AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2013/40/EU IRÁNYELVE

(2013. augusztus 12.)

az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 83. cikke (1) bekezdésére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére [1],

rendes jogalkotási eljárás keretében [2],

mivel:

(1) Ezen irányelv célja, hogy a bűncselekmények tényállására és vonatkozó szankcióikra vonatkozó minimumszabályok megállapítása révén közelítse a tagállamok büntetőjogát az információs rendszerek elleni támadások terén, és hogy javítsa a tagállamok illetékes hatóságai, így a rendőrség és az egyéb bűnüldözési szakszolgálatok, valamint az Unió illetékes szakosított ügynökségei és szervei – például az Eurojust, az Europol és annak a számítástechnikai bűnözés elleni európai központja, valamint az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) – közötti együttműködést.

(2) Az információs rendszerek a politikai, a társadalmi és a gazdasági interakció kulcstényezői az Unióban. A társadalom nagy- és egyre növekvő mértékben függ e rendszerektől. E rendszerek zökkenőmentes működése és biztonsága az Unióban létfontosságú a belső piac és a versenyképes és innovatív gazdaság fejlődése szempontjából. Az információs rendszerek megfelelő szintű védelmének biztosítása részét kell, hogy képezze a számítástechnikai bűnözésre adott büntetőjogi válaszokat kísérő megelőző intézkedések hatékony és átfogó keretének.

(3) Az Unióban és világszinten egyaránt növekvő veszélyt jelentenek az információs rendszerek elleni támadások és különösen a szervezett bűnözéshez kapcsolódó támadások, valamint egyre nagyobb aggodalmat okoz a tagállamok és az Unió kritikus infrastruktúrájának részét képező információs rendszerek elleni terror- vagy politikai indíttatású támadások lehetősége. Ez veszélyezteti a biztonságosabb információs társadalom, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség megvalósítását, ezért uniós szinten kell fellépni ellene, nemzetközi szinten pedig jobb együttműködésre és koordinációra van szükség.

(4) Az Unióban számos olyan kritikus infrastruktúra van, amelyek működési zavara vagy megsemmisítése több tagállamban is komoly következményekkel járna. A kritikus infrastruktúra védelmére irányuló uniós képességek növelésének igényéből nyilvánvalóvá vált, hogy az informatikai támadások elleni intézkedéseket olyan szigorú büntetőjogi szankcióknak kell kiegészíteniük, amelyek tükrözik az ilyen támadások súlyosságát. Kritikus infrastruktúra alatt a tagállamokban található azon eszközöket, rendszereket, illetve azok részeit lehetne érteni, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok, az egészségügy, a biztonság, a védelem, valamint az emberek gazdasági és szociális jólétének fenntartásához – ilyenek például az erőművek, a közlekedési hálózatok és a kormányzati hálózatok –, és amelyek megzavarása vagy megsemmisítése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna valamely tagállamban.

(5) Bizonyított az olyan, egyre veszélyesebb, ismétlődő és átfogó támadások előfordulása, amelyeket a tagállamok szempontjából, vagy a köz- és magánszféra bizonyos feladatai tekintetében gyakran kulcsfontossággal bíró információs rendszerek ellen intéznek. Ezt a tendenciát egyre kifinomultabb módszerek megjelenése, például az ún. „botnetek” létrehozása és használata kíséri, ami egy bűncselekmény több szakaszát foglalja magában, amely szakaszok külön-külön is komoly veszélyt jelenthetnek a közérdekre. Ennek az irányelvnek többek között az a célja, hogy büntetőjogi szankciókat állapítson meg a botnetek létrehozására, vagyis azon cselekményre vonatkozóan, amellyel célzott informatikai támadások révén jelentős számú számítógép felett veszik át a távvezérelt irányítást oly módon, hogy rosszindulatú számítástechnikai programokkal fertőzik meg őket. A botnetként működő fertőzött számítógép-hálózat létrehozását követően a számítógépek tulajdonosainak tudta nélkül aktiválható, hogy olyan átfogó informatikai támadást hajtsanak végre róla, amely az ezen irányelvben említetteknek megfelelően általában súlyos károkat képes okozni. A tagállamok számára lehetővé kell tenni annak meghatározását, hogy nemzeti joguk és gyakorlatuk alapján mi minősül súlyos kárnak, amilyen például a fontos és közérdekű rendszerszolgáltatások megzavarása, jelentős költségek okozása, vagy személyes adatok, illetve különleges adatokinformációk elvesztése.

(6) Az átfogó informatikai támadások jelentős gazdasági károkat okozhatnak, az információs rendszerek és a kommunikáció megszakítása, valamint a kereskedelmi szempontból fontos bizalmas információ vagy más adatok elvesztése, illetve megváltoztatása révén. Különös figyelmet kell fordítani az innovatív kis- és középvállalkozások ilyen támadások veszélyeivel kapcsolatos tájékozottságának növelésére, valamint az említett vállalkozások ilyen támodásokkal szembeni sebezhetőségére, mivel e vállalkozások nagymértékben függnek az információs rendszerek megfelelő működésétől és hozzáférhetőségétől, az információbiztonságra fordítható forrásaik pedig sok esetben korlátozottak.

