ISACA CONFERENCE 2026

Tikos Anita

IKT szolgáltatók kezelésével kapcsolatos kihívások a pénzügyi szektorban

2026.06.02.

ISACA
Budapest Chapter

Pénzügyi szektor legfőbb fenyegetettségei (NIS360 ENISA jelentés alapján)

Pénzügyi szektor főbb fenyegetései:

- DDoS
- Ransomware
- Adatlopás
- Csalás (social engineering-vel)

A szektorok érettségét és felkészültségét 3 aspektus jelentősen befolyásolja és alakítja:

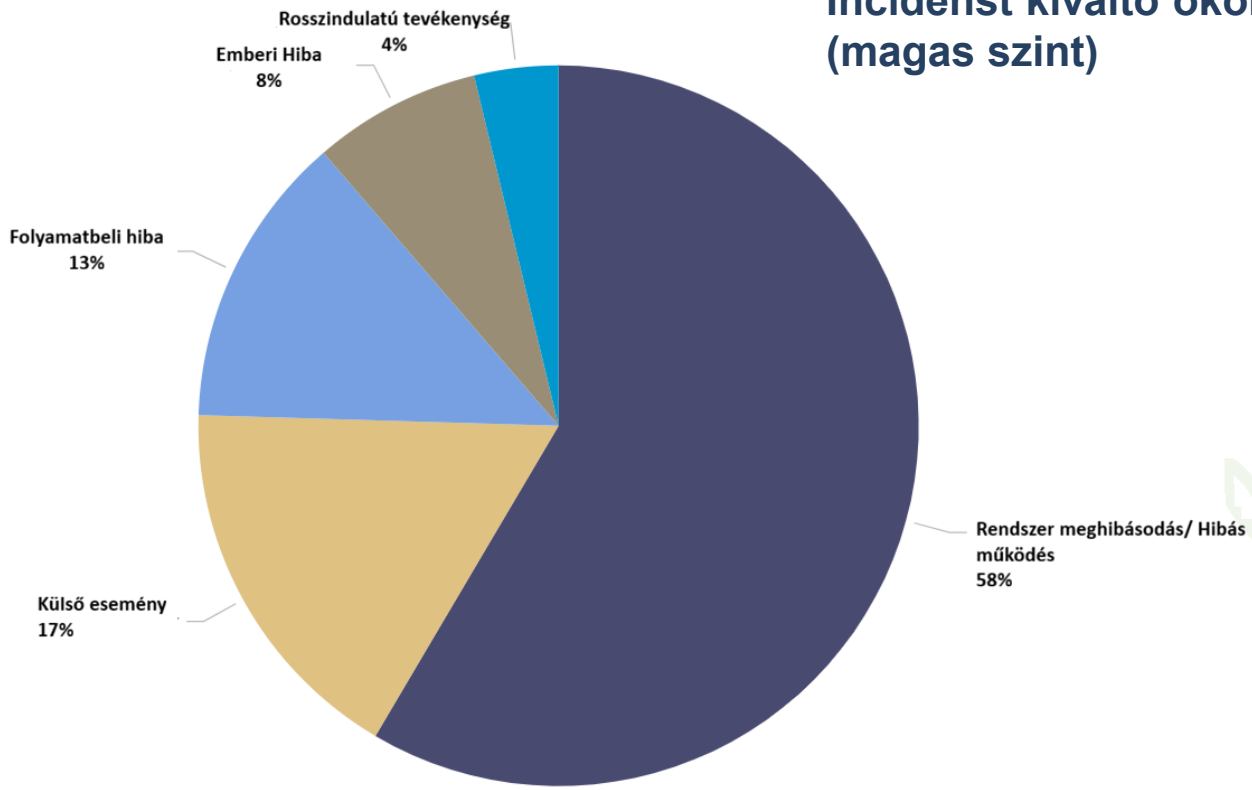
- AI alkalmazásának terjedése
- Szolgáltatói láncok és harmadik fél szolgáltatókkal kapcsolatos kockázatok
- Geopolitikai helyzet

Forrás: ENISA, NIS360 report, 2026.

