A BIZOTTSÁG (EU) 2018/151 VÉGREHAJTÁSI RENDELETE

(2018. január 30.)

a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelvre [1] és különösen annak 16. cikke (8) bekezdésére,

mivel:

(1) Az (EU) 2016/1148 irányelv értelmében a digitális szolgáltatók továbbra is szabadon hozhatnak olyan műszaki és szervezeti intézkedéseket, amelyeket a hálózati és információs rendszerek biztonságát fenyegető kockázat kezeléséhez megfelelőnek és arányosnak tartanak, amennyiben ezek az intézkedések megfelelő biztonsági szintet biztosítanak és figyelembe veszik az említett irányelvben előírt elemeket.

(2) A megfelelő és arányos műszaki és szervezeti intézkedések meghatározásakor a digitális szolgáltatónak kockázatalapú megközelítést alkalmazva, módszeresen kell eljárnia az információbiztonság tekintetében.

(3) A digitális szolgáltatóknak a rendszerek és a létesítmények biztonságának garantálása érdekében értékelő és elemző eljárásokat kell végezniük. E tevékenységek során foglalkozniuk kell a hálózati és információs rendszerek szisztematikus irányításával, a fizikai és környezeti biztonsággal, az ellátás biztonságával és a hozzáférés ellenőrzésével.

(4) A digitális szolgáltatókat arra kell ösztönözni, hogy a hálózati és információs rendszerek szisztematikus irányítása keretében végzett kockázatelemzés során azonosítsák a konkrét kockázatokat és számszerűsítsék azok súlyosságát, például oly módon, hogy azonosítják a kritikus létesítményeket fenyegető veszélyeket és azoknak a működésre gyakorolt potenciális hatását, továbbá meghatározzák, hogy e veszélyeket hogyan lehet a legeredményesebben csökkenteni a mindenkori képességek és az erőforrásokra vonatkozó követelmények fényében.

(5) Az emberi erőforrásokra vonatkozó előírások vonatkozhatnak a készségek kezelésére, ideértve a biztonsággal kapcsolatos készségek fejlesztésével és a tudatosság növelésével kapcsolatos szempontokat is. A digitális szolgáltatókat arra kell ösztönözni, hogy a biztonságos működésre vonatkozó megfelelő előírásokra irányuló döntéseik során vegyék figyelembe a változásmenedzsmentnek, a sebezhetőség kezelésének, a működési és adminisztratív gyakorlat hivatalossá tételének, valamint a rendszerek feltérképezésének a szempontjait.

(6) A biztonsági architektúrára vonatkozó előírások magukban foglalhatják különösen a hálózatok és a rendszerek szétválasztását, valamint tartalmazhatnak kritikus műveletekre, például adminisztratív műveletekre vonatkozó konkrét biztonsági intézkedéseket. A hálózatok és a rendszerek szétválasztása lehetővé tenné a digitális szolgáltatók számára, hogy különbséget tegyenek az olyan elemek között, mint az ügyfél, az ügyfelek egy csoportja, a digitális szolgáltató vagy harmadik felek tulajdonát képező adatok és számítástechnikai erőforrások.

(7) A fizikai és környezeti biztonság tekintetében hozott intézkedéseknek biztosítaniuk kell az adott szervezet hálózati és információs rendszereinek biztonságát olyan események okozta károkkal szemben, mint lopás, tűz, árvíz és más időjárási hatások, illetőleg távközlési és áramellátási zavarok.

(8) Az áram-, tüzelőanyag és a hűtőanyag-ellátás biztonságára irányuló intézkedések kiterjedhetnek például egy ellátási lánc biztonságára, ezen belül pedig különösen a külsős vállalkozók és alvállalkozók, valamint azok menedzsmentjének biztonságára. A kritikus szolgáltatások és termékek nyomonkövethetősége azt jelenti, hogy a digitális szolgáltató képes azonosítani és nyilvántartani a szóban forgó szolgáltatások és termékek forrását.

(9) A digitális szolgáltatások felhasználóinak körébe olyan természetes és jogi személyeknek kell tartozniuk, akik egy online piactér vagy egy felhőalapú számítástechnikai szolgáltatás ügyfelei vagy előfizetői, vagy kulcsszóalapú keresés végrehajtása céljából online keresőprogramot tartalmazó weboldalt keresnek fel.

