

## Szemelvények egy felsőoktatási rendszer informatikai védelmének tapasztalataiból

Koczka Ferenc

*Eszterházy Károly Katolikus Egyetem, Információtechnológiai Tanszék,  
Nemzeti Közszoigálati Egyetem, Kiberbiztonsági Tanszék  
[koczka.ferenc@uni-eszterhazy.hu](mailto:koczka.ferenc@uni-eszterhazy.hu).*

### Absztrakt

A felsőoktatásban működő informatikai rendszerek védelmével kapcsolatban meglehetősen kevés tudományos mű áll rendelkezésre. Csak néhány publikusan elérhető nemzetközi forrásban lelhetők fel olyan adatok, melyek részleges képet nyújtanak az oktatási intézményeket érintő informatikai incidensekről. Tekintettel arra, hogy hazai viszonylatban ezek elenyésző mértékben állnak rendelkezésre, a magyar oktatási intézmények kibervédelmi incidenseinek számáról, azok okairól és a támadások motivációiról nincs reális képünk. Adatok hiányában a nemzetközi tapasztalatokra hagyatkozhatunk: az azokból kiolvasható tendenciák várhatóan hazai viszonylatban is érvényesek lehetnek. Cikkemben egy ilyen adatforrás elemzését végzem el.

**Kulcsszavak:** oktatási intézmények védelme, kibervédelem, informatikai incidensek.

### Abstract

There are a limited number of academic resources on the protection of IT systems in higher education. Only a few international public sources provide detailed data, which only give an overview of the number and nature of IT incidents affecting educational institutions. Such data on Hungarian incidents are scarce, so not much is known about cyber security incidents in Hungarian educational institutions and their causes and motivations. In the absence of data, we can rely on international experience, the trends of which may be partly applicable to Hungary.

**Keywords:** protection of educational institutions, cyber defense, IT incidents.

### Bevezetés

Az oktatási intézmények informatikai védelmével kapcsolatos nemzetközi tudományos szakirodalom és adatforrások köre meglehetősen szűkös. Ulven és Wangen 2021-es szakirodalmi áttekintésében [1] 18 tudományos igényű cikket, és 14 egyéb forrást (fehér könyveket, műszaki jelentéseket, szakdolgozatokat, szakmai weboldalakat) kutatott fel. Rahim és szerzőtársai bibliometriai elemzésükben az elmúlt tíz év online forrásból elérhető szakirodalmát vizsgálták. Ezekben 418 dokumentumot azonosítottak, amelyek többségükben nem tudományos igényű cikkek, hanem konferencia előadások voltak, közülük is csak hat volt publikusan is elérhető. A hivatkozott források közt egyetlen magyar sem volt [2], és utalás sem szerepelt a hazai egyetemekre. Bár a hazai és nemzetközi összehasonlításban számos azonosság jelenik meg, melyet a linzi székhelyű Johannes Kepler Universitát-en végzett tanulmányutam is megerősített, a hazai felsőoktatás védelmi kérdéseinek vizsgálatakor számos különbség is feltételezhető. Ezek azonosításához fel kell térképezni a felsőoktatás

értékeit, a szférát érő informatikai incidenseket, sebezhető pontjaikat és azokat a tényezőket, amelyek következtében a védelmi megoldások szükségszerűen eltérnek más területekétől. Külföldi gyakorlatban sem találtam példát kifejezetten oktatási intézményekre szabott szabályzásra, de egyes országokban elindultak olyan folyamatok, melyek a felsőoktatási intézményeket is érintik. A felsőoktatási intézmények jogszabályi környezetében várhatóan a NIS2 irányelv hoz változást [3]. 2016-os elődjének célja a kiberbiztonság javításával kapcsolatos jogszabályi környezet javítása volt, melyet az informatikai rendszereket ért incidensek számának akkori jelentős növekedése indokolt. A NIS2 számos új követelményt fogalmaz meg, miközben a korábbiak szigorítását javasolja, és jelentősen bővíti az érintett intézmények körét is. Deklarálja a biztonsági intézkedések jóváhagyási és felügyeleti feladatkörét, az egyes szervezeti egységek vezetőinek informatikai biztonsági képzését és az intézményi vezetők személyes felelősségét is, emellett a szervezet bevételeivel arányos, nagy összegű bírság kiszabásának lehetőségét írja elő.

