EUROPOS KOMISIJA

Briuselis, 2011.3.31
KOM(2011) 163 galutinis

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

dėl ypatingos svarbos informacinės infrastruktūros apsaugos

„Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

dėl ypatingos svarbos informacinės infrastruktūros apsaugos

„Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“

1. ĮŽANGA

2009 m. kovo 30 d. Komisija priėmė Komunikatą dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Europos apsauga nuo didelio masto kibernetinių antpuolių ir veiklos sutrukdymo – geresnė parengtis, didesnis saugumas ir atsparumas“[1], kuriame nustatytas esminės informacinių ir ryšių technologijų (IRT) infrastruktūros saugumo ir atsparumo didinimo planas (Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planas). Taip siekta skatinti ir nacionaliniu, ir Europos lygmeniu vystyti aukšto lygio parengties, saugumo ir atsparumo pajėgumus ir remti šių pajėgumų vystymą. 2009 m. Taryba šiam požiūriui iš esmės pritarė[2].

Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planas grindžiamas penkiais ramsčiais: parengtis ir prevencija, atpažinimas ir reagavimas, padarinių mažinimas ir veiklos atkūrimas, tarptautinis bendradarbiavimas, taip pat IRT srities Europos ypatingos svarbos infrastruktūros kriterijai. Jame nustatyta, kokius su kiekvienu ramsčiu susijusius darbus turi atlikti Komisija, valstybės narės ir (arba) sektoriaus atstovai, padedami Europos tinklų ir informacijos apsaugos agentūros (angl. ENISA).

2010 m. gegužės mėn. priimtoje Europos skaitmeninėje darbotvarkėje[3] ir susijusiose Tarybos išvadose[4] pabrėžiama bendra nuomonė, kad pasitikėjimas ir saugumas yra esminės plataus IRT diegimo, taigi ir su pažangaus augimo aspektu susijusių strategijos „Europa 2020“[5] tikslų įgyvendinimo sąlygos. Europos skaitmeninėje darbotvarkėje pabrėžiama, jog visos suinteresuotosios šalys turi kartu dėti bendras pastangas, kad būtų užtikrintas IRT infrastruktūros saugumas ir atsparumas, daugiausia dėmesio skiriant prevencijai, parengčiai ir informuotumui, ir kad būtų sukurti veiksmingi ir suderinti reagavimo į naujas ir vis sudėtingesnes kibernetines atakas ir elektroninius nusikaltimus mechanizmai. Tokiu požiūriu užtikrinama, kad sprendžiant šį uždavinį būtų tinkamai atsižvelgiama ir į prevencijos, ir į reagavimo aspektus.

Pastaraisiais mėnesiais imtasi šių Skaitmeninėje darbotvarkėje paskelbtų priemonių: 2010 m. rugsėjo mėn. Komisija priėmė Direktyvos dėl atakų prieš informacines sistemas pasiūlymą[6]. Jo tikslas – griežčiau kovoti su elektroniniais nusikaltimais, o tam siekiama suderinti

---

1 COM(2009) 149.

2 2009 m. gruodžio 18 d. Tarybos rezoliucija dėl bendradarbiavimu paremto Europos požiūrio į tinklų ir informacijos saugumą (2009/C 321/01).

3 COM(2010) 245.

4 2010 m. gegužės 31 d. Tarybos išvados dėl Europos skaitmeninės darbotvarkės (10130/10).

5 COM(2010) 2020 ir 2010 m. kovo 25–26 d. Europos Vadovų Tarybos išvados (EUCO 7/10).

6 COM(2010) 517 galutinis.

valstybių narių baudžiamosios teisės sistemas ir sustiprinti teisminių ir kitų kompetentingų institucijų bendradarbiavimą. Jame taip pat pateikiama nuostatų, skirtų su naujų rūšių kibernetinėmis atakomis, visų pirma kenkėjišku programiniu kodu apkrėstų kompiuterių tinklais (angl. *botnets*), susijusiems uždaviniams spręsti. Papildydama šį pasiūlymą, Komisija tuo pat metu pateikė pasiūlymą[7] dėl naujo įgaliojimo, kad, siekiant padidinti pasitikėjimą ir tinklų saugumą, būtų sustiprinta ir modernizuota Europos tinklų ir informacijos apsaugos agentūra (ENISA). Sustiprinus ir modernizavus ENISA, ES, valstybės narės ir privačios suinteresuotosios šalys galės didinti savo pajėgumus ir parengtį užkirsti kelią kibernetinio saugumo problemoms, jas nustatyti ir spręsti.

Galiausiai Europos skaitmeninėje darbotvarkėje, Stokholmo programoje ir veiksmų plane[8], taip pat dokumente „ES vidaus saugumo strategijos įgyvendinimas“[9] pabrėžiamas Komisijos įsipareigojimas sukurti skaitmeninę aplinką, kurioje kiekvienas (-a) europietis (-ė) galėtų išreikšti visą savo ekonominį ir socialinį potencialą.

Rengiant šį komunikatą remtasi nuo 2009 m., kai buvo priimtas Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planas, pasiektais rezultatais. Jame aprašomos su kiekvienu veiksmu susijusios tolesnės planuojamos ir Europos, ir tarptautinio lygmens priemonės. Siekiant atsižvelgti į visuotines sąsajas, jame taip pat pabrėžiamas visuotinis uždavinių pobūdis, taip pat tai, kad svarbu stiprinti valstybių narių ir privačiojo sektoriaus atstovų nacionalinio, Europos ir tarptautinio lygmens bendradarbiavimą.

2. ĮVYKIŲ RAIDA

Prie Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų plano pridėtame poveikio vertinime[10] ir įvairiuose privačiojo ir viešojo sektorių suinteresuotųjų šalių atliktuose tyrimuose ir parengtose ataskaitose pabrėžiama ne tik tai, kad Europa yra socialiniu, politiniu ir ekonominiu atžvilgiu priklausoma nuo IRT, bet ir tai, kad savaiminių ar žmonių sukeliamų pavojų nuolat daugėja, jų mastas didėja, jie tampa vis sudėtingesni ir gali turėti vis stipresnį poveikį.