[1] HL C 218., 2011.7.23., 130. o.

[2] Az Európai Parlament 2013. július 4-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2013. július 22-i határozata.

(7) A tagállamok ezen irányelv alkalmazására vonatkozó következetes megközelítésének biztosítása érdekében fontosak a közös fogalommeghatározások e területen.

(8) Közös megközelítést kell kialakítani a bűncselekmények tényállási elemeire vonatkozóan az információs rendszerhez való jogosulatlan hozzáférés, a rendszereket, illetve adatokat érintő jogellenes beavatkozás, valamint a jogellenes adatszerzés egységesen meghatározott bűncselekménytípusainak bevezetése révén.

(9) Adatszerzés különösen a kommunikáció tartalmának lehallgatása, ellenőrzése vagy figyelemmel kísérése és az adattartalmak közvetlenül, az információs rendszerhez való hozzáférés és az információs rendszer használata által történő, vagy közvetetten, elektronikus megfigyelő vagy lehallgató eszközök révén történő megszerzése.

(10) A tagállamoknak szankciókat kell megállapítaniuk az információs rendszerek elleni támadások esetére. E szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük, és szabadságvesztést és/vagy pénzbüntetést is magukban kell foglalniuk.

(11) Ezen irányelv büntetőjogi szankciókat ír elő a bűncselekményeknek legalább azon eseteire, amelyek nem számítanak kevésbé súlyosnak. A tagállamok számára lehetővé kell tenni annak meghatározását, hogy mi minősül a nemzeti joguk és gyakorlatuk alapján kevésbé súlyos esetnek. Egy eset például kevésbé súlyosnak minősülhet, ha a bűncselekmény által okozott kár és/vagy a köz- vagy magánérdekre – például egy számítógépes rendszer vagy bizonyos számítógépes adatok integritására, egy személy integritására, jogaira vagy egyéb érdekeire – jelentett kockázat jelentéktelen, vagy az eset a jellegéből adódóan nem teszi szükségessé büntetőjogi szankciók kiszabását a jogi határokon belül vagy a büntetőjogi felelősségre vonást.

(12) Az informatikai támadásokban rejlő veszélyek és kockázatok és az információs rendszerek ezzel összefüggő sebezhetőségének felismerése és bejelentése meghatározó eleme az informatikai támadások hatékony megelőzésének és kezelésének, valamint az információs rendszerek biztonsága javításának. A biztonság terén fennálló hiányosságok bejelentését célzó ösztönzők nyújtása révén ennek hatása növelhető. A tagállamoknak arra kell törekedniük, hogy lehetőséget teremtsenek a biztonság terén fennálló hiányosságok jogi feltárására és bejelentésére.

(13) Helyénvaló súlyosabb szankciókat megállapítani, ha az információs rendszer elleni támadást a szervezett bűnözés elleni küzdelemről szóló, 2008. október 24-i 2008/841/IB tanácsi kerethatározat [1] értelmében vett bűnszervezetben követik el, vagy ha a támadás átfogó, azaz jelentős számú információs rendszert érint vagy súlyos kárt okoz, ideértve azokat a támadásokat is, amelyek célja egy botnet létrehozása, vagy amelyeket botnet révén hajtanak végre, és ezáltal súlyos kárt okoznak. Helyénvaló arra az esetre is súlyosabb szankciókat megállapítani, ha a támadás valamely tagállam vagy az Unió kritikus infrastruktúrája ellen irányul.

(14) A számítástechnikai bűnözésre alkalmazott integrált megközelítés egy másik fontos eleme a személyazonosság-lopás és a személyazonossághoz kapcsolódó egyéb bűncselekmények elleni hatékony intézkedések meghozatala. Egy átfogó horizontális uniós eszköz szükségességének felmérése során az ilyen típusú büntetendő magatartással szembeni uniós fellépés szükségessége is fontolóra vehető.

(15) A Tanács 2008. november 27–28-i következtetéseiben jelezte, hogy a tagállamokkal és a Bizottsággal közösen új stratégiát kell kidolgozni, figyelembe véve az Európa Tanács számítástechnikai bűnözésről szóló 2001. évi egyezményét. Ez az egyezmény szolgál a számítástechnikai bűnözés, többek között az információs rendszerek elleni támadásokkal szembeni küzdelem irányadó jogi keretéül. Ez az irányelv az említett egyezményre épül. Kiemelten fontos feladatként kell kezelni azt, hogy valamennyi tagállam esetében mihamarabb lezáruljon az említett egyezmény megerősítésére vonatkozó eljárás.

