ISACA KONFERENCIA 2026

Kommunikáció mint kiberbiztonsági kontroll: fogalmi hiányok és NIS2 tapasztalatok

Bor Olivér
Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola I EY

2026.06.02.

ISACA
Budapest Chapter

Aktualitás – Kiberfenyegetések mértéke

ENISA Threat Landscape 2025 | Statista 2026 | PurpleSec 2024

+85%

Európai DDoS-támadások növekedése

Éves növekedés (2024. júl. – 2025. jún.)

76,7%

minden EU-s incidens DDoS-támadás (ENISA ETL 2025)

4 875 elemzett incidens (2024.júl. – 2025.jún.)

60%

kezdeti betörési vektorok phishing-alapúak

e-mail, vishing, malspam, malvertising (ENISA ETL 2025)

79,4%

az incidensek ideológiaivezérelt hacktivizmus (DDoS)

AI-alapú phishing: támadások 80%+-ában AI-t alkalmaznak

$15,6T

globális kiberbűnözési kár előrejelzése 2029-re

Meghaladja minden állam GDP-jét az USA és Kína kivételével

38,2%

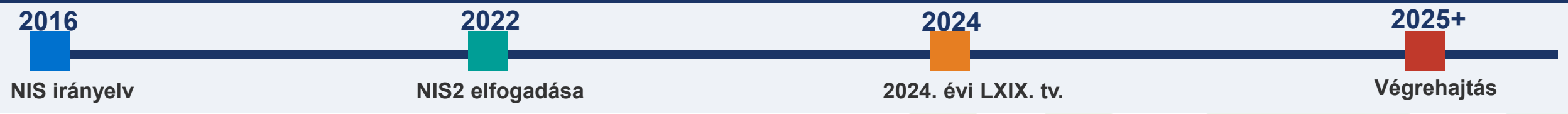
Közigazgatás: az EU-ban legtöbbször célzott ágazat

53,7% incidensek NIS2-esszenciális szervezeteket érint

Forrás: ENISA Threat Landscape 2025 (4 875 incidens, 2024. júl. – 2025. jún.) | Statista 2026 | PurpleSec 2024

ISACA Budapest Chapter

NIS2 és hazai szabályozási kontextus



NIS2 IRÁNYELV – MI VÁLTOZOTT?

- 18 kritikus szektorra terjed ki (korábban sokkal szűkebb érintetti kör)
- Köz- és a piaci szféra egyaránt hatály alatt
- Felsővezetés személyes jogi felelőssége
- Kötelező incidensbejelentés: 24h / 72h / 30 nap
- Szigorúbb szankciók
- Ellátási lánc biztonsága kötelezővé vált

NIS2 Art. 9: Nemzeti kiberkrízis-kezelési keret
- Kiberkrízis-hatóság kijelölése kötelező
- Nemzeti nagyskálájú incidensés krízisválasz-terv

MAGYARORSZÁG – 2024. évI LXIX. TÖRVÉNY

- Felváltja az Ibtv-t és a Kibertantv-t
- Az állami fókusz megszűnt
- Kötelező biztonsági auditok bevezetése, NIST 800-53 rev.5
- Felügyeleti hatóság: NBSZ, SZTFH, MNB, HM
- Kockázatalapú, proaktív biztonsági megközelítés
- Erős végrehajtási hatáskör + szankciók

EU-CyCLONe – operációs szintű koordináció
- Magyarország az EU-ban elsők között implementálta
- KKE-régió: empirikusan feltáratlan vakfolt a szakirodalomban

Forrás: NIS2 irányelv (EU) 2022/2555 | 2024. évi LXIX. tv. | Korm. rendelet 7/2024 | SZTFH rendelet 1/2025 | ENISA (2024): Best Practices for Cyber Crisis Management

ISACA Budapest Chapter

A kommunikáció mint kiberbiztonsági kontroll

Három kommunikációs típus – eltérő logika, eszköz és időhorizont

① Kríziskommunikáció

- Reaktív, időkritikus, jogi kötelezettséghez kötött
- NIS2 Art. 23: 24h / 72h / 1 hónap bejelentési határidők
- ENISA BP#14: egységes és transzparens üzenet – áldozat kommunikációjának támogatása