Atsirado naujų ir technologiškai sudėtingesnių pavojų. Jų pasaulinis geopolitinis mastas tampa vis aiškesnis. Pastebima, kad IRT linkstama naudoti politiniam, ekonominiam ir kariniam dominavimui įtvirtinti, be kita ko, naudojantis ir puolimo galimybėmis. Šiame kontekste kartais minimas ir kibernetinis karas ar kibernetinis terorizmas.

Be to, kaip neseniai parodė įvykiai Vidužemio jūros regiono pietinėje dalyje, tam tikruose režimuose yra pasirengta ir įmanoma dėl politinių priežasčių savo nuožiūra neleisti arba kliudyti savo piliečiams naudotis IT ryšių priemonėmis, visų pirma internetu ir judriojo ryšio priemonėmis. Tokia vienašališka intervencija šalyje gali turėti reikšmingų padarinių kituose pasaulio kraštuose[11].

Kad šiuos įvairius pavojus būtų galima nuodugniau suprasti, gali būti naudinga juos suskirstyti į tokias kategorijas:

---

7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.
11 Bendras komunikatas dėl ES ir pietinių Vidužemio jūros regiono šalių partnerystės siekiant demokratijos ir bendros gerovės, COM(2011) 200, 2011 3 8.

– susiję su **išnaudojimo** tikslais, pavyzdžiui, ekonominio ir politinio šnipinėjimo tikslais sukeliama sudėtingo lygmens nuolatinė grėsmė (angl. *advanced persistent threat*)[12] (pvz., „GhostNet“[13]), tapatybės vagystės, neseniai surengtos atakos prieš Apyvartinių taršos leidimų prekybos sistemą[14] arba prieš vyriausybės IT sistemas[15];

– susiję su **trukdymo** tikslais, pavyzdžiui, paskirstytosios atakos, kuriomis siekiama nutraukti paslaugų teikimą (angl. *Distributed Denial of Service attacks*) arba brukalo siuntimas naudojantis kenkėjišku programiniu kodu apkrėstų kompiuterių tinklais (pvz., tinklu „Conficker“, kurį sudaro 7 mln. įrenginių, ar iš Ispanijos valdomu tinklu „Mariposa“, kurį sudaro 12,7 mln. įrenginių[16]), „Stuxnet“[17] ir ryšių nutraukimo priemonės;

– susiję su **naikinimo** tikslais. Kol kas taip dar nebuvo įvykę, tačiau, atsižvelgiant į tai, kad ypatingos svarbos infrastruktūroje IRT naudojamos vis intensyviau (pvz., pažangieji elektros energijos tinklai ir vandens sistemos), tokios galimybės atmesti negalima[18].

3. EUROPOS SĄJUNGA PASAULIO KONTEKSTE

Tokių uždavinių kils ne tik Europos Sąjungai, ir Europos Sąjunga viena jų išspręsti negalės. IRT ir internetui įsiskverbus į įvairias sritis, suinteresuotosios šalys gali palaikyti ryšius, koordinuoti veiklą ir bendradarbiauti našiau, veiksmingiau ir ekonomiškiau, ir taip sukuriama visas gyvenimo sritis apimanti dinamiška inovacijų ekosistema. Tačiau dabar pavojų gali kilti bet kuriame pasaulio krašte ir dėl visuotinių sąsajų jie gali turėti poveikio bet kurioje pasaulio dalyje.

Tokiems kilsiantiems uždaviniams išspęsti vien europinio požiūrio nepakanka. Tikslas Europos Sąjungoje suformuoti nuoseklų ir bendradarbiavimu grindžiamą požiūrį tebėra labai svarbus, tačiau jį reikia įtraukti į pasaulinę veiklos koordinavimo strategiją, kurią įgyvendinant dalyvautų pagrindiniai partneriai – atskiros valstybės ar susijusios tarptautinės organizacijos.

Turime ne tik siekti, kad su plačiu ir intensyviu IRT naudojimu visuose visuomenės segmentuose susiję pavojai būtų suprantami pasauliniu mastu, bet ir parengti strategijas, kaip tokius pavojus tinkamai ir veiksmingai valdyti – užkirsti jiems kelią, juos šalinti, mažinti ir į juos reaguoti. Europos skaitmeninėje darbotvarkėje raginama „kad būtų galima veiksmingai kovoti su saugumo pavojais ir juos mažinti, […] užtikrinti suinteresuotųjų šalių

---

12 Tai yra nuolatinės ir koordinuojamos atakos prieš valstybės agentūras ir viešąjį sektorių. Dabar ši problema kyla ir privačiajame sektoriuje (žr. RSA 2011 m. elektroninių nusikaltimų tendencijų ataskaitą).

13 Žr. projekto „Information Warfare Monitor“ ataskaitas „*GhostNet* sekimas. Kibernetinio šnipinėjimo tinklo tyrimai“ (angl. "Tracking GhostNet: investigating a Cyber Espionage Network") (2009 m.) ir „Šešėliai debesyje. Kibernetinio šnipinėjimo 2.0 tyrimai“ (angl. "Shadows in the Cloud: Investigating Cyber Espionage 2.0") (2010 m.).

14 Žr. klausimus ir atsakymus http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 Pvz., neseniai surengtos atakos prieš Prancūzijos Vyriausybę.

16 Žr. OECD (IFP) projektą dėl būsimų pasaulinių sukrėtimų (angl. "Future Global Shocks") „Sisteminių kibernetinio saugumo pavojų mažinimas“ (angl. "Reducing systemic cyber-security risks"), 2011 m. sausio 14 d., http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Žr. http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis.

18 Žr. Pasaulio ekonomikos forumo 2011 m. Pasaulinių pavojų (angl. „Global Risks“) ataskaitą.

bendradarbiavimą pasaulio mastu“ ir nustatomas tikslas „bendradarbiauti su suinteresuotosiomis šalimis visame pasaulyje, siekiant stiprinti **rizikos valdymą pasaulio mastu** skaitmeninėje ir fizinėje erdvėse, taip pat imtis tarptautiniu mastu koordinuojamų veiksmų prieš kompiuterinius nusikaltimus ir kibernetines atakas“.

4. YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS APSAUGOS VEIKSMŲ PLANO ĮGYVENDINIMAS. TAM TIKRI ESMINIAI ASPEKTAI

Įgyvendinant Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planą pasiektų laimėjimų ir tolesnių veiksmų išsami ataskaita pateikta priede. Toliau nurodyti keli esminiai esamos padėties aspektai.

