaitas teikia atitinkamam pagrindiniam GD, o šis savo ruožtu – Komisijos vadovaujančiajai tarnybai.

— *CERT-ES* techninės ataskaitas teikia CSIRT tinklui, ES institucijoms ir agentūroms (kai tinkama) ir ARGUS (jei aktyvinta).

— *Europolo EC3* ([3]) *ir CERT-ES* teikia techninių artefaktų ekspertizės duomenis ir kitą techninę informaciją CSIRT tinklui.

— Europos išorės veiksmų tarnybos SIAC: INTCEN pavedimu ES hibridinių grėsmių analizės ir informavimo centras teikia ataskaitas atitinkamiems Europos išorės veiksmų tarnybos padaliniams.

Atsakas

— CSIRT tinklas keičiasi techniniais ir incidento analizės duomenimis, kaip antai IP adresai, užvaldymo rodikliai ([4]) ir kt. Tokia informacija nedelsiant ir ne vėliau kaip per 24 val. nuo incidento nustatymo turėtų būti pateikta ENISA'ai.

— Vadovaudamiesi CSIRT tinklo standartinėmis veiklos procedūromis, jo nariai deda bendras pastangas išanalizuoti žinomus techninius artefaktus ir kitą su incidentu susijusią techninę informaciją, siekdami nustatyti priežastis ir galimas technines poveikio mažinimo priemones.

— CSIRT vykdyti techninę veiklą padeda ENISA remdamasi savo ekspertinėmis žiniomis ir įgaliojimais ([5]).

([1]) Priklausomai nuo incidento pobūdžio ir poveikio įvairiems veiklos sektoriams (finansų, transporto, energetikos, sveikatos priežiūros ir kt.) įsitrauks atitinkamos ES agentūros ar įstaigos.
([2]) ES kibernetinio saugumo incidento padėties ataskaita – valstybių narių CSIRT pateiktų nacionalinių ataskaitų suvestinė. Ataskaitos formatas turėtų būti apibūdintas CSIRT tinklo standartinėse veiklos procedūrose.
([3]) Vadovaudamasis EC3 pagrindiniuose teisės aktuose nustatytomis sąlygomis ir procedūromis.
([4]) Užvaldymo rodiklis – atliekant kompiuterių ekspertizę tinkle arba operacinėje sistemoje stebimas artefaktas, patikimai rodantis, jog prie kompiuterio buvo neteisėtai prisijungta. Tipiniai užvaldymo rodikliai yra virusų kodai ir IP adresai, kenkimo programinės įrangos failų MD5 maišos kodai, botnetų valdymo serverių URL arba domenų vardai.
([5]) Reglamento dėl Europos kibernetinio saugumo agentūros ENISA ir dėl informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, pasiūlymas (Kibernetinio saugumo aktas), 2017 m. rugsėjo 13 d.

— Valstybių narių CSIRT koordinuoja savo techninę reagavimo veiklą, joms padeda ENISA ir Komisija.

— Europos išorės veiksmų tarnybos SIAC: INTCEN pavedimu ES hibridinių grėsmių analizės ir informavimo centras inicijuoja pradinių įrodymų surinkimo procesą.

Viešoji komunikacija

— CSIRT parengia techninių patarimų ([1]) ir apie pažeidžiamumą įspėjančių pranešimų ([2]) ir šią informaciją išplatina atitinkamoms bendruomenėms ir visuomenei, laikydamosi atitinkamu atveju taikomų procedūrų.

— Parengti ir platinti bendrus CSIRT tinklo pranešimus padeda ENISA.

— ENISA savo viešojo komunikavimo veiklą derina su CSIRT tinklu ir Komisijos atstovo spaudai tarnyba.

— ENISA ir EC3 derina savo viešojo komunikavimo veiklą, remdamiesi valstybių narių sutarta bendro informuotumo apie padėtį samprata. Abi šios struktūros derina savo viešojo komunikavimo veiklą su Komisijos atstovo spaudai tarnyba.

— Jeigu krizė susijusi su išoriniais arba bendros saugumo ir gynybos politikos (BSGP) aspektais, viešoji komunikacija derinama su Europos išorės veiksmų tarnyba ir vyriausiojo įgaliotinio atstovo spaudai tarnyba.

Operatyvinis bendradarbiavimas

Veiklos apimtis

— Pasirengimas priimti sprendimus politiniu lygmeniu

— Kibernetinio saugumo krizių valdymo koordinavimas (kai reikia)

— Padarinių ir poveikio ES lygmeniu vertinimas ir galimų poveikio mažinimo veiksmų siūlymas

Potencialūs veikiantys subjektai

— Valstybės narės

  — Kompetentingos institucijos ir bendrieji informaciniai centrai, įsteigti pagal Tinklų ir informacijos saugumo direktyvą

  — CSIRT, kibernetinio saugumo agentūros

  — Kitos nacionalinės atskirų sektorių institucijos (jei incidentas arba krizė apima kelis sektorius)

— ES įstaigos, organai ir agentūros

  — ENISA

  — Europolo EC3

  — CERT-ES

— Europos Komisija

  — Generalinio sekretoriaus (pavaduotojas) (ARGUS procesas)

  — Ryšių tinklų, turinio ir technologijų GD / Migracijos ir vidaus reikalų GD

  — Komisijos saugumo institucija

  — Kiti generaliniai direktoratai (jei incidentas arba krizė apima kelis sektorius)

([1]) Techninio pobūdžio patarimas, pvz., paaiškinamos incidento priežastys ir nurodomos galimos poveikio mažinimo priemonės.
([2]) Informacija apie techninį pažeidžiamumą, kuriuo gali būti pasinaudota siekiant neigiamai paveikti IT sistemas.

— Europos išorės veiksmų tarnyba

  — Už reagavimą į krizes atsakingas Generalinio sekretoriaus (pavaduotojas) ir SIAC (ES INTCEN ir EUMS INT)

  — ES hibridinių grėsmių analizės ir informavimo centras

— Taryba

  — Tarybai pirmininkaujanti valstybė narė (Kibernetinių klausimų horizontaliosios darbo grupės pirmininkas arba Nuolatinių atstovų komitetas ([1])), kuriai padeda Tarybos Generalinis sekretoriatas arba Politinis ir saugumo komitetas ([2]) ir IPCR mechanizmas, jei inicijuotas jo taikymas

Informuotumas apie padėtį

— Padėti parengti politinės bei strateginės padėties ataskaitas (pvz., integruotą informuotumo apie padėtį ir analizės ataskaitą, jei inicijuotas IPCR mechanizmo taikymas)

— *Tarybos Kibernetinių klausimų horizontalioji darbo grupė* prireikus rengia Nuolatinių atstovų komiteto arba Politinio ir saugumo komiteto posėdį

— Jei inicijuotas IPCR mechanizmo taikymas:

  — Tarybai pirmininkaujanti valstybė narė, siekdama pasiruošti Nuolatinių atstovų komiteto arba Politinio ir saugumo komiteto posėdžiui, gali sušaukti apskritojo stalo posėdį, kuriame dalyvauja valstybių narių suinteresuotieji subjektai, institucijos, agentūros ir trečiosios šalys, tokios kaip ES nepriklausančios valstybės ir tarptautinės organizacijos. Šiuose posėdžiuose dėl krizės siekiama nustatyti spragas ir parengti kompleksinių klausimų sprendimo pasiūlymų.

  — *Komisijos vadovaujančiajai tarnybai arba Europos išorės veiksmų tarnybai*, vadovaujančioms integruotos informuotumo ir analizės (ISAA) ataskaitos rengimui, ją parengti padeda ENISA, CSIRT tinklas, Europolo EC3, EUMS INT, INTCEN ir visi kiti susiję subjektai. ISAA ataskaita – ES mastu atliktas vertinimas, paremtas techninių incidentų ir krizių vertinimo (grėsmių analizės, rizikos vertinimo, netechninių padarinių ir poveikio, nekibernetinių incidento arba krizės aspektų ir pan.) sąryšiu ir pritaikytas operatyvinės ir politinės grandžių reikmėms.