(16) Mivel a támadásokat a legkülönbözőbb módokon követik el, a hardverek és a számítástechnikai programok pedig gyorsan fejlődnek, ez az irányelv minden olyan eszközre utal, amelyet az ebben az irányelvben felsorolt bűncselekmények elkövetésére lehet használni. Ilyen eszközök lehetnek például az informatikai támadások elkövetésére használt rosszindulatú számítástechnikai programok, köztük azok, amelyek botnetek létrehozására alkalmasak. Lehetséges, hogy egy ilyen eszközt - még abban az esetben is, ha alkalmas, sőt különösen alkalmas az ezen irányelvben meghatározott bűncselekmények valamelyikének elkövetésére - jogszerű céllal állítottak elő, például az információs technológiai termékek megbízhatóságának vagy az információs rendszerek biztonságának tesztelése céljából. Ebben az esetben nem elegendő, ha a szándék az ezen irányelvben meghatározott valamely bűncselekmény objektív kritériumainak teljesítésére irányul; a szándéknak közvetlenül arra kell irányulnia, hogy az eszközt az ezen irányelvben meghatározott bűncselekmények közül egynek vagy többnek az elkövetésére használják fel.

(17) Ezen irányelv nem állapít meg büntetőjogi felelősséget abban az esetben, ha az ezen irányelvben felsorolt bűncselekmények objektív kritériumai teljesülnek, azonban a cselekményeket nem jogsértő szándékkal követték el, például ha az érintett személy nem tud arról, hogy az adott hozzáférés jogosulatlan, vagy ha az információs rendszerek tesztelésével vagy védelmével bízták meg, pl. ha egy társaság vagy egy forgalmazó kijelöl valakit a biztonsági rendszerének a tesztelésére. Ezen irányelvvel összefüggésben az információs rendszerekhez való hozzáférést felhasználói szabályzat vagy szolgáltatási feltételek révén korlátozó szerződéses kötelezettségek vagy megállapodások, valamint a munkáltató információs rendszereihez való magáncélú hozzáféréssel és azok magáncélú használatával kapcsolatos munkaügyi jogviták nem vonhatnak maguk után büntetőjogi felelősséget, amennyiben a hozzáférés az említett körülmények között minősülne jogosulatlannak, és ezáltal a büntetőeljárás kizárólagos alapját képezné. Ez az irányelv nem érinti az információhoz való hozzáférésnek a nemzeti és az uniós jogszabályokban meghatározott jogát, ugyanakkor ez a jog nem szolgálhat az információhoz való jogellenes vagy önkényes hozzáférés igazolásául.

[1] HL L 300., 2008.11.11., 42. o.

(18) Az informatikai támadásokat számos körülmény megkönnyítheti, például ha az elkövetőnek alkalmazotti minőségében hozzáférése van az érintett információs rendszerek részét képező biztonsági rendszerekhez. A nemzeti jog keretében a büntetőeljárás során megfelelően figyelembe kell venni az említett körülményeket.

(19) A tagállamoknak a jogrendszerük által a súlyosító körülményekre vonatkozóan megállapított szabályokkal összhangban súlyosító körülményeket kell meghatározniuk a nemzeti jogukban. A tagállamoknak gondoskodniuk kell arról, hogy a bírák az elkövető elítélésekor figyelembe vehessék e súlyosító körülményeket. Továbbra is a bírák mérlegelési jogkörébe tartozik, hogy e körülményeket a konkrét esetek egyéb tényállási elemeivel együtt miként értékelik.

(20) Ez az irányelv nem szabályozza az általa említett bűncselekményekkel kapcsolatos joghatóság gyakorlásához szükséges feltételeket, mint például az áldozat által a bűncselekmény elkövetésének helyén tett bejelentést, a bűncselekmény elkövetésének helye szerinti államtól érkező feljelentést, vagy azt, hogy az elkövetőt a bűncselekmény elkövetésének helyén nem vonták büntetőeljárás alá.

(21) Ezen irányelvvel összefüggésben a tagállamok és harmadik országok, valamint közjogi szerveik továbbra is maradéktalanul kötelesek a fennálló uniós és nemzetközi kötelezettségekkel összhangban tiszteletben tartani az emberi jogokat és az alapvető szabadságokat.