[1] HL L 194., 2016.7.19., 1. o.

(10) A biztonsági esemény hatása jelentőségének meghatározásakor az e rendeletben meghatározott jelentős eseményeket a jelentős események nem kimerítő jegyzékének kell tekinteni. A kockázatokkal és biztonsági eseményekkel kapcsolatos bevált gyakorlatra vonatkozó információk összegyűjtése és a biztonsági eseményekkel kapcsolatban tett bejelentésekre vonatkozó szabályok megvitatása szempontjából – amelyekről az (EU) 2016/1148 irányelv 11. cikke (3) bekezdésének i), illetve m) pontja rendelkezik – hasznos volna levonni e rendelet végrehajtásának és az együttműködési csoport munkájának tanulságait. Ennek eredménye egy átfogó iránymutatás lehet a bejelentési paraméterek mennyiségi küszöbértékeire vonatkozóan, amelyek elérésekor életbe lép a digitális szolgáltatóknak az (EU) 2016/1148 irányelv 16. cikke (3) bekezdése szerinti bejelentési kötelezettsége. A Bizottság adott esetben fontolóra veheti az e rendeletben foglalt, jelenleg hatályos küszöbértékek felülvizsgálatát.

(11) Annak érdekében, hogy az illetékes hatóságok értesülhessenek a potenciális új kockázatokról, a digitális szolgáltatókat arra kell ösztönözni, hogy önkéntes alapon jelentsenek be minden olyan eseményt, amelyek számukra addig ismeretlen jellemzőkkel bírtak, legyenek azok új exploitok (sérülékenységet kihasználó módszerek), támadási vektorok vagy támadó felek, sebezhető pontok vagy fenyegetések.

(12) E rendeletet az (EU) 2016/1148 irányelv átültetésének határidejét követő naptól indokolt alkalmazni.

(13) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2016/1148 irányelv 22. cikkében említett hálózati és információs rendszerek biztonsági bizottságának véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Tárgy

Ez a rendelet pontosabban meghatározza azokat az elemeket, amelyeket a digitális szolgáltatóknak figyelembe kell venniük az (EU) 2016/1148 irányelv III. mellékletében említett szolgáltatások nyújtásával összefüggésben általuk használt hálózati és információs rendszerek biztonsági szintjének biztosítását szolgáló intézkedések meghatározásakor és elfogadásakor, valamint tovább pontosítja azokat a paramétereket, amelyeket a digitális szolgáltatóknak figyelembe kell venniük annak meghatározáskor, hogy egy biztonsági esemény jelentős hatást gyakorol-e a szóban forgó szolgáltatások nyújtására.

2. cikk

Biztonsági elemek

(1) Az (EU) 2016/1148 irányelv 16. cikke (1) bekezdésének a) pontjában említett rendszerek és létesítmények biztonsága a hálózati és információs rendszerek, valamint azok fizikai környezetének biztonságát jelenti, és a következő elemeket foglalja magában:

a) a hálózati és információs rendszerek szisztematikus irányítása, ami az információs rendszerek feltérképezését és az információbiztonság kezelésére vonatkozó megfelelő előírások megállapítását jelenti, beleértve a kockázatelemzésre, az emberi erőforrásokra, a működés biztonságára, a biztonsági architektúrára, a biztonságos adat- és rendszerélet-ciklus-kezelésre, valamint a titkosításra és annak kezelésére vonatkozó előírásokat;

b) fizikai és környezeti biztonság, ami azt jelenti, hogy intézkedések állnak rendelkezésre a digitális szolgáltató hálózati és információs rendszerei biztonságának károkkal szembeni védelme céljából egy olyan, valamennyi fenyegetésre kiterjedő kockázatalapú megközelítés alkalmazásán keresztül, amely foglalkozik egyebek mellett a rendszermeghibásodásokkal, az emberi mulasztásokkal, a rosszhiszemű tevékenységekkel és a természeti eseményekkel;

c) az ellátás biztonsága, ami azt jelenti, hogy megfelelő előírásokat határoznak meg és tartanak fenn a szolgáltatásnyújtáshoz felhasznált kritikus szolgáltatások és termékek hozzáférhetőségének és adott esetben nyomonkövethetőségének a biztosítása érdekében;

d) a hálózati és információs rendszerekhez való hozzáférés ellenőrzése, amely olyan intézkedések rendelkezésre állását jelenti, amelyek biztosítják, hogy a hálózati és információs rendszerekhez való fizikai és logikai hozzáférést – ideértve a hálózati és információs rendszerek adminisztratív biztonságát is – üzleti és biztonsági követelmények alapján engedélyezzék, illetve korlátozzák.

