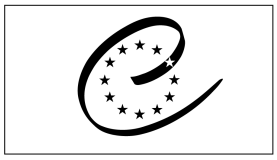

Одељење за привредни криминал
Генерални директорат за људска права
и правне послове
Стразбур, Француска
2. априла 2008.

Serbian version

Смернице за сарадњу између полиције и интернет провајдера на сузбијању високотехнолошког криминала

Донете на глобалној Конференцији
Сарадња на сузбијању
високотехнолошког криминала
Савета Европе,
у Стразбуру, 1.-2. априла 2008.

Ове смернице израђене су као резултат неколико кругова разговора вођених између представника привредног сектора и полицијских органа који су се састајали у периоду од октобра 2007. до фебруара 2008. године под покровитељством Пројекта о високотехнолошком криминалу Савета Европе. Смернице су допуњене детаљном студијом основних информација.

О смерницама се расправљало и даље, да би на крају биле донете на глобалној Конференцији „Сарадња на сузбијању високотехнолошког криминала" (Савета Европе, одржаној у Стразбуру у Француској) током 1. и 2. априла 2008. године.

Ове смернице су необавезујући инструмент који сада може да се објави и да се користи као подршка полицији и интернет провајдерима у било којој земљи у свету, у циљу организовања сарадње у сузбијању високотехнолошког криминала, уз истовремено узајамно поштовање одговорности и права корисника интернета.

Смернице за сарадњу између полиције и интернет провајдера у сузбијању високотехнолошког криминала[1]

Увод

1. Изградња информационог друштва захтева јачање поверења у информационе и комуникационе технологије (ИКТ), заштиту података о личности и приватности, као и подстицање глобалне културе компјутерске безбедности у контексту све веће зависности друштава у свету од информационе и комуникационе технологије, а самим тиме и све веће изложености високотехнолошком криминалу;

2. Први и Други светски скуп о информационом друштву (Женева 2003, Тунис 2005.), који су, између осталог, били усмерени ка изградњи свеобухватног информационог друштва у коме свако може да створи, да има приступ, да користи и да са другима подели информације и знање, да оствари своје могућности и да унапреди квалитет живота, утемељеног на циљевима и начелима Повеље Уједињених нација, поштујући и у потпуности подржавајући Општу декларацију о људским правима и тражећи нове облике партнерства и сарадње између влада, приватног сектора, цивилног друштва и међународних организација;

3. Интернет провајдери (ИП) и тела за спровођење закона (ТСЗ) имају кључну улогу у реализацији те визије;

4. Национално законодавство усклађено с Конвенцијом о кибернетичком криминалу Савета Европе (Конвенција из Будимпеште) помаже државама у изградњи поуздане законске основе за јавно-приватну сарадњу, истражна овлашћења и међународну сарадњу;

5. Циљ ових смерница није да се њима замене постојећи правни инструменти, већ да се постулирају одговарајући законски инструменти који обезбеђују уравнотежен састав истражних инструмената и са њима повезаних заштитних мера, као и заштиту основних људских права, као што су право на слободу изражавања, поштивања приватности, дома и преписке и право на заштиту података. С тих разлога, препоручује се да државе донесу прописе у свом националном законодавству ради целовитог спровођења процесних одредаба Конвенције о кибернетичком криминалу, као и да дефинишу истражна тела и обавезе полиције, уз истовремено осигуравање услова и мера безбедности предвиђених чланом 15. Конвенције. То ће:

- осигурати ефикасан рад тела за спровођење закона
- заштитити способност пружања услуга интернет провајдера
- осигурати да национални прописи буду уподобљени глобалним стандардима
- подстицати глобалне стандарде уместо изолованих националних решења
- помоћи у обезбеђивању законитости поступања и владавине права, укључујући ту начело законитости, сразмерности и нужности;

6. У смислу ових Смерница користимо дефиницију интернет провајдера из члана 1. Конвенције о кибернетичком криминалу која "интернет провајдера" дефинише у ширем контексту као:

i свако физичко или правно лице које корисницима својих услуга пружа могућност комуникације помоћу компјутерског система, и

[1] Овај документ не мора нужно да одражава званичне ставове Савета Европе. Додатне информације могу се добити на адреси Alexander.seger@coe.int

ii сваки други субјекат који обрађује или складишти компјутерске податке за такву комуникацијску услугу или кориснике те услуге;