### Kiberfenyegetettség a felsőoktatásban

Számos egyetem szenvedett már el különböző típusú informatikai incidenseket. A média kibervédelemmel foglalkozó híreiben szinte alig található oktatási intézmény ellen irányuló támadásról szóló híradás, de az egyetemi informatikai üzemeltetők több ilyenről is beszámolnak. Ezek mennyiségi és súlyossági besorolásához, valamint statisztikai módszerekkel történő elemzésükhöz konkrét adatokra van szükség, ugyanakkor ilyenek alig állnak rendelkezésre. Nemzetközi viszonylatban több, elsősorban amerikai adatforrásokra támaszkodhatunk [4] és az ottani tendenciákból vonhatunk le következtetéseket a várható hazai változásokra is. Az Open Security Foundation szerint az összes biztonsági incidens 35%-a a felsőoktatásban történik, ezt személy szerint túlzónak tartom. Giszczak kutatása szerint [5] 2016 első felében 50%-kal nőtt a felsőoktatási adatokkal kapcsolatos jogsértések száma. Munkájában bemutatja, hogy a reputációs veszteség megjelenik a kutatási támogatások és az adományok megszerzésekor, amelynek mértékét kiszivárgott rekordonként körülbelül 300 dolláros kárként határozza meg.

A Verizon 2022-es „Data Breaches in Education” [6] riportjának az oktatási szférát elemző fejezetének főbb pontjai szerint az USA-ban 1.241 incidens történt, ebből 282-t több forrásból is megerősítettek. Eszerint a rendszerekbe történő belépés, alapvető webes alkalmazások támadása és egyéb hibák a jogsértések 80%-át teszik ki. A betörések 25%-át belső szereplők, 75%-ukat külső támadó kezdeményezi, melyek célja 95%-ban anyagi haszonszerzés, és csak 5%-ban valamilyen kémkedési szándék. Az incidensek 63%-a személyes, 41%-a hitelesítő, 23%-a egyéb, 10%-a pedig belső adatok megszerzésére irányul. A jelentés az összegzésében kiemeli: „Az oktatási szolgáltatások kísértetiesen hasonló tendenciát követnek, mint a többi iparág többsége; drámaian megnövekedett a ransomware-támadások száma, mely a jogsértések több mint 30%-a. Ezen túlmenően ennek az iparágak meg kell védenie magát az ellopt hitelesítő adatokkal és az adatahalász támadásokkal szemben, amelyek potenciálisan felfedhetik az alkalmazottak és diákok személyes adatait”.

A hackmageddon.com<sup>1</sup> havi bontásban közöl statisztikákat a szerkesztő által számos különböző forrásból gyűjtött támadásokról és incidensekről. Ez a forrás sem rendelkezik teljes körű adatbázissal, de a vizsgálatom tárgyaként választott időszakban, 2016 és 2022 között nagyszámú, összesen 12.743 kibervédelmi incidenst dokumentált úgy, hogy

1 Hackmageddon. Lásd: [www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/](https://www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/)

adataiban kiválaszthatók az oktatási intézményeket érintő incidensek és azok részletei is<sup>2</sup>. Ezek elemzése céljából felvettem a kapcsolatot a site üzemeltetőjével, aki kutatási célú hozzáférést biztosított a nyers adataihoz. Sajnos ez nem tartalmazza az oktatási intézmények típusait, így az ez alapján levont következtetések az oktatási szféra egészére érvényesek.

Trendek meghatározhatósága érdekében elsőként az oktatási intézményeket ért incidensek számát évekre bontva gyűjtöttem ki. A NemOkt oszlopban az adott évben ismertté vált, nem oktatási intézményekre irányult adatsértések száma szerepel, melyet az adott év oktatási szférát érintő incidensek száma követ (Okt). A két adat százalékos aránya évről évre mutatja az oktatási intézmények az oktatási szférára irányuló támadások részarányát. Az *Éves részarány* a vizsgált évek összes adatsértésének az adott évre eső arányát írja le, mely az adott évben az adott területre jutó adatsértések számának és az összes támadásnak (11.940, illetve 803) százalékos értékben kifejezett hányadosa.