(2) A digitális szolgáltató által az (EU) 2016/1148 irányelv 16. cikke (1) bekezdésének b) pontjában említett biztonsági-esemény-kezelés tekintetében hozott intézkedések a következőket foglalják magukban:

a) a rendellenes események kellő időben történő és megfelelő tudatosítása érdekében karbantartott és tesztelt felderítési folyamatok és eljárások;

b) az események bejelentésére, valamint információs rendszerei hiányosságainak és sebezhető pontjainak feltárására vonatkozó eljárások és előírások;

c) a megállapított eljárásoknak megfelelő reagálás, valamint a meghozott intézkedés eredményeinek bejelentése;

d) a biztonsági esemény súlyosságának értékelése, a biztonsági események elemzéséből származó ismeretek dokumentálása és az olyan releváns információk összegyűjtése, amelyek bizonyítékként szolgálhatnak és támogathatják a folyamatos fejlesztési folyamatot.

(3) Az (EU) 2016/1148 irányelv 16. cikke (1) bekezdésének c) pontjában említett üzletmenetfolytonosság-menedzsment a szervezet azon képességét jelenti, hogy egy zavart okozó biztonsági eseményt követően elfogadható, előre meghatározott szinteken fenntartsa, illetve adott esetben ilyen szintekre visszaállítsa a szolgáltatásnyújtást, és a következőket foglalja magában:

a) üzleti hatásvizsgálaton alapuló vészhelyzeti tervek létrehozása és használata a digitális szolgáltatók által nyújtott szolgáltatások folytonosságának biztosítása érdekében, amelyeket például gyakorlatok útján rendszeres időközönként értékelni és tesztelni kell;

b) katasztrófaelhárítási képességek, amelyeket például gyakorlatok útján rendszeres időközönként értékelni és tesztelni kell.

(4) Az (EU) 2016/1148 irányelv 16. cikke (1) bekezdésének d) pontjában említett monitoring, ellenőrzés és vizsgálat a következőkre vonatkozó előírások megállapítását és fenntartását foglalja magában:

a) megfigyelések vagy mérések tervezett sorrendjének végrehajtása annak értékelésére, hogy a hálózati és információs rendszerek rendeltetésszerűen működnek-e;

b) annak vizsgálata és ellenőrzése, hogy betartják-e az előírásokat és iránymutatásokat, a nyilvántartások pontosak-e, és teljesülnek-e a hatékonyságra és az eredményességre vonatkozó célkitűzések;

c) olyan eljárás, amelynek célja feltárni a hálózati és információs rendszer biztonsági mechanizmusainak hiányosságait az adatok védelme és a rendeltetésszerű működés fenntartása érdekében. Ez az eljárás magában foglalja az egymást követő műveletek részét képező műszaki eljárásokat és személyzetet.

(5) Az (EU) 2016/1148 irányelv 16. cikke (1) bekezdésének e) pontjában említett nemzetközi szabványok az 1025/2012/EU európai parlamenti és tanácsi rendelet ([1]) 2. cikke (1) bekezdésének a) pontjában említett nemzetközi szabványügyi testület által elfogadott szabványok. Az (EU) 2016/1148 irányelv 19. cikke értelmében a hálózati és információs rendszerek biztonságának szempontjából releváns európai vagy nemzetközileg elfogadott szabványok és előírások is alkalmazhatók, ideértve a meglévő nemzeti szabványokat is.

(6) A digitális szolgáltatók gondoskodnak azon megfelelő dokumentumok rendelkezésre állásáról, amelyek lehetővé teszik az (1), (2), (3), (4) és (5) bekezdésben meghatározott biztonsági elemek megfelelőségének illetékes hatóság általi ellenőrzését.

