EUROPOS BENDRIJŲ KOMISIJA

Briuselis, 31.5.2006
COM(2006) 251 galutinis

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

Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“

{SEK(2006) 656}

TURINYS

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

Saugios informacinės visuomenės strategija – „Dialogas, partnerystė ir teisių suteikimas“

1. ĮŽANGA

Komunikate „i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti“[1] pabrėžiama tinklų ir informacijos saugumo svarba kuriant bendrą Europos informacinę erdvę. Tinklų ir informacinių sistemų prieinamumas, patikimumas ir saugumas tampa vis reikšmingesni mūsų ekonomikai ir visuomenei.

Šio komunikato tikslas – atnaujinti 2001 m. Europos komisijos strategiją, pateiktą Komunikate „Tinklų ir informacijos saugumas. Pasiūlymas dėl Europos politikos požiūrio“[2]. Komunikate apžvelgiamos informacinei visuomenei šiuo metu kylančios grėsmės ir nustatomi papildomi veiksmai, kurių būtina imtis siekiant pagerinti tinklų ir informacijos saugumą (TIS).

Remiantis valstybių narių bei Europos bendrijos sukaupta patirtimi, siekiama toliau plėtoti saugumo kultūra ir **dialogo, partnerystės bei teisių suteikimo principais** pagrįstą dinamišką visuotinę Europos strategiją.

Siekdama įveikti su informacinės visuomenės saugumu susijusius sunkumus, Europos bendrija parengė trijų dalių modelį, kuris apima: konkrečias tinklų ir informacijos apsaugos priemones, elektroninių ryšių reguliavimo sistemą (įskaitant privatumo ir duomenų apsaugos klausimus) ir kovą su elektroniniais nusikaltimais. Nors visus šiuos aspektus tam tikru mastu galima plėtoti atskirai, tačiau jie yra labai tarpusavyje susiję, todėl reikalinga bendra strategija. Šiuo komunikatu nustatoma strategija ir pateikiami pagrindiniai principai, kaip paspartinti ir patobulinti vieningą požiūrį į tinklų ir informacijos saugumą.

2001 m. komunikate tinklų ir informacijos saugumas apibrėžiamas kaip „*tinklo ar informacinės sistemos atsparumas tam tikru lygmeniu atsitiktiniams įvykiams ar nusikalstamiems veiksmams, kurie kelia pavojų šiuose tinkluose ir sistemose sukauptų ir jais perduodamų duomenų bei susijusių paslaugų prieinamumui, tikrumui, vientisumui ir konfidencialumui“*. Pastaraisiais metais Europos bendrija jau įgyvendino nemažai veiksmų, padedančių gerinti tinklų ir informacijos saugumą.

Šiuo metu peržiūrimoje elektroninius ryšius reglamentuojančioje teisinėje bazėje yra ir su saugumu susijusių nuostatų. Ypač Direktyvoje dėl privatumo ir elektroninių ryšių[3] viešųjų elektroninių ryšių paslaugų teikėjams numatytas įsipareigojimas užtikrinti savo teikiamų

---

1 COM(2005) 229 galutinis, 2005 6 1
2 COM(2001) 298 galutinis, 2001 6 6
3 Direktyva 2002/58/EB.

paslaugų saugumą. Direktyvoje taip pat yra nuostatų, reglamentuojančių kovą su elektroninio pašto šiukšlėmis (angl. *spam*)[4] ir „šnipukais“ (angl. *spyware*)[5].

Europos bendrijos mokslinių tyrimų ir technologijų plėtros programose didelis dėmesys tenka patikimumui bei saugumui. Jiems užtikrinti Šeštojoje bendrojoje mokslinių tyrimų programoje numatyta daug įvairių projektų. Septintojoje pagrindų programoje numatyta vykdyti dar daugiau su saugumu susijusių mokslinių tyrimų ir šiam tikslui bus sukurta Europos saugumo mokslinių tyrimų programa (ESMTP)[6]. Be to, „Saugesnis internetas plius“ programa remia tinklų kūrimo projektus ir geros patirties mainus, siekiant užkirsti kelią žalingo turinio informacijos plitimui informaciniuose tinkluose.

