Áttekintés

Az információs rendszerek és hálózatok biztonságára vonatkozó OECD irányelvek: Útban a biztonságkultúra felé

Overview

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Hungarian translation

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

GAZDASÁGI EGYÜTTMŰKÖDÉSI ÉS FEJLESZTÉSI SZERVEZET

Előszó

Az információs rendszerek és hálózatok használata és az egész informatikai környezet drámai módon változott meg 1992 óta, amikor az OECD először közzétette az *Információs rendszerek biztonságára vonatkozó irányelvek* című dokumentumot. E folyamatos változások jelentős előnyöket kínálnak, ugyanakkor megkövetelik a kormányoktól, üzleti vállalkozásoktól, egyéb szervezetektől és egyéni felhasználóktól, akik az információs rendszereket fejlesztik, biztosítják, szolgáltatásaikat szervezik és felhasználják, valamint az információs rendszerek tulajdonosaitól („résztvevők") hogy sokkal nagyobb hangsúlyt helyezzenek a biztonságra.

Az egyre nagyobb teljesítőképességű személyi számítógépek, a konvergens technológiák és az Internet széleskörű felhasználása felváltotta az elsősorban zárt hálózatokban működő, szerényebb teljesítményű, önálló rendszereket. Manapság, a résztvevők egyre inkább kölcsönös kapcsolatban vannak, és e kapcsolatok átlépnek az országos határokon. Továbbá, az Internetet kritikus fontosságú infrastruktúrák támogatására használják, mint például az energetika, a közlekedés és a pénzügyek, valamint fontos szerepet játszik abban, hogy a vállalatok hogyan folytatják üzleti tevékenységüket, a kormányok hogyan nyújtják szolgáltatásaikat az állampolgárok és a vállalkozások számára, valamint, a privát állampolgárok hogyan kommunikálnak és folytatnak információcserét. A kommunikációs és információs infrastruktúrát alkotó technológiák jellege és típusa úgyszintén jelentős mértékben megváltozott. Az infrastruktúra-hozzáférést biztosító eszközök száma és fajtája megsokszorozódott, s ezek tartalmazzák a rögzített, vezeték nélküli és mobil készülékeket, valamint a hozzáférés egyre növekvő százaléka „mindig bekapcsolt" csatlakozásokon keresztül történik. Ennek következtében a kicserélt információ jellege, mennyisége és érzékenysége jelentősen megnövekedett.

A kölcsönös összeköttetések növekvő mértéke miatt az információs rendszerek és hálózatok napjainkban növekvő számú és változatosabb fenyegetéseknek vannak kitéve, és sebezhetőségük mértéke és változatossága is megnőtt. Ez új biztonsági kérdéseket vet fel. Ezen okok miatt, a jelen Irányelvek az új információs társadalom összes résztvevőjére vonatkoznak, és indítványozzák a biztonsági kérdések fokozottabb felismerésének és megértésének, valamint egy „biztonságkultúra" kifejlesztésének szükségszerűségét.

I. Útban a biztonságkultúra felé

Ezen Irányelvek válaszul szolgálnak egy folyamatosan változó biztonsági környezet számára azáltal, hogy elősegítik a biztonságkultúra kialakítását – azaz, a biztonságra való odafigyelést az információs rendszerek és hálózatok fejlesztése során, valamint új gondolkodás- és viselkedésmódok meghonosítását az információs rendszerek és hálózatok használata és a segítségükkel történő kapcsolattartás közben. Az Irányelvek egyértelmű szakítást jeleznek azzal a korszakkal, amikor a hálózatok és rendszerek biztonságos tervezése és használata gyakran utólagos megfontolás tárgyát képezte. A résztvevők egyre inkább függővé válnak az információs rendszerektől, hálózatoktól és az azokkal kapcsolatos szolgáltatásoktól, melyeknek mindegyike megbízható és biztonságos kell, hogy legyen. Csupán egy olyan módszer tud hatékony biztonságot teremteni, mely megfelelően számításba veszi az összes résztvevő érdekeit, valamint a rendszerek, hálózatok és az azokkal kapcsolatos szolgáltatások jellegét.