— Jei naudojama sistema ARGUS:

  — CERT-ES ir EC3 ([3]) tiesiogiai padeda keistis informacija Komisijoje.

— Jei naudojamas Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmas:

  — SIAC intensyviau renka savo informaciją, apibendrina iš visų šaltinių gautą informaciją ir išanalizuoja bei įvertina incidentą.

Atsakas (politinio lygmens prašymu)

— Tarpvalstybinis bendradarbiavimas su bendraisiais informaciniais centrais ir nacionalinėmis kompetentingomis institucijomis (Tinklų ir informacijos saugumo direktyva) siekiant mažinti padarinius ir poveikį.

— Visų techninių poveikio mažinimo priemonių naudojimas ir techninių pajėgumų koordinavimas siekiant sustabdyti išpuolius prieš informacines sistemas arba sumažinti jų poveikį.

— Bendradarbiavimas ir, jei nusprendžiama, techninių pajėgumų koordinavimas bendrai ar kolektyviai reaguojant vadovaujantis ***CSIRT tinklo standartinėmis veiklos procedūromis***.

— Būtinybės bendradarbiauti su atitinkamomis trečiosiomis šalimis įvertinimas.

— Sprendimų priėmimas vykdant ARGUS procesą (jei inicijuotas).

— Sprendimų rengimas ir koordinavimas pagal IPCR mechanizmą (jei inicijuotas jo taikymas).

— Pagalba Europos išorės veiksmų tarnybai priimti sprendimus taikant Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmą (jei inicijuotas jo taikymas), įskaitant ryšius su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, taip pat priemones, skirtas BSGP misijoms ir operacijoms bei ES delegacijoms apsaugoti.

([1]) Nuolatinių atstovų komitetas, arba COREPER, pagal Sutarties dėl Europos Sąjungos veikimo 240 straipsnį yra atsakingas už Europos Sąjungos Tarybos darbo rengimą.

([2]) Politinis ir saugumo komitetas – Europos Sąjungos sutarties 38 straipsnyje nurodytas Europos Sąjungos Tarybos komitetas, nagrinėjantis bendros užsienio ir saugumo politikos (BUSP) klausimus.

([3]) Vadovaudamasis EC3 pagrindiniuose teisės aktuose nustatytomis sąlygomis ir procedūromis.

Viešoji komunikacija

— Susitariama dėl viešų pranešimų apie incidentą.

— Jeigu krizė susijusi su išoriniais arba bendros saugumo ir gynybos politikos (BSGP) aspektais, viešasis komunikavimas derinamas su Europos išorės veiksmų tarnyba ir vyriausiojo įgaliotinio atstovo spaudai tarnyba.

Strateginis bei politinis bendradarbiavimas

Potencialūs veikiantys subjektai

— Valstybių narių – už kibernetinį saugumą atsakingi ministrai

— Europos Vadovų Tarybos – Pirmininkas

— Tarybos – Tarybai rotacijos tvarka pirmininkaujanti valstybė narė

— Jei taikomos Kibernetinio saugumo diplomatijos priemonių rinkinio priemonės – Politinis ir saugumo komitetas ir Horizontalioji darbo grupė

— Europos Komisijos – Pirmininkas arba įgaliotas Pirmininko pavaduotojas ar Komisijos narys

— Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai ir (arba) Komisijos pirmininko pavaduotojas

Veiklos apimtis: strateginis bei politinis kibernetinių ir nekibernetinių krizės aspektų valdymas, įskaitant bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą priemones.

Informuotumas apie padėtį

— Nustatomas krizės sukeltų sutrikimų poveikis Sąjungos veikimui.

Atsakas

— Priklausomai nuo incidento pobūdžio ir poveikio, inicijuojamas papildomų krizės valdymo mechanizmų ir (arba) priemonių taikymas. Tai gali būti, pvz., Civilinės saugos mechanizmas.

— Imamasi bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą priemonių.

— Paveiktoms valstybėms narėms prireikus teikiama skubi parama, pvz., naudojamas Reagavimo į kibernetinio saugumo krizes fondas ([1]).

— Bendradarbiavimas ir veiksmų koordinavimas, jei reikia, su tarptautinėmis organizacijomis, kaip antai Jungtinės Tautos (JT), Europos saugumo ir bendradarbiavimo organizacija (ESBO) ir ypač NATO.

— Nacionalinio saugumo ir gynybos aspektų vertinimas.

Viešoji komunikacija

Priklauso nuo bendros viešojo komunikavimo strategijos.

SU VALSTYBĖMIS NARĖMIS SUDERINTAS ATSAKAS ES LYGMENIU, KAI TAIKOMAS IPCR MECHANIZMAS

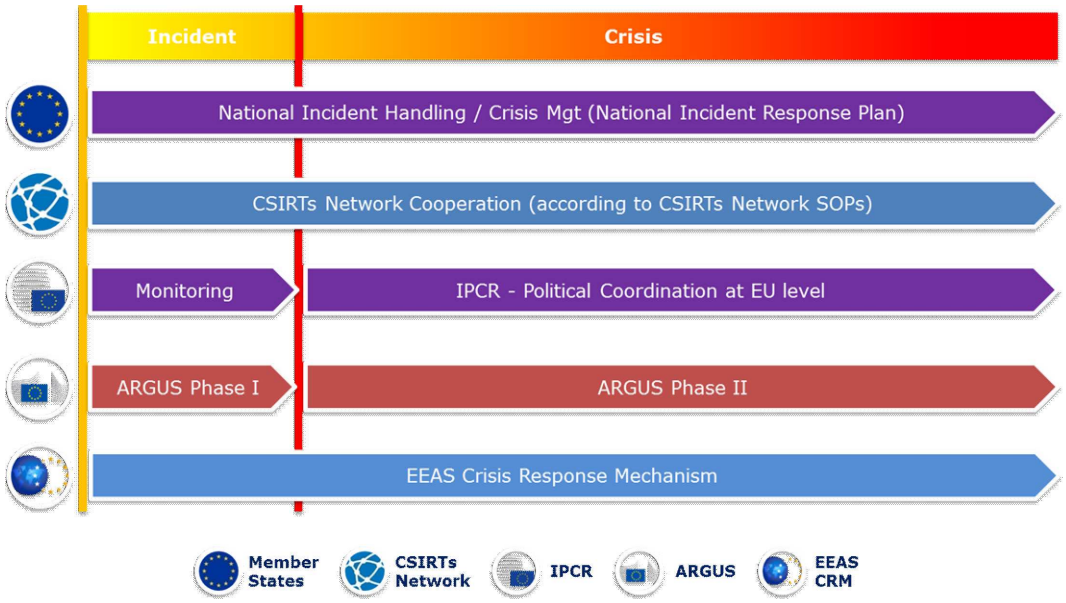
Laikantis papildomumo principo ES lygmeniu, šiame skirsnyje pristatomas (daugiausia dėmesio skiriama) pagrindinis tikslas ir valstybių narių institucijų, CSIRT tinklo, ENISA'os, CERT-ES, Europolo EC3, INTCEN, ES hibridinių grėsmių analizės ir informavimo centro ir Tarybos Kibernetinių klausimų horizontaliosios darbo grupės pareigos ir veikla taikant IPCR mechanizmą. Subjektai veikia laikydamiesi ES arba nacionaliniu lygmeniu nustatytos tvarkos.

Pažymėtina, kad nepriklausomai nuo to, ar inicijuojamas ES krizių valdymo mechanizmų taikymas, kaip pavaizduota 1 paveiksle, nacionalinio masto veikla ir bendradarbiavimas CSIRT tinkle (jei reikia) įvykus bet kokiam incidentui ar krizei vykdomi laikantis subsidiarumo ir proporcingumo principų.

([1]) Įsteigti Reagavimo į kibernetinio saugumo krizes fondą siūloma bendrame komunikate „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“, JOIN(2017) 450/1.