Reaguodama į grėsmes saugumui, 2004 m. Europos bendrija nusprendė įsteigti Europos tinklų ir informacijos saugumo agentūrą (ETISA). Ši agentūra prisideda prie tinklų ir informacijos saugumo kultūros plėtojimo, siekdama kuo geriau apsaugoti piliečius, vartotojus, įmones ir viešojo sektoriaus organizacijas visoje Europos Sąjungoje (ES).

Europos Sąjunga taip pat aktyviai dalyvauja sprendžiant šiuos klausimus tarptautiniuose forumuose, tokiuose kaip Ekonominio bendradarbiavimo ir plėtros organizacija, Europos Taryba ir Jungtinės Tautos. Tunise vykusio Pasaulio aukščiausio lygio susitikimo informacinės visuomenės klausimais metu, ES aktyviai rėmė diskusijas dėl tinklų ir informacijos prieinamumo, patikimumo ir saugumo. Tuniso darbotvarkėje[7], kurioje, kaip ir Tuniso įsipareigojime, numatomi tolesni politinių diskusijų dėl pasaulio informacinės visuomenės veiksmai, kuriuos remia daugelio pasaulio valstybių vadovai, pabrėžiamas poreikis tęsti kovą su elektroniniais nusikaltimais ir elektroninio pašto šiukšlėmis, kartu užtikrinant privatumo ir išraiškos laisvę. Darbotvarkėje taip pat pabrėžiama, kad būtina vienodai suvokti su interneto saugumu susijusias problemas ir toliau bendradarbiauti, siekiant palengvinti tokios informacijos rinkimą ir sklaidą bei geros patirties, kaip kovoti su grėsmėmis saugumui, mainus tarp visų suinteresuotųjų šalių.

2. INFORMACINĖS VISUOMENĖS APSAUGOS GERINIMAS: PAGRINDINIAI SUNKUMAI

Nepaisant didžiulių pastangų tarptautiniu, Europos ir nacionaliniu lygmeniu, saugumas vis dar kelia didelį susirūpinimą.

Pirmiausia, atakos prieš informacines sistemas vis dažniau būna paremtos pelno siekimu, o ne tik noru įsibrauti. Duomenys vis dažniau renkami neteisėtai, be vartotojo žinios, o vadinamųjų „kenkėjų“[8] atmainų skaičius (kaip ir jų vystymosi tempai) greitai auga. Elektroninio pašto šiukšlės – puikus šios evoliucijos pavyzdys: tai jau tampa virusų, nesąžiningos ir nusikalstamos veiklos, pasireiškiančios kaip „šnipukai“, duomenų vagystės (angl. *phishing*)[9] ir kitomis formomis, priemone. Jų didžiulis paplitimas vis labiau priklauso nuo vadinamųjų

---

4 arba nepageidaujamais reklaminiais elektroniniais laiškais.

5 Šnipukai - šnipinėjimo programinė įranga, įdiegiama be vartotojo įspėjimo, sutikimo ar kontrolės.

6 ESPR rengiama 2004–2006 m. imantis parengiamųjų veiksmų dėl mokslinių tyrimų saugumo srityje.

7 *Pasaulinės partnerystės informacinėje visuomenėje link: Pasaulio viršūnių susitikimo informacinės visuomenės klausimais (WSIS) Tuniso etapo tolesni veiksmai* , COM(2006) 181 galutinis, 2006 4 27

8 Kenkėjai - „kenkėjiška programinė įranga“.

9 Duomenų vagystės – apgavystės internetu forma, kai siekiama pavogti vertingą informaciją, tokią kaip kreditinių kortelių, banko sąskaitų numerius, vartotojo tapatybės numerius ir slaptažodžius.

„zombių“ (angl. *botnet*)[10], t.y. serverių ir asmeninių kompiuterių, į kuriuos jau įsilaužta ir kuriais yra naudojamasi kaip kanalais be jų savininkų žinios.

Sparčiai besivystant IP paslaugoms, vis platesnis judriojo ryšio priemonių (įskaitant trečiosios kartos (3G) mobiliuosius telefonus, nešiojamus vaizdo žaidimus ir kt.) ir judriojo ryšio paslaugų naudojimas taps nauju iššūkiu. Tai gali virsti net įprastesniu elektroninių atakų taikiniu nei asmeniniai kompiuteriai, kadangi pastarieji jau yra pakankamai saugūs. Išties, naujos ryšių platformos ir informacinių sistemų formos neišvengiamai atveria naujas galimybes įvairioms kenksmingoms elektroninėms atakoms.