Mindegyik résztvevő fontos szerepet játszik a biztonság garantálásában. A résztvevőknek, szerepüknek megfelelően, tudatosítaniuk kell a rájuk vonatkozó lényeges biztonsági kockázatokat és megelőző intézkedéseket, valamint felelősséget kell vállalniuk és megfelelő lépéseket kell tenniük az információs rendszerek és hálózatok biztonságának növelése érdekében.

Egy biztonságkultúra előmozdítása vezetői képességet és széleskörű részvételt igényel, és fokozott elsőbbséget kell, hogy eredményezzen a biztonságtervezés és szervezés számára, valamint szükséges, hogy minden résztvevő megértse a biztonság szükségét. A biztonsággal kapcsolatos kérdésekkel a kormányzat és az üzleti élet minden szintjén, valamint az összes résztvevőnek foglalkozni kell, illetve értük felelősséget kell vállalni. A jelen Irányelvek egy, a társadalom egészét felölelő biztonságkultúra kifejlesztését célzó munka alapját képezik. Ez lehetővé teszi a résztvevők számára, hogy a biztonságot fontos tényezőként beépítsék az összes információs rendszer és hálózat tervezésébe és használatába. A jelen dokumentum azt javasolja, hogy az összes résztvevő tegye magáévá és segítse elő a biztonsági kultúrát, mint az információs rendszerek és hálózatok működéséről való gondolkodás módját, illetve azok felmérésének és a velük kapcsolatos tevékenységek módszerét.

II. Célok

A jelen Irányelv céljai a következők:

- Biztonságkultúra támogatása az összes résztvevő körében, mint az információs rendszerek és hálózatok védelmének eszköze.
- Tudatosítani az információs rendszerekre és hálózatokra vonatkozó kockázatokat; valamint az ezen kockázatok kezelésére rendelkezésre álló politikai irányelveket, gyakorlatokat, intézkedéseket és eljárásokat; és az elfogadásuk és alkalmazásuk szükségszerűségét.

- Nagyobb bizalom elősegítése az összes résztvevő körében az információs rendszerek és hálózatok, valamint annak módja iránt, ahogy rendelkezésre bocsátják és használják őket.
- Általános hivatkozási keret létrehozása, mely segíti a résztvevőket, hogy megértsék a biztonsággal kapcsolatos problémákat, és tiszteljék az etikai értékeket az információs rendszerek biztonsága érdekében létrejött koherens politikai irányelvek, gyakorlatok, intézkedések és eljárások kifejlesztése és alkalmazása során
- Megfelelő mértékű együttműködés és információmegosztás elősegítése az összes résztvevő körében a biztonsággal kapcsolatos politikai irányelvek, gyakorlatok, intézkedések és eljárások során.
- A biztonság figyelembe vételének, mint fontos célnak előmozdítása a szabványok fejlesztésében és alkalmazásában tevékenykedő összes résztvevő körében.

III. Alapelvek

Az alábbi kilenc alapelv egymást kiegészíti, és egészként olvasandó. Az összes szinten tevékenykedő résztvevőt érintik, beleértve a politikai és működési szinteket. Ezen Irányelvek értelmében, a résztvevők felelőssége szerepüknek megfelelően változik. Az összes résztvevő segítséget kap a tudatosítás, oktatás, információmegosztás és képzés által, mely a biztonság jobb megértését és jobb biztonsági gyakorlatokat eredményezhet. Az információs rendszerek és hálózatok biztonságának növelését szolgáló erőfeszítéseknek összhangban kell lenniük a demokratikus társadalom értékeivel, különös tekintettel az információ nyílt és szabad áramlására, valamint a személyes adatok titokvédelmének alapvető vonatkozásaira.[1]

1) Tudatosítás

A résztvevőknek tudatosítaniuk kell az információs rendszerek és hálózatok biztonságának szükségszerűségét és azt, hogy mit tehetnek a biztonság növelése érdekében.

A kockázatok és a rendelkezésre álló védelmi eszközök tudatosítása az első védelmi vonal az információs rendszerek és hálózatok biztonságának elérésére. Az információs rendszerekre és hálózatokra belső és külső kockázatok is hatással lehetnek. A résztvevőknek meg kell érteniük, hogy a biztonsági hibák jelentősen károsíthatják az irányításuk alatt lévő rendszereket és hálózatokat. Tudatosítaniuk kell a másokra nézve fennálló potenciális veszélyeket a kölcsönös összeköttetésből és függőségből eredően. A résztvevőknek ismerniük kell a rendszerük konfigurációját és a számára elérhető frissítési lehetőségeket, a hálózatokban elfoglalt helyét, valamint az általuk a biztonság növelése érdekében alkalmazható megfelelő gyakorlatokat, és a többi résztvevő igényeit.