② Rutinkommunikáció

- Proaktív, megelőzési, edukációs célzatú
- ENISA BP#12: kommunikációs stratégia definiálása előre – formátum, csatornák, időzítés

③ Tudatosságnövelő kampányok

- Hosszú távú magatartásváltozást céloz – legkevésbé vizsgált típus
- H1 hipotézis: tartalom típusa és rendszeressége szignifikánsan hat a tudatosságra

→ **Az irodalomban hiányzó megkülönböztés: ez a kutatás strukturáló elve**

ISACA Budapest Chapter

Fogalmi hiányok a szakirodalomban – öt azonosított kutatási rés

Irodalmi elemzés alapján: Scopus, Elicit | 2024–2025

Rés 1 **H1**

Közszektor kiberbiztonsági tartalom-hatás

- Interaktív vs. passzív tartalom hatásáról nincs empirikus közszektor-adat
- Az irodalom analógián alapul: közegészségügyi és turisztikai kontextusok

Rés 2 **H2**

Célzott kommunikáció hatékonysága

- Összehasonlító vizsgálat hiányzik: célzott vs. Általános
- Közszektor kontextusban egyetlen empirikus forrás sem mérte

Rés 3 **H3**

Kríziskomm. terv → intézményi bizalom

- Equifax/CrowdStrike: csak magánszektor – nem transzferálható
- Közszektorára vonatkozó hatásvizsgálat feltáratlan

Rés 4 **NIS2**

Bejelentési kötelezettség vs. stratégiai érdek

- NIS2 Art. 23: 24h/72h határidő – kommunikációs mozgástér szűkül
- ENISA (2024): feszülség empirikusan feltáratlan

Rés 5 **KKE**

Közép-Kelet-Európa alulreprezentáltsága

- Eriksson (2018): ajánlások 67%-a am. kontextusból ered
- Egyetlen elemzett forrás sem vizsgál KKE esetet

Az irodalomban hiányzik: empirikus közszektor-adat a kiberbiztonsági kommunikáció hatásáról EU/KKE kontextusban.

ISACA Budapest Chapter

Forrás: Scopus, Elicit (2024–2025) | Eriksson (2018) | ENISA (2024): Best Practices for Cyber Crisis Management

Elméleti háttér: a domináns kommunikációs modellek és kiberbiztonsági korlátaik

A meglévő elméleti keretek egyike sem készült kiberbiztonsági kontextusra – integrált keret szükséges.

SCCT

Situational Crisis Communication Theory

Scheiwiller & Zizka (2021)
7 237 Twitter- és sajtóközlemény – reputációközpontú megközelítés

⚠ Korlát: A kibertámadó monitorozhatja az intézmény nyilvános kommunikációját – az SCCT ezt nem kezeli

→ Nem alkalmazható: aszimmetrikus fenyegetési helyzet

SARF + CERC

Social Amplification of Risk Framework + Crisis & Emergency Risk Communication

Panagiotopoulos et al. (2016)
10 020 Twitter-üzenet, 2010-es hóvihar és 2011-es zavargások

⚠ Korlát: Lineáris fázismodell – nem illeszkedik kiberbiztonság diffúz, folyamatos fenyegetési tájképéhez

→ Korlátozott: kiberbiztonság nem fázisos

CT + PMT

Cultivation Theory + Protection Motivation Theory

Tang et al. (2021) ★ egyetlen empirikus kiber-közszektor modell
SEM n=240, kínai WeChat-fiókok: fenyegetéssúlyosság, önhatékonyság, válaszhatékonyság

⚠ Korlát: Kínai digitális/politikai kontextus → KKE-re korlátosan általánosítható

★ **Legközelebb a saját kutatáshoz**

➔ Saját integrált keret: kommunikációelmélet + kiberbiztonsági GRC + viselkedéstudomány

NIS2 implementációs tapasztalatok

ENISA (2024): Háromszintű eszkalációs logika – és a kommunikáció szerepe minden szinten

- Kiberbiztonsági incidens ➔ Nagyskálájú incidens ➔ Kiberkrízis (NIS2 Art. 6 + 16)
- Nagyskálájú: meghaladja 1 tagállam kapacitását / 2+ MS érintett
- Kiberkrízis: nagyrészt POLITIKAI döntés – kockázat-appetítus függvénye (ENISA 2024, p.14)

NIS2 Art. 9 – Nemzeti kiberkrízis-kezelési keret (kötelezettségek 2024-ig)