4.1. Parengtis ir prevencija

- **Valstybių narių Europos forumas** (angl. EFMS) padarė reikšmingą pažangą skatindamas atitinkamų institucijų diskusijas ir keitimąsi geraja politikos patirtimi, susijusia su IRT infrastruktūros saugumu ir atsparumu. Valstybės narės pripažįsta, kad EFMS yra svarbi diskusijų ir keitimosi geraja politikos patirtimi platforma[19]. ENISA ir toliau rems būsimą šio forumo veiklą, o ją vykdant daugiausia dėmesio bus skiriama nacionalinių (valstybinių) kompiuterinių incidentų tyrimo tarnybų (angl. CERT) bendradarbiavimui, nustatant ekonomines ir reguliavimo paskatas didinti saugumą ir atsparumą (laikantis taikomų konkurencijos ir valstybės pagalbos taisyklių), vertinant, kaip tvirtai Europoje užtikrinamas kibernetinis saugumas, vadovaujant europinėms pratyboms, taip pat svarstant saugumo ir atsparumo klausimų sprendimo tarptautiniu mastu prioritetus.

- **Europos viešojo ir privačiojo sektorių partnerystė atsparumui užtikrinti** (angl. EP3R) pradėta kaip europinė valdymo sistema, siekiant užtikrinti IRT infrastruktūros atsparumą. Jos tikslas – skatinti viešojo ir privačiojo sektorių bendradarbiavimą strateginiais ES saugumo ir atsparumo politikos klausimais. ENISA sudarė palankesnes sąlygas vykdyti EP3R veiklą, o pagal 2010 m. Komisijos pasiūlymą modernizuoti ENISA, pastaroji EP3R užtikrintų ilgalaikį ir tvarų pagrindą. Naudojantis EP3R, taip pat bus galima su saugumu ir atsparumu susijusius viešosios politikos, ekonomikos ir rinkos klausimus spręsti tarptautiniu mastu, ypač siekiant stiprinti IRT infrastruktūros rizikos valdymą pasaulio mastu.

- Parengtas **būtinasis bazinių pajėgumų ir paslaugų rinkinys**[20] ir susijusios **politikos rekomendacijos**[21], kad nacionalinės (valstybinės) CERT veiktų efektyviai ir būtų pagrindinė nacionalinių parengties, informacijos mainų, koordinavimo ir reagavimo pajėgumų sudedamoji dalis. Be kita ko, remiantis šiais rezultatais, taip pat naudojantis ENISA teikiama parama, iki 2012 m. visose valstybėse narėse bus sukurtas veiksmingų nacionalinių (valstybinių) CERT tinklas. Šiuo tinklu bus grindžiama piliečiams ir MVĮ

---

19 Jungtinės Karalystės Vyriausybės atsakyme į Lordų Rūmų Europos Sąjungos komiteto pateiktą penktąją Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų plano ataskaitą teigiama, kad EFMS „veikla buvo sėkminga ir padėjo patenkinti tikrą politikos kūrėjų poreikį turėti galimybę keistis patirtimi“.

20 Žr. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Žr. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

skirta Europos informacijos mainų ir įspėjimo sistema (angl. EISAS), kuri, naudojantis nacionaliniais ištekliais ir pajėgumais, turi būti sukurta iki 2013 m.

4.2. Atpažinimas ir reagavimas

- ENISA parengė Europos informacijos mainų ir įspėjimo sistemos (**EISAS**) sukūrimo iki 2013 m. aukšto lygmens veiksmų planą[22], grindžiamą *bazinių paslaugų* įgyvendinimu nacionalinių (valstybinių) CERT lygmeniu ir *sąveikos paslaugų* įgyvendinimu, kad nacionalinės informacijos mainų ir įspėjimo sistemos būtų integruotos į EISAS. Tinkama asmens duomenų apsauga bus vienas iš pagrindinių šios veiklos elementų.

4.3. Padarinių mažinimas ir veiklos atkūrimas

- Kol kas tik 12 valstybių narių surengė reagavimo į didelio masto tinklų saugumo incidentus ir veiklos atkūrimo po ekstremalių įvykių pratybas[23]. Siekdama paremti valstybių narių veiklą, kuri turėtų būti vykdoma aktyviau, ENISA parengė **nacionalinių pratybų gerosios patirties gaires**[24] ir nacionalinių strategijų kūrimo **politikos rekomendacijas**[25].

- 2010 m. lapkričio 4 d. vyko pirmosios **europinės su didelio masto tinklų saugumo incidentais susijusios pratybo**s („Cyber Europe 2010“), į kurias įsitraukė visos valstybės narės (iš jų 19 dalyvavo aktyviai), taip pat Šveicarija, Norvegija ir Islandija. Ateityje rengiant europines kibernetines pratybas, neabejotinai būtų naudinga bendra sistema, kuri būtų grindžiama nacionaliniais nenumatytų atvejų planais ir užtikrintų jų sąsajas ir kuria remiantis būtų sukurti baziniai valstybių narių ryšių ir bendradarbiavimo mechanizmai ir tvarka.

4.4. Tarptautinis bendradarbiavimas

- Vykdant EFMS veiklą buvo apsvarstyti ir parengti **europiniai interneto atsparumo ir stabilumo principai ir gairės**[26]. Komisija tuos principus aptars su atitinkamomis suinteresuotosiomis šalimis, visų pirma su privačiojo sektoriaus atstovais (naudodamasi EP3R), dvišališkai su pagrindiniais tarptautiniais partneriais, visų pirma su JAV, taip pat daugiašališkai, ir skatins tuos principus taikyti. Pagal savo kompetenciją ji tai darys tokiuose forumuose, kaip G8, OECD, NATO (ypač remdamasi 2010 m. lapkričio mėn. priimta nauja strategine koncepcija ir Bendro kibernetinės gynybos pavyzdinio centro veikla), ITU (didinant pajėgumus kibernetinio saugumo srityje), ESBO (jos Saugumo bendradarbiavimo forume), ASEAN, „Meridian“[27] ir kt. Siekiama, kad šie principai ir gairės taptų tarptautinio bendro įsipareigojimo užtikrinti ilgalaikį interneto atsparumą ir stabilumą bendra sistema.

---

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Šaltinis – ENISA.