[1] Ezen Biztonsági Irányelvek mellett, az OECD kiegészítő ajánlásokat is kialakított, melyek egyéb, a világ információs társadalma számára fontos kérdésekre vonatkozó irányelveket tartalmaznak. Ezek a személyes információra (az 1980-ban kiadott *OECD irányelvek a személyes információ védelmére és a személyes adatok határokon keresztül történő áramlására vonatkozóan*) és a kriptográfiára (az 1997-ben kiadott *OECD irányelvek a kriptográfiai politikára vonatkozóan*) vonatkoznak. A jelen Biztonsági Irányelveket ezekkel együtt kell olvasni.

2) Felelősség

Az összes résztvevő felelős az információs rendszerek és hálózatok biztonságáért

A résztvevők a kölcsönös összeköttetésben levő lokális és globális információs rendszerektől függenek, és meg kell érteniük saját felelősségüket azon információs rendszerek és hálózatok biztonsága érdekében. Elszámolásra kötelezhetők kell, hogy legyenek egyéni szerepüknek megfelelő módon. A résztvevőknek rendszeresen felül kell vizsgálniuk saját irányelveiket, gyakorlataikat, intézkedéseiket és eljárásaikat, és fel kell mérniük, hogy ezek megfelelőek-e a környezetükhöz viszonyítva. A termékek és szolgáltatások fejlesztésében, tervezésében és szállításában résztvevőknek foglalkozniuk kell a rendszerek és hálózatok biztonságával és időben terjeszteniük kell a megfelelő információt, beleértve a frissítéseket, hogy a felhasználók jobban érthessék a termékek és szolgáltatások biztonsági vonatkozásait és a saját felelősségüket a biztonsággal kapcsolatban.

3) Válaszintézkedések

A résztvevőknek kellő időben, kooperatív módon kell eljárni a váratlan biztonsági zavarok megelőzése, észlelése, illetve az ezekre vonatkozó megfelelő válaszintézkedések érdekében

Az információs rendszerek és hálózatok kölcsönös összeköttetését, valamint a gyors és széleskörű károsodás veszélyét felismerve, a résztvevőknek kellő időben és kooperatív módon kell eljárni a váratlan biztonsági zavarok kezelése érdekében. Meg kell osztaniuk a fenyegetésekkel és sebezhetőségekkel kapcsolatos információt, és megfelelő eljárásokat kell alkalmazni a gyors és hatékony együttműködés érdekében, hogy a váratlan biztonsági zavarokat megelőzzék, észleljék, illetve ezekre válaszintézkedéseket tegyenek. Megengedhető esetben ez határon keresztül történő információmegosztást és kooperációt is magában foglalhat.

4) Etika

A résztvevőknek tiszteletben kell tartaniuk mások jogos érdekeit

Abból a tényből kiindulva, hogy az információs rendszerek és hálózatok társadalmunkat áthatják, a résztvevőknek fel kell ismerniük, hogy cselekedeteik, vagy azok hiánya mások számára káros lehet. Ennélfogva az etikus magatartás kritikus fontosságú, és a résztvevőknek törekedniük kell arra, hogy kialakítsák és elfogadják az erre vonatkozó legmegfelelőbb gyakorlatokat, és hogy olyan magatartásmódot mozdítsanak elő, mely elfogadja a biztonság iránti igényt, és tiszteli a mások jogos érdekeit.

5) Demokrácia

Az információs rendszerek és hálózatok biztonságának összeférhetőnek kell lenni egy demokratikus társadalom lényeges értékeivel

A biztonságot olyan mértékben kell foganatosítani, mely összeférhető a demokratikus társadalmak által elismert értékekkel, beleértve a gondolatok és eszmék cseréjének szabadságát, az információ szabad áramlását, az információ és kommunikáció titkosságát, a személyes adatok megfelelő védelmét, a nyitottságot és az átláthatóságot.