1 paveikslas

Atsakas į kibernetinio saugumo incidentus ir krizes ES lygmeniu



Visa toliau apibūdinta veikla vykdoma laikantis atitinkamų bendradarbiavimo mechanizmų standartinių veiklos procedūrų ir taisyklių, atskiriems subjektams ir institucijoms nustatytų įgaliojimų ir kompetencijų. Šias procedūras ir taisykles gali reikėti papildyti ar pakeisti, kad bendradarbiavimas ir atsakas į didelio masto kibernetinio saugumo incidentus ir krizes būtų kuo veiksmingesni.

Įvykus konkrečiam incidentui, veiksmų imtis privalo ne visi toliau nurodyti subjektai. Tačiau galimas jų įsitraukimas turėtų būti numatytas šiame projekte ir atitinkamų bendradarbiavimo mechanizmų standartinėse veiklos procedūrose.

Atsižvelgiant į galimą skirtingą kibernetinio saugumo incidento arba krizės poveikį visuomenei, reikalingas didelis lankstumas, susijęs su atskirų sektorių subjektų dalyvavimu visais lygmenimis tiek kibernetinio, tiek nekibernetinio poveikio mažinimo veikloje.

Kibernetinio saugumo krizių valdymas: kibernetinio saugumo integravimas į IPCR procesą

Taikant IPCR mechanizmą, apibūdintą IPCR standartinėse veiklos procedūrose ([1]), iš eilės veikiama toliau nurodytais etapais (kai kurių iš jų reikalingumas priklauso nuo situacijos).

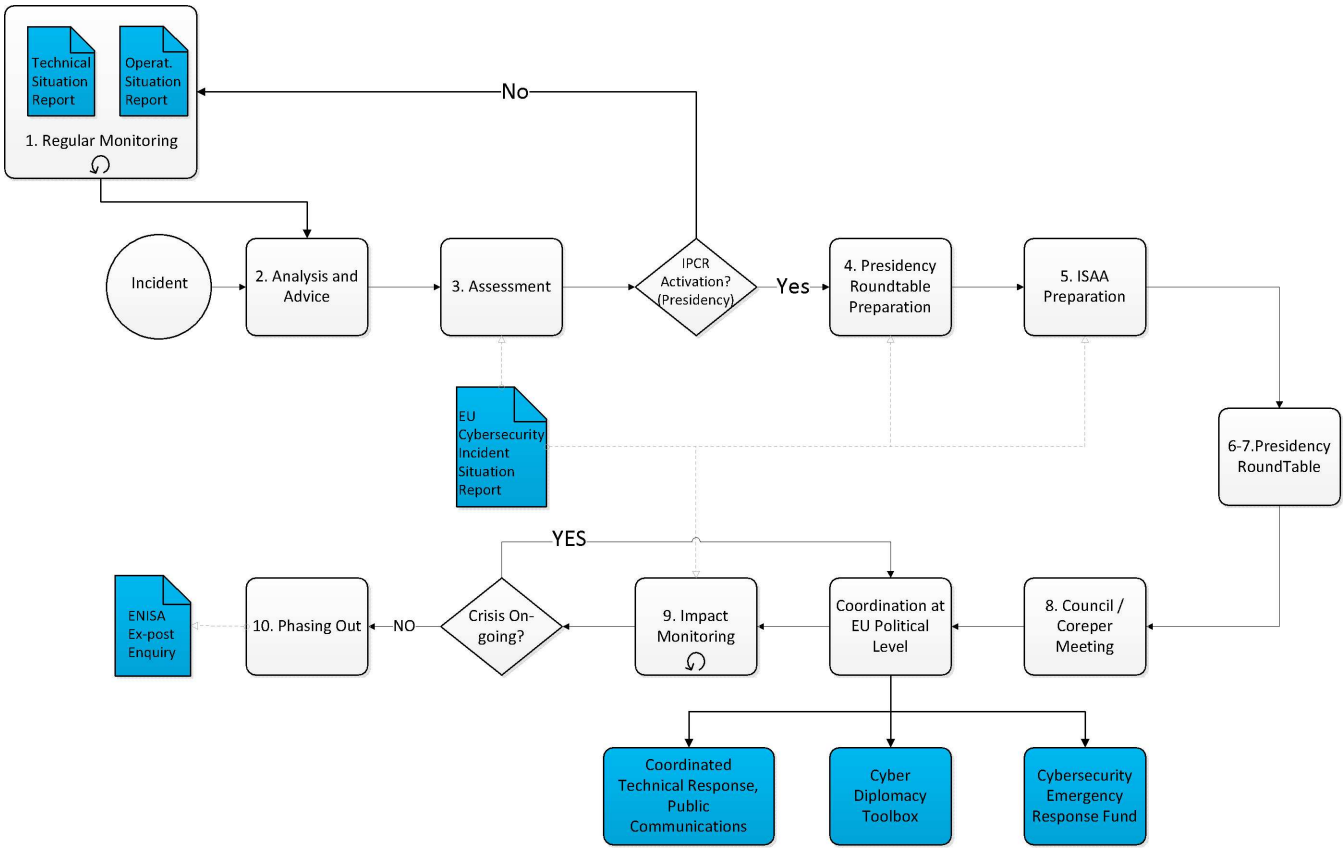
Nustatoma, kokie kibernetinio saugumo veiksmai atliekami kiekvienu etapu ir kurie subjektai jų imasi. Kad skaitytojams būtų patogiau, kiekvieno etapo aprašymas pradedamas IPCR standartinių veiklos procedūrų tekstu, o po jo pateikiama šiame projekte numatyta veikla. Be to, apibūdinant etapus paeiliui galima aiškiai pamatyti esamas reikiamo pajėgumo ir procedūrų **spragas**, trukdančias veiksmingai reaguoti į kibernetinio saugumo krizes.

IPCR procesas pavaizduotas 2 paveiksle ([2]), nauji jo elementai paryškinti mėlynai.

([1]) Dokumentas 12607/15 „IPCR standartinės veiklos procedūros“, dėl kurio sutarta „Pirmininkaujančios valstybės narės draugų“ grupėje ir su kuriuo Nuolatinių atstovų komitetas susipažino 2015 m. spalio mėn.
([2]) Didesnė paveikslo versija pateikta priedėlyje.

2 paveikslas

Kibernetiniam saugumui skirti IPCR elementai



Pastaba. Atsižvelgiant į hibridinės grėsmės kibernetinėje erdvėje pobūdį, dėl kurio neperžengiama riba, rodanti, kad kilo krizė, ES turi imtis prevencijos ir parengties priemonių. ES hibridinių grėsmių analizės ir informavimo centro užduotis – greitai išnagrinėti atitinkamus incidentus ir apie tai informuoti reikiamas koordinavimo struktūras. Šio centro reguliariai teikiama informacija gali padėti informuoti atskirų sektorių politikos formuotojus ir taip geriau pasirengti krizėms.

— **1 etapas. Reguliarus sektorių stebėjimas ir įspėjimas**: iš esamų reguliariai teikiamų padėties sektoriuose ataskaitų ir įspėjimų pirmininkaujanti valstybė narė gali sužinoti apie besiformuojančią krizę ir jos galimą raidą.

— **Nustatyta spraga**: šiuo metu Sąjungos lygmeniu nenumatytas reguliarus ir koordinuotas kibernetinio saugumo padėties ataskaitų ir įspėjimų apie kibernetinius incidentus (ir grėsmes) teikimas.

— **Projektas: ES kibernetinio saugumo padėties stebėjimas ir ataskaitų teikimas**

— ENISA reguliariai rengs **ES kibernetinio saugumo techninės padėties ataskaitą**, kurioje apžvelgiami incidentai ir grėsmės ir kuri grindžiama viešai prieinama informacija, pačios agentūros atliekama analize ir ataskaitomis, kurias agentūrai pateikia valstybių narių CSIRT (savanoriškai) arba pagal Tinklų ir informacijos saugumo direktyvą įsteigti bendrieji informaciniai centrai, Europolo Europos kovos su elektroniniu nusikalstamumu centras (EC3), CERT-ES ir Europos išorės veiksmų tarnybai priklausantis ES žvalgybos analizės centras (INTCEN). Ataskaita turėtų būti pateikti atitinkamoms Tarybos instancijoms, Komisijai ir CSIRT tinklui.