Év	NemOkt	Okt	%	Éves részarány	
2016	1.082	49	<b>4,5%</b>	9,1%	6,1%
2017	901	68	<b>7,5%</b>	7,5%	8,5%
2018	619	42	<b>6,8%</b>	5,2%	5,2%
2019	1.671	135	<b>8,1%</b>	14,0%	16,8%
2020	2.169	183	<b>8,4%</b>	18,2%	22,8%
2021	2.374	174	<b>7,3%</b>	19,9%	21,7%
2022	3.124	152	<b>4,9%</b>	26,2%	18,9%
Összesen	11.940	803	<b>6,7%</b>	100%	100%

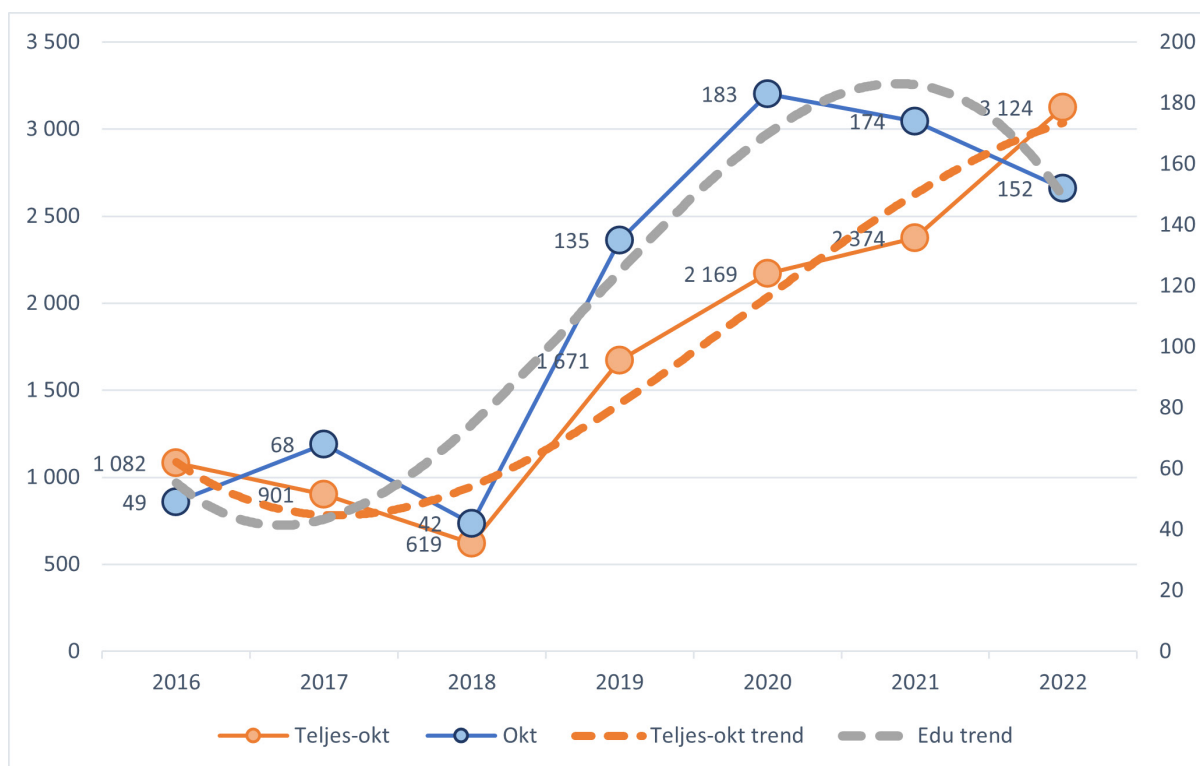
1. táblázat. Az oktatási szektort ért támadások összevetése a támadások teljes számával éves bontásban.

*Forrás: saját szerkesztés a Hackmageddon adatai alapján.*

Az adatok alapján megállapítható, hogy az oktatási intézményeket érő adatsértések aránya a vizsgált időszakban összességében 6,7%, mely az egyes években 4,5-8,4% között változott. Az évről évre emelkedő számú támadások mellett az oktatási szektorra irányuló számok 2021-ben megtorpant, majd csökkenni kezdett. Mindkét adatsort egy diagramban ábrázoltam, melynek pontjait kizárólag a jobb áttekinthetőség érdekében összekötöttem (a két pont közötti értékek alakulásáról az ábra nem ad információt). A diagram az összehasonlíthatóság érdekében az y tengelyen kettős skálázást alkalmaz. Az ábra szaggatott vonalai az adott értéksor harmadfokú regresszióval kifejezett trendjét ábrázolják. Ezek egyértelműen rámutatnak arra, hogy míg a narancsszínnel jelölt, összes támadást leíró trend 2018 óta egyértelmű emelkedő tendenciát követ, az oktatási szektor esetében ez a trend 2021-ben megfordult<sup>3</sup>.