Kita svarbi naujovė – „aplinkos intelekto“ radimasis, kai visur įsigalės naujausiomis kompiuterinėmis ir ryšių tinklų technologijomis pagrįsti „protingi“ prietaisai (pvz., kuriuose naudojami RFID[11], IPv6 ir sensoriniai tinklai). Visiškai susietas ir ryšių tinklais paremtas kasdienis gyvenimas suteiks ypač dideles galimybes. Tačiau tuo pačiu metu kils ir papildoma rizika saugumui ir privatumui. Taigi nors bendros platformos ir programos teigiamai prisideda prie informacijos ir ryšių technologijų (IRT) tarpusavio sąveikos ir jų pritaikymo, jos taip pat gali padidinti riziką. Štai, pvz., kuo naujesnė programinė įranga naudojama, tuo daugiau žalos padaroma kai pasinaudojama jos trūkumais ar kilus jos gedimui. Tam tikrų „monokultūrų“ atsiradimas programinės įrangos platformose ir taikomosiose programose gali gerokai paskatinti naujų grėsmių saugumui, tokių kaip „kenkėjai“ ir virusai, atsiradimą ir plitimą. **Taigi įvairovė, atvirumas ir sąveikumas yra neatsiejamos saugumo dalys, ir juos būtina skatinti**.

Informacijos ir ryšių technologijų sektoriaus svarba Europos ekonomikai ir Europos visuomenei yra neginčytina. Informacijos ir ryšių technologijos yra neatskiriama naujovių dalis. Nuo jų priklauso beveik 40 % viso produktyvumo augimo. Be to, ketvirtadalis Europos mokslinių tyrimų yra susiję su šiuo ypač pažangiu sektoriumi, kuris taip pat vaidina itin svarbų vaidmenį skatinant ekonomikos pažangą ir kuriant naujas darbo vietas. Vis daugiau europiečių gyvena iš tiesų informacinėje visuomenėje, kur informacijos ir ryšių technologijų naudojimas sparčiai auga kaip pagrindinis žmonių socialinio ir ekonominio bendravimo būdas. Remiantis Eurostato duomenimis, 2004 m. 89 % visų Europos Sąjungos įmonių dažnai naudodavosi internetu ir net apie 50 % visų vartotojų interneto paslaugomis naudojosi pastaruoju metu[12].

Kai kurie tinklų ir informacijos saugumo pažeidimų padariniai gali būti ne tik ekonominiai. Pamažu pastebimas susirūpinimas, kad su saugumu susijusios problemos gali sumažinti vartotojų aktyvumą, taip pat ir informacijos ir ryšių technologijų taikymo mastą, kadangi prieinamumas, patikimumas ir saugumas yra būtina sąlyga norint užtikrinti pagrindines teises elektroninėje erdvėje.

Be to, stiprėjant ryšiams tarp tinklų, kitos svarbios infrastruktūros sritys (transportas, energetika ir kt.) taip pat vis labiau priklauso nuo jų informacinių sistemų saugumo.

Tačiau tiek Europos verslo sektorius, tiek ir patys gyventojai vis dar neįvertina rizikos. Taip yra dėl daugelio priežasčių, bet pagrindine priežastimi būtų galima laikyti tai, kad įmonėms

---

[10] Zombiai – robotų, t.y. taikomųjų programų, atliekančių nuotoliniu būdu valdomus veiksmus, ir įdiegtų aukos kompiuteryje, tinklai.

[11] Radijo dažninis atpažinimas.

[12] Eurostatas, *Interneto veikla Europos Sąjungoje*, 40/2005.

investicijų į saugumą grąža nėra akivaizdi, o gyventojai nevisiškai suvokia savo, kaip pasaulinio saugumo grandies, atsakomybę.