7. Како би се унапредила кибернетичка безбедност, коришћење услуга у незаконите сврхе свело на минимум и како би се изградило поверење у информационе и комуникационе технологије, од кључног је значаја да интернет провајдери и полицијски органи узајамно сарађују на ефикасан начин, водећи рачуна о улози сваког од њих, као и о трошковима такве сарадње и о правима грађана;

8. Ове Смернице имају сврху која се своди на пружање помоћи телима за спровођење закона и интернет провајдерима у структурисању њихове узајамне сарадње на плану решавања питања високотехнолошког криминала. Та сарадња се заснива на постојећим добрим примерима из праксе и требало би да буде примењива у било којој земљи у света, у складу са националним законодавством, и уз поштовање слободе изражавања, приватности, заштите података о личности и осталих основних права која грађани уживају;

9. С тих разлога се препоручује да државе, полицијски органи и интернет провајдери предузму следеће мере на националном нивоу:

Опште смернице

10. Полицијске органе и интернет провајдере требало би подстаћи да размењују информације како би на тај начин ојачали своју способност откривања и сузбијања нових врста високотехнолошког криминала. Полиције би требало подстаћи да обавесте интернет провајдере о трендовима у развоју високотехнолошког криминала;

11. Полицијски органи и интернет провајдери требало би да подстичу културу сарадње – а не конфронтације – укључујући ту и размену добрих примера из праксе. Ваљало би стимулисати одржавање редовних састанака у циљу размене искустава и решавања проблема;

12. Полицијске органе и интернет провајдере требало би подстаћи на израду процедура (пословника односно протокола) за узајамну сарадњу у писменој форми. Кад год је то могуће требало би подстаћи обе стране на размену структурисаних повратних информација о сарадњи у тим поступцима;

13. Требало би размотрити формално партнерство између полицијса и интернет провајдера како би се успоставили дугорочни односи који би једној и другој страни гарантовали да њихово партнерство неће повредити законска права зајамчена привредном сектору нити ће нарушавати законска овлашћења полицијских органа;

14. И полицијски органи и интернет провајдери би требало да штитите основна права грађана у складу са стандардима Уједињених нација и осталим релевантним европским и међународним стандардима, као што су Конвенција за заштиту људских права и основних слобода Савета Европе из 1950. године, Међународни пакт о грађанским и политичким правима Уједињених нација из 1966. године, Конвенција Савета Европе о заштити појединаца у вези са аутоматском обрадом података о личности из 1981. године, као и у складу са националним законодавством. То у извесној мери ограничава ниво могуће сарадње;

15. Полицијске органе и интернет провајдере треба подстаћи на узајамну сарадњу у погледу спровођења стандарда за заштиту приватности и података на националном нивоу, али исто тако и у погледу прекограничног протока података. У том погледу своје препоруке у активностима којима се баве већ су дали Савет Европе и Организација за економску сарадњу и развој (ОЕЦД);

16. Обе стране би требало да воде рачуна о трошковима који су везани за давање захтева и одговарања/реаговања на захтеве. Требало би установити поступке (протоколе) узимајући у обзир финансијски учинак свих тих активности, као и питање надокнађивања трошкова или правичне накнаде одговарајућим странкама.

Мере које треба да спроводе полицијски органи

17. Свеобухватна и стратешка сарадња – требало би подстицати полицијске органе да пружају помоћ интернет провајдерима тако што ће се укључити у свеобухватну и стратешку сарадњу са привредним сектором, што подразумева одржавање редовитих семинара за стручну обуку и обуку у области правних наука, као и давање повратних информација о истрагама које су спроведене на основи приговора интернет провајдера или на основу обавештења прикупљених на темељу познатих кривичних активности о којима пријаве подносе интернет провајдери;

18. Поступци (протоколи) за законски обавезујуће захтеве – требало би подстаћи полицијске органе на утврђивање и израду поступака (протокола) у писаној форми, с тим што би те процедуре требало да обухвате одговарајуће мере законитог поступања у складу са важећим прописима за издавање и обраду законски обавезујућих захтева, с тим што се истовремено мора обезбедити да се ти захтеви спроводе у складу са договореним поступцима;

19. Обука – Требало би подстаћи полицијске органе да за одабрану групу запослених организују обуку о начину спровођења тих поступака, укључујући ту и начин на који се од интернет провајдера могу добити евиденциони подаци, као и начин обраде примљених информација; та обука би, међутим, морала да буде посвећена и технологијама коришћења интернета и укупном дејству интернета, као и начину поштовања законитости поступања и основних људских права;