— SIAC vardu ES hibridinių grėsmių analizės ir informavimo centras turėtų parengti **ES kibernetinio saugumo operatyvinės padėties ataskaitą**. Ši ataskaita taip pat naudojama bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemai.

— Abi ataskaitos išplatinamos ES ir nacionaliniams suinteresuotiesiems subjektams, kad jie būtų geriau informuoti apie padėtį, būtų priimami informacija pagrįsti sprendimai ir palengvinamas tarpvalstybinis regioninis bendradarbiavimas.

Nustačius incidentą

— **2 etapas. Analizė ir rekomendacijos**: remdamiesi turima stebėjimo ir įspėjimo informacija, Komisijos tarnybos, Europos išorės veiksmų tarnyba ir Tarybos Generalinis sekretoriatas vieni kitus informuoja apie galimus įvykius, kad būtų pasirengę patarti Tarybai pirmininkaujančiai valstybei narei dėl galimo IPCR mechanizmo taikymo (visapusišku arba informacijos dalijimo režimu) inicijavimo.

  — **Projektas:**

    — Komisija – Ryšių tinklų, turinio ir technologijų GD, Migracijos ir vidaus reikalų GD, Žmogiškųjų išteklių ir saugumo GD ir Saugumo direktoratas, jiems padeda ENISA, EC3 ir CERT-ES.

    — Europos išorės veiksmų tarnyba. Remdamasis ES situacijų kabineto darbu ir žvalgybos šaltiniais, ES hibridinių grėsmių analizės ir informavimo centras teikia informaciją apie padėtį, susijusią su faktinėmis ir potencialiomis hibridinėmis grėsmėmis ES ir jos partneriams, įskaitant kibernetines grėsmes. Jeigu ES hibridinių grėsmių analizės ir informavimo centro analizė ir vertinimas rodo, kad yra potenciali grėsmė kuriai nors valstybei narei, šaliai partnerei arba organizacijai, INTCEN, laikydamasis nustatytų procedūrų, informuos (visų pirma) operatyvinę grandį. Operatyvinė grandis parengs politinei ir strateginei grandžiai skirtas rekomendacijas, be kita ko, dėl krizių valdymo mechanizmų (pvz., Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmo arba IPCR stebėjimo tinklalapio) galimo taikymo stebėjimo režimu inicijavimo.

    — CSIRT tinklo pirmininkas, kuriam padeda ENISA, parengia ES kibernetinio saugumo incidento padėties ataskaitą ([1]), kurią per Tarybai rotacijos tvarka pirmininkaujančios valstybės narės CSIRT pateikia pirmininkaujančiai valstybei narei, Komisijai ir vyriausiajam įgaliotiniui.

— **3 etapas. IPCR mechanizmo taikymo inicijavimo vertinimas / sprendimas**: pirmininkaujanti valstybė narė įvertina politinio koordinavimo, keitimosi informacija ar sprendimų priėmimo ES lygmeniu būtinybę. Tuo tikslu pirmininkaujanti valstybė narė gali surengti neformalų apskritojo stalo posėdį. Pirmininkaujanti valstybė narė preliminariai nustato sritis, reikalaujančias Nuolatinių atstovų komiteto arba Tarybos įsikišimo. Tai bus integruotų informuotumo apie padėtį ir analizės (ISAA) ataskaitų rengimo gairių pagrindas. Pirmininkaujanti valstybė narė, atsižvelgdama į krizės ypatybes, galimus padarinius ir susijusias politines reikmes, nusprendžia, ar reikia sušaukti atitinkamų Tarybos darbo grupių ir (arba) Nuolatinių atstovų komiteto ar Politinio ir saugumo komiteto posėdžius.

  — **Projektas:**

    — Apskritojo stalo posėdžio dalyviai:

      — Komisijos tarnybos ir Europos išorės veiksmų tarnyba konsultuos pirmininkaujančią valstybę narę atitinkamais jų kompetencijos klausimais.

      — Valstybių narių atstovai Kibernetinių klausimų horizontaliojoje darbo grupėje, padedami savo ekspertų (iš CSIRT, už kibernetinį saugumą atsakingų institucijų, kitų organizacijų).

      — Politinės ir strateginės ISAA ataskaitų rengimo gairės, paremtos naujausia ES kibernetinio saugumo incidento padėties ataskaita ir papildoma apskritojo stalo posėdžio dalyvių pateikta informacija.

      — Susijusios darbo grupės ir komitetai:

        — Kibernetinių klausimų horizontalioji darbo grupė.

  Komisija, Europos išorės veiksmų tarnyba ir Tarybos Generalinis sekretoriatas, visiškai pritariant ir bendradarbiaujant pirmininkaujančiai valstybei narei, taip pat gali nuspręsti inicijuoti IPCR mechanizmo taikymą informacijos dalijimosi režimu sukuriant krizės tinklalapį it taip pasirengiant galimam visapusiškam mechanizmo taikymui.

— **4 etapas. IPCR mechanizmo taikymo inicijavimas / informacijos rinkimas ir mainai**: inicijavus IPCR mechanizmo taikymą (dalijimosi informacija režimu ar visapusišką), jo internetinėje platformoje sukuriamas krizės tinklalapis, skirtas keistis informacija koncentruojantis į aspektus, padėsiančius surinkti duomenis ISAA ataskaitai ir pasirengti politinio lygmens diskusijoms. ISAA ataskaitos rengimui vadovaujančios tarnybos (viena iš Komisijos tarnybų arba Europos išorės veiksmų tarnyba) parinkimas priklausys nuo aplinkybių.

— **5 etapas. ISAA ataskaitos rengimas**: bus inicijuojamas ISAA ataskaitų rengimas. Komisija arba Europos išorės veiksmų tarnyba pateiks ISAA ataskaitas, kaip nurodyta ISAA standartinėse veiklos procedūrose, ir gali dar paraginti

([1]) ES kibernetinio saugumo incidento padėties ataskaita – valstybių narių CSIRT pateiktų nacionalinių ataskaitų suvestinė. Ataskaitos formatas turėtų būti apibūdintas CSIRT tinklo standartinėse veiklos procedūrose.

keistis informacija IPCR internetinėje platformoje arba atskirai paprašyti informacijos. ISAA ataskaitos bus rengiamos pagal politinio lygmens (t. y. Nuolatinių atstovų komiteto arba Tarybos) poreikius, nustatytus pirmininkaujančios valstybės narės ir nurodytus jos rekomendacijose, tai leis strategiškai apžvelgti padėtį ir turėti informacijos pirmininkaujančios valstybės narės organizuojamoms diskusijoms darbotvarkės klausimais. Vadovaujantis ISAA standartinėmis veiklos procedūromis, kuris subjektas – ar viena iš Komisijos tarnybų (Ryšių tinklų, turinio ir technologijų GD arba Migracijos ir vidaus reikalų GD), ar Europos išorės veiksmų tarnyba – rengs ISAA ataskaitą, priklausys nuo kibernetinio saugumo krizės pobūdžio.

Inicijavus IPCR mechanizmo taikymą, pirmininkaujanti valstybė narė nustatys konkrečias sritis, kurioms ISAA ataskaitoje reikia skirti daugiausia dėmesio, kad ji palengvintų politinį koordinavimą ir (arba) sprendimų priėmimą Taryboje. Pirmininkaujanti valstybė narė, pasikonsultavusi su Komisijos tarnybomis arba Europos išorės veiksmų tarnyba, taip pat nustatys ataskaitos rengimo tvarkaraštį.

— **Projektas:**

— Į ISAA ataskaitą įtraukiama informacija, kurią teikia susijusios tarnybos:

— CSIRT tinklas ES kibernetinio saugumo incidento padėties ataskaitoje,

— EC3, ES situacijų kabinetas, ES hibridinių grėsmių analizės ir informavimo centras, CERT-ES. ES hibridinių grėsmių analizės ir informavimo centras prireikus padės ir pateiks nuomonę ISAA ataskaitos rengimui vadovaujančiai tarnybai ir IPCR apskritojo stalo posėdžiams,

— atskirų sektorių ES agentūros ir įstaigos pagal tai, kurie sektoriai buvo paveikti,

— valstybių narių institucijos (ne CSIRT).