3. cikk

A biztonsági események hatása jelentőségének megállapításakor figyelembe veendő paraméterek

(1) A biztonsági esemény által érintett, az (EU) 2016/1148 irányelv 16. cikke (4) bekezdésének a) pontjában említett felhasználók száma tekintetében, különös tekintettel azon felhasználókra, akik az érintett szolgáltatásra alapozzák a saját szolgáltatásaik nyújtását, a digitális szolgáltatónak képesnek kell lennie az alábbiak valamelyikének megbecslésére:

a) azon érintett természetes és jogi személyek száma, akikkel a szolgáltatásnyújtásra vonatkozó szerződést kötöttek; vagy

b) a szolgáltatást a múltban igénybe vevő érintett felhasználók száma, elsősorban a korábbi forgalmi adatok alapján.

(2) A biztonsági esemény 16. cikk (4) bekezdésének b) pontjában említett időtartama az az időszak, amely a megfelelő szintű szolgáltatásnak a rendelkezésre állás, a hitelesség, a sértetlenség és a bizalmasság szempontjából vett megszakításától a szolgáltatás helyreállításáig tart.

(3) Ami az (EU) 2016/1148 irányelv 16. cikke (4) bekezdésének c) pontja szerinti, a biztonsági esemény által érintett terület földrajzi kiterjedését illeti, a digitális szolgáltatónak meg kell tudnia állapítani, hogy az esemény befolyásolja-e szolgáltatásainak meghatározott tagállamokban történő nyújtását.

(4) Az (EU) 2016/1148 irányelv 16. cikke (4) bekezdésének d) pontjában említett, a szolgáltatás működésében támadt zavar mértékét az esemény által károsított következő jellemzők közül egy vagy több vonatkozásában kell mérni: az adatok vagy a kapcsolódó szolgáltatások rendelkezésre állása, hitelessége, sértetlensége, illetve bizalmassága.

([1]) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről (HL L 316., 2012.11.14., 12. o.).

(5) Az (EU) 2016/1148 irányelv 16. cikke (4) bekezdésének e) pontja szerinti, a gazdasági és társadalmi tevékenységekre gyakorolt hatás mértéke tekintetében a digitális szolgáltatónak olyan információk alapján, mint az ügyféllel fennálló szerződéses viszonyának jellege vagy adott esetben az érintett felhasználók lehetséges száma, meg kell tudnia állapítani, hogy az esemény például az egészség, a biztonság vagy a vagyoni kár tekintetében jelentős anyagi, illetve nem anyagi veszteséget okozott-e a felhasználók számára.

(6) Az (1), (2), (3), (4) és (5) bekezdés alkalmazásában nem írható elő a digitális szolgáltatók számára olyan kiegészítő információk gyűjtése, amelyekhez nem rendelkeznek hozzáféréssel.

4. cikk

Jelentős hatású esemény

(1) A biztonsági esemény akkor tekinthető jelentős hatásúnak, ha az alábbi helyzetek közül legalább az egyik előáll:

a) a digitális szolgáltató által nyújtott szolgáltatás több mint 5 000 000 felhasználóóra erejéig nem érhető el, ahol a „felhasználóóra” kifejezés az esemény által hatvan perces időszak alatt az Unió területén érintett felhasználók számát jelenti;

b) az esemény következtében sérül a tárolt, továbbított vagy feldolgozott adatok vagy a digitális szolgáltató hálózati és információs rendszere által nyújtott vagy azon keresztül elérhető, kapcsolódó szolgáltatások sértetlensége, hitelessége vagy bizalmassága, és ez Unió-szerte több mint 100 000 felhasználót érint;

c) az esemény veszélyt jelent a közvédelemre, a közbiztonságra vagy az emberi életre;

d) az esemény az Unió területén legalább egy felhasználó számára 1 000 000 EUR-t meghaladó kárt okoz;

(2) A Bizottság az együttműködési csoport által az (EU) 2016/1148 irányelv 11. cikkének (3) bekezdése szerinti feladatai ellátása során összegyűjtött bevált gyakorlatok, valamint a 11. cikk (3) bekezdésének m) pontja szerinti viták eredménye alapján felülvizsgálhatja az (1) bekezdésben megállapított küszöbértékeket.

5. cikk

Hatálybalépés

(1) Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

(2) Ezt a rendelet 2018. május 10-étől kell alkalmazni.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2018. január 30-án.

a Bizottság részéről

az elnök

Jean-Claude JUNCKER