(22) Ez az irányelv megerősíti az olyan hálózatok fontosságát, mint amilyen a G8 és az Európa Tanács kapcsolattartó pontjainak a hét minden napján 24 órában működő hálózata. Ezeknek a kapcsolattartó pontoknak hatékony segítséget kell tudni nyújtaniuk, ezáltal például elősegítve a rendelkezésre álló vonatkozó információk cseréjét vagy a technikai segítségnyújtást és a jogi információk szolgáltatását a megkereső tagállam szempontjából releváns információs rendszereket és a bennük foglalt adatokat érintő bűncselekményekkel kapcsolatos nyomozások vagy eljárások céljából. A hálózatok zavartalan működésének biztosítása érdekében valamennyi kapcsolattartó pontnak kapacitással kell rendelkeznie ahhoz, hogy egy másik tagállam kapcsolattartó pontjával gyorsított kommunikációt folytasson, többek között képzett és felszerelt személyzet révén. A nagyszabású informatikai támadások végrehajtásának sebességét figyelembe véve minden tagállamnak képesnek kell lennie arra, hogy haladéktalanul válaszoljon a kapcsolattartó pontok hálózatától érkező sürgős megkeresésekre. Ilyen esetekben célszerű lehet, ha az információkérést telefonos kapcsolatfelvétel is kíséri annak érdekében, hogy a megkeresett tagállam gyorsan eleget tudjon tenni a megkeresésnek, és 8 órán belül visszajelzést lehessen adni.

(23) Az információs rendszerek elleni támadások megelőzése és az ellenük folytatott küzdelem során nagyon fontos, hogy a hatóságok együttműködjenek a magánszférával és a civil társadalommal. Ösztönözni és javítani kell a szolgáltatók, a gyártók, a bűnüldöző szervek és az igazságügyi hatóságok közötti együttműködést, a jogállamiság teljes mértékű tiszteletben tartása mellett. Az ilyen együttműködés kiterjedhetne a szolgáltatók által a potenciális bizonyíték megőrzéséhez, az elkövetők azonosítását segítő elemek biztosításához és legvégső esetben az ahhoz nyújtott segítségre is, hogy a nemzeti joggal és gyakorlattal összhangban teljes egészében vagy részben kiiktassák a fertőzött vagy a jogellenes célra használt információs rendszereket vagy funkciókat. A tagállamoknak fontolóra kell venniük azt is, hogy az ezen irányelv hatálya alá tartozó bűncselekményekkel kapcsolatos információk cseréje érdekében együttműködési és partnerségi hálózatokat alakítsanak ki a szolgáltatókkal és a gyártókkal.

(24) Az ezen irányelvben meghatározott bűncselekményekre vonatkozóan összehasonlítható adatokat kell gyűjteni. A megfelelő adatokat az illetékes szakosított uniós ügynökségek és szervek – például az Europol, valamint az ENISA – rendelkezésére kell bocsátani a feladataikkal és az információszükségleteikkel összhangban, hogy uniós szinten átfogóbb képet lehessen kapni a számítástechnikai bűnözés, illetve a hálózat- és információbiztonság problémájáról, és ezáltal hatékonyabb válaszlépések kialakításához lehessen hozzájárulni. A számítástechnikai bűnözéssel kapcsolatos stratégiai elemzéseknek és az általa való fenyegetettség értékelésének az Európai Rendőrségi Hivatal (Europol) létrehozásáról szóló, 2009. április 6-i 2009/371/IB tanácsi határozattal ([1]) összhangban történő elvégzése céljából a tagállamoknak az elkövetők által alkalmazott módszerekre vonatkozó információkat be kell nyújtaniuk az Europolhoz és annak a számítástechnikai bűnözés elleni európai központjához. Az információszolgáltatás elősegítheti a jelenlegi és a jövőbeli fenyegetettség jobb megértését, és ezáltal hozzájárulhat az információs rendszerek elleni támadásokkal szembeni küzdelemmel és a megelőzésükkel kapcsolatos megfelelőbb és célzottabb döntéshozatalhoz.

(25) A Bizottságnak jelentést kell benyújtania ezen irányelv alkalmazásáról, és az ezen irányelv hatályának esetleges kiterjesztésével járó jogalkotási javaslatokat kell tennie, a számítástechnikai bűnözés terén bekövetkező fejlődésre figyelemmel. Ilyen fejlődés lehet az olyan technológiai fejlesztés, amely például az információs rendszerek elleni támadások területén hatékonyabb fellépést tesz lehetővé, vagy amelyek megkönnyítik e támadások megelőzését vagy hatásuk minimalizálását. A Bizottságnak e célból figyelembe kell vennie az érintett szereplők – különösen az Europol és az ENISA – által készített, rendelkezésre álló elemzéseket és jelentéseket.