— ISAA ataskaitai rengti teikiamos informacijos ([1]) rinkimas:

— Komisija ir ES agentūros: pagrindinis vidinis tinklas ISAA ataskaitos informacijai rinkti bus IT sistema ARGUS. ES agentūros savo informaciją siųs savo generaliniams direktoratams, o šie savo ruožtu reikiamą informaciją pateiks sistemoje ARGUS. Komisijos tarnybos ir agentūros rinks informaciją iš esamų atskirų sektorių tinklų, kuriems priklauso valstybės narės ir tarptautinės organizacijos, ir iš kitų atitinkamų šaltinių.

— Europos išorės veiksmų tarnyba: pagrindinis vidinis tinklas ir bendrasis informacinis centras ISAA ataskaitos informacijai rinkti bus ES situacijų kabinetas, padedamas kitų susijusių Europos išorės veiksmų tarnybos padalinių. Europos išorės veiksmų tarnyba rinks informaciją iš trečiųjų šalių ir atitinkamų tarptautinių organizacijų.

— **6 etapas. Pasirengimas neformaliems pirmininkaujančios valstybės narės apskritojo stalo posėdžiams**: pirmininkaujanti valstybė narė, padedama Tarybos Generalinio sekretoriato, nustatys neformalaus apskritojo stalo posėdžio tvarkaraštį, darbotvarkę, dalyvius ir tikėtinus rezultatus (galimus siekinius). Tarybos Generalinis sekretoriatas pirmininkaujančios valstybės narės pavedimu perduos susijusią informaciją IPCR internetinėje platformoje ir paskelbs pranešimą apie posėdį.

— **7 etapas. Pirmininkaujančios valstybė narės apskritojo stalo posėdis ir pasirengimas ES politiniam koordinavimui ir sprendimų priėmimui**: pirmininkaujanti valstybė narė sušauks neformalų apskritojo stalo posėdį, per kurį apžvelgiama padėtis ir suformuluojami bei apsvarstomi klausimai, į kuriuos dėmesį turėtų atkreipti Nuolatinių atstovų komitetas arba Taryba. Neformaliame pirmininkaujančios valstybė narės apskritojo stalo posėdyje taip pat bus rengiami, svarstomi ir aptariami visi Nuolatinių atstovų komitetui arba Tarybai teiksimi veiksmų pasiūlymai.

— **Projektas:**

— Tarybos Kibernetinių klausimų horizontalioji darbo grupė rengia Politinio ir saugumo komiteto arba Nuolatinių atstovų komiteto posėdį.

— **8 etapas. Politinis koordinavimas ir sprendimų priėmimas Nuolatinių atstovų komitete arba Taryboje**: nuolatinių atstovų komiteto arba Tarybos posėdžių rezultatai yra reagavimo visais lygmenimis veiksmų koordinavimas, sprendimai dėl išskirtinių priemonių, politiniai pareiškimai ir t. t. Šie sprendimai yra ir atnaujintos politinės ir strateginės tolesnių ISAA ataskaitų rengimo gairės.

— **Projektas:**

— Politinis atsako į kibernetinio saugumo krizes koordinavimo sprendimas įgyvendinamas vykdant 1 skirsnyje „Techninis, operatyvinis ir strateginis bei politinis bendradarbiavimas“ punktuose **Atsakas** ir **Viešoji komunikacija** apibūdintą veiklą (ją vykdo atitinkami subjektai).

— ISAA ataskaita rengiama remiantis techniniu, operatyviniu ir politiniu bei strateginiu bendradarbiavimu siekiant **informuotumo apie padėtį**, kaip išdėstyta 1 skirsnyje.

([1]) ISAA standartinės veiklos procedūros.

— **9 etapas. Poveikio stebėjimas**: ISAA ataskaitos rengimui vadovaujanti tarnyba, padedama informaciją jai teikiančių subjektų, pateiks informaciją apie krizės raidą ir priimtų politinių sprendimų poveikį. Toks grįžtamasis ryšys padės tobulinti procesą, o pirmininkaujančiai valstybei narei – nuspręsti, ar ir toliau reikalingas ES politinio lygmens dalyvavimas, ar nutraukti IPCR mechanizmo taikymą.

— **10 etapas. Laipsniškas taikymo nutraukimas**: laikydamasi tokios pat kaip ir mechanizmo taikymo inicijavimo procedūros, pirmininkaujanti valstybė narė gali sušaukti neformalų apskritojo stalo posėdį, per kurį įvertinama galimybė toliau taikyti IPCR mechanizmą ar nutraukti jo taikymą. Pirmininkaujanti valstybė narė gali nuspręsti nutraukti taikymą arba sumažinti jo lygį.

— **Projektas:**

— ENISA gali būti paprašyta atlikti arba padėti atlikti incidento techninį *ex post* tyrimą pagal jos įgaliojimų nuostatas.

PRIEDĖLIS

1. ES LYGMENS KRIZIŲ VALDYMAS, BENDRADARBIAVIMO MECHANIZMAI IR DALYVIAI

Krizių valdymo mechanizmai

Integruotas politinio atsako į krizes mechanizmas (IPCR). 2013 m. birželio 25 d. Tarybos patvirtintas ES integruotas politinio atsako į krizes mechanizmas ([1]) sukurtas siekiant sudaryti sąlygas didelės krizės atveju laiku koordinuoti veiksmus ir reaguoti ES politiniu lygmeniu. Be to, IPCR mechanizmu remiamas atsako į solidarumo sąlygos taikymą (Sutarties dėl Europos Sąjungos veikimo 222 straipsnis) koordinavimas politiniu lygmeniu, kaip apibrėžta 2014 m. birželio 24 d. Tarybos sprendime 2014/415/ES dėl tvarkos, kuria Sąjunga įgyvendina solidarumo sąlygą. IPCR standartinėse veiklos procedūrose ([2]) nustatytas aktyvinimo procesas ir tolesni veiksmai, kurių turi būti imtasi.

ARGUS. 2005 m. Europos Komisijos sukurta krizių koordinavimo sistema, kurioje nustatytas specialus koordinavimo procesas didelės daugiasektorinės krizės atveju. Ji remiama to paties pavadinimo bendrąja skubaus įspėjimo sistema (IT priemone). Sistemoje ARGUS numatyti du etapai, antrajame etape (didelės daugiasektorinės krizės atveju) Komisijos pirmininko arba Komisijos nario, kuriam paskirta ši pareiga, pavedimu šaukiami Krizių koordinavimo komiteto posėdžiai. Krizių koordinavimo komitete dalyvauja atitinkamų Komisijos generalinių direktoratų, kabinetų ir kitų ES tarnybų atstovai, kad būtų galima vadovauti ir koordinuoti Komisijos atsaką į krizę. Krizių koordinavimo komitetas, kuriam pirmininkauja Tarybos Generalinio sekretoriaus pavaduotojas, įvertina padėtį, apsvarsto galimybes ir priima sprendimus Komisijos atsakomybe imtis veiksmų dėl ES priemonių bei užtikrina, kad tie sprendimai būtų įgyvendinti ([3]) ([4]).

Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmas. Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmas yra struktūrinė sistema, kuria naudodamasi Europos išorės veiksmų tarnyba reaguoja į krizes ir ekstremaliąsias situacijas, kurios yra išorės pobūdžio arba kurioms būdingas svarbus išorės aspektas – taip pat ir hibridinę grėsmę – ir kurios gali paveikti arba paveikia ES arba valstybių narių interesus. Užtikrindamas atitinkamų Komisijos ir Tarybos sekretoriato pareigūnų dalyvavimą posėdžiuose, reagavimo į krizes mechanizmas sudaro diplomatinių, saugumo ir gynybos pastangų sinergijos su finansų, prekybos ir bendradarbiavimo priemonėmis, kurias valdo Komisija, sąlygas. Krizės laikotarpiui gali būti suburta krizės grupė.