ISACA Budapest Chapter

Pénzügyi szektor főbb fenyegetettségei Magyarországon

Beküldött incidensek száma	Beküldött bejelentések száma	Beküldött fenyegetések száma	Érintett intézmények száma
107	406	1	31
Kezdeti és időközi állapotú incidensek: 7	Kezdeti: 99, Időközi: 142, Záró: 154,	Nyitott fenyegetettségek: 1	Intézmények (kezdeti és időközi incidenssel): 5



Incidenst kiváltó okok (magas szint)

Külső esemény:

- Természeti katasztrófák
- Harmadik felek által elkövetett hibák
- Egyéb

Rendszer meghibásodás:

- Hardverkapacitás és teljesítmény
- Hardverkarbantartás
- Hardverek elavulása
- Szoftver kompatibilitás/konfiguráció
- Szoftverteljesítmény
- Hálózati konfiguráció
- Fizikai sérülés

ISACA Budapest Chapter

DORA rendelet IKT szolgáltatásokkal kapcsolatos elvárásai

ISACA®
Budapest Chapter

Harmadik fél IKT szolgáltatás

- harmadik fél IKT-szolgáltató: IKT-szolgáltatásokat nyújtó vállalkozás

- **IKT-szolgáltatások:** IKT-rendszerek útján egy vagy több belső vagy külső felhasználó részére folyamatos jelleggel nyújtott digitális és adatszolgáltatások, ideértve a hardvert mint szolgáltatást és a hardverszolgáltatásokat, ami magában foglalja a hardverszolgáltató általi szoftver- vagy belsőrendszervezérlőprogram-(firmware-) frissítéseket is, ide nem értve a hagyományos analóg telefonszolgáltatásokat

- **Segítség: 63. preambulum**
- **Bizottság válasza a Q&A kérdésre: Q&A030 on Definition of ICT services and their interplay with financial services. 2999 - DORA030 - EIOPA**

ISACA Budapest Chapter

Harmadik fél IKT szolgáltatási keretrendszer

IKT harmadik fél szolgáltatók (TPP) kockázatainak kezelésének harmonizálása	• Minimum követelmények meghatározása • Az IKT TPP-k kockázatok teljes körű monitorozása a szerződéses jogviszony teljes életciklusán (átvilágítás, szerződéskötés, teljesítés, megszüntetés)
TPP-vel kötendő szerződéses megállapodások	• **Főbb alapelvek** (arányosság; Pü intézmény felelőssége, dokumentáció) • **Register of information:** intézményi lista a szerződéses TPP-kről (Részletek RTS- ben) • Koncentrációs kockázat előzetes felmérése • Főbb szerződéses követelmények (SLA, adatvédelmi intézkedések, ellenőrzés stb).
Uniós felvigyázói keretrendszer a kritikus IKT harmadik fél szolgáltatókra vonatkozóan	• **Felvigyázó: ESA-k (EBA, EIOPA, vagy ESA-k)** • Kritikus kijelölés: ESA-k által (tagállami adatszolg. alapján) • Felvigyázói Fórum – szektorokon átívelő koordináció az IKT kockázatok vonatkozásában, tagjai az NCA-k i, itt történik a döntések és javaslatok előkészítése • JET: vizsgáló csapat