Taigi, atsižvelgiant į visa apimantį informacijos ir ryšių technologijų ir informacinių sistemų paplitimą, tinklų ir informacijos saugumas pateikia iššūkių visiems:

- **viešojo valdymo institucijos** turi atkreipti dėmesį į naudojamų sistemų saugumą, siekdamos ne tik užtikrinti viešojo sektoriaus informacijos saugumą, bet ir kad parodytų pavyzdį kitiems rinkos dalyviams;

- **įmonės** turi žiūrėti į tinklų ir informacijos saugumą kaip į turtą ir privalumą konkurencijos sąlygomis, o ne kaip į „neigiamas išlaidas“;

- **atskiri vartotojai** turi suvokti, kad jų namų sistemos yra svarbi bendro saugumo grandis.

Siekiant sėkmingai įveikti pirmiau minėtas problemas, visoms suinteresuotosioms šalims būtina pateikti patikimus duomenis apie informacijos saugumo pažeidimus ir šioje srityje pastebimas tendencijas. Tačiau dėl daugelio priežasčių pakankamai sunku surinkti patikimus ir išsamius duomenis apie tokius pažeidimus. Tam gali kliudyti tai, kad saugumo pažeidimai įvyksta labai greitai, ar kai kurių organizacijų nenoras atskleisti ir viešinti su saugumu susijusius pažeidimus. Vis dėlto vienas pagrindinių saugumo kultūros plėtros aspektų – **geriau suvokti šias problemas**.

Svarbu, kad visuomenės informavimo programose, skirtose atkreipti vartotojų dėmesį į grėsmes saugumui, būtų akcentuojami ne tik neigiami saugumo aspektai, kad dėl to nesumažėtų vartotojų pasitikėjimas. Todėl visais įmanomais būdais, **tinklų ir informacijos saugumas turi būti pateikiamas kaip vertybė ir galimybė,** o ne įsipareigojimas ir išlaidos. Jis turi būti suvokiamas kaip vertybė kuriant vartotojų pasitikėjimą, kaip konkurencinis privalumas įmonėms, naudojančioms informacines sistemas ir kaip paslaugų kokybės požymis tiek viešojo, tiek ir privačiojo sektoriaus paslaugų teikėjams.

Pagrindinis politikos kūrėjų uždavinys – suformuoti holistinį požiūrį, pagal kurį pripažįstamas atitinkamas skirtingų suinteresuotųjų grupių vaidmuo. Taip pat turi būti užtikrinamas tinkamas įvairių viešosios politikos ir reglamentavimo nuostatų, tiesiogiai arba netiesiogiai susijusių su tinklų ir informacijos saugumu, koordinavimas. Tačiau dėl liberalizavimo, reglamentavimo panaikinimo ir suartėjimo procesų įvairiose suinteresuotųjų šalių grupėse atsiradus nuomonių įvairovei, tai tampa gana sudėtinga užduotimi. Siekiant šio tikslo, didelę reikšmę galėtų turėti Europos tinklų ir informacijos saugumo agentūra (ETISA). Ji galėtų tapti informacijos ir geros patirties mainų, visų suinteresuotųjų šalių bendradarbiavimo centru ne tik Europoje, bet ir visame pasaulyje, siekiant padidinti mūsų informacijos bei ryšių technologijų pramonės ir puikiai veikiančios vidaus rinkos konkurencingumą.

3. DINAMIŠKO POŽIŪRIO Į SAUGIĄ INFORMACINĘ VISUOMENĘ FORMAVIMAS

Saugi informacinė visuomenė turi būti paremta **didesniu tinklų ir informacijos saugumu** bei plačiai paplitusia **saugumo kultūra**. Todėl Europos Komisija siūlo visas suinteresuotąsias šalis apimantį **dinamišką ir integruotą požiūrį,** paremtą **dialogu, partneryste ir teisių suteikimu**. Kadangi tiek viešasis, tiek ir privatusis sektoriai padeda formuoti saugumo kultūrą, saugumo politikos iniciatyvos turi būti paremtos **atviru ir įvairias suinteresuotąsias šalis apimančiu dialogu**.

