A PÉNZÜGYI ÁGAZAT DIGITÁLIS MŰKÖDÉSI ELLENÁLLÓKÉPESSÉGE

- **A pénzügyi ágazat digitális működési rezilienciájáról szóló 2022/2554 uniós rendelet által érintett főbb szabályozandó területek:**
  - **követelmények az IKT (információs és kommunikációs technológia) kockázatkezeléssel szemben,**
  - **IKT-vonatkozású események kezelése, osztályozása és bejelentése,**
  - **a digitális működési ellenállóképesség tesztelése,**
  - **harmadik féltől eredő IKT-kockázat kezelése és a felvigyázási keretrendszer,**
  - **információmegosztásra vonatkozó megállapodások.**
- **A rendeletet 2025. január 17-től kell alkalmazni.**
- **Európai felügyeleti hatóságok (ESAs, European Supervisory Authorities):**
  - **Európai Értékpapír-piaci Hatóság (ESMA, European Securities and Markets Authority),**
  - **Európai Bankhatóság (EBA, European Banking Authority),**
  - **Európai Biztosítás- és Foglalkoztatói nyugdíj-hatóság (EIOPA, European Insurance and Occupational Pensions Authority).**

A Kormány T/7730. számon benyújtott törvényjavaslata kapcsán az Infojegyzet ismerteti „a pénzügyi ágazat digitális működési rezilienciájáról” szóló uniós rendelet (DORA) főbb rendelkezéseit.

A pénzügyi ágazat digitális működési rezilienciáját (ellenállóképességét) megalapozó rendelet (EU 2022/2554, továbbiakban rendelet) megalkotását a pénzügyi piacok megnövekedett digitalizációja és az információs és kommunikációs technológián (IKT) alapuló rendszerekkel való összekapcsoltságának megnövekedése indokolta. Ez a tendencia növelte a pénzügyi rendszerek kiszolgáltatottságát, az IKT-kockázatokat, felerősítve a kiber-fenyegetések és az IKT-zavarok, incidensek okozta sérülékenységet.

A pénzügyi szolgáltatások nyújtása során az IKT-rendszerek használata elengedhetetlenné vált, elsősorban az alábbi, kritikus területeken: digitális fizetések, értékpapír-elszámolás és -kiegyenlítés, elektronikus kereskedés, hitelnyújtás és finanszírozás, hitelminősítés, követeléskezelés és mindezen folyamatok háttértevékenysége.

A rendelet hatálya: a pénzügyi intézmények és a számukra harmadik félként IKT-szolgáltatásokat nyújtó vállalatok.

Annak érdekében, hogy nemzeti, nemzetközi és uniós szinten is fokozzák a digitális ellenállóképességet, megállapítsanak standardokat, továbbá összehangolják a felügyeleti és szabályozói munkát az európai felügyeleti hatóságok (továbbiakban EFH-k) javaslatot tettek egy olyan ágazatspecifikus kezdeményezésre, mely biztosítja a pénzügyi szolgáltatási ágazat és azt támogató IKT-szolgáltatásokat nyújtó szektor közös,

1. ábra: Az érintett pénzügyi szervezetek

Forrás: Infoszolg/(EU) 2022/2254 rendelet

harmonizált megerősítését.

Egységes szabálykönyv és felügyeleti rendszer létrehozásával az illetékes hatóságok hatékonyan tudják majd felügyelni az ágazatban felmerülő IKT-kockázatok kezelését. Az egységes szabályozással elhárulhatnak az akadályok a nemzeti fejlesztésekből adódó eltérések okozta ellentmondások, diszharmóniák okozta pénzügy instabilitások egységes kezelése elől.

Az IKT-kockázatkezeléssel szembeni követelmények

A digitális működési ellenállóképesség magas fokú biztosítása érdekében a pénzügyi szervezeteknek rendelkezniük kell erre vonatkozó **vállalati stratégiával**, ami IKT-kockázatkezelési keretrendszert jelent. Ennek a keretrendszernek a feladata a felmerülő IKT-kockázatok gyors, hatékony és átfogó kezelése. **IKT-kockázat**nak minősül minden olyan informatikai (hálózati és információs rendszerek használata során előálló) körülmény, mely veszélyeztetheti ezen rendszerek biztonságát. Ezen felül káros hatásokkal járhat a digitális vagy fizikai környezetre azáltal, hogy veszélyezteti a szolgáltatásnyújtás biztonságát vagy egyéb technológiafüggő folyamatokat, műveleteket.

Az IKT-kockázatkezelési keretrendszer magába foglalja azon stratégiákat, eljárásokat, IKT-protokollokat, szabályzatokat, amelyek valamennyi információs vagyonelem és IKT-eszköz védelméhez szükségesek.