20. Технички ресурси – Полицијски органи надлежни за сарадњу са интернет провајдерима требало би да имају одговарајуће потребне техничке ресурсе, укључујући ту и приступ интернету, електронску адресу коју је издала агенција/посредник, из које је јасно видљива адреса сродне агенције, уз све остале техничке ресурсе који омогућују безбедан пријем информација које електронским путем стижу од интернет провајдера;

21. Одабрано особље и тачке за контакт – узајамна сарадња између полицијских органа и интернет провајдера требало би да се ограничи на изабрано особље. Требало би подстаћи полиције да одреде тачке за контакт које би биле предодређене за сарадњу са интернет провајдерима;

22. Овлашћење за захтеве – Требало би подстаћи полицијске органе да у писаној форми јасно дефинишу које је то особље овлашћено за коју врсту мера и захтева упућених интернет провајдерима, и на који начин интернет провајдери могу да провере веродостојност таквих захтева;

23. Требало би подстаћи полицијске органе да интернет провајдерима омогуће приступ информацијама о властитим поступцима и да, онда када је то могуће, доставе информацију о томе које је особље, односно која су одређена радна места надлежна за сарадњу са интернет провајдерима;

24. Провера/верификација извора захтева – Интернет провајдери би требало да имају могућност да провере извор захтева који су им упутили полицијски органи:

- Сваки допис би требало да садржи назив контакта, телефонски број и адресу електронске поште полицијског органа/агента који тражи евиденцију, тако да у случају потребе интернет провајдер може ступити у контакт са особом која тражи податке;

- не би требало тражити да интернет провајдери обављају преписку са агентом преко његове личне електронске поште, већ преко одговарајуће електронске адресе која би била осигурана од агенције;

- сви дописи би требало да буду достављени на обрасцу који садржи заглавље одељења, а преписка би морала да садржи и број централе канцеларије интернет адресу (адресу интернет странице), тако да интернет провајдер,, ако то сматра потребним, може да предузме све мере како би проверио веродостојност захтева;

25. Захтеви – Полиције треба да достављају захтеве интернет провајдерима у писаној форми (или на други законом предвиђени електронски начин) ради материјалне евиденције докумената. У изузетно хитним случајевима када су дозвољени и усмени захтеви, то захтеви треба одмах да буду пропраћени писаном документацијом (или другим законом дозвољеним видом електронске комуникације);

26. Стандардни образац захтева – Полицијске органе требало би подстицати да како на националном, тако и на, у мери могућности, међународном нивоу, користе стандардизовани и структурисани образац за слање захтева и одговора на захтеве. Захтеви би требало да садрже бар следеће информације:

- Регистарски број
- Позивање на законску/правну основу
- Посебне податке који се траже
- Информације које су потребне за проверу извора захтева;

27. Конкретност и прецизност захтева – Полицијске органе требало би подстицати да се постарају да захтеви који се шаљу буду конкретни, потпуни и јасни, као и да обезбеде довољан ниво прецизности који је неопходан интернет провајдерима за утврђивање релевантних података. Полицијске органе треба подстаћи да се постарају да се захтеви шаљу евидентираним/регистрованим интернет провајдерима. Требало би избегавати захтеве који садрже вишеструке и недовољно конкретизоване, односно недовољно прецизиране податке;

28. Полицијске органе би требало подстицати да доставе што је могуће више података о истрази не доводећи ту истрагу у питање и не угрожавајући ниједно основно право, како би се омогућило да интернет провајдери идентификују релевантне податке;

29. Полицијске органе би требало подстицати да пружају објашњења и помоћ интернет провајдерима у погледу истражних техника које нису повезане са датим конкретним случајем, како би сами интернет провајдери схватили да ће њихова сарадња имати за резултат ефикаснију истрагу кривичних дела и бољу заштиту грађана;

30. Одређивање приоритета – Полицијске органе би требало подстицати на утврђивање приоритета захтева, посебно када је реч о захтевима који су везани завелику количину података, како би се интернет провајдерима омогућило приоритетно решавање по најважнијим захтевима. То одређивање приоритета најбоље је спроводити доследно у свим националним полицијама, а по могућности и на међународном нивоу;