24 Žr. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Žr. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

26 Žr. http://ec.europa.eu/information_society/policy/nis/index_en.htm.

27 Vykdant procesą „Meridian“, siekiama viso pasaulio valstybių vyriausybėms suteikti priemonę, kuria naudodamosi jos galėtų diskutuoti, kaip politiniu lygmeniu bendradarbiauti ypatingos svarbos informacinės infrastruktūros apsaugos srityje. Žr. http://meridianprocess.org/.

4.5. IRT sektoriaus Europos ypatingos svarbos infrastruktūros kriterijai

- Po techninio pobūdžio diskusijų EFMS parengtas **pirmasis specialių IRT sektoriaus kriterijų**, kuriais remiantis būtų nustatoma Europos ypatingos svarbos infrastruktūra, **projektas**, kuriame daugiausia dėmesio skiriama **fiksuotajam ir judriajam ryšiui ir internetui**. Techninio pobūdžio diskusijos vyks ir toliau, ir jose bus pasinaudota dėl kriterijų projekto surengtų nacionalinio ir Europos (naudojantis EP3R) lygmens konsultacijų su privačiojo sektoriaus atstovais rezultatais. Be to, Komisija su valstybėmis narėmis aptars IRT sektoriui būdingus elementus, į kuriuos reikėtų atsižvelgti 2012 m. persvarstant Direktyvą dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo[28].

5. TOLESNI VEIKSMAI

Įgyvendinant Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planą, pasiekta teigiamų rezultatų, ypač susijusių su pripažinimu, kad būtinas bendradarbiavimu grindžiamas požiūris į tinklų ir informacijos saugumą, kurį palaikytų visos suinteresuotosios šalys. Įgyvendinant šį planą iš esmės laikomasi 2009 m. nustatytų etapų ir tvarkaraščio. Tačiau atsipalaiduoti nederėtų, nes siekiant užtikrinti, kad šios pastangos būtų sėkmingos, dar daug reikia nuveikti ir nacionaliniu, ir Europos lygmeniu.

Taip pat itin svarbu šias pastangas įtraukti į pasaulinę veiklos koordinavimo strategiją ir taip su visomis susijusiomis suinteresuotosiomis šalimis užtikrinti tarptautinį tų pastangų mastą, kad būtų įtraukti kiti regionai, valstybės ar organizacijos, kuriuose sprendžiami panašūs klausimai, ir užmegzti partnerystės ryšiai siekiant keistis požiūriais ir susijusios veiklos rezultatais ir išvengti pastangų dubliavimo.

Privalome skatinti pasaulinę rizikos valdymo kultūrą. Visų pirma turėtų būti skatinami suderinti veiksmai siekiant užkirsti kelią visų rūšių – žmonių sukeliamam ar savaiminiam – veiklos sutrukdymui, jį nustatyti, švelninti jo padarinius ir į jį reaguoti, taip pat taikyti baudžiamąją atsakomybę už susijusius elektroninius nusikaltimus. Tuo tikslu, be kita ko, reikia imtis tikslinių veiksmų kovojant su pavojais saugumui ir kompiuteriniais nusikaltimais.

Šiuo tikslu **Komisija**:

- **Skatins taikyti interneto atsparumo ir stabilumo principus** – naudojantis esamais forumais ir procesais, pavyzdžiui, susijusiais su interneto valdymu, kartu su kitomis valstybėmis, tarptautinėmis organizacijomis ir tam tikrais atvejais pasaulinėmis privačiojo sektoriaus organizacijomis reikėtų sukurti tarptautinius interneto atsparumo ir stabilumo principus. Šie principai turėtų padėti visoms suinteresuotosioms šalims tinkamai nukreipti su interneto stabilumu ir atsparumu susijusią jų veiklą. Tuo tikslu būtų galima remtis Europos principais ir gairėmis.

- **Užmegs strateginę tarptautinę partnerystę** – strateginė partnerystė turėtų būti užmezgama remiantis ypatingos svarbos srityse, pavyzdžiui, kibernetinių incidentų valdymo srityje, vykdoma veikla, įskaitant pratybas ir CERT bendradarbiavimą. Ypač svarbu, kad dalyvautų pasauliniu mastu veiklą vykdantys privačiojo sektoriaus atstovai. Siekiant šių tikslų, 2010 m. lapkričio mėn. vykusiame ES ir JAV aukščiausio lygio

[28] Tarybos direktyva 2008/114/EB.

susitikime įsteigta ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupė yra svarbus laimėjimas. Darbo grupė daugiausia dėmesio skirs kibernetinių incidentų valdymui, viešojo ir privačiojo sektorių partnerystei, informuotumo didinimui ir kovai su elektroniniais nusikaltimais. Ji taip pat gali svarstyti galimybes prireikus įtraukti ir kitus regionus ar valstybes, ypač tuos, kuriuose sprendžiami panašūs klausimai, kad būtų galima keistis požiūriais ir susijusios veiklos rezultatais ir išvengti pastangų dubliavimo. Užtikrinti dar didesnę aprėptį ir geresnį koordinavimą turėtų būti siekiama tarptautiniuose forumuose, visų pirma G8. Europos lygmeniu pagrindiniai sėkmės veiksniai būtų geras visų ES institucijų, atitinkamų agentūrų (visų pirma ENISA ir Europolo) ir valstybių narių veiklos koordinavimas.

- **Didins pasitikėjimą nuotoliniu išteklių valdymu** – būtina intensyvinti diskusijas dėl pasaulinį poveikį turinčių kuriamų technologijų, tokių kaip nuotolinio išteklių valdymo kompiuterija (angl. *cloud computing*), geriausio valdymo strategijų. Be kita ko, tokiose diskusijose būtinai turėtų būti aptariama tinkama asmens duomenų apsaugos valdymo sistema. Siekiant pasinaudoti visomis teikiamomis galimybėmis, pasitikėjimas yra būtinas[29].