(26) A számítástechnikai bűnözés elleni hatékony fellépés érdekében fontos az információs rendszerek ellenállóbbá tétele azáltal, hogy az informatikai támadásokkal szembeni hatékonyabb védelmet célzó, megfelelő intézkedések meghozatalára kerül sor. A tagállamoknak meg kell tenniük a szükséges intézkedéseket a kritikus infrastruktúráik részét képező információs rendszerek informatikai támadásokkal szembeni védelme érdekében, aminek részeként mérlegelniük kell az információs rendszereik és a bennük foglalt adatok védelmét. Az információs

([1]) HL L 121., 2009.5.15., 37. o.

rendszerek megfelelő szintű védelmének és biztonságának a jogi személyek általi biztosítása – például a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása esetében a magánélet védelméről, az elektronikus hírközlésről és az adatvédelemről szóló, meglévő uniós jogszabályokkal összhangban – nélkülözhetetlen része a számítástechnikai bűnözés elleni hatékony küzdelemre alkalmazott átfogó megközelítésnek. Az ésszerűen feltárható veszélyekkel és sebezhetőséggel szemben megfelelő mértékű védelmet kell biztosítani, az egyes ágazatokra vonatkozó legkorszerűbb technológiákkal és az adott adatfeldolgozási helyzetekkel összhangban. Az e védelemmel járó költségeknek és terheknek az informatikai támadás által az érintettek számára valószínűen okozható kárral arányosaknak kell lenniük. A tagállamokat ösztönözni kell arra, hogy felelősségre vonással járó, megfelelő intézkedéseket hozzanak arra az esetre, ha valamely jogi személy nyilvánvalóan nem biztosított megfelelő szintű védelmet az informatikai támadásokkal szemben.

(27) A tagállamok jogában és büntetőeljárásaiban az információs rendszerek elleni támadások területére vonatkozó szabályozottság mértékében és módjában fennálló jelentős különbségek akadályozhatják a szervezett bűnözés és a terrorizmus elleni küzdelmet, és megnehezíthetik a hatékony rendőrségi és igazságügyi együttműködést e területen. A modern információs rendszerek transznacionális és határok nélküli jellegéből adódóan az ilyen rendszerek elleni támadások határokon átnyúló természetűek, így hangsúlyozottan sürgős szükség van a büntetőjog e területen történő közelítését célzó további intézkedésekre. Ezen túlmenően az információs rendszerek elleni támadások miatt indított büntetőeljárások összehangolását a joghatóság gyakorlásával kapcsolatos, büntetőeljárások során felmerülő összeütközések megelőzéséről és rendezéséről szóló, 2009. november 30-i 2009/948/IB tanácsi kerethatározat ([1]) megfelelő átültetésével és alkalmazásával kell elősegíteni. Emellett a tagállamoknak az Unióval együttműködve arra kell törekedniük, hogy javítsák a nemzetközi együttműködést az információs rendszerek, a számítógépes hálózatok és a számítógépes adatok biztonsága területén. Az adatátvitel és az adattárolás biztonságára megfelelő figyelmet kell fordítani minden olyan nemzetközi megállapodásban, amely adatcserére is vonatkozik.

(28) A számítástechnikai bűnözés elleni hatékony fellépés szempontjából elengedhetetlen az Unió egészében az illetékes bűnüldöző szervek és igazságügyi hatóságok közötti együttműködés javítása. Ezzel összefüggésben ösztönözni kell az arra irányuló fokozott erőfeszítéseket, hogy az érintett hatóságok megfelelő képzésben részesüljenek a számítástechnikai bűnözéssel és annak hatásával kapcsolatos ismeretek bővítése, valamint az együttműködés és a legjobb gyakorlatok cseréjének előmozdítása érdekében, például az illetékes szakosított uniós ügynökségek és szervek útján. Az említett képzésnek többek között a különböző tagállami jogrendszerekkel, a bűnügyi nyomozás lehetséges jogi és technikai kihívásaival és az érintett nemzeti hatóságok közötti hatáskörmegosztással kapcsolatos tájékozottság növelését kell céloznia.

(29) Ez az irányelv tiszteletben tartja az emberi jogokat és alapvető szabadságokat, és betartja a különösen az Európai Unió Alapjogi Chartájában, valamint az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben kifejezésre juttatott alapelveket, beleértve a személyes adatok védelmét, a magánélet tiszteletben tartásához való jogot, a véleménynyilvánítás és a tájékozódás szabadságát, a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét és a védelemhez való jogot, valamint a bűncselekmények és a szankciók törvényességének és arányosságának az elveit. Ennek az irányelvnek a célja különösen az említett jogok és alapelvek teljes tiszteletben tartásának biztosítása, ezért azt ennek megfelelően kell végrehajtani.

(30) A személyes adatok védelme az EUMSZ 16. cikkének (1) bekezdése és az Európai Unió Alapjogi Chartájának 8. cikke értelmében alapvető jog. Ennélfogva a személyes adatok ezen irányelv végrehajtásával összefüggő feldolgozásának maradéktalanul meg kell felelnie a vonatkozó uniós adatvédelmi jogszabályoknak.

(31) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló jegyzőkönyv 3. cikkével összhangban e tagállamok bejelentették, hogy részt kívánnak venni ennek az irányelvnek az elfogadásában és alkalmazásában.

(32) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, Dánia helyzetéről szóló jegyzőkönyv 1. és 2. cikkével összhangban Dánia nem vesz részt ennek az irányelvnek az elfogadásában, az rá nézve nem kötelező és nem alkalmazandó.