2 A forrás harmadik normálformába alakítása az eredeti adatsorok számának növekedését eredményezte. A közölt adat a folyamat végén keletkezett rekordok száma.

3 A harmadfokú regresszió természeténél fogva nem alkalmazható hosszútávú előrejelzésre, a diagramon szereplő trendvonal a szférát ért támadások csökkenő tendenciáját prognosztizálja.



1. ábra. A támadások teljes és az oktatási szektorra irányuló adatai és változásainak trendje.

Forrás: saját szerkesztés.

Ez a tendencia ellentmond a külföldi szakirodalomban széles körben elemzett, a Covid19 által megkövetelt rapid informatikai változtatások következményeként megvalósított, a távolléti oktatás támogatását szolgáló informatikai fejlesztések biztonságcsökkentő hatásának. Zalat és szerzőtársai tanulmányukban arra a következtetésre jutottak, hogy az online tanulásra való átállás a tanulás támogatásához szükséges informatikai szolgáltatásokban működési zavarokat eredményezett, melyek jellemzően szolgáltatáskiesések vagy szolgáltatás megtagadásos támadások következtében alakultak ki [7]. A 2022-es évben mért csökkenés valószínűsíthető oka pedig az orosz-ukrán háború következményeként a kiberműveletek célpontjainak áthelyezése.

A Hackmageddon adatbázisában a támadások motiváció szerinti besorolását is elvégezték, melyek a Cybercrime (CC), Cyber Espionage (CE), a Cyber Warfare (CW) és a Hacktivism (H) kategóriákba esnek<sup>4</sup>. Ezeket az oktatási intézmények vonatkozásában szintén év szerinti bontásban vizsgáltam annak érdekében, hogy változásuk trendje mellett a támadók motivációinak változásokra is következtetni lehessen. Az adatok elemzése alapján elmondható, hogy az oktatási szférát ért támadásokat a kiberbűnözés, főként az anyagi előnyök megszerzése hajtja. A kiberkémkedésként azonosított esetek kivétel nélkül célzott támadások voltak, melyek többségében a tanulók befolyásolására, vagy kutatóintézeti adatok megszerzésére irányultak. Egy példa erre a 2022.09.01-én rögzített incidens, melynek leírása szerint „Kína feljelenti az Egyesült Államok pekingi nagykövetségét, miután az ország két legjelentősebb kiberhatósága (a kínai Nemzeti Számítógépes Vírus Veszélyhelyzeti Reagáló Központ (CVERC) és a 360 nevű cég) közös jelentésében vádolja a Nemzetbiztonsági Ügynökséget, miszerint érzékeny információkat lopott kínai intézményekből, legfőképp az Északnyugati Műszaki Egyetemről”. Az egyetlen Cyber Warfare eset az orosz-ukrán háborúhoz kötődik: a jelentés szövege szerint „a Wordfence kutatói az orosz megszállás

4 Néhány adat besorolása hiányzott, vagy nem volt egyértelmű, ezeket a táblázatban nem tüntettem fel.

kezdeté óta hatalmas támadási hullámot regisztráltak ukrán WordPress oldalak ellen, céljuk ezek leállítása és általános morál rombolása”. Érdemes megjegyezni, hogy a besorolás nem minden esetben egyértelmű, pl. Vatikán hivatalos honlapjának megtámadását az orosz invázió pápai elítélése után, vagy az NLB hackercsoport által hárommillió orosz iskolás személyes adatainak közzétételét nem a Cyber Warfare-be, hanem a Hacktivizmusba sorolja. Összességében azonban elmondható, hogy ezek szerepe az oktatási szektorban csupán 4%.

	2016	2017	2018	2019	2020	2021	2022	Összesen	%
CC	41	65	40	123	179	173	145	766	95,8%
CE	3	1	1	11	3	1	3	23	2,9%
CW		0	0	0	0	0	1	1	0,1%
H	3	2	0	1	1	0	3	10	1,3%
Összesen	47	68	41	135	183	174	152	800	100,0%
%	5,9%	8,5%	5,1%	16,9%	22,9%	21,8%	19,0%	100,0%	

2. táblázat. Az oktatási szektort ért incidensek motivációinak évek szerinti megoszlása.