Už saugumą bendrai atsakingi visi, todėl visos valstybės narės turi užtikrinti, kad jų nacionalinės priemonės ir pastangos kartu padėtų nustatyti suderintą Europos požiūrį siekiant užkirsti kelią visų rūšių kibernetiniam veiklos sutrukdymui ir atakoms, juos nustatyti, švelninti jų padarinius ir į juos reaguoti. Atsižvelgdamos į tai, **valstybės narės turėtų įsipareigoti**:

- **Didinti ES parengtį – tuo tikslu iki 2012 m. sukurti veiksmingų nacionalinių (valstybinių) CERT tinklą.** Iki 2012 m. ES institucijos taip pat įsteigs savo lygmens CERT. Imantis visos šios veiklos reikėtų pasinaudoti ENISA parengtu susijusiu būtinuoju bazinių pajėgumų ir paslaugų rinkiniu ir susijusiomis politikos rekomendacijomis, o ENISA toliau rems šias iniciatyvas. Vykdant šią veiklą taip pat bus paspartintas Europos informacijos mainų ir įspėjimo sistemos (EISAS) kūrimas, kad platesnė visuomenė ja galėtų pradėti naudotis iki 2013 m.

- **Iki 2012 m. parengti su kibernetiniais incidentais susijusį Europos nenumatytų atvejų planą ir reguliariai rengti europines kibernetines pratybas.** Ir nacionaliniu, ir Europos lygmeniu kibernetinės pratybos yra svarbi nuoseklios su kibernetiniais incidentais susijusių nenumatytų atvejų planų rengimo ir veiklos atkūrimo strategijos dalis. Ateityje europinės kibernetinės pratybos turėtų būti rengiamos remiantis su kibernetiniais incidentais susijusiu Europos nenumatytų atvejų planu, kuris būtų grindžiamas nacionaliniais nenumatytų atvejų planais ir užtikrintų jų sąsajas. Tokiame plane turėtų būti nustatyti baziniai valstybių narių ryšių mechanizmai ir tvarka, taip pat – tai ne mažiau svarbu – jis turėtų padėti apibrėžti būsimų europinių pratybų mastą ir jas rengti. Bendradarbiaudama su valstybėmis narėmis, ENISA tokį su kibernetiniais incidentais susijusį Europos nenumatytų atvejų planą parengs iki 2012 m. Laikydamosi to paties tvarkaraščio, visos valstybės narės turėtų parengti

[29] Pvz., žr. ENISA ataskaitas „Nuotolinio išteklių valdymo kompiuterijos informacijos saugumo užtikrinimo sistema“ ("Cloud Computing Information Assurance Framework") (2009 m.) http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) ir „Vyriausybinių nuotolinių išteklių saugumas ir atsparumas“ ("Security and resilience in governmental clouds") (2011 m.) http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

įprastinius nacionalinius nenumatytų atvejų planus, taip pat rengti reagavimo ir veiklos atkūrimo pratybas.

- **Užtikrinti, kad tarptautiniuose forumuose ir diskusijose dėl interneto saugumo ir atsparumo didinimo Europos pastangos būtų suderintos.** Valstybės narės turėtų bendradarbiauti tarpusavyje ir su Komisija siekdamos skatinti plėtoti principais ar normomis grindžiamą požiūrį į interneto visuotinio stabilumo ir atsparumo klausimą. Turėtų būti siekiama visais lygiais didinti visų suinteresuotųjų šalių prevencijos pajėgumus ir parengtį ir taip pasiekti pusiausvyrą diskusijose, kuriose šiuo metu daugiausia dėmesio linkstama skirti kariniams ir (arba) nacionalinio saugumo aspektams.

6. IŠVADA

Patirtis rodo, kad sprendžiant saugumo ir atsparumo užtikrinimo uždavinius grynai nacionalinių ar regioninių požiūrių nepakanka. Nuo 2009 m. Europos mastu bendradarbiaujama gerokai intensyviau ir pasiekta vilties teikiančių laimėjimų, visų pirma surengtos pratybos „Cyber Europe 2010“. Tačiau Europa ir toliau turėtų stengtis, kad visoje ES būtų suformuotas nuoseklus ir bendradarbiavimu grindžiamas požiūris. Siekiant šio ilgalaikio tikslo, modernizuota ENISA turėtų valstybėms narėms, ES institucijoms ir privačiojo sektoriaus atstovams teikti didesnę paramą.

Kad Europos pastangos būtų sėkmingos, jas būtina pasauliniu lygmeniu integruoti į suderintą požiūrį. Tuo tikslu Komisija skatins visuose atitinkamuose tarptautiniuose forumuose diskutuoti kibernetinio saugumo klausimais.

2011 m. balandžio 14–15 d. vyks ES pirmininkaujančios Vengrijos organizuojama ministrų konferencija dėl ypatingos svarbos informacinės infrastruktūros apsaugos. Tai bus puiki proga tvirčiau įsipareigoti ir Europos, ir tarptautiniu lygmeniu stiprinti valstybių narių bendradarbiavimą ir veiklos koordinavimą.

PRIEDAS

Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planas. Išsami laimėjimų ir tolesnių veiksmų apžvalga

Įgyvendinant Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planą vykdytos veiklos rezultatai iš esmės atitinka 2009 m. Komisijos nustatytus etapus ir tvarkaraštį. Toliau aprašyti su visais ramsčiais susiję laimėjimai ir tolesni veiksmai. Šioje glaustoje apžvalgoje atsižvelgiama į tai, kad tam tikra veikla buvo išsamiau apibūdinta Europos skaitmeninėje darbotvarkėje ir dokumente „Vidaus saugumo strategijos įgyvendinimas“ (toliau – Vidaus saugumo strategija).

1. Parengtis ir prevencija

Bendradarbiauti Europos mastu reikalinga pajėgumų ir paslaugų bazė

Laimėjimai

– 2009 m. ENISA kartu su Europos kompiuterinių incidentų tyrimo tarnybų (CERT) bendruomene parengė ir suderino bazinių pajėgumų ir paslaugų, būtinų nacionalinėms (valstybinėms) CERT, kad jos veiksmingai vykdytų veiklą palaikydamos bendradarbiavimą Europos mastu, rinkinį. Susitarta dėl veiklos, techninių pajėgumų, įgaliojimo ir bendradarbiavimo sričių būtinųjų reikalavimų sąrašo[30].

– 2010 m., bendradarbiaudama su Europos CERT bendruomene, ENISA dėjo pastangas, kad pagal minėtuosius funkcinius reikalavimus būtų parengtos politikos rekomendacijos[31], kad nacionalinės (valstybinės) CERT būtų pagrindinė nacionalinių parengties, informacijos mainų, koordinavimo ir reagavimo pajėgumų sudedamoji dalis.