ISACA Budapest Chapter

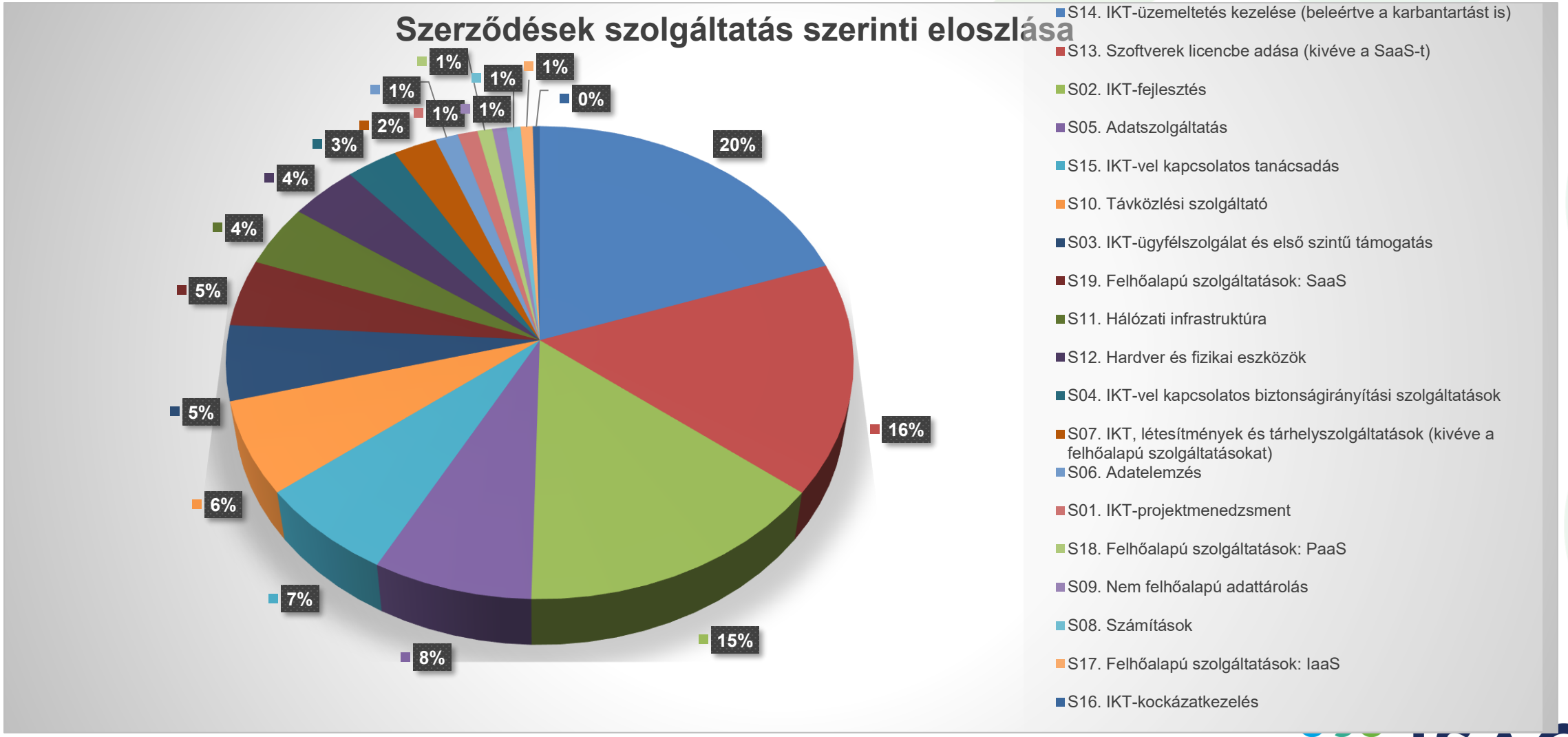
Harmadik féltől eredő IKT-kock. kezelés

- A pénzügyi intézmény **üzleti tevékenysége folytatásához** IKT szolg.-t vesz igénybe, **mindenkor felelősséggel tartozik** a rendelet és egyéb jogszabályokban előírt kötelezettségekért és azoknak való megfelelésért.

- A harmadik féltől eredő IKT-kockázatra vonatkozó stratégiát (kivéve Mini DORA és mikrovállalk.) kell kidolgozni
- A kritikus vagy fontos funkciókat támogató IKT szolgáltatások igénybevételére vonatkozó szabályzat kidolgozása.
- Szolgáltatói szerződések nyilvántartása: RoI
- A vezető testületnek rendszeresen felül kell vizsgálnia a kritikus v. fontos funkciókat támogató IKT szolgáltatások igénybevételéről szóló megállapításokkal kapcsolatos kockázatokat.
- Adatszolgáltatási kötelezettségek:
  - Kritikus vagy fontos funkciót támogató szerződések
  - RoI

ISACA Budapest Chapter

Szerződések szolgáltatás szerinti eloszlása (MNB)