Bendradarbiavimo mechanizmai

CSIRT tinklas. Reagavimo į kompiuterių saugumo incidentus tarnybų tinkle sutelktos visos nacionalinės ir Vyriausybinės CSIRT ir CERT-ES. Šio tinklo tikslas – užtikrinti galimybę CSIRT geriau dalytis informacija apie grėsmę ir kibernetinio saugumo incidentus tarpusavyje ir bendradarbiauti reaguojant į kibernetinio saugumo incidentus ir krizes.

Tarybos Kibernetinių klausimų horizontalioji darbo grupė. Darbo grupė suburta Taryboje, siekiant užtikrinti strateginį ir horizontalųjį koordinavimą kibernetinės politikos klausimais, ir gali dalyvauti teisėkūros ir su teisėkūra nesusijusioje veikloje.

Dalyviai

ENISA. Europos Sąjungos tinklų ir informacijos apsaugos agentūra įsteigta 2004 m. Agentūra glaudžiai bendradarbiauja su valstybėmis narėmis ir privačiuoju sektoriumi, kad pateiktų rekomendacijas ir sprendimus klausimais, susijusiais su europinėmis kibernetinio saugumo pratybomis, nacionalinių kibernetinio saugumo strategijų rengimu, CSIRT bendradarbiavimu ir pajėgumo stiprinimu. Europos Sąjungos tinklų ir informacijos apsaugos agentūra tiesiogiai bendradarbiauja su CSIRT visoje ES ir vykdo CSIRT tinklo sekretoriato funkciją.

ERCC. Komisijos Reagavimo į nelaimes koordinavimo centras (pavaldus Europos civilinės saugos ir humanitarinės pagalbos operacijų generaliniam direktoratui) remia ir koordinuoja įvairią prevencijos, pasirengimo ir reagavimo veiklą visą parą septynias dienas per savaitę. Iškilmingai atidarytas 2013 m., jis veikia kaip Komisijos reagavimo į krizes centras (užtikrina ryšius su kitais ES krizių kabinetais) ir visą parą septynias dienas per savaitę veikia kaip centrinis IPCR kontaktinis punktas.

([1]) 2013 m. birželio 24 d. Tarybos patvirtintas dokumentas 10708/13 „Krizių koordinavimo mechanizmo peržiūros proceso užbaigimas. ES integruoto politinio atsako į krizes mechanizmas“.

([2]) Dokumentas 12607/15 „IPCR standartinės veiklos procedūros“, dėl kurio sutarta „Pirmininkaujančios valstybės narės draugų“ grupėje ir su kuriuo Nuolatinių atstovų komitetas susipažino 2015 m. spalio mėn.

([3]) Komisijos nuostatos dėl ARGUS bendros skubaus įspėjimo sistemos, KOM(2005) 662 galutinis, 2005 m. gruodžio 23 d.

([4]) 2005 m. gruodžio 23 d. Komisijos sprendimas 2006/25/EB, Euratomas, pakeičiantis jos vidaus darbo tvarkos taisykles (OL L 19, 2006 1 24, p. 20), dėl ARGUS bendros skubaus įspėjimo sistemos.

Europolo EC3. Europos kovos su elektroniniu nusikalstamumu centras (EC3) įkurtas 2013 m. Europole ir remia teisėsaugos atsaką į kibernetinius nusikaltimus Europos Sąjungoje. EC3 teikia operatyvinę ir analitinę paramą valstybių narių tyrimams ir yra keitimosi informacija apie nusikaltimus ir žvalgybine informacija centras, remiantis valstybių narių veiklą ir tyrimus operatyvine analize, koordinavimu ir dalijimusi patirtimi, taip pat teikia labai specializuotos techninės ir skaitmeninės ekspertizės paramą.

CERT-ES. Europos institucijų, įstaigų ir agentūrų Kompiuterinių incidentų tyrimo tarnyba įgaliota gerinti ES institucijų, įstaigų ir agentūrų apsaugą nuo kibernetinės grėsmės. Ji yra CSIRT tinklo narė. CERT-ES yra sudariusi techninius susitarimus su NATO CIRC, tam tikromis trečiosiomis šalimis ir dideliais komerciniais kibernetinio saugumo srities subjektais dėl dalijimosi informacija apie kibernetinę grėsmę.

ES žvalgybos bendruomenę sudaro ES žvalgybos analizės centras (**INTCEN**) ir ES karinio štabo žvalgybos skyrius (EUMS INT) pagal susitarimą dėl **Bendro žvalgybinės informacijos analizės centro** (SIAC). SIAC misija – teikti žvalgybos analizės, ankstyvojo įspėjimo ir informuotumo apie padėtį paslaugas Sąjungos vyriausiajam įgaliotiniui užsienio reikalams ir saugumo politikai ir Europos išorės veiksmų tarnybai. SIAC teikia paslaugas įvairioms ES įstaigoms, priimančioms sprendimus bendros užsienio ir saugumo politikos (BUSP), bendros saugumo ir gynybos politikos (BSGP) ir kovos su terorizmu srityse, taip pat valstybėms narėms. ES INTCEN ir EUMS INT nėra operatyvinės agentūros ir neturi jokių informacijos rinkimo galimybių. Už žvalgybos operatyvinį lygmenį atsakingos valstybės narės. SIAC užsiima tik strategine analize.

ES hibridinių grėsmių analizės ir informavimo centras. 2016 m. balandžio mėn. bendrame komunikate dėl kovos su mišriomis grėsmėmis ES hibridinių grėsmių analizės ir informavimo centras įvardytas kaip pagrindinė mišraus pobūdžio grėsmių analizės vieta ES; per tarnybų tarpusavio konsultacijas 2016 m. gruodžio mėn. jo įgaliojimus patvirtino Komisija. ES žvalgybos analizės centre įsikūręs ES hibridinių grėsmių analizės ir informavimo centras yra SIAC dalis, taigi dirba kartu su EUMS INT ir jame yra nuolatinis karinis atstovas. Hibridinis reiškia valstybės ar nevalstybinių subjektų tyčinį įvairių slaptų / atvirų, karinių / civilinių priemonių ir svertų, pvz., kibernetinių išpuolių, dezinformacijos kampanijų, šnipinėjimo, ekonominio spaudimo, tarpininkų naudojimo ar kitos ardomosios veiklos, derinio naudojimą. ES hibridinių grėsmių analizės ir informavimo centras turi platų kontaktinių punktų Komisijoje ir valstybėse narėse tinklą, kad galėtų užtikrinti integruotą reagavimą / visos Vyriausybės požiūrį įvairiems iššūkiams atremti.

ES situacijų kabinetas. ES situacijų kabinetas yra ES žvalgybos analizės centro (ES INTCEN) dalis ir teikia Europos išorės veiksmų tarnybai operacijų vykdymo pajėgumą, kad būtų galima užtikrinti greitą ir veiksmingą reagavimą į krizes. Tai nuolatinė civilinė ir karinė budinčioji tarnyba, užtikrinanti stebėjimą ir informuotumą apie padėtį visame pasaulyje visą parą septynias dienas per savaitę.

Atitinkamos priemonės

Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema. Sistema, dėl kurios susitarta 2017 m. birželio mėn., yra ES kibernetinio saugumo diplomatijos metodo, padedančio išvengti konfliktų, mažinti kibernetinio saugumo grėsmę ir didinti tarptautinių santykių stabilumą, dalis. Sistemoje panaudojamos visos bendros užsienio ir saugumo politikos priemonės, įskaitant, jei reikia, ribojamąsias priemones. Šių priemonių panaudojimas sistemoje turėtų skatinti bendradarbiavimą, sudaryti sąlygas sumažinti tiesioginę bei ilgalaikę grėsmę ir paveikti atsakingo kaltininko ir potencialių agresorių elgesį ilguoju laikotarpiu.

2. KIBERNETINIO SAUGUMO KRIZIŲ KOORDINAVIMAS TAIKANT IPCR MECHANIZMĄ. HORIZONTALIOJO KOORDINAVIMO LYGMUO IR POLITINIS ESKALAVIMAS

IPCR mechanizmas gali būti (ir buvo) naudojamas siekiant spręsti techninius ir operatyvinius klausimus, tačiau visada politiniu ir (arba) strateginiu aspektu.