31. Примереност захтева – Полицијске органе би требало подстицати да узимају у обзир трошкове које интернет провајдери имају када је реч о таквим захтевима, као и да интернет провајдерима обезбеде довољно времена за одговор. Треба имати на уму да интернет провајдер такође треба да одговори и на захтеве потекле од других полицијских органа, па би стога ваљало подстаћи полиције да пажљиво прате количину података коју достављају;

32. Поверљивост података – Полицијски органи би требало да обезбеде поверљивост примљених података;

33. Избегавање непотребних трошкова и прекида пословања – Полицијске органе би требало подстицати да избјегавају непотребне трошкове и прекид пословања интернет провајдера као и осталих пословних субјеката;

34. Полицијске органе би требало подстицати да коришћења тачака за контактних у хитним ситуацијама заиста користе искључиво за хитне случајеве, како би се онемогућила злоупотреба услуга тих служби.

35. Полицијске органе би требало подстицати да после издавања решења о заштити података и о доношењу других привремених мера благовремено доставе и решења о обавезном обелодањивању података, или да интернет провајдере благовремено обавесте о томе да више нема потребе за заштитом података;

36. Међународни захтеви – Требало би подстицати националне полиције да када је реч о захтевима које шаљу страним интернет провајдерима не достављају такве захтеве директно страним интернет провајдерима, него да користе процедуре описане у међународним уговорима, као што су Конвенција о кибернетичком криминалу и мрежа тачака за контакт која је активна 24 сата дневно сваког дана у недељи за хитне мере, укључујући ту и решења/захтеве за заштиту података;

37. Захтеви за међународну правну помоћ - Полицијске органе и правосудна тела требало би подстицати на то да предузимање све потребне мере да би се обезбедило да после захтева за предузимања привремених мера уследе међународни поступци (процедуре) за узајамну правну помоћ, односно да интернет провајдер буде благовремено обавештен да више не постоји потреба за заштитом података;

38. Координација између полицијских органа – полиције би требало подстаћи на то да координишу сарадњу са интернет провајдерима и да размењују добре примере из праксе, како на националном, тако и на међународном нивоу. Када је реч о размени на међународном нивоу требало би користити релевантна међународна представничка тела која су формирана управо у ту сврху;

39. Програми заштите законитости поступања – Полицијске органе би требало подстицати на то да организују и успоставе описану међусобну сарадњу са интернет провајдерима у виду свеобухватног програма заштите законитости поступања, као и достављање описа таквих програма интернет провајдеру, укључујући следеће:

- Информације потребне за ступање у контакт са изабраним полицијским особљем за заштиту законитости поступања, као и информације о времену у ком је то особље доступно;
- Информације које су интернет провајдеру потребне за обезбеђивање докумената особља за заштиту законитости поступања;
- Остале појединости које се конкретно односе на особље за заштиту законитости поступања (на пример област у којој неки полицијски орган сарађује у различитим земљама, документи које треба превести на одређени језик итд.);

40. Ревизија система за заштиту законитости поступања – Полицијска тела би требало подстаћи на праћење и ревидирање система обраде захтева за потребе статистике, на утврђивање предности и недостатака и, ако је могуће, на саопштавање резултата такве ревизије.

Мере које треба да предузму интернет провајдери

41. Сарадња у циљу смањења коришћења услуга у незаконите сврхе на најмању могућу меру – У складу са примењивим правима и слободама, као што су слобода изражавања, слобода на заштиту приватности и остало што јемче национални и међународни закони и кориснички уговори склопљени са интернет провајдерима, требало би подстицати интернет провајдере на сарадњу са полицијским органима, како би се помогло у смањењу обима у коме се услуге користе за криминалне активности, онако како су те криминалне активности дефинисане законом;

42. Требало би подстицати интернет провајдере на то да извештавају полицијске органе о кривичним случајевима који утичу на интернет провајдере, а које су ти интернет провајдери уочили. То међутим не обавезује интернет провајдере на активно тражење чињеница или околности које указују на незаконите активности;

43. Требало би подстицати интернет провајдере да пружају помоћ полицијским органима у образовању и обуци, као и давању осталих видова подршке за њихове услуге и пословање;

44. Праћење захтева које достављају полицијске власти – Требало би подстицати интернет провајдере да предузму све прихватљиве иницијативе у циљу обезбеђивања помоћи полицијским органима у реализацији захтева;

45. Поступци за одговарање на захтеве – Требало би подстицати интернет провајдере на израду писмених поступака (процедура), које обухватајуодговарајуће законске мере за поступање по таквим захтевима, као и осигурање праћења тих захтева у складу са договореним поступцима;