6) Kockázatfelmérés

A résztvevőknek kockázatfelmérést kell végezniük

A kockázatfelmérés azonosítja a fenyegetéseket és a sebezhetőségeket, és ennek megfelelően széleskörűnek kell lennie, hogy a legfőbb belső és külső tényezőket, mint például a technológia, a fizikai és emberi tényezők, politikai irányelvek és harmadik személy által nyújtott biztonsági vonatkozású szolgáltatások, felöleljék. A kockázatfelmérés lehetővé teszi az elfogadható kockázati szint meghatározását, és segítséget nyújt a megfelelő szabályozások kiválasztásában az információs rendszerek és hálózatok kockázatának és potenciális károsodásának kezelésére, a megvédendő információ jellege és fontossága fényében. Az információs rendszerek növekvő kölcsönös összeköttetése miatt, a kockázatfelmérésnek tartalmaznia kell a másoktól származó, vagy a mások részére okozható potenciális károk tekintetbe vételét.

7) Biztonságtervezés és végrehajtás

A résztvevőknek a biztonságot az információs rendszerek és hálózatok lényeges elemeként kell beépíteniük.

A rendszereket, hálózatokat és politikai irányelveket megfelelően kell megtervezni, alkalmazni és koordinálni a biztonság optimalizálása érdekében. A jelen erőfeszítés fő, de nem kizárólagos fókuszpontja a megfelelő óvintézkedések és megoldások tervezése és elfogadása annak érdekében, hogy az azonosított fenyegetésekből és sebezhetőségekből származó potenciális károsodást elkerüljék vagy korlátok közé szorítsák. Mind technikai, mind nem technikai óvintézkedésekre és megoldásokra szükség van, s ezeknek arányosnak kell lenniük a szervezet rendszereiben és hálózataiban található információ értékével. A biztonság az összes termék, szolgáltatás, rendszer és hálózat alapvető elemét, valamint a rendszertervezés és architektúra szerves részét kell, hogy képezze. A végfelhasználók számára a biztonságtervezés és alkalmazás nagyrészt a termékeknek és szolgáltatásoknak a rendszerük számára történő kiválasztásából és konfigurálásából áll.

8) Biztonságszervezés

A résztvevőknek átfogó megközelítést kell alkalmazniuk a biztonságszervezés irányában

A biztonságszervezésnek a kockázatfelmérésre kell alapulnia, és dinamikusnak kell lennie, mely felöleli a résztvevők tevékenységének minden szintjét és működésének minden vonatkozását**.** Előremutató válaszokat kell tartalmaznia a kialakuló fenyegetésekre vonatkozóan, és foglalkoznia kell a véletlen zavarok előrejelzésével, kimutatásával, illetve a velük kapcsolatos válaszintézkedésekkel, a rendszer helyreállításával, a folyamatos karbantartással, ellenőrzéssel és felülvizsgálattal. Az információs rendszerek és hálózatok biztonságával kapcsolatos politikai irányelveket, gyakorlatokat, intézkedéseket és eljárásokat koordinálni és integrálni kell, hogy összefüggő biztonsági rendszer jöjjön létre. A biztonságszervezés követelményei a részvétel szintjétől, a résztvevő szerepétől, a szóban forgó kockázattól és rendszerkövetelményektől függenek.

9) Újraértékelés

A résztvevőknek felül kell vizsgálniuk és újra kell értékelniük az információs rendszerek és hálózatok biztonságát és megfelelő módosításokat kell eszközölniük a biztonsági irányelvek, gyakorlatok, intézkedések és eljárások terén.

Folyamatosan jelennek meg új és változó fenyegetések, valamint sebezhetőségek. A résztvevőknek a biztonság minden vonatkozását folyamatosan felül kell vizsgálni, át kell értékelni és módosítani kell, ezen kialakuló kockázatok kezelése érdekében.