*Forrás: Hackmageddon adatai alapján saját szerkesztés.*

A motivációk elemzését érdemes az oktatási szektoron kívül eső intézményekre is megvizsgálni és azzal összehasonlítani. Bár ott is magas a kiberbűnözés aránya (81,2%) ugyanakkor jelentősen nagyobb számban történnek kiberkémkedés vagy hacktivizmus célú esetek. A kiberhadviselés 4,2%-os értéke pedig arra utal, hogy az ilyen indíttatású támadások ellen ebben a szférában lényegesen hatékonyabb védekezést kell folytatni.

A motivációk ismerete nagyban befolyásolhatja a védekezés módszertanának kidolgozását, a védendő rendszerek azonosítását és a védelmükre szolgáló eszközök kiválasztását is. Ez alapján az oktatási intézményeknek elsősorban azokra a rendszerekre kell koncentrálniuk, melyek a támadók számára anyagi haszonszerzés lehetőségét kínálják, tehát érzékeny adatok megszerzésére vagy ransomware aktiválásra irányulnak.

Az adatbázis elemzésével az alkalmazott módszerek is azonosíthatók voltak. A támadók által használt eljárásokat 29 támadási technikába sorolják be, viszont ezek több mint felét a vizsgált időszakban csak egyszer alkalmazták.

Az így kapott adatok elemzésével kimutatható, hogy az oktatási intézményekkel szemben leginkább a malware-re alapozott támadási technikákat alkalmazzák, ezek aránya hozzávetőleg 40%. Bár ez a módszer már 2016-ban is megjelent, alkalmazásának növekvő tendenciája valószínűsíti, hogy az hatékony módszert jelent. Ismeretlen marad a támadási technikák közel negyede, és ennek trendje is erősödött az elmúlt években, ráadásul a támadások egyre nagyobb részét ez a típus teszi ki. Az account hijacking során ellopják vagy átirányítják egy személy valamilyen hozzáférését. Annak ellenére, hogy legnagyobb anyagi hasznot a célzott támadások kivitelezésével lehet elérni, azok száma elenyésző, és releváns változás nem is fedezhető fel a vizsgált időszakban. A Covid19 alatt alkalmazott, a távolléti oktatást segítő szoftverek hibáinak kihasználására a támadók az átálláshoz rendelkezésre álló rövid idő okozta zűrzavart igyekeztek kihasználni.

A további technikák aránya az előzetes feltételezéseimet messze alulmúlták. A sérülékenységek általános kihasználását az adatok alig támasztják alá, és kis számban detektáltak a szektorral szemben kezdeményezett túlterheléses támadást, vagy SQL injection-t. A lista utolsó helyén megjelenő jelszófeltörési eljárást pedig csak három esetben regisztrálták.

Megjegyzendő, hogy ezek az értékek hirtelen megváltozhatnak, amennyiben a szektorban tömegesen alkalmazott szoftver (esetleg hardver) biztonsága sérül. Magyar viszonylatban ilyen incidens volt az eKréta rendszer elleni támadás, mely során egy megtévesztő levél alkalmazásával, rendszerben jelen levő a többszörös konfigurációs hibák kihasználásával végül magyar tanulók adatai nagy mennyiségben szivárogtak ki. Az eset példa nélküli volt, egy közérdekű adatigénylés tanúsága szerint a Nemzeti Adatvédelmi Hatóság felé 2018. február és 2023. március között jelentett 124 esetből 62 az eKréta rendszer feltörésével volt kapcsolatos, ami az összes jelentett incidens 50%-a.

Technika	2016	2017	2018	2019	2020	2021	2022	Össz.	Arány
Malware	3	18	10	71	101	75	75	353	44,1%
Unknown	20	19	13	18	33	54	53	210	26,3%
Account hijacking	9	24	15	33	22	20	14	137	17,1%
Targeted attack	2	2	2	5	2	0	3	16	2,0%
Zoom bombing	0	0	0	0	9	6	0	15	1,9%
Vulnerability	0	0	1	0	0	12	1	14	1,8%
DDOS	2	1	0	0	7	0	0	10	1,3%
Defacement	2	3	0	1	2	1	1	10	1,3%
SQL Injection	5	0	0	0	1	0	0	6	0,8%
Brute Force	1	0	0	2	0	0	0	3	0,4%

3. táblázat. Az oktatási szektort ért releváns támadási technikák évek szerinti eloszlása.