A **digitális működési ellenállóképességre vonatkozó stratégiának** az alábbi követelményeket kell teljesítenie (6. cikk):

- a pénzügyi szervezet kockázatvállalási hajlandóságát összhangba kell hozni az IKT-kockázat toleranciaszintjével;
- a kockázati mérőszámokat és teljesítménymutatókat egyértelműen kell megállapítani;
- az egyes üzleti célkitűzésekhez speciális IKT-referenciaszerkezetet kell rendelni, a szükséges változtatásokat is figyelembe véve;
- az IKT-vonatkozású események megelőzése, észlelése és hatásaik kivédése céljából megelőző mechanizmusokat kell beépíteni;
- a digitális működési ellenállóképesség aktuális helyzetének elemzése során a bejelentett IKT-események és az eredményes megelőző intézkedések számát is figyelembe kell venni.

A stratégia fontos alkotóeleme a tesztelés, mellyel a rendelet IV. fejezete külön foglalkozik.

A kockázatkezelési keretrendszer további fontos elemei a **biztonsági mentés**re vonatkozó szabályzatok és eljárások, valamint a helyreállítási protokollok. A pénzügyi szervezeteknek olyan biztonsági mentési rendszereket kell létrehozniuk, amelyek nem veszélyeztetik a hálózati és információs rendszerek biztonságát, ugyanakkor biztosítják az adatok rendelkezésre állását, hitelességét és bizalmas kezelését. A biztonsági mentési rendszereknek fizikailag el kell különülniük a forrásoldali IKT-rendszerektől, illetve a központi értéktárak esetében a másodlagos adatfeldolgozási helyszínnel kapcsolatos földrajzi távolság meghatározása szigorú szabályozás alá esik (12. cikk).

IKT-vonatkozású események kezelése, osztályozása, bejelentése

Az IKT-események osztályozása és a kiberfenyegetések jelentőségének megítélése az alábbi szempontok mentén történik (18. cikk):

- az esemény által érintett ügyfelek, pénzügyi partnerek és érintett tranzakciók száma;
- van-e hírnevet érintő hatása az eseménynek;
- az esemény és az általa okozott leállás időtartama;
- az esemény földrajzi kiterjedése;
- az adatvesztés mértéke;
- az érintett szolgáltatások kritikusságának foka;
- az esemény gazdasági hatása, közvetlen és közvetett költségei.

Tesztelés

A digitális működési ellenállóképesség tesztelése a keretrendszer fontos eleme. A pénzügyi szervezeteknek a tesztelésre megbízható és átfogó programot kell készíteniük; és biztosítaniuk kell, hogy a teszteket független belső vagy külső fél végezze el. Gondoskodniuk kell arról, hogy validált módszertan használjanak és a tervezési és végrehajtási folyamatok során ne merüljenek fel összeférhetetlenségek.

2. ábra: IKT-eszközök és -rendszerek tesztelésének fajtái

Forrás: Infoszolg/(EU) 2022/2254 rendelet

Harmadik féltől eredő IKT-kockázatok kezelése

Azon pénzügyi szervezetek, amelyek harmadik IKT-szolgáltatásokat vesznek igénybe, hasonló felelősséget viselnek a harmadik féltől eredő IKT-kockázatokkal szemben, mint a pénzügyi szolgáltatásokra vonatkozó jogszabályokban előírt kötelezettségeikben. A pénzügyi szervezet IKT-kockázatának kezelése függ a két fél (pénzügyi szervezet és IKT-szolgáltató) függőségének jellegétől, nagyságától, összetettségétől és fontosságától, valamint a vonatkozó szolgáltatások kritikusságától. Mindez a két fél közötti szerződésben kerül megállapításra.

A pénzügyi szervezetek számára a rendelet előírja, hogy **harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát** kell elfogadniuk és azt rendszeresen felülvizsgálniuk.

Fontos előírás továbbá, hogy a harmadik fél IKT-szolgáltatók által nyújtott IKT-szolgáltatások igénybevételéről szóló valamennyi megállapodásról a pénzügyi szervezeteknek naprakész információ-nyilvántartást kell vezetniük. A kritikus vagy fontos funkciókat támogató IKT-szolgáltatásokra vonatkozóan külön nyilvántartást kell vezetni (28. cikk).

A rendelet Preambuluma (63) szerint harmadik fél IKT-szolgáltatónak számítanak azok a szolgáltatók, amelyek a pénzügyi szolgáltatások folyamatos, zavarmentes nyújtását biztosítják az alábbi területeken: felhőalapú számítástechnikai szolgáltatások, szoftverek, adatelemzés, adatközpont-szolgáltatások, pénzforgalmi szolgáltatások, fizetési infrastruktúra biztosítása.