- Kiberkrízis-kezelő hatóság kijelölése: Magyarországon 4 szereplős struktúra
  - NBSZ NKI | SZTFH | Magyar Nemzeti Bank | Honvédelmi min.
- Nemzeti nagy-skálájú incidens és krízisválasz-terv elfogadása

NIS2 Art. 23 – Bejelentési határidők = kommunikációs feszülség forrása

- 24 óra → Közbenső figyelmeztető értesítés a hatóság felé
- 72 óra → Incidens-értesítés – kézbesíthető információköré korlátozott
- 1 hónap → Zárójelentés – stratégiai kommunikációs érdekekkel feszülségben

ISACA® Budapest Chapter

Stratégiai kommunikáció és közösségi média

Mit tud és mit nem tud az irodalom? – konszenzus vs. korlátok

A közösségi média hatása valós, de mérhetősége korlátozott – és a Twitter-dominancia torzítja az összes ajánlást.

✓ KONSZENZUSOS ÁLLÁSPONTOK

Rasmussen & Ihlen (2017)
200 tanulmány – gyors terjedés, bizalomnyújtás válságban

Cool et al. (2015)
WHO Haiyan tájfun – pre-krízis jelenlét döntő előny; semmiből indulók lassabbak

Riddell (2024)
Hurricane Harvey – intézményi források megbízhatóbbak egyéni fiókoktól

ENISA BP#14 (2024)
Áldozat kommunikációjának támogatása: egységes, transzparens üzenet

⚠ KORLÁTOK ÉS MÓDSZERTANI VAKFOLT

Thackeray (2012)
n=60 áll. hivatal – 1 bejegyzés/nap; kizárólag egyirányú tájékoztatás, nincs dialógus

Giustini et al. (2018)
42 metaelemzés – összességében »minimális« hatás; longitudinális bizonyíték szinte nincs

Terry et al. (2023)
338 tanulmány – Twitter: 99 munka, Facebook: 13, LinkedIn: szinte nulla

ENISA Rec.#5 (2024)
Médiaképézés vezérigazgatói szinten – EU-szinten sem megoldott

Forrás: Rasmussen & Ihlen (2017) | Cool et al. (2015) | Giustini et al. (2018) | Terry et al. (2023) | Riddell (2024) | ENISA (2024)

Budapest Chapter

Kríziskommunikáció kiberbiztonsági incidensaknál

ENISA (2024): 4 fázisú kiberkrízis-kezelési ciklus – a kommunikáció szerepe minden fázisban

A kiberbiztonsági kríziskommunikációnak saját logikája van – és csak egy specifikus keretrendszer létezik rá.

01 Megelőzés
Prevention

BP#1 – Nemzeti kiberkrízis-definíció

- Hollandia: 8 kritérium, határon átnyúló dimenzió hangsúlyozva
- A definíció meghatározza a mozgósítandó erőforrásokat

02 Felkészülség
Preparedness

BP#12 – Kommunikációs stratégia előre

- Hollandia: Nemzeti Kríziskommunikációs Csapat – koordinált időzítés és tartalom
- Formátum + érintett felek + prioritási szintek + csatornák előre definiálva

03 Reagálás
Response

BP#14 – Áldozat kommunikációjának támogatása

- 2017 WannaCry/Renault: első vállalat, amely elismerte az áldozati szerepet
- ANSSI: kerülni kell az okot, felelőst, nyomozási adatokat – időt kell nyerni

04 Helyreállítás
Recovery

BP#16 – Visszacsatolási egység és tanulságok

- Francia kórház 2021 (ransomware): »hotwash« + 30 napos utóértékelés
- Interjúk érintettekkel → összefoglaló + akcióterv a kerét fejlesztésére

Llamas Covarrubias (2025): az egyetlen kiber-specifikus kommunikációs keretrendszer-javaslat

Időbeli közzététel + konzisztens üzenetek + proaktív érintett-bevonás | ISO 27035 / NIST 800-61 / GDPR: kommunikációra korlátozott iránymutatás

Közszektorbeli alkalmazás kihívásai

A közszektor speciális kommunikációs környezete – empirikus megállapítások és ENISA-ajánlások

A közszektorbeli szervek strukturálisan más kommunikációs kihívásokkal néznek szembe – és az ENISA két ajánlása ezt már nevesíti.