Forrás: Hackmageddon adatai alapján saját szerkesztés.

## Összegzés

A Hackmageddon adatbázisának vizsgálata alapján megállapítható, hogy az elsősorban amerikai, továbbá angol, kanadai, ausztrál, indiai és ír források által szolgáltatott adatok alapján az oktatási intézmények fenyegetettsége 7% körüli mértékre tehető, mely kismértékű ingadozás mellett 2016 óta jelentős mértékben nem változott. A támadók előszeretettel alkalmaznak malware-ekre alapozott támadási módszereket, de lehetőség szerint igyekeznek megszerezni és felhasználni a felhasználók különböző hozzáféréseit. A 2022-ben folyó háború ellenére ezeknek az intézményeknek a kiberhadviselésben nem látszik szerepük. A támadók tevékenysége elsősorban a kibertérre vagy ott elkövetett bűncselekményekre alapozott, így feltehetően az anyagi haszon megszerzésére irányul. Annak ellenére, hogy az elemzésekben bemutatott tendenciák nemzetközi adatokon alapulnak, azok érvényesek lehetnek a hazai intézményekre is, így a bemutatott elemzések és következtetések segíthetik az informatikai rendszerek védelmi pontjainak meghatározását.

## Irodalom

- [1] G. Wangen és J. B. Ulven: „A Systematic Review of Cybersecurity Risks in Higher Education”, *Future Internet*, 1. kötet 13, 1-40 o., 2021.
- [2] N. Rahima, Z. Othmanb és F. Z. Hamidc: „Cyber Security and the Higher Education Literature: A Bibliometric Analysis”, *International Journal of Innovation, Creativity and Change*, 12. kötet 1. szám 2020. 12.
- [3] Az Európai Parlament és a Tanács (EU) 2022/2555 Irányelve, 2022.
- [4] F. Inc.: „Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about It. White paper.”, Fireeye Inc., 2015.



- [5] J. J. Giszczak és D. A. Paluzzi: „Ass or Fail? Data Privacy and Cybersecurity Risks in Higher Education”, McDonald Hopkins, 2016.
- [6] Verizon: „Educational Services,” 2022. [Online]. Elérhető: <https://www.verizon.com/business/resources/reports/dbir/2022/data-breaches-in-education/>. [Hozzáférés dátuma: 2022.04.03.].
- [7] M. Z. Zalat, S. M. Hamed, A. B. Bolbol: „The experiences, challenges, and acceptance of e-learning as a tool for teaching during the COVID-19 pandemic among university medical staff”, *PLoS One*, 16. kötet 1. szám, 1-12. o.
- [8] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 2020.
- [9] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 2013.
- [10] Cyber security and defence European Parliament resolution of 22 November 2012 on Cyber Security and Defence (2012/2096(INI)), 2012.
- [11] *Stratégiai Koncepció az Észak-atlanti Szerződés Szervezete tagállamainak védelméért és biztonságáért.*
- [12] NATO: *Defending the networks - The NATO Policy on Cyber Defence*, 2011.
- [13] D. Appelmann: „California Requires Disclosure of Database Security Breaches”, Usenix, 2004.
- [14] „Australian Government Department of Home Affairs,” 2020. 11. [Online]. Elérhető: <https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf>. [Hozzáférés dátuma: 2022.01.11.].
- [15] 2011. évi CCIV. törvény a nemzeti felsőoktatásról, 2011.
- [16] 2012. évi C. törvény a Büntető Törvénykönyvről, 2012.
- [17] „Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete,” 2016.04.27. [Online]. Elérhető: [https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.HUN&toc=OJ:L:2016:119:FULL119%3AFULL#d1e1459-1-1](https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.HUN&toc=OJ:L:2016:119:FULL119%3AFULL#d1e1459-1-1). [Hozzáférés dátuma: 2022.01.10.].
- [18] National Institute of Standards and Technology, „Framework for Improving Critical Infrastructure Cybersecurity,” 2018.04.16. [Online]. Elérhető: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. [Hozzáférés dátuma: 2019.15.23.].
- [19] P. J. Ballard: „Measuring Performance Excellence: Key Performance Indicators for Institutions Accepted into the Academic Quality Improvement Program (AQIP),” 2013.
- [20] E. K. Kwaa-Aidoo és M. Agbeko: „An Analysis of Information System Security of a Ghanaian University”, *International Journal of Information Security Science*, 7. kötet, 1. szám, 90-99. o., 2017.
- [21] *Rendszeres szociális ösztöndíjakkal kapcsolatos adatkezelés a Budapesti Műszaki és Gazdaságtudományi Egyetemen.*, NAIH/2020/54.
- [22] *Állásfoglalás a koronavírus elleni védetség tényének felsőoktatási intézmény általi megismerhetőségéről, nyilvántarthatóságáról kollégiumi elhelyezés és egyetemi rendezvények kapcsán.*, NAIH-6298-2/2021.
- [23] I. G. Butnaru, V. Nita, A. Anichiti és G. Brînză: „The Effectiveness of Online Education during Covid 19 Pandemic—A Comparative Analysis between the Perceptions of Academic Students and High School Students from Romania”, *Sustainability*, 13. kötet, 9. szám 1-20. o., 2021.
- [24] L. W. Loo: „Student Hacking into University’s Learning Management System to Save His Grades: A Cautionary Tale,” Singapore Management University, Singapore, 2016.
- [25] „Unit-Department for ICT and Joint Services in Higher Education and Research,” Direktoratet for IKT og fellestjenester i høyere tdanning og forskning, Norway, 2019.