Eskalavimo atžvilgiu IPCR gali būti naudojamas, priklausomai nuo krizės lygio, pereiti iš stebėjimo režimo į dalijimosi informacija režimą (pirmasis IPCR aktyvinimo lygis) ir į visišką IPCR aktyvinimą.

Dėl visiško aktyvinimo režimo sprendžia ES Tarybai rotacijos tvarka pirmininkaujanti valstybė narė. Komisija, Europos išorės veiksmų tarnyba ir Tarybos Generalinis sekretoriatas gali aktyvinti IPCR dalijimosi informacija režimą. Vykdant

stebėjimą ir dalijantis informacija aktyvinami informacijos mainai įvairiais lygmenimis, o suaktyvinus dalijimosi informacija režimą atsiranda būtinybė rengti ISAA ataskaitas. Visiškas aktyvinimas priemonių rinkinį papildo IPCR apskritojo stalo susitikimais, kuriuose dalyvauja pirmininkaujanti valstybė narė (paprastai Nuolatinių atstovų komiteto (COREPER II) pirmininkas arba nuolatinės atstovybės patarėjo lygmens dalyko ekspertas, tačiau išimties tvarka buvo surengta ministrų lygmens apskritojo stalo susitikimų).

Dalyviai

Vadovauja Tarybai rotacijos tvarka pirmininkaujanti valstybė narė (paprastai Nuolatinių atstovų komiteto pirmininkas),

Europos Vadovų Tarybai atstovauja Pirmininko kabinetas,

Europos Komisijai atstovaujama Generalinio sekretoriaus pavaduotojo / GD ir (arba) dalyko ekspertų lygmeniu,

Europos išorės veiksmų tarnybai atstovaujama Generalinio sekretoriaus pavaduotojo / GD ir (arba) dalyko ekspertų lygmeniu,

Tarybos Generaliniam sekretoriatui atstovauja Generalinio sekretoriaus kabinetas, IPCR grupė ir atsakingi GD.

Veiklos apimtis: susidaryti bendrą padėties vaizdą ir didinti informuotumą apie silpnąsias vietas ir trūkumus kiekviename iš trijų lygmenų, siekiant spręsti šiuos klausimus politiniu lygmeniu ir, jei jie priklauso dalyvių kompetencijai, iš karto priimti sprendimus arba parengti veiksmų pasiūlymus Nuolatinių atstovų komitetui (COREPER II) ar Tarybai.

Bendras informuotumas apie padėtį

(Neaktyvintas): gali būti generuojami IPCR stebėjimo tinklalapiai, siekiant sekti kintančią padėtį, kuri gali peraugti į ES lygmens krizę;

(IPCR dalijimasis informacija): ISAA vadovas rengia ISAA ataskaitas remdamasis Komisijos tarnybų, Europos išorės veiksmų tarnybos ir valstybių narių (per IPCR klausimynus) teikiama informacija;

(IPCR visiškas aktyvinimas): be ISAA ataskaitų, neoficialiose IPCR apskritojo stalo diskusijose dalyvauja įvairūs valstybių narių, Komisijos, Europos išorės veiksmų tarnybos, atitinkamų agentūrų ir t. t. atstovai, kad aptartų trūkumus ir silpnąsias vietas.

Bendradarbiavimas ir reagavimas

Priklausomai nuo incidento pobūdžio ir poveikio, aktyvinami / sinchronizuojami papildomi krizių valdymo mechanizmai / priemonės. Tai gali būti, pvz., Civilinės saugos mechanizmas, Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema arba Bendra kovos su mišriomis grėsmėmis sistema.

Ryšiai krizės sąlygomis

Pirmininkaujanti valstybė narė, pasikonsultavusi su atitinkamomis Komisijos tarnybomis, Tarybos Generaliniu sekretoriatu ir Europos išorės veiksmų tarnyba, gali aktyvinti IPCR krizės informuotojų tinklą, kad padėtų formuluoti bendrus pranešimus arba nuodugniai parengti veiksmingiausias ryšio priemones.

3. KIBERNETINIO SAUGUMO KRIZIŲ VALDYMAS SISTEMOJE ARGUS. DALIJIMASIS INFORMACIJA EUROPOS KOMISIJOJE

Susidūrusi su netikėtomis krizėmis, į kurias būtina reaguoti Europos lygmeniu, t. y. Madrido teroristų atakomis (2004 m. kovo mėn.), cunamiu Pietryčių Azijoje (2004 m. gruodžio mėn.) ir Londono teroristų atakomis (2005 m. liepos mėn.), Komisija 2005 m. sukūrė koordinavimo sistemą ARGUS, remiamą to paties pavadinimo bendra skubaus įspėjimo sistema ([1]) ([2]). Ja siekiama nustatyti konkretų **krizių koordinavimo procesą** įvykus didelei daugiasektorinei krizei, kad būtų galima dalytis su krize susijusia informacija tikruoju laiku ir užtikrinti greitą sprendimų priėmimą.

Sistemoje ARGUS pagal įvykio sunkumą nustatyti du etapai:

I etape dalijamasi informacija apie riboto masto krizę

([1]) Europos Bendrijų Komisija, 2005 m. gruodžio 23 d. Komisijos komunikatas Europos Parlamentui, Tarybai, Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Komisijos nuostatos dėl ARGUS bendros skubaus įspėjimo sistemos“, KOM(2005) 662 galutinis.
([2]) Sprendimas 2006/25/EB, Euratomas.

Pavyzdžiui, pastaruoju metu I etapu pranešta apie miškų gaisrus Portugalijoje ir Izraelyje, 2016 m. Berlyno ataką, potvynius Albanijoje, uraganą „Matthew“ Haityje ir sausrą Bolivijoje. Bet kuris GD gali paskelbti I etapo įvykį, jei mano, kad padėtis yra jo kompetencijos srityje ir pakankamai svarbi, kad būtų galima arba naudinga dalytis informacija. Pavyzdžiui, Ryšių tinklų, turinio ir technologijų generalinis direktoratas arba Migracijos ir vidaus reikalų generalinis direktoratas gali paskelbti I etapo įvykį, jei mano, kad kibernetinė padėtis jo kompetencijos srityje yra pakankamai svarbi, kad būtų naudinga dalytis informacija.

II etapas aktyvinamas, kai įvyksta didelė daugiasektorinė krizė arba kyla numatoma arba tiesioginė grėsmė Sąjungai.

II etape pradedamas specialus koordinavimo procesas, užtikrinantis Komisijai galimybę priimti sprendimus ir valdyti greitą, koordinuotą ir darnų atsaką aukščiausiu lygmeniu savo kompetencijos srityje ir bendradarbiaujant su kitomis institucijomis. II etapas skirtas didelėms daugiasektorinėms krizėms arba numatomai arba tiesioginei jų grėsmei. Pavyzdžiui, pastarojo meto II etapo įvykiai yra migracijos ir pabėgėlių krizė (nuo 2015 m., vis dar vyksta), Fukušimoje įvykusi trejopa nelaimė (2011 m.) ir Ejafjadlajokudlio ugnikalnio išsiveržimas Islandijoje (2010 m.).

II etapą aktyvina Pirmininkas savo iniciatyva arba paprašius Komisijos nariui. Politinę atsakomybę už Komisijos reagavimą Pirmininkas gali paskirti Komisijos nariui, kurio tarnyba yra labiausiai susijusi su įvykusia krize, arba prisiimti ją pats.

Šiame etape numatyti skubūs Krizių koordinavimo komiteto posėdžiai. Jie sušaukiami Pirmininko arba Komisijos nario, kuriam buvo paskirta atsakomybė, pavedimu. Posėdžius sušaukia Generalinis sekretoriatas, naudodamasis ARGUS IT priemone. Krizių koordinavimo komitetas yra speciali operatyvinio krizių valdymo struktūra, sukurta siekiant užtikrinti vadovavimą Komisijos atsakui į krizę ir jo koordinavimą; komitete dirba atitinkamų Komisijos generalinių direktoratų, kabinetų ir kitų ES tarnybų atstovai. Krizių koordinavimo komitetui pirmininkauja Generalinio sekretoriaus pavaduotojas. **Komitetas įvertina padėtį, apsvarsto galimybes ir priima sprendimus, taip pat užtikrina, kad sprendimai ir veiksmai būtų įgyvendinami**, kartu užtikrindamas, kad būtų reaguojama darniai ir nuosekliai. Krizių koordinavimo komitetui padeda Generalinis sekretoriatas.