Šis požiūris bei su juo susiję veiksmai papildys ir praplės Komisijos planus toliau formuoti išsamią ir dinamišką politiką įvairiomis 2006 m. rengiamomis iniciatyvomis:

(1) atkreipiant dėmesį į elektroninio pašto šiukšlių ir grėsmių, tokių kaip „šnipukai“ ir kitos „kenkėjų“ formos, vystymąsi šiuos konkrečius klausimus nagrinėjančiame komunikate;

(2) teikiant pasiūlymus dėl teisėsaugos institucijų bendradarbiavimo gerinimo ir sutelkiant dėmesį į naujas nusikalstamos veikos, atliekamos naudojantis internetu ir sutrikdančios svarbiausios infrastruktūros veiklą, formas. Šia tema bus parengtas atskiras komunikatas apie kompiuterinius nusikaltimus.

Šios politikos iniciatyvos taip pat prisideda prie tikslų, numatytų Komisijos žaliojoje knygoje apie Europos programą dėl ypatingos svarbos infrastruktūros objektų apsaugos (EPCIP)[13], kuri parengta atsižvelgiant į 2004 m. gruodžio mėn. Europos Vadovų Tarybos reikalavimą. Įgyvendinant žaliojoje knygoje numatytą procesą, greičiausiai bus parengtas veiksmų planas, kuriame bus suderinta bendra visapusiška itin svarbių infrastruktūros objektų apsauga su reikiamų sektorių, taip pat ir IRT sektoriaus, politika. Formuojant informacijos ir ryšių technologijų sektoriaus politiką vyktų **dialogas su įvairiomis suinteresuotosiomis šalimis**, kuris padėtų ištirti ekonominius, verslo ir socialinius veiksnius siekiant sustiprinti saugumą ir tinklų bei informacinių sistemų atsparumą.

Be to, 2006 m. numatytos elektroninių ryšių reguliavimo sistemos peržiūros metu bus aptariami būdai, kaip padidinti tinklų ir informacijos saugumą, pvz., techninės ir organizacinės priemonės, kurių turi imtis paslaugų teikėjai, nuostatos, numatančios pranešimus apie saugumo pažeidimus, ir konkrečius veiksmus bei baudas už įpareigojimų nesilaikymą.

Didžiausia atsakomybė už sprendimų, paslaugų ir saugumą užtikrinančių produktų pateikimą galutiniam vartotojui tenka privačiajam sektoriui. Todėl itin svarbu, kad **Europos pramonė būtų ir reiklus** saugumo produktų bei paslaugų **vartotojas, ir pajėgus konkuruoti** su TIS susijusių produktų bei paslaugų **tiekėjas**.

Nacionalinės valdžios institucijos turi sugebėti nustatyti ir įgyvendinti geriausią politikos formavimo patirtį, taip pat pačios laikytis šių politikos tikslų saugiai administruodamos savo informacines sistemas. Valstybės institucijoms tenka labai svarbus vaidmuo tiek nacionaliniu, tiek visos Europos Sąjungos lygmeniu tinkamai informuoti vartotojus ir paskatinti juos prisidėti prie jų pačių saugumo užtikrinimo. Šių institucijų prioritetai turi būti informuoti vartotojus apie tinklų ir informacijos saugumą bei su juo susijusias problemas, taip pat teikti aktualią informaciją specialiuose elektroniniam saugumui skirtuose portaluose apie grėsmes, riziką ir galimus pavojus bei geriausią patirtį. Todėl galimybė **sukurti Europos daugiakalbę informacijos mainų ir įspėjimo sistemą**, paremtą esamomis ir planuojamomis nacionalinėmis viešojo ir privačiojo sektoriaus iniciatyvomis bei jas sujungiančią, galėtų tapti pagrindiniu Europos tinklų ir informacijos saugumo agentūros tikslu.

Kadangi tinklų ir informacijos saugumas yra aktualus visam pasauliui, tai verčia Komisiją tiek tarptautiniu lygmeniu, tiek ir bendradarbiaujant su valstybėmis narėmis, dėti daugiau pastangų **skatinant pasaulinį bendradarbiavimą tinklų ir informacijos saugumo klausimais**, ypač

[13] COM (2005) 576 galutinis, 2005 11 17.

įgyvendinant 2005 m. lapkričio mėn. įvykusio Pasaulio viršūnių susitikimo informacinės visuomenės klausimais (WSIS) darbotvarkę.