– Kol kas nacionalines (valstybines) CERT sukūrė 20 valstybių narių[32], o beveik visos kitos ketina tai padaryti. Kaip paskelbta Europos skaitmeninėje darbotvarkėje ir išsamiau nurodyta Vidaus saugumo strategijoje, Komisija pasiūlė priemonių, kad iki 2012 m. būtų įsteigta ES institucijoms skirta CERT.

Tolesni veiksmai

– Siekdama užtikrinti, kad iki 2011 m. pabaigos visose valstybėse narėse būtų įkurtos veiksmingos nacionalinės (valstybinės) CERT, ENISA toliau rems valstybes nares, kurios dar neįsteigė minėtuosius suderintus bazinius reikalavimus atitinkančių nacionalinių (valstybinių) CERT. Įgyvendinus šį etapą bus galima **iki 2012 m.** nacionaliniu lygmeniu sukurti veiksmingą CERT tinklą, kaip numatyta Europos skaitmeninėje darbotvarkėje.

– Bendradarbiaudama su nacionalinėmis (valstybinėmis) CERT, ENISA svarstys būtinybę ir būdus išplėsti bazinius pajėgumus siekiant tinkamai panaudoti CERT galimybes remti valstybes nares užtikrinant ypatingos svarbos IRT infrastruktūros atsparumą ir stabilumą ir

---

30 Žr. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 Žr. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Šaltinis – ENISA.

tapti pagrindu, kuriuo remiantis būtų kuriama piliečiams ir MVĮ skirta Europos informacijos mainų ir įspėjimo sistema (EISAS), kuri, kaip paskelbta Vidaus saugumo strategijoje, naudojantis nacionaliniais ištekliais ir pajėgumais, turi būti sukurta **iki 2013 m.**

Europos viešojo ir privačiojo sektorių partnerystė atsparumui užtikrinti (EP3R)

Laimėjimai

– 2009 m. EP3R pradėta kaip europinė valdymo sistema, kuria siekta užtikrinti IRT infrastruktūros atsparumą ir tuo tikslu skatintas viešojo ir privačiojo sektorių bendradarbiavimas saugumo ir atsparumo tikslų, bazinių reikalavimų, gerosios politikos patirties ir priemonių klausimais. Kaip nurodyta Vidaus saugumo strategijoje, EP3R šalys taip pat „bendraus su tarptautiniais partneriais gerindamos bendrą IT tinklų rizikos valdymą“. ENISA sudarė palankesnes sąlygas vykdyti EP3R veiklą.

– Siekiant apibrėžti EP3R tikslus, principus ir struktūrą, taip pat nustatyti paskatas, kad susijusios suinteresuotosios šalys aktyviai dalyvautų veikloje, konsultuotasi su privačiojo ir viešojo sektorių suinteresuotosiomis šalimis[33]. Pasiūlyme modernizuoti ENISA[34] nustatytos EP3R veiklos pirmenybinės sritys.

– Apibrėžiant EP3R struktūrą, 2010 m. pabaigoje kartu pradėjo veikti trys darbo grupės, kurių veikla susijusi su a) pagrindiniu turtu, ištekliais ir funkcijomis, būtinais siekiant sklandžiai ir saugiai užtikrinti tarpvalstybinius elektroninius ryšius; b) elektroninių ryšių saugumo ir atsparumo baziniais reikalavimais; c) koordinavimo ir bendradarbiavimo reikmėmis ir mechanizmais siekiant pasirengti didelio masto veiklos sutrukdymo atvejams, kurie turėtų įtakos elektroniniams ryšiams, ir reaguoti į tokį veiklos sutrukdymą.

– 2010 m. Komisijos pasiūlymu modernizuoti ENISA sukurtas ilgalaikis ir tvarus EP3R pagrindas – jame pasiūlyta, kad ENISA turėtų „remti viešojo ir privačiojo sektorių suinteresuotųjų šalių bendradarbiavimą Europos Sąjungos lygiu, *inter alia*, skatindama keitimąsi informacija ir geresnį informavimą, kurdama geresnes sąlygas jų pastangoms parengti rizikos valdymo, taip pat elektroninių gaminių, sistemų, tinklų ir paslaugų saugumo standartus ir jų laikytis“.

Tolesni veiksmai

– Remiantis EP3R, 2011 m. bus toliau stiprinamas viešojo ir privačiojo sektorių suinteresuotųjų šalių bendradarbiavimas siekiant naujoviškomis priemonėmis ir įrankiais didinti saugumą ir atsparumą, taip pat nustatyti suinteresuotųjų šalių įpareigojimus. Naudodamosi ENISA sudaromomis palankiomis sąlygomis ir jos teikiama parama, EP3R darbo grupės pateiks pirmuosius veiklos rezultatus. Ateityje vykdant Komisijos ir ENISA atliekamu parengiamuoju darbu grindžiamą veiklą, taip pat bus sprendžiami pažangiųjų elektros energijos tinklų kibernetinio saugumo užtikrinimo uždaviniai.

– Naudojantis EP3R, bus galima su saugumu ir atsparumu susijusius viešosios politikos, ekonomikos ir rinkos klausimus spręsti pasauliniu mastu. Komisija ketina išnaudoti EP3R

[33] Žr. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm.

[34] COM(2010) 521.

teikiamas galimybes, kad paremtų ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupės veiklą, siekdama sukurti nuoseklias viešojo ir privačiojo sektorių bendradarbiavimo sąlygas ir kartu laikydamasi taikomų konkurencijos ir valstybės pagalbos taisyklių.

– Atsižvelgiant į naujo reglamento dėl ENISA pasiūlymą, numatoma, kad EP3R ilgainiui turėtų tapti viena iš pagrindinių modernizuotos ENISA veiklos krypčių.

Valstybių narių Europos forumas (EFMS)

Laimėjimai

– 2009 m. EFMS įsteigtas, kad skatintų atitinkamų valdžios institucijų diskusijas ir keitimąsi gerąja politikos patirtimi siekiant su IRT infrastruktūros saugumu ir atsparumu susijusių bendrų politikos tikslų ir prioritetų, tiesiogiai naudojantis ENISA darbo rezultatais ir jos teikiama parama. EFMS susitikimai vyksta kas ketvirtį, o nuo 2010 m. vidurio jam skirtas ENISA tvarkomas specialus interneto portalas.