46. Обука – Требало би подстицати интернет провајдере да осигурају довољну обуку за своје особље које је надлежно за провођење тих поступака;

47. Изабрано особље и тачке за контактне – Требало би подстицати интернет провајдере да одреде обучено особље као тачке за контакт преко којих ће се остваривати сарадња с полицијским органима;

48. Помоћ у хитним случајевима – Требало би подстицати интернет провајдере на проналажење начина на који полицијски органи могу да ступе у контакт са особљем за заштиту законитости поступања изван уобичајеног радног времена, како би решавали хитни случајеви. Требало би подстицати интернет провајдере да полицијским органима обезбеде релевантне информације за помоћ у хитним случајевима;

49. Ресурси – Требало би подстицати интернет провајдере на то да својим тачкама за контакт или особљу надлежном за сарадњу с полицијским органима обезбеде ресурсе који су неопходни да би они могли да изађу у сусрет захтевима полицијских органа;

50. Програми заштите законитости поступања – Требало би подстицати интернет провајдере на то да са полицијским органима организују сарадњу у виду свеобухватног програма заштите законитости поступања као и на то да доставе описе таквих програма полицијским органима, с тим да ти програми треба да садрже следеће:

- Информације потребне за ступање у контакт са изабраним особљем интернет провајдера за заштиту законитости поступања, као и информације о времену у коме је то особље доступно;
- Информације потребне полицијским органима за обезбеђивање докумената потребних особљу за заштиту законитости поступања;
- Све остале подробности које су специфичне за особље за заштиту законитости поступања интернет провајдера (на пример, обим пословања интернет провајдера у различитим земљама, документи које треба превести на неки језик итд.);
- Како би се полицијским органима омогућило издавање конкретних и одговарајућих захтева, требало би подстицати интернет провајдере на то да обезбеде информације о врсти услуга које се нуде корисницима, укључујући ту интернет везе за услуге и додатне информације, као и податке о могућности контакта за достављање даљих информација;
- Онда када је то могуће требало би подстицати интернет провајдере да на захтев обезбеде попис врста података које могу бити дате полицијском органу за сваку услугу, по пријему ваљаног захтева за обелодањивање података (такав захтев доставља полицијски орган), уз прихватање чињенице да неће сви ти подаци бити доступни за сваку кривичну истрагу;

51. Провера извора захтева – Требало би подстицати интернет провајдере на то да прдузимају мере за проверу веродостојности захтева који приме од полицијског органа у мери у којој је то могуће и потребно како би се осигурало да се евиденција корисника не обелодани пред неовлашћеним лицем;

52. Одговор – Требало би подстицати интернет провајдере да одговоре на писмене захтеве полицијских органа (или друге врсте законом предвиђене електронске комуникације) као и да обезбеде да буде доступно праћење докумената у односу на захтеве и одговоре на те захтеве, уз прихватање чињенице да такво праћење можда неће обухватити ниједан податак о личности;

53. Стандардни формат одговора на захтеве – Узимајући у обзир формат за захтеве који користе полицијски органи, требало би подстицати интернет провајдере да користе стандардни формат за достављање информација полицијским органима;

54. Требало би подстицати интернет провајдере да благовремено поступају по захтевима, у складу са писменим процедурама (поступцима) које су већ дефинисали,а као и да полицијским органима предоче смернице о томе колико је просечно кашњење услед реаговања на неки захтев;

55. Проверавање послате информације – Требало би подстицати интернет провајдере да осигурају да информације које се прослеђују полицијском органу буду потпуне, тачне и заштићене;

56. Поверљивост захтева – Интернет провајдери би требало да обезбеде повјерљивост примљених захтева;

57. Објашњење у погледу информације која се не може дати - Интернет провајдери би требало да буду подстицани да пруже објашњење полицијском органу који је доставио захтев у случају да је тај захтев одбијен или да није могућно дати тражену информацију;

58. Ревизија система заштите законитости – Требало би подстицати интернет провајдере на то да прате и ревидирају систем обраде захтева за статистичке потребе, да утврде предности слабости тог система и да, ако је потребно, објаве резултате тих својих анализа;

59. Међусобна координација интернет провајдера – Узимајући у обзир антимонополске прописе и прописе за заштиту тржишне конкуренције, требало би подстицати интернет провајдере на координацију сурадње са полицијским органима и на размену добрих примера из праксе, и, у те сврхе, ваљало би користити удружења интернет провајдера.