ISACA Budapest Chapter

IKT szolgáltatói keretrendszerrel kapcsolatos tapasztalatok

- IKT szolgáltatás definíciója sok kérdést vet fel, hibás minősítés is gyakori
- Kritikus vagy fontos funkció támogatásának félreértelmezése
- Szolgáltatók több esetben vitatják hogy IKT szolgáltatásnak számít –e a szolgáltatásuk
- Szolgáltató nem ért egyet a funkció besorolással
- Szerződéses követelmények részlegesen érvényesülnek
- BCP, EXIT és RD terveket a szolgáltatóval szeretné elkészíttetni az intézmény
- A szolgáltató felmérését és kockázatelemzését is a szolgáltatótól várja az intézmény
- Kiszervezés és IKT szolgáltatás esetén csak az egyik került alkalmazásra
- DORA addendum:
  - átfogóak és nem elég specifikusak (SLA, incidens kezelés stb.)
  - Egyes aspektusok szerepelnek itt is, a főszerződésben és más addendumban is csak eltérően (pl. adatkezelés helye)
  - Általános: IKT –ra és kritikus vagy fontos funkciót támogató IKT-ra is vonatkoznak (de nem derül ki, hogy mely követelmény érvényesítendő)
  - Alvállalkozói követelmények nem térnek ki az alvállalkozói RTS-ben foglaltakra

ISACA Budapest Chapter

Kritikus szolgáltatók felvigyázása

Feladatok	• IKT kockázatkezelés, fizikai biztonság, irányítás, pü szerveket érő incidenskezelés ellenőrzése • Adathordozhatóság megvalósíthatóságának ellenőrzése • IKT tesztelés ellenőrzése • Nemzeti és nemzetközi szabványok, követelményrendszer alapján
Ellenőrzési jogok	• Dokumentumok, információk bekérése • Ellenőrzések végrehajtása – akár on-site vizsgálat • Riportok kérése • Követelmények megfogalmazása
Nem megfelelés esetén	• **ESA közzéteszi honlapján a meg nem felelést** • **Tájékoztatja a nemzeti felügyeleti hatóságot** • **Harmadik fél szolg.-nak értesítenie kell ügyfeleit a meg nem felelésről** • **Az intézménynek kezelnie kell a kockázatot**
Felvigyázói bírság	• Előírt intézkedésnek való nem vagy részleges megfelelés esetén, • Adatszolgáltatás elmaradása, a hozzáférés és az ellenőrzés megtagadása esetén
Nemzeti szintű végrehajtás	• NCA részvétele a vizsgálati csapatban • **NCA kikényszeríti és nyomon követi a végrehajtást (felügyelt intézmények oldaláról)**

KIJELÖLT KRITIKUS IKT HARMADIK FÉL SZOLGÁLTATÓK

In accordance with Article 31(9) of the Digital Operational Resilience Act, the list of designated critical ICT third-party service providers at Union level (in alphabetic order) is the following:

- Accenture plc
- Amazon web Services EMEA Sarl
- Bloomberg L.P.
- Capgemini SE
- Colt Technology Services
- Deutsche Telekom AG
- Equinix (EMEA) B.V.
- Fidelity National Information Services, Inc.
- Google Cloud EMEA Limited
- International Business Machine Corporation
- InterXion HeadQuarters B.V.
- Kyndryl Inc.
- LSEG Data and Risk Limited
- Microsoft Ireland Operations Limited
- NTT DATA Inc.
- Oracle Nederland B.V.
- Orange SA
- SAP SE
- Tata Consultancy Services Limited

- Kijelölés 2025 november
- RoI-k alapján történt
- 2026-ban begyűjtött RoI alapján akár új kijelölés is lehet Felvigyázás kezdete: 2026
- Munkatervek elfogadásra kerültek

[Forrás: The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act | European Banking Authority]

ISACA Budapest Chapter

Gyakori kérdések

- Ha kritikus IKT szolgáltatóval szerződünk akkor az átvilágítást, kockázatelemzést és ellenőrzést elvégzi helyettünk a felvigyázó?
- Kritikus szolgáltató: intézményi és nemzeti szinten is kell kijelölni?
- Milyen extra feladatokat jelenthet ha kritikus IKT szolgáltatóval szerződünk?
- Kritikus IKT szolgáltatókkal kapcsolatos felvigyázási információk hol találhatóak? (ESAk oldalán pl.: https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/dora-oversight)

ISACA Budapest Chapter

Thank you!