– EFMS padarė reikšmingą pažangą šiose srityse: a) kriterijų, pagal kuriuos, atsižvelgiant į Direktyvą dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems[35], būtų nustatoma Europos IRT infrastruktūra, apibrėžimo; b) su interneto atsparumu ir stabilumu susijusių Europos prioritetų, principų ir gairių nustatymo; c) keitimosi gerąja politikos patirtimi, ypač susijusia su kibernetinėmis pratybomis.

– Valstybės narės pripažįsta, kad EFMS yra svarbi diskusijų ir keitimosi gerąja politikos patirtimi platforma[36].

Tolesni veiksmai

– 2011 m. EFMS užbaigs techninio pobūdžio diskusijas dėl Europos ypatingos svarbos infrastruktūros IRT srities kriterijų, taip pat nustatys su tinklų ir informacijos saugumu susijusių europinių didelio masto pratybų ilgalaikes kryptis ir prioritetus.

– EFMS ir toliau dalyvaus diskusijose dėl saugumo ir atsparumo užtikrinimo tarptautiniu mastu prioritetų, ypač susijusių su ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupės veikla.

– EFMS veiklos, kuri bus vykdoma remiantis ir naudojantis tiesiogine ENISA parama, pirmenybinės sritys[37]: veiksmingo nacionalinių (valstybinių) CERT bendradarbiavimo metodų kūrimas; būtinųjų reikalavimų taikymas viešųjų pirkimų srityje, siekiant padidinti kibernetinį saugumą; ekonominių ir reguliavimo paskatų didinti saugumą ir atsparumą (laikantis taikomų konkurencijos ir valstybės pagalbos taisyklių) nustatymas; vertinimas, kaip tvirtai Europoje užtikrinamas kibernetinis saugumas.

---

35 Tarybos direktyva 2008/114/EB.

36 Jungtinės Karalystės Vyriausybės atsakyme į Lordų Rūmų Europos Sąjungos komiteto pateiktą penktąją Ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų plano ataskaitą teigiama, kad EFMS „veikla buvo sėkminga ir padėjo patenkinti tikrą politikos kūrėjų poreikį turėti galimybę keistis patirtimi“.

37 COM(2010) 251.

2. Atpažinimas ir reagavimas

Europos informacijos mainų ir įspėjimo sistema (EISAS)

Laimėjimai

– Šiuo metu rengiami galutiniai Komisijos finansuotų dviejų pavyzdinių projektų (FISHAS ir NEISAS) rezultatai.

– Remdamasi savo 2007 m. galimybių ataskaita[38] ir atitinkamų nacionalinio ir Europos lygmens projektų analize, ENISA parengė EISAS sukūrimo iki 2013 m. aukšto lygmens veiksmų planą[39].

Tolesni veiksmai

– 2011 m. ENISA padės valstybėms narėms įgyvendinti EISAS veiksmų planą plėtodama bazines paslaugas, kurios valstybėms narėms būtinos, kad jos galėtų sukurti savo nacionalinių (valstybinių) CERT pajėgumais grindžiamas nacionalines informacijos mainų ir įspėjimo sistemas (angl. ISAS).

– 2012 m. ENISA plėtos sąveikos paslaugas, kad būtų galima kiekvieną nacionalinę ISAS funkciškai integruoti į EISAS. ENISA taip pat padės valstybėms narėms išbandyti tokias paslaugas palaipsniui integruojant nacionalines sistemas.

– 2011–2012 m. ENISA sudarys sąlygas nacionalinėms (valstybinėms) CERT į jų teikiamas paslaugas įtraukti ISAS pajėgumus.

3. Padarinių mažinimas ir veiklos atkūrimas

Nacionalinių nenumatytų atvejų planų rengimas ir pratybos

Laimėjimai

– 2010 m. pabaigoje 12 valstybių narių buvo parengusios nacionalinį nenumatytų atvejų planą ir (arba) surengusios reagavimo į didelio masto tinklų saugumo incidentus ir veiklos atkūrimo po ekstremalių įvykių pratybas[40].

– Remdamasi nacionaline ir tarptautine patirtimi, ENISA parengė nacionalinių pratybų gerosios patirties gaires[41]; su valstybėmis narėmis ir viso pasaulio CERT organizavo su nacionalinėmis pratybomis susijusius renginius; taip pat neseniai paskelbė nacionalinių strategijų kūrimo politikos rekomendacijas, kuriose nacionalinėms (valstybinėms) CERT ir (arba) reagavimo į kompiuterinius saugumo incidentus tarnyboms (angl. CSIRT) skirtas pagrindinis vaidmuo vadovaujant nacionalinėms nenumatytų atvejų planų rengimo

38 Žr. http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf.

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

40 Žr. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

41 Žr. http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

pratyboms ir bandymams, kuriuose dalyvauja privačiojo ir viešojo sektorių suinteresuotosios šalys[42].

Tolesni veiksmai

– Siekiant, kad veikla būtų koordinuojama visos Europos mastu, ENISA toliau rems valstybių narių pastangas parengti nacionalinius nenumatytų atvejų planus ir reguliariai organizuoti reagavimo į didelio masto tinklų saugumo incidentus ir veiklos atkūrimo po ekstremalių įvykių pratybas.

Su didelio masto tinklų saugumo incidentais susijusios europinės pratybos

Laimėjimai

– 2010 m. lapkričio 4 d. vyko pirmosios europinės su didelio masto tinklų saugumo incidentais susijusios pratybos („Cyber Europe 2010“), į kurias įsitraukė visos valstybės narės (iš jų 19 dalyvavo pačiose pratybose), taip pat Šveicarija, Norvegija ir Islandija. Pratybas surengė ir įvertino[43] ENISA, planavimo grupės veikloje taip pat aktyviai dalyvavo aštuonios valstybės narės, o technologinę paramą teikė Jungtinis tyrimų centras.

Tolesni veiksmai

– 2011 m. valstybės narės bus paskatintos diskutuoti dėl 2012 m. planuojamų kitų europinių kibernetinių pratybų tikslo ir masto. Bus svarstoma galimybė veiklą vykdyti etapais, rengiant nuodugnesnes pratybas, kuriose dalyvautų mažesnė valstybių narių grupė ir galbūt tarptautiniai subjektai. ENISA ir toliau rems šį procesą.