(33) Mivel ezen irányelv céljait, nevezetesen azt, hogy az információs rendszerek elleni támadásokat minden tagállamban hatékony, arányos és visszatartó erejű szankciókkal büntessék, valamint hogy az igazságügyi és egyéb illetékes hatóságok közötti együttműködést javítsák és ösztönözzék, a tagállamok nem tudják kielégítően megvalósítani, és ezért a léptékük vagy hatásuk miatt azok uniós szinten jobban megvalósíthatók, az Unió intézkedéseket hozhat az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritás elvének megfelelően. Az említett cikkben foglalt arányosság elvének megfelelően ez az irányelv nem lépi túl az e célok eléréséhez szükséges mértéket.

(34) Ezen irányelv célja az információs rendszerek elleni támadásokról szóló, 2005. február 24-i 2005/222/IB tanácsi kerethatározat ([2]) rendelkezéseinek módosítása és kiterjesztése. Mivel nagyszámú és lényeges módosításra van szükség, az egyértelműség érdekében a 2005/222/IB kerethatározatot az ezen irányelv elfogadásában részt vevő tagállamok tekintetében teljes egészében fel kell váltani,

([1]) HL L 328., 2009.12.15., 42. o.

([2]) HL L 69., 2005.3.16., 67. o.

ELFOGADTÁK EZT AZ IRÁNYELVET:

1. cikk

Tárgy

Ez az irányelv megállapítja az információs rendszerek elleni támadások terén elkövetett bűncselekmények és szankciók meghatározására vonatkozó minimumszabályokat. Célja továbbá az ilyen bűncselekmények megelőzésének elősegítése, valamint az igazságügyi és egyéb illetékes hatóságok közötti együttműködés javítása.

2. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

a) „információs rendszer”: minden olyan eszköz, illetve összekapcsolt vagy kapcsolódó eszközökből álló eszközcsoport, amelyek közül egy vagy több valamely program alapján automatikus adatfeldolgozást hajt végre számítógépes adatokon, valamint a működése, használata, védelme és karbantartása céljából az ezen eszköz vagy eszközcsoport által tárolt, feldolgozott, helyreállított vagy továbbított számítógépes adatokon;

b) „számítógépes adatok”: tények, információk vagy fogalmak megjelenítése olyan formában, amely alkalmassá teszi azokat egy információs rendszer általi feldolgozásra, beleértve azon programokat is, amelyek alkalmasak valamely funkciónak egy információs rendszer általi elvégeztetésére;

c) „jogi személy”: bármely jogalany, amely az alkalmazandó nemzeti jog szerint jogi személynek minősül; ide nem értve a tagállamokat, harmadik országokat, az állami hatáskört gyakorló közjogi szerveket, valamint a nemzetközi közjogi szervezeteket;

d) „jogosulatlanul”: ezen irányelvben említett olyan magatartás, ideértve a belépést, beavatkozást vagy adatszerzést, amelyet a rendszernek vagy a rendszer részének tulajdonosa vagy egyéb jogosultja nem engedélyezett, vagy amelyet a nemzeti jog nem tesz lehetővé.

3. cikk

Információs rendszerekhez való jogellenes hozzáférés

A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszerhez vagy annak egy részéhez való, szándékosan és jogosulatlanul történő hozzáférés legalább a súlyosabb esetekben bűncselekménynek minősüljön akkor, ha a bűncselekményt valamely biztonsági intézkedés megsértésével követték el.

4. cikk

Rendszert érintő jogellenes beavatkozás

A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer működésének számítógépes adatok szándékos és jogosulatlan bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása vagy elrejtése, vagy ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele révén történő súlyos akadályozása vagy megszakítása, legalább a súlyosabb esetekben bűncselekménynek minősüljön.

5. cikk

Adatot érintő jogellenes beavatkozás

A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a valamely információs rendszer számítógépes adatainak szándékos és jogosulatlan törlése, megrongálása, minőségi rontása, megváltoztatása vagy elrejtése, vagy az ilyen adatok szándékos és jogosulatlan hozzáférhetetlenné tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön.

6. cikk

Jogellenes adatszerzés

A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő, szándékos és jogosulatlan megszerzése, legalább a súlyosabb esetekben bűncselekménynek minősüljön.

7. cikk

A bűncselekmények elkövetéséhez használt eszközök

A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a következő eszközök jogosulatlan és bármely, a 3–6. cikkben említett bűncselekmény elkövetéséhez való felhasználásának szándékával való előállítása, árusítása, használatra történő beszerzése, behozatala, forgalomba hozatala vagy egyéb módon történő hozzáférhetővé tétele legalább a súlyosabb esetekben bűncselekménynek minősüljön:

a) olyan számítógépes programok, amelyek elsősorban a 3–6. cikkben említett bármely bűncselekmény elkövetésére készültek vagy lettek átalakítva;

b) olyan számítógépes jelszavak, belépési kódok vagy hasonló adatok, amelyekkel egy információs rendszerhez vagy annak egy részéhez hozzá lehet férni.