A rendelet újonnan bevezetett elemének (31. cikk) tekinthető a kulcsfontosságú vagy **kritikus harmadik fél IKT-szolgáltatók** nevesítésének követelménye, mely szolgáltatókat a felügyeleti hatóságok jelölik ki, az alábbi kritériumok alapján:

- tevékenységük rendszerszintű hatással van a pénzügyi szervezet szolgáltatásainak stabilitására, folytonosságára és minőségére;
- ha az IKT-szolgáltatást igénybe vevő pénzügyi szervezet globális rendszerszinten jelentős intézménynek számít;
- ha kritikus vagy fontos funkciót lát el a pénzügyi szervezet az érintett harmadik fél IKT-szolgáltató igénybevételével;
- ha a harmadik fél IKT-szolgáltató helyettesíthetősége nem valós alternatíva.

IKT-koncentrációs kockázatnak nevezi a rendelet a harmadik fél IKT-szolgáltatóval szembeni kritikus kitettséget, ami olyan mértékű függőséget jelent a pénzügyi szervezet számára, hogy a szolgáltató rendelkezésre nem állása, meghibásodása vagy más hiányossága veszélyezteti a pénzügyi szervezet működési képességét vagy akár az Unió egészének pénzügyi stabilitását.

A felvigyázási keretrendszer

A **felvigyázási keretrendszer** előírásainak megfelelően létrejön a **felvigyázási fórum**, melynek tagjai a felügyeleti hatóságok elnökei, tagállamonként az illetékes hatóságok egy-egy

magas rangú képviselője és megfigyelői státusban a kritikus harmadik fél IKT-szolgáltató felügyeletéért felelős képviselő. A felvigyázási fórum független szakértőkkel együtt dolgozik.

A fórum évente egyszer készít értékelést, mely a kritikus harmadik fél IKT-szolgáltatásokra vonatkozik, értékeli azok tevékenységét, biztosítva a pénzügyi szervezetek digitális működési ellenállóképességét.

A felügyeleti hatóságok nevezik ki a **vezető felvigyázó**t, aki az alábbi hatáskörökkel (35. cikk) rendelkező háromtagú közös felvigyázói hálózatot (KFH) vezeti:

- információkérés a kritikus harmadik fél IKT-szolgáltatótól;
- vizsgálati ellenőrzési jogkör;
- jelentéskérés az előírt intézkedések és korrekciók végrehajtásáról;
- ajánlásokat fogalmazhat meg a szolgáltatók felé.

Információmegosztásra vonatkozó megállapodások

A pénzügyi szervezetek **kiberfenyegetéssel kapcsolatos információkat és hírszerzési információkat** oszthatnak meg egymással, ha azok illetéktelen hozzáférésre, taktikákra, módszerekre, kiberbiztonsági riasztásokra vonatkoznak. Az információ és hírszerzésmegosztásnak arra kell irányulnia, hogy a kiberfenyegetéssel kapcsolatos tudatosság növekedjen, a kiberfenyegetés terjedési képessége csökkenjen vagy megszűnjön, és támogassa a pénzügyi szervek védelmi képességét, fenyegetésészlelési módszereit, mérsékelési stratégiáit, reagálási és helyreállítási megoldásait.

Az információmegosztással kapcsolatos megállapodásoknak rögzíteniük kell, hogy megvédik az megosztott információk érzékenységét, biztosítják az üzleti titoktartást, a személyes adatok védelmét és betartják a versenypolitikára vonatkozó szabályokat.

Források:

- Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról (DORA–Digital Operational Resilience Act)
- dr. Horváth Katalin: DORA rendelet (Fintechzone.hu, 2022–2023. 1., 2., 3., 4. rész)
- Deloitte: EU rendelet a pénzügyi ágazat digitális működési ellenállóképességéről (DORA) - A pénzügyi szektor GDPR-ja? (deloitte.com, 2022. április)
- KMPG: Harmonizált elvárásokat fogalmazott meg a DORA rendelet a pénzügyi szereplők széles körére (kpmg.com, 2023. szeptember)
- PwC Miért releváns az Ön számára a DORA? – (pwc.com, 2023)

Készítette: Horváth Irén
Képviselői Információs Szolgálat
E-mail: infoszolg@parlament.hu

infoszolg

Internet: www.parlament.hu/infoszolg
Intranet: intra.parlament.hu/infoszolg/
Telefon: (1) 441-6486