– Komisija skiria finansinę paramą projektui „EuroCybex“, pagal kurį 2011 m. antroje pusėje bus vykdomos modeliavimu grindžiamos pratybos.

– Ir nacionaliniu, ir Europos lygmeniu kibernetinės pratybos yra svarbi nuoseklios su kibernetiniais incidentais susijusių nenumatytų atvejų planų rengimo strategijos dalis. Todėl ateityje europinės kibernetinės pratybos turėtų būti rengiamos remiantis su kibernetiniais incidentais susijusiu Europos nenumatytų atvejų planu, kuris būtų grindžiamas nacionaliniais nenumatytų atvejų planais ir užtikrintų jų sąsajas. Tokiame plane turėtų būti nustatyti baziniai valstybių narių ryšių mechanizmai ir tvarka, taip pat – tai ne mažiau svarbu – jis turėtų padėti apibrėžti būsimų europinių pratybų mastą ir jas rengti. Bendradarbiaudama su valstybėmis narėmis, ENISA tokį su kibernetiniais incidentais susijusį Europos nenumatytų atvejų planą parengs iki 2012 m. Laikydamosi to paties tvarkaraščio, visos valstybės narės parengs įprastinius nacionalinius nenumatytų atvejų planus, taip pat rengs reagavimo ir veiklos atkūrimo pratybas. Šiam rezultatui pasiekti būtiną koordinavimą užtikrins EFMS.

[42] Žr. http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

[43] Žr. http://www.enisa.europa.eu/.

Tvirtesnis nacionalinių (valstybinių) CERT bendradarbiavimas

Laimėjimai

– Nacionalinės (valstybinės) CERT ėmė bendradarbiauti intensyviau. Su nacionalinių (valstybinių) CERT baziniais pajėgumais, CERT pratybomis ir nacionalinėmis pratybomis, taip pat su kibernetinių incidentų valdymu susijusi ENISA veikla padėjo paskatinti ir palaikyti glaudesnį nacionalinių (valstybinių) CERT bendradarbiavimą Europos mastu.

Tolesni veiksmai

– ENISA ir toliau rems nacionalinių (valstybinių) CERT bendradarbiavimą. Tuo tikslu 2011 m. ji atliks reikalavimų tyrimą ir pateiks gaires dėl tinkamo saugaus ryšių su CERT kanalo, įskaitant įgyvendinimo ir būsimos plėtros veiksmų planą. ENISA taip pat išnagrinės Europos lygmens veiklos spragas ir pateiks ataskaitą, kaip galima stiprinti tarpvalstybinį CERT ir atitinkamų suinteresuotųjų šalių bendradarbiavimą, ypač reagavimo į incidentus koordinavimo srityje.

– Europos skaitmeninėje darbotvarkėje valstybės narės raginamos **iki 2012 m.** nacionaliniu lygmeniu sukurti veiksmingą CERT tinklą.

4. Tarptautinis bendradarbiavimas

Interneto atsparumas ir stabilumas

Laimėjimai

– Remiantis EFMS veiklos rezultatais parengti europiniai interneto atsparumo ir stabilumo principai ir gairės[44].

Tolesni veiksmai

– 2011 m. Komisija skatins taikyti ir svarstys tuos principus tiek dvišališkai bendradarbiaudama su tarptautiniais partneriais, visų pirma su JAV, tiek G8, OECD, „Meridian“ ir ITU vykstančiose daugiašalėse diskusijose; Europos lygmeniu (naudodamasi EP3R) ir tarptautiniu mastu (Interneto valdymo forume ir kituose atitinkamuose forumuose) konsultuosis su atitinkamomis suinteresuotosiomis šalimis, visų pirma su privačiojo sektoriaus atstovais; taip pat skatins diskusijas su pagrindiniais interneto subjektais ir (arba) organizacijomis.

– 2012 m. tarptautiniai partneriai bus skatinami siekti, kad tie principai ir gairės taptų tarptautinio bendro įsipareigojimo užtikrinti ilgalaikį interneto atsparumą ir stabilumą bendra sistema.

[44] Žr. http://ec.europa.eu/information_society/policy/nis/index_en.htm.

Veiklos atkūrimo po didelio masto interneto incidentų ir tokių incidentų padarinių švelninimo pasaulinės pratybos

Laimėjimai

– Septynios valstybės narės[45] dalyvavo JAV kibernetinėse pratybose „Cyber Storm III“ kaip tarptautinės partnerės. Komisija ir ENISA dalyvavo stebėtojų teisėmis.

Tolesni veiksmai

– 2011 m., vykdant ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupės veiklą, Komisija kartu su JAV parengs bendrą programą ir veiksmų planą, kad 2012–2013 m. būtų surengtos bendros ir (arba) suderintos tarpžemyninės kibernetinės pratybos. Taip pat bus svarstomos galimybės įtraukti ir kitus regionus ar valstybes, kuriuose sprendžiami panašūs klausimai, kad būtų galima keistis požiūriais ir susijusios veiklos rezultatais.

5. IRT sektoriaus Europos ypatingos svarbos infrastruktūros kriterijai

IRT sektoriuje taikytini Europos ypatingos svarbos infrastruktūros nustatymo kriterijai

Laimėjimai

– Po EFMS vykusių techninio pobūdžio diskusijų dėl specialių IRT sektoriaus kriterijų parengtas fiksuotajam ir judriajam ryšiui ir internetui skirtų kriterijų projektas.

Tolesni veiksmai

– EFMS bus tęsiamos techninio pobūdžio diskusijos dėl specialių IRT sektoriaus kriterijų; jas numatoma baigti 2011 m. pabaigoje. Kartu tam tikrose valstybėse narėse ir Europos lygmeniu naudojantis EP3R planuojama dėl IRT sektoriaus kriterijų projekto konsultuotis su privačiojo sektoriaus atstovais.

– Komisija su valstybėmis narėmis aptars IRT sektoriui būdingus elementus, į kuriuos reikia atsižvelgti 2012 m. persvarstant Direktyvą 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems.

–

[45] Jungtinė Karalystė, Italija, Nyderlandai, Prancūzija, Švedija, Vengrija ir Vokietija.