8. cikk

Felbujtás, bűnsegély és kísérlet

(1) A tagállamok biztosítják, hogy a 3–7. cikkben említett bűncselekményekre való felbujtás, vagy az azok elkövetéséhez nyújtott bűnsegély bűncselekménynek minősüljön.

(2) A tagállamok biztosítják, hogy a 4. és 5. cikkben említett bűncselekmények elkövetésének kísérlete bűncselekménynek minősüljön.

9. cikk

Szankciók

(1) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a 3–8. cikkben említett bűncselekményeket hatékony, arányos és visszatartó erejű büntetőjogi szankciókkal sújtsák.

(2) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a 3–7. cikkben említett bűncselekmények szabadságvesztéssel legyenek büntetendők, amelynek felső határa – legalább a súlyosabb esetekben – legalább két év.

(3) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a 4. és 5. cikkben említett bűncselekmények – amennyiben azokat szándékosan követték el, és azok egy, a 7. cikkben említett eszköz használata révén jelentős

számú információs rendszert érintettek – szabadságvesztéssel legyenek büntetendők, amelynek felső határa legalább három év.

(4) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a 4. és 5. cikkben említett bűncselekmények szabadságvesztéssel legyenek büntetendők, amelynek felső határa legalább öt év, amennyiben:

a) azokat a 2008/841/IB kerethatározat értelmében vett bűnszervezet keretében követték el, függetlenül az e kerethatározatban meghatározott szankciótól;

b) azok súlyos kárt okoztak; vagy

c) azokat valamely, a kritikus infrastruktúra részét képező információs rendszer ellen követték el.

(5) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy ha a 4. és 5. cikkben említett bűncselekményeket egy másik személy személyes adataival visszaélve követték el egy harmadik fél bizalmának elnyerése céljából, és ezáltal kárt okoztak a személyazonosság jogos tulajdonosának, akkor ezt a nemzeti joggal összhangban súlyosító körülménynek lehessen tekinteni, kivéve, ha e körülmény a nemzeti jog értelmében már egy másik bűncselekményt valósít meg.

10. cikk

A jogi személyek felelőssége

(1) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a jogi személyek felelősségre vonhatók legyenek a 3–8. cikkben említett azon bűncselekményekért, amelyeket akár saját nevében, akár a jogi személy valamely szervének tagjaként eljárva olyan személy követett el a jogi személy javára, aki a jogi személyen belül vezető tisztséget tölt be, amely a következők egyikén alapul:

a) a jogi személy képviseletének joga;

b) a jogi személy nevében történő döntéshozatal joga;

c) a jogi személyen belüli ellenőrzés joga.

(2) A tagállamok megteszik a szükséges intézkedéseket annak érdekében, hogy a jogi személyek felelősségre vonhatók legyenek, amennyiben az (1) bekezdésben említett személy általi felügyelet vagy ellenőrzés hiánya tette lehetővé, hogy az adott jogi személy javára egy neki alárendelt személy a 3–8. cikkben említett valamely bűncselekményt elkövesse.

(3) A jogi személyeknek az e cikk (1) és (2) bekezdése alapján fennálló felelőssége nem zárja ki a büntetőeljárást azon természetes személyek ellen, akik a 3–8. cikkben említett bármely bűncselekményben tettesként, felbujtóként vagy bűnsegédként működtek közre.

11. cikk

A jogi személyekkel szemben alkalmazandó szankciók

(1) A tagállamok megteszik a szükséges intézkedéseket annak érdekében, hogy a 10. cikk (1) bekezdése alapján felelősségre vont jogi személy olyan hatékony, arányos és visszatartó erejű szankciókkal legyen büntetendő, amelyek magukban foglalnak büntetőjogi és nem büntetőjogi pénzbüntetéseket vagy bírságokat, és amelyek magukban foglalhatnak egyéb szankciókat is, mint például:

a) az állami kedvezményekből és támogatásokból való kizárás;

b) a kereskedelmi tevékenység folytatásától való átmeneti vagy végleges eltiltás;

c) a bírósági felügyelet alá helyezés;

d) a bíróság által elrendelt felszámolás;

e) a bűncselekmény elkövetésére használt létesítmények ideiglenes vagy végleges bezárása.

(2) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy a 10. cikk (2) bekezdése alapján felelősségre vont jogi személy hatékony, arányos és visszatartó erejű szankciókkal vagy egyéb intézkedésekkel büntetendő legyen.