A Tanács ajánlása az információs rendszerek és hálózatok biztonságára való irányelvekkel kapcsolatban

Utban a biztonságkultúra felé

A TANÁCS,

Figyelembe véve a Gazdasági Együttműködési és Fejlesztési Szervezetről szóló 1960. december 14-i Konvenciót, és különösen annak 1 b), 1 c), 3 a) és 5 b) cikkelyeit;

Figyelembe véve a Tanács 1980. szeptember 23-i Ajánlását a személyes információ védelmét és a személyes adatok határokon túli áramlását szabályzó irányelvekre vonatkozóan [C(80)58(végleges)];

Figyelembe véve az OECD-tagországok Kormányai által 1985. április 11-én elfogadott Nyilatkozatot a határokon túli adatáramlásra vonatkozóan [a C(85) 139 Függeléke];

Figyelembe véve a Tanács 1997. március 27-i ajánlását a Kriptográfiai Eljárásokra Vonatkozó Irányelvekkel kapcsolatban [C(97)62/VÉGLEGES];

Figyelembe véve az 1998. december 7-9-i keltezésű Miniszteri nyilatkozatot a globális hálózatok titkosságának védelméről [a C(98)177/VÉGLEGES Melléklete];

Figyelembe véve az 1998. december 7-9-i keltezésű Miniszteri nyilatkozatot az elektronikus kereskedelem hitelesítésére vonatkozóan [a C(98)177/VÉGLEGES Melléklete];

Felismervén, hogy az információs rendszerek és hálózatok növekvő hasznosságúak és értékűek a kormányok, üzleti vállalkozások, egyéb szervezetek és egyéni felhasználók számára;

Felismervén, hogy az információs rendszerek és hálózatok egyre jelentősebb szerepe, valamint a tőlük való egyre fokozódó függés a stabil és hatékony nemzetgazdaságok és nemzetközi kereskedelem érdekében, valamint a társadalmi, kulturális és politikai életben különleges erőfeszítéseket igényel a beléjük fektetett bizalom védelme és erősítése érdekében;

Felismervén, hogy az információs rendszereket és hálózatokat, valamint világszerte történő elterjedésüket új és növekvő kockázatok kísérik;

Felismervén, hogy az információs rendszerekben és hálózatokban tárolt és a rajtuk keresztül továbbított információk fenyegetésnek vannak kitéve különféle illetéktelen hozzáférés, felhasználás, jogellenes használat, módosítás, rosszhiszemű kódtovábbítás, szolgáltatásmegtagadás vagy rombolás révén, és megfelelő óvintézkedéseket igényelnek;

Felismervén, hogy szükség van az információs rendszerekre és hálózatokra vonatkozó kockázatok, valamint az ilyen kockázatokra válaszintézkedésként alkalmazható politikai irányelvek, gyakorlatok, intézkedések és eljárások tudatosítására, s megfelelő magatartás ösztönzésére, mint kritikus fontosságú lépésre a biztonságkultúra kifejlesztésének útján;

Felismervén, hogy szükség van a jelenlegi politikai irányelvek, gyakorlatok, intézkedések és eljárások felülvizsgálatára, hogy elősegítsék annak biztosítását, hogy megfeleljenek az információs rendszerek és hálózatok fenyegetettsége által kialakuló kihívásoknak;

Felismervén, hogy közös érdekeltség áll fenn az információs rendszerek és hálózatok biztonságának elősegítésére olyan biztonságkultúra réven, mely elősegíti a nemzetközi koordinációt és kooperációt annak érdekében, hogy megfeleljenek a biztonsági hibákból származó potenciális károk által képviselt kihívásoknak, melyek a nemzetgazdaságokat, a nemzetközi kereskedelmet és a társadalmi, kulturális és politikai életben történő részvételt érintik;

Valamint továbbá felismervén, hogy a jelen Ajánlás Függelékében ismertetett, *Az információs rendszerek és hálózatok biztonságára vonatkozó irányelvek: Útban a biztonságkultúra felé* című dokumentum alkalmazása önkéntes és nem befolyásolja a nemzetek szuverenitását;

Továbbá felismervén, hogy a jelen Irányelveknek nem szándéka, hogy azt sugallja, bármely egyedi megoldás létezik a biztonságra nézve, vagy, hogy mely politikai irányelvek, gyakorlatok, intézkedések és eljárások megfelelőek egy adott, különleges helyzetben, hanem az a célja, hogy keretelveket nyújtson annak jobb megértése érdekében, hogy a résztvevők miként húzhatnak hasznot a biztonságkultúra fejlesztéséből, illetve miként járulhatnak hozzá az utóbbihoz.