SZERVEZÉSI KORLÁTOK

Thackeray (2012)

n=60 állami hivatal

1 bejegyzés/nap, kizárólag egyirányú tájékoztatás, interakció: nulla

Erkkilä & Luoma-aho (2023)

14 vez. kommunikátor, Finnország

Reaktív alkalmazás, nincs szisztematikus social media listening, válság-kényszer

Hoştut et al. (2023)

2 997 tweet elemzése

Egyirányú, felülről lefelé kommunikáció a digitális térben is fennmarad

ENISA AJÁNLÁSOK (2024)

Biztonságos kommunikációs platform

- Vég-vég titkosítás, archiválás, nyílt forráskód
- Németország (BSI): Wire platform – 30+ minisztérium és hatóság
- Informális kommunikációra is ajánlott kriticizálható hely

Médiaképzés vezetői szinten

- Sajtó, rádió, TV, közösségi média – egységes álláspontközlés
- Kiberbiztonsági szakkifejezések általános közönségnek: fő kihívás
- EU-szinten sem megoldott – kutatási gap

JOGI ÉS KULTURÁLIS KORLÁTOK

GDPR

Korlátozza a valós idejű fenyegetési információ-megosztást köz- és magánszektor között

Shan et al. (2015)

Brit és ír élelmiszer-hatóságok: a közösségi médiát »kipipálható lista-elemként« kezelik

Összefoglaló pattern

- Reaktív > proaktív: szervek előre nem terveznek
- Egyirányú > dialog: a párbeszédre nincs kapacitás
- Legal > stratégia: jogi megfelelés előbbre kerül
- Ad hoc > rendszeres: social listening nem szervez.

Forrás: Thackeray (2012) | Erkkilä & Luoma-aho (2023) | Hoştut et al. (2023) | Shan et al. (2015) | ENISA (2024): Best Practices for Cyber Crisis Management

ISACA Budapest Chapter

Hipotézisek és tervezett módszertan

Három hipotézis – közvetlenül a kutatási résekből levezetve

H1: Tartalom típusa + rendszeressége → kiberbiztonsági tudatosság

- Rendszeres + interaktív + edukációs tartalom szignifikánsan hat (Rés 1 lefedése)

H2: Célzott kommunikáció > általános tájékoztatás kockázat-közvétítésben

- Személy re szabott üzenetek hatékonyabbak (Rés 2 lefedése – teljesen nyitott kérdés)

H3: Kríziskommunikációs terv → bizalom + reputációvédelém

- Tervszerű kommunikáció csökkenti negatív hatásokat (ENISA BP#14 + Riddell 2024)

Vegyes módszertan – 4 komponens (2026–2028)

- Kérdőív: n=200-300, közszektor – attítüd + szokás + csatornapreferenciák
- Mélyinterjú: 15-20 fő kiberbiztonsági és kommunikációs szakértők
- Tartalomelemzés: 50-100 hazai közszektorbeli intézmény – rendszeresség, interaktivitás
- Hálózatelemzés: terjedési mintázatok (Bobar et al. 2020: fuzzy AHP-MABAC)

ISACA® Budapest Chapter

Következtetések és tudományos hozzájárulás

A kutatás hozzájárulása – három dimenzióban

① Elméleti újdonság

- Elsőként tárja fel közösségimédia-jellemzők és kiberbiztonsági tudatosság összefüggéseit EU/KKE közszektor-kontextusban
- Integrált kommunikációs keret: krízis / rutin / kampány eltérő logikájának elméleti rögzítése

② Módszertani hozzájárulás

- Vegyes módszertanú protokoll: referenciakeret más kutatók számára is
- Nem csak elérési mutatók: attítüd-, magatartás- és bizalommérés kombinálva

③ Gyakorlati és szabályozási hozzájárulás

- NIS2 / 2024. LXIX. tv.: kommunikációs kötelezettségek teljesítéséhez iránymutatás
- ENISA Rec.#5 implementációjához konkrét hazai empirikus adatok
- V4-régióra adaptálható keret – KKE-s vakfolt lefedése

→ **A kommunikáció nem csupán következmény, hanem KONTROLL – empirikusan igazolandó**

ISACA Budapest Chapter

KÖSZÖNÖM A FIGYELMET!