4. EUROPOS IŠORĖS VEIKSMŲ TARNYBOS REAGAVIMO Į KRIZES MECHANIZMAS

Europos išorės veiksmų tarnybos reagavimo į krizes mechanizmas aktyvinamas susidarius kritinei padėčiai, susijusiai su ES išorės aspektu. Reagavimo į krizes mechanizmą aktyvina Generalinio sekretoriaus pavaduotojas reagavimo į krizes klausimais, pasikonsultavęs su vyriausiuoju įgaliotiniu ir pirmininko pavaduotoju arba Generaliniu sekretoriumi. Aktyvinti reagavimo į krizes mechanizmą Generalinio sekretoriaus pavaduotojo reagavimo į krizes klausimais taip pat gali paprašyti vyriausiasis įgaliotinis ir pirmininko pavaduotojas, Generalinis sekretorius arba kitas Generalinio sekretoriaus pavaduotojas ar vykdantysis direktorius.

Reagavimo į krizes mechanizmas padeda užtikrinti ES reagavimo į krizes nuoseklumą įgyvendinant saugumo strategiją. Visų pirma reagavimo į krizes mechanizmas sudaro diplomatinių, saugumo ir gynybos pastangų sinergijos su finansų, prekybos ir bendradarbiavimo priemonėmis, kurias valdo Komisija, sąlygas.

Reagavimo į krizes mechanizmas yra susietas su Komisijos bendra skubaus įspėjimo sistema (ARGUS) ir ES integruotu politinio atsako į krizes mechanizmu (IPCR), kad būtų galima panaudoti sinergiją, kai jie aktyvinami tuo pačiu metu. Europos išorės veiksmų tarnybos situacijų kabinetas yra Europos išorės veiksmų tarnybos ryšių su Tarybos ir Komisijos reagavimo į nepaprastąją padėtį sistemomis centras.

Paprastai pirmas su reagavimo į krizes mechanizmo įgyvendinimu susijęs veiksmas yra **posėdžio dėl krizės**, kuriame dalyvauja vyresnieji Europos išorės veiksmų tarnybos, Komisijos ir Tarybos vadovai, tiesiogiai susiję su konkrečia krize, sušaukimas. Posėdyje dėl krizės įvertinamas trumpalaikis krizės poveikis ir gali būti sutarta nedelsiant imtis veiksmų arba suburti krizės grupę arba sušaukti krizės platformą. Šie veiksmai gali būti įgyvendinami bet kuria laiko seka.

Krizės grupė yra nedidelių operacijų kabinetas, kuriame renkasi su reagavimu į krizę susiję Europos išorės veiksmų tarnybos, Komisijos ir Tarybos tarnybų atstovai, kad nuolat stebėtų padėtį ir teiktų paramą Europos išorės veiksmų tarnybos štabo sprendimų priėmėjams. Aktyvinta krizės grupė veikia visą parą septynias dienas per savaitę.

Krizės platformoje renkasi atitinkamos Europos išorės veiksmų tarnybos, Komisijos ir Tarybos tarnybos, kad pateiktų krizių poveikio vidutiniu ir ilguoju laikotarpiu vertinimą ir sutartų, kokių veiksmų imtis. Jai pirmininkauja vyriausiasis įgaliotinis ir pirmininko pavaduotojas arba Generalinis sekretorius arba Generalinio sekretoriaus pavaduotojas reagavimo į krizes klausimais. Krizės platformoje įvertinamas ES veiksmų efektyvumas krizės šalyje arba regione, sprendžiama dėl papildomų priemonių pakeitimų ir aptariami Tarybos veiksmų pasiūlymai. Krizės platforma yra *ad hoc* susitikimas; todėl ji nėra nuolat aktyvi.

Darbo grupė sudaroma iš tarnybų, susijusių su reagavimu į krizę, atstovų ir gali būti suburta siekiant sudaryti sąlygas įgyvendinti ES atsaką ir imtis tolesnių veiksmų. Ji vertina ES veiksmų poveikį, parengia politikos ir galimybių dokumentus, padeda rengti politinę reagavimo į krizę programą, pranešimų strategiją ir nustato kitą tvarką, kuria gali būti sudaromos sąlygos įgyvendinti ES atsaką.

5. INFORMACINIAI DOKUMENTAI

Toliau pateikiamas sąrašas informacinių dokumentų, į kuriuos atsižvelgta rengiant planą.

— *The European Cyber Crises Cooperation Framework*, 1 leidimas, 2012 m. spalio 17 d.

— *Report on Cyber Crisis Cooperation and Management*, Europos Sąjungos tinklų ir informacijos apsaugos agentūra, 2014 m.

— *Actionable Information for Security Incident Response*, Europos Sąjungos tinklų ir informacijos apsaugos agentūra, 2014 m.

— *Common practices of ES-level crisis management and applicability to cyber crises*, Europos Sąjungos tinklų ir informacijos apsaugos agentūra, 2015 m.

— *Strategies for Incident Response and Cyber Crisis Cooperation*, Europos Sąjungos tinklų ir informacijos apsaugos agentūra, 2016 m.

— *ES Cyber Standard Operating Procedures*, Europos Sąjungos tinklų ir informacijos apsaugos agentūra, 2016 m.

— *A good practice guide of using taxonomies in incident prevention and detection*, Europos Sąjungos tinklų ir informacijos apsaugos agentūra, 2017 m.

— Komunikatas „Europos kibernetinio atsparumo sistemos stiprinimas ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimas“, COM(2016) 410 *final*, 2016 m. liepos 5 d.

— Tarybos išvados dėl Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo. Tarybos išvados (2016 m. lapkričio 15 d.), 14540/16.

— 2014 m. birželio 24 d. Tarybos sprendimas 2014/415/ES dėl tvarkos, kuria Sąjunga įgyvendina solidarumo sąlygą (OL L 192, 2014 7 1, p. 53).

— Krizių koordinavimo mechanizmo peržiūros proceso užbaigimas. ES integruoto politinio atsako į krizes mechanizmas, 10708/13, 2013 m. birželio 7 d.

— *Integrated Situational Awareness and Analysis (ISAA) – Standard Operating Procedures*, DS 1570/15, 2015 m. spalio 22 d.

— Komisijos nuostatos dėl ARGUS bendros skubaus įspėjimo sistemos, KOM(2005) 662 galutinis, 2005 m. gruodžio 23 d.

— 2005 m. gruodžio 23 d. Komisijos sprendimas 2006/25/EB, Euratomas pakeičiantis jos vidaus darbo tvarkos taisykles (OL L 19, 2006 1 24, p. 20).

— *ARGUS Modus Operandi*, Europos Komisija, 2013 m. spalio 23 d.

— Tarybos išvados dėl bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos („Kibernetinio saugumo diplomatijos priemonių rinkinio“), dokumentas 9916/17.

— ES operatyvinių veiksmų protokolas dėl kovos su hibridinėmis grėsmėmis (ES scenarijus), SWD(2016) 227.

— *EEAS Crisis Response Mechanism*, 2016 m. lapkričio 8 d. Ares(2017)880661. Bendras tarnybų darbinis dokumentas „ES operatyvinių veiksmų protokolas dėl kovos su hibridinėmis grėsmėmis (ES scenarijus)“, SWD(2016) 227 *final*, 2016 m. liepos 5 d.

— Bendras komunikatas Europos Parlamentui ir Tarybai „Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas“ JOIN/2016/018 *final*, 2016 m. balandžio 6 d.

— EEAS(2016) 1674. *Working Document of the European External Action Service – ES Hybrid Fusion Cell – Terms of Reference*

6. SU KIBERNETINIU SAUGUMU SUSIJĘ IPCR PROCESO ELEMENTAI