AJÁNLJA ezen dokumentumot, melynek címe *Az információs rendszerek és hálózatok biztonságára vonatkozó irányelvek: Útban a biztonságkultúra felé* a kormányok, üzleti vállalkozások, egyéb szervezetek és egyéni felhasználók számára, akik információs rendszerek és hálózatok fejlesztésével, nyújtásával, szervezésével és használatával foglalkoznak, valamint, akiknek ilyen rendszerek és hálózatok a tulajdonát képezik.

JAVASOLJA, hogy a Tagországok:

Új politikai irányelveket, gyakorlatokat, intézkedéseket és eljárásokat hozzanak létre, illetve a meglévőket módosítsák, mely tükrözi és figyelembe veszi *Az információs rendszerek és hálózatok biztonságára vonatkozó irányelvek: Útban a biztonságkultúra felé* című dokumentumot egy biztonságkultúra elfogadásával és előmozdításával, amint az Irányelvekben ismertetésre került;

Konzultációs, koordinációs és kooperációs tevékenységeket folytassanak nemzetközi szinten az Irányelvek alkalmazása érdekében;

Az Irányelveket terjesszék az állami és a magánszektor minden részében, beleértve a kormányokat, üzleti vállalkozásokat, egyéb szervezeteket és egyéni felhasználókat, annak érdekében, hogy elősegítsék a biztonságkultúra kialakulását, és az összes érintett felet arra indítsák, hogy felelősséget vállaljanak, és megtegyék a szükséges lépéseket az Irányelvek alkalmazására olyan módon, mely megfelel egyéni szerepüknek;

Tegyék hozzáférhetővé az Irányelveket a nem tagországok részére időben és megfelelő módon;

Ötévenként vizsgálják felül az Irányelveket, hogy elősegítsék a nemzetközi kooperációt az információs rendszerek és hálózatok biztonságával kapcsolatos kérdésekben;

UTASÍTJA az OECD Információs, Számítógép- és Kommunikációpolitikai Bizottságot az Irányelvek alkalmazásának elősegítésére;

A jelen Ajánlás felváltja a Tanács 1992. november 26-i keltezésű ajánlását az Információs Rendszerek Biztonságával kapcsolatos irányelvekre vonatkozóan [C(92)188/VÉGLEGES].

Az eljárás története

A Biztonsági Irányelveket először 1992-ben készítették el, majd 1997-ben felülvizsgálatra kerültek. A jelen felülvizsgálatot 2001-ben végezte el az Információ Biztonságáért és Titkosságáért Felelős Munkacsoport (WPISP) az Információs Számítógépes és Kommunikációs Politikáért Felelős Bizottságtól (ICCP) kapott megbízás alapján, valamint a szeptember 11-i tragédia utóhatásai által sürgetve.

A megszövegezést a WPISP Szakértői Csoportja végezte el, mely 2001. december 10-11-én találkozott Washingtonban, 2002. február 12-13-án Sydneyben és 2002. március 4-én és 6-án Párizsban. A WPISP Párizsban ült össze 2002. március 5-6-án, 2002. április 22-23-án és 2002. június 25-26-án.

A jelenlegi, *Az információs rendszerek és hálózatok biztonságára vonatkozó oecd irányelvek: Útban a biztonságkultúra felé* című dokumentumot az OECD Tanács Ajánlásaként fogadták el a Tanács 2002. július 25-én megrendezett 1037. ülésén.

A kiadvány eredeti angol nyelvű változatának tartalomjegyzéke

(mellékletek, valamint a dobozok, táblázatok és grafikonok jegyzéke nélkül):

Ez az *Áttekintés* egy OECD kiadvány kivonatos fordítása, mely eredeti formájában a következő angol és francia címen került publikálásra:

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité

Az OECD kiadványai és az *Áttekintések* a www.oecd.org/bookshop/ címen állnak rendelkezésre.

Írja be az "overview" szót a "Title search" mezőbe az Online Könyvesbolt honlapján vagy írja be a könyv angol címét (az Áttekintések az eredeti angol nyelvű könyvhöz vannak csatolva).

Az *Áttekintések* készítését a Közügyi és Kommunikációs Igazgatóság jogi és fordítási csoportja végzi.
E-mail: rights@oecd.org / Fax: +33 1 45 24 13 91