Galiausiai, moksliniai tyrimai ir technologijų plėtra, ypač ES lygmeniu, padės sukurti naujas ir pažangias partnerystes, kurios savo ruožtu skatins Europos IRT pramonės plačiąja prasme, o ypač Europos IRT saugumo pramonės, augimą. Todėl Komisija sieks užtikrinti, jog Septintojoje ES pagrindų programoje numatytiems tinklų ir informacijos saugumo ir patikimumo technologijų moksliniams tyrimams būtų skirta pakankamai lėšų.

3.1. Dialogas

3.1.1. Pirmasis žingsnis siekiant sustiprinti dialogą tarp valstybės institucijų – Komisijos pasiūlymas ***palyginti valstybių narių tinklų ir informacijos saugumo politiką,*** *įskaitant ir konkrečiai viešajam sektoriui skirtą saugumo politiką. Toks bandymas padėtų nustatyti geriausią patirtį, kurią būtų galima pritaikyti platesniu mastu visoje Europoje ir kuri padėtų valstybės valdymo institucijoms skatinti gerą patirtį saugumo srityje. Šiuo atžvilgiu ypač svarbu dėti dideles pastangas elektroninio identifikavimo srityje, pvz., kaip numatyta e.vyriausybės veiksmų plane.*

Tinkamai susisteminti politikos palyginimo rezultatai padės **atskleisti geriausią patirtį, kaip padėti smulkaus ir vidutinio verslo įmonėms bei gyventojams suvokti, kad būtina** atkreipti dėmesį į konkrečias su tinklų ir informacijos saugumu susijusias problemas ir reikalavimus, su kuriais jie susiduria. Tokiame dialoge ypač svarbų vaidmenį turėtų atlikti ETISA, kuri taip pat turėtų aktyviai dalyvauti sisteminant ir keičiantis geriausia patirtimi.

3.1.2. Norint nustatyti geriausią būdą kaip, pasinaudojant esamomis reglamentavimo priemonėmis, pasiekti socialinę saugumo ir pagrindinių teisių pusiausvyrą, įskaitant teisę į privatumą, būtina ***sisteminga įvairių suinteresuotųjų šalių diskusija****. Ją papildys Suomijos, kuri netrukus perims pirmininkavimą ES, rengiama konferencija „i2010 – Informacinė visuomenė visuose Europos kampeliuose“ ir konsultacijos dėl radijo dažninio atpažinimo poveikio saugumui ir privatumui, kurios yra neseniai Komisijos inicijuotų platesnio masto konsultacijų dalis. Be to, Komisija dar ketina surengti:*

- verslo renginį, skirtą sustiprinti pramonės sektoriaus įsipareigojimą taikyti veiksmingus metodus plėtojant saugumo kultūrą **pramonėje**;
- seminarą, skirtą aptarti būdus, kaip geriau informuoti **galutinius vartotojus** saugumo klausimais ir skatinti jų pasitikėjimą elektroniniais tinklais ir informacinėmis sistemomis.

3.2. Partnerystė

3.2.1. Siekiant efektyvių politinių sprendimų, būtina aiškiai suvokti problemų esmę ir sudėtingumą. Todėl būtina turėti ne tik naujausius patikimus statistinius ir ekonominius duomenis apie informacijos saugumo pažeidimus ir vartotojų pasitikėjimo laipsnį, bet ir naujausius duomenis apie Europos IRT saugumo pramonės apimtį ir kryptis. Europos komisija ketina prašyti ETISA sukurti ***patikimą partnerystę su valstybėmis narėmis ir su suinteresuotosiomis šalimis*** *ir parengti* ***tinkamą duomenų rinkimą reglamentuojantį teisinį pagrindą****, kuris apimtų visos*

ES duomenų apie saugumo pažeidimus ir vartotojų pasitikėjimą rinkimo ir analizės procedūras bei mechanizmus.