12. cikk

Joghatóság

(1) A tagállamok megállapítják joghatóságukat a 3–8. cikkben említett bűncselekmények tekintetében, amennyiben a bűncselekményt:

a) egészben vagy részben a területükön követték el; vagy

b) egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

(2) Az (1) bekezdés a) pontja szerinti joghatóság megállapításakor a tagállamok biztosítják, hogy joghatósággal rendelkezzenek abban az esetben, ha:

a) az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e; vagy

b) a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön.

(3) A tagállamok tájékoztatják a Bizottságot, ha úgy döntenek, hogy a 3–8. cikkben említett, a területükön kívül elkövetett bűncselekményekre vonatkozóan további joghatóságot állapítanak meg, többek között amennyiben:

a) az elkövető szokásos tartózkodási helye a területükön van; vagy

b) a bűncselekményt a területükön letelepedett jogi személy javára követték el.

13. cikk

Információcsere

(1) A tagállamok a 3–8. cikkben említett bűncselekményekre vonatkozó információk cseréjének céljából gondoskodnak saját operatív nemzeti kapcsolattartó pontjuk létrehozásáról, és arról, hogy igénybe veszik a meglévő, a hét minden napján 24 órában rendelkezésre álló operatív kapcsolattartó hálózatot. A tagállamok olyan eljárások működését is biztosítják, amelyek révén sürgős segítségkérés esetén az illetékes hatóság a kézhezvételtől számított 8 órán belül jelezheti legalább azt, hogy teljesíti-e a segítségkérést, valamint hogy ezt milyen formában és várhatóan mikor teszi.

(2) A tagállamok tájékoztatják a Bizottságot az (1) bekezdésben említett kijelölt kapcsolattartó pontjukról. A Bizottság továbbítja ezeket az információkat a többi tagállamnak, valamint az illetékes szakosított uniós ügynökségeknek és szerveknek.

(3) A tagállamok meghozzák a szükséges intézkedéseket annak érdekében, hogy megfelelő jelentéstételi csatornák álljanak rendelkezésre annak elősegítéséhez, hogy az illetékes nemzeti hatóságok felé indokolatlan késedelem nélkül be lehessen jelenteni a 3–6. cikkben említett bűncselekményeket.

14. cikk

Nyomon követés és statisztika

(1) A tagállamok biztosítják egy olyan rendszer meglétét, amely rögzíti, előállítja és rendelkezésre bocsátja a 3–7. cikkben említett bűncselekményekre vonatkozó statisztikai adatokat.

(2) Az (1) bekezdésben említett statisztikai adatoknak legalább a tagállamok által nyilvántartásba vett, a 3–7. cikkben említett bűncselekmények számára és a 3–7. cikkben említett bűncselekmények miatt büntetőeljárás alá vont és elítélt személyek számára vonatkozó, meglévő adatokat kell tartalmaznia.

(3) A tagállamok továbbítják a Bizottsághoz az e cikknek megfelelően gyűjtött adatokat. A Bizottság gondoskodik a statisztikai jelentések egységes áttekintésének közzétételéről, és annak az illetékes szakosított uniós ügynökségeknek és szerveknek történő megküldéséről.

15. cikk

A 2005/222/IB kerethatározat felváltása

Ez az irányelv az elfogadásában részt vevő tagállamok vonatkozásában a 2005/222/IB kerethatározat helyébe lép, a kerethatározat nemzeti jogba történő átültetésére vonatkozó határidővel kapcsolatos tagállami kötelezettségek érintése nélkül.

Az ezen irányelv elfogadásában részt vevő tagállamok vonatkozásában a felváltott 2005/222/IB kerethatározatra való hivatkozásokat az ezen irányelvre való hivatkozásként kell értelmezni.

16. cikk

Átültetés a nemzeti jogba

(1) A tagállamok hatályba léptetik azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek 2015. szeptember 4-ig megfeleljenek.

(2) A tagállamok továbbítják a Bizottságnak azon intézkedések szövegét, amelyek az ezen irányelvből eredő kötelezettségeket nemzeti jogukba átültetik.

(3) Amikor a tagállamok elfogadják ezeket az intézkedéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

17. cikk

Jelentés

A Bizottság 2017. szeptember 4-ig jelentést nyújt be – szükség esetén jogalkotási javaslatok kíséretében – az Európai Parlamentnek és a Tanácsnak, amelyben értékeli, hogy a tagállamok milyen mértékben tették meg a szükséges intézkedéseket annak érdekében, hogy ezen irányelvnek megfeleljenek. A Bizottság figyelembe veszi a számítástechnikai bűnözés területére vonatkozó technikai és jogi fejleményeket is, különösen ezen irányelv hatályára való tekintettel.

18. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

19. cikk

Címzettek

Ennek az irányelvnek a Szerződéseknek megfelelően a tagállamok a címzettjei.

Kelt Brüsszelben, 2013. augusztus 12-én.

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*
M. SCHULZ	L. LINKEVIČIUS