- [26] G. Vámosi: „Ezerhét száz hallgató adatait vesztette el a veszprémi egyetem,” 2008.12.10. [Online]. Elérhető: <https://www.origo.hu/techbazis/20081210-1717-hallgato-adatait-vesztette-el-a-veszpremi-egyetem.html>. [Hozzáférés dátuma: 2022.01.10.].
- [27] „Zsarolóvírus-támadás érte a Pázmányt, leállt a Neptun,” HVG, 2020.04.24. [Online]. Elérhető: [https://hvg.hu/tudomany/20200424\\_pazmany\\_peter\\_katolikus\\_egyetem\\_zsarolovirus\\_neptun\\_tanulmanyi\\_rendszer\\_szakdolgozat\\_leadasi\\_hatarido](https://hvg.hu/tudomany/20200424_pazmany_peter_katolikus_egyetem_zsarolovirus_neptun_tanulmanyi_rendszer_szakdolgozat_leadasi_hatarido). [Hozzáférés dátuma: 2022.10.01.].
- [28] Nemzeti Adatvédelmi és Információszabadság Hatóság, „Közérdekű adatigénylés”, 2018. 12.08. [Online]. Elérhető: <https://kimitud.hu/request/12018/response/17739/attach/3/NAIH%202019%20741.pdf>. [Hozzáférés dátuma: 2022.10.12.].





# ÚJ TECHNOLÓGIÁKKAL, ÚJ TARTALMAKKAL A JÖVŐ DIGITÁLIS TRANSZFORMÁCIÓJA FELÉ

32. Networkshop: országos konferencia

2023. április 12–14.  
Pannon Egyetem, Veszprém



# ÚJ TECHNOLÓGIÁKKAL, ÚJ TARTALMAKKAL A JÖVŐ DIGITÁLIS TRANSZFORMÁCIÓJA FELÉ

**32. Networkshop: országos konferencia**

2023. április 12–14.  
Pannon Egyetem, Veszprém

Szerkesztette: Tick József, Kokas Károly, Holl András

HUNGARNET Egyesület  
Budapest, 2023



Szerkesztette: Tick József, Kokas Károly, Holl András

Tipográfia és tördelés: Vas Viktória

Networkshop

2023. április 12–14. Pannon Egyetem, Veszprém konferencia előadásainak közleményei

ISBN 978-615-82243-1-4

DOI: [10.31915/NWS.2023](https://doi.org/10.31915/NWS.2023)

Kiadja a HUNGARNET Egyesület  
az MTA Könyvtár és Információs Központ közreműködésével  
Budapest  
2023

Borítókép: [freepik.com](https://www.freepik.com)