Be to, dėl itin susiskaldžiusios ES rinkos ir jos gana išskirtinio pobūdžio, Komisija, siekdama užtikrinti, kad būtų prieinami duomenys apie informacijos ir ryšių technologijų saugumo pramonę ir besikeičiančių produktų ir paslaugų rinkos tendencijas ES, ragins valstybes nares, privataus sektoriaus atstovus ir mokslininkus **sudaryti strateginę partnerystę.**

*3.2.2. Kad Europa galėtų geriau reaguoti į grėsmes tinklų saugumui, Komisija paprašys ETISA ištirti **Europos informacijos mainų ir įspėjimo sistemos sukūrimo galimybes,** kuri padėtų veiksmingai kovoti su esamais ir naujai atsirandančiais pavojais elektroniniams tinklams. Tokia sistema turėtų veikti **ES oficialiomis kalbomis parengtame portale,** kuriame bus pateikiama speciali informacija apie grėsmes, riziką ir pavojaus signalus.*

3.3. Teisių suteikimas

Teisių kiekvienai suinteresuotųjų šalių grupei suteikimas yra būtina sąlyga siekiant kuo geriau informuoti apie saugumą ir su juo susijusią riziką, kad paskatintų tinklų ir informacijos saugumą.

*3.3.1. Todėl Komisija ragina **valstybes nares**:*

- aktyviai dalyvauti lyginant valstybių narių tinklų ir informacijos saugumo politiką;
- bendradarbiaujant su ETISA, skatinti informavimo kampanijas apie veiksmingų saugumo technologijų, tvarkos ir veiksmų taikymo privalumus, naudą ir rezultatus;
- skatinti pradėti teikti elektroninės valdžios paslaugas siekiant perteikti ir paskatinti gerą saugumo patirtį, kurią vėliau būtų galima perkelti į kitus sektorius;
- skatinti, kad aukštojo mokslo institucijų mokymo programose būtų numatyta kurti tinklų ir informacijos saugumo programas.

***3.3.2.** Komisija taip pat kviečia **privačiojo sektoriaus** suinteresuotąsias šalis imtis iniciatyvos:*

- tinkamai apibrėžti programinės įrangos gamintojų ir interneto paslaugų teikėjų atsakomybę užtikrinti pakankamą ir kontroliuojamą saugumą. Šiuo atveju būtina paremti nustatytus standartinius procesus, kurie atitiktų visuotinai pripažintus saugumo standartus ir geriausią patirtį;
- skatinti įvairovę, atvirumą, sąveikumą, naudojimą ir konkurenciją kaip pagrindinius saugumą užtikrinančius veiksnius bei saugumą didinančių produktų, procesų ir paslaugų naudojimą siekiant užkirsti kelią asmens tapatybės duomenų vagystėms ir kitokioms privatumą pažeidžiančiomis atakoms;

- tinklo operatoriams, paslaugų teikėjams ir MVĮ skleisti gerą saugumo patirtį, kuri yra saugumo ir verslo tęstinumo užtikrinimo minimumas;

- skatinti verslo sektoriui, ypač MVĮ, skirtas mokymo programas siekiant suteikti darbuotojams žinių ir įgūdžių, kurie būtini norint veiksmingai įgyvendinti saugumo praktikas;

- siekti prieinamų saugumo sertifikavimo schemų produktams, procesams ir paslaugoms, kurios atitiktų specifinius ES poreikius (ypač privatumo);

- įtraukti draudimo sektorių į tinkamų rizikos valdymo priemonių ir būdų, kaip išvengti su informacijos ir ryšių technologijomis susijusios rizikos, kūrimo procesą bei skatinti rizikos valdymo kultūrą organizacijose ir įmonėse (ypač MVĮ).

4. IŠVADOS

Siekiant nustatyti ir tinkamai reaguoti į ES informacinių sistemų ir tinklų saugumui tenkančius iššūkius, būtinos visų suinteresuotųjų šalių pastangos. Toks yra šiame Komunikate pateikto politinio metodo tikslas, kurio siekiama **įtraukiant įvairias suinteresuotąsias šalis**. Bus ieškoma bendrų interesų, nustatomi atitinkami vaidmenys ir kuriamas dinamiškas pagrindas efektyviam viešosios politikos formavimui ir privataus sektoriaus iniciatyvoms skatinti.

Apie pradėtus veiksmus, preliminarius rezultatus ir vykdomų atskirų iniciatyvų, įskaitant ETISA, atskirose valstybėse narėse ir privačiajame sektoriuje, padėtį Komisija praneš Europos Tarybai ir Parlamentui 2007 m. viduryje. Prireikus, Komisija pateiks Rekomendacijos dėl tinklų ir informacijos saugumo (TIS) pasiūlymą.