## TARTALOMJEGYZÉK

Előszó.....	5
Király Sándor, Balla Tamás: Flipped classroom az sqlsuli.hu-ban.....	7
Wirágh András: Abaújszántótól Zombolyáig. Megjegyzések egy új sajtóadatbázishoz .....	14
Albert Ágota Katalin: Az EGT-tagállamok adatvédelmi felügyeleti hatóságainak szankcionálási gyakorlata az oktatási szektorban a GDPR alkalmazása óta .....	19
Simon András: Digitális dokumentumok gyűjteménykezelési gyakorlatának támogatása a digitális tartalmak számossága, mérete és féleségeik vizsgálatával .....	24
Bódog András: Az Annif gépi tárgyszavazó rendszer magyarországi adaptációjának feltételei és lehetőségei .....	31
Dezső Krisztina: A Pécsi Egyetemtörténeti Gyűjtemény online adatbázisai és digitális gyűjteményei .....	36
Ungváry Rudolf, Király Péter: Nemzeti könyvtárak és az OSZK MARC21 állományainak összehasonlító elemzése néhány adatmező alapján .....	42
Szemes-Révész Enikő Evelin: Kapocs a tudáshoz – A könyvtár szerepe a civilek és a tudomány kapcsolatában .....	50
Tóth Zoltán: Az RO-Crate alapú kutatási objektum csomagolás keretrendszere az ELKH ARP platformban .....	54
Király Roland, Király Sándor, Palotai Martin Marcell: Neurális hálózatok oktatási alkalmazását támogató keretrendszer Virtual (VR) és Augmented Reality (AR) eszközökkel .....	60
T. Nagy László: Mesterséges intelligencia, multimédia, tanulástámogatás .....	69
Horváth Péter: Egy automatikusan generált rímshótár fejlesztése és a magyar kanonikus költészet rímshótárjainak néhány jellemzője .....	77
Héjja Balázs, Tóth-Jávorka Brigitta, Tóth Máté: Digitális tartalomfejlesztés közkönyvtári környezetben .....	85
Koczka Ferenc: Szemelvények egy felsőoktatási rendszer informatikai védelmének tapasztalataiból .....	91
Bolya Mátyás: A digitális gyűjtésrekonstrukció lehetőségei: az Ethiofolk projekt .....	99
Dobás Kata, Sidó Zsuzsa, Szabó-Reznek Eszter: A Kolozsvári Állami Magyar Színház jelmezterveinek digitalizációja és felvitele az ITdata adatbázisba .....	108
Köpösdí Zsuzsa: H5P-ben létrehozható interaktív és adaptív tananyagok .....	116
Fülöp Tiffany, Molnár Tamás, Hoczopán Szabolcs: Komplex kutatástámogató szolgáltatási portfólió az SZTE Klebelsberg Könyvtárban .....	122
Vass Johanna: Az Open Science könyvtári vonatkozásai .....	129
Antal Péter, Czeglédi László: A digitális oktatás módszertana a gyakorlatban .....	135
Máray Tamás: A szuperszámítástechnika mint európai stratégiai ágazat .....	143
Frankó Máté, Zeller Rozália: Szoftveres Cutter-keresés az SZTE Klebelsberg Könyvtárban .....	151
Zsiborács Judit, Dési Ádám Dániel, Nagy Attila Árpád, Urbán Katalin: Tudományometriai műhely könyvtári környezetben .....	157

<b>Palkó Gábor, Szekrényes István, Bobák Barbara: A Digitális Örökség Nemzeti</b>	
Laboratórium webszolgáltatásai automatikus kézírás-felismertetéshez .....	164
<b>Szűcs Kata Ágnes: Adatvizualizációs lehetőségek a bölcsészettudományban .....</b>	<b>170</b>
<b>Leitgéb Mária: A BME Építészettörténeti és Műemléki Tanszék repozitóriuma .....</b>	<b>178</b>
<b>Mihály Eszter, Micsik András: Szerkesztői környezet TEI-alapú szövegkiadásokhoz .....</b>	<b>186</b>
<b>Dobás Kata, Fellegi Zsófia, Palkó Gábor: A kis gömböc meséje</b>	
– az ITIdata irodalomtudományos adatbázis fejlesztése 2022–2023-ban .....	192
<b>Alföldi István, Szemigán Dorottya Henrietta, Palkó Gábor, Fellegi Zsófia:</b>	
Kutatói e-mail hagyaték archiválása és feldolgozása .....	199