HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 1. szám 139–153.
DOI: 10.32567/hm.2022.1.9

Koczka Ferenc[1]

A felsőoktatási intézmények informatikai védelmének szektorspecifikus kérdései

Sector-specific Issues of IT Security in Higher Education Institutions

A felsőoktatási intézmények sajátosságai következtében az informatikai rendszereik is a szokványostól eltérők, amelyek egyes területeken markánsan különböznek a gazdasági szektor rendszereitől. A nyitott egyetemi környezet következményei, az információk minél szélesebb körű közzététele, az oktatói és kutatói szabadság támogatása jelentősen megnehezíti az informatikai védelmi feladatok ellátását. Ezért az egyetemi környezet bizonyos területeken egyedi attitűdöket és speciális módszereket kíván meg az üzemeltetőktől, miközben értékeinek tudományos értékű azonosítására, fenyegetettségének és incidenseinek elemzésére és specialitásainak vizsgálatára csak néhány, a hazai vonatkozásokat teljesen mellőző szakirodalom áll rendelkezésre.

A cikk célja az akadémiai szféra informatikai védelmét tárgyaló tudományos szakirodalom áttekintése, a szektorra jellemző problémák feltárása és magyar vonatkozásainak bemutatása, valamint azonosságok és különbségek meghatározása a szerző egyetemi informatikai vezetői tapasztalatai alapján.

Kulcsszavak: **felsőoktatás, felsőoktatás értékei, felsőoktatás kiberfenyegetettsége**

Due to the special properties of higher education institutions, their IT systems are also different from the usual ones, which in some areas significantly differ from those of market players. The consequences of the open university environment, the need to make information more widely available and the promotion of academic and research freedom make it much more difficult to fulfil IT security tasks. Therefore, the university environment requires specific attitudes and specific methods from IT professionals in certain areas, while there is little literature available on the

[1] Informatikai osztályvezető, Eszterházy Károly Katolikus Egyetem, e-mail: koczka.ferenc@uni-eszterhazy.hu

identification of its values, the analysis of its threats and incidents, and its specificities, with no Hungarian relevance.

The aim of the article is to review the academic literature on IT protection in the academic sector, to identify the problems specific to the sector and their Hungarian implications, and to identify similarities and differences based on the author's experience as an IT manager in a university.

Keywords: **higher education, values of higher education, cyber threat to higher education**

1. Bevezetés

Az akadémiai szféra intézményei[2] működésük során számos különböző informatikai rendszert alkalmaznak, amelyeket főként az oktatási és kutatási tevékenység, valamint a gazdasági, működési és adminisztrációs folyamatai támogatására vezettek be. Bár az elmúlt években a kormányzat központosította az egyetemek gazdasági működését biztosító szoftvert, és egységesítette a tanulmányi rendszert is, a működtetett rendszerek többsége az intézmények saját infrastruktúráján, saját üzemeltetésben van. Az elmúlt években Magyarországon azonban nemcsak az egyetemek mentek keresztül jelentős szervezeti átalakulásokon, hanem a kutatóintézmények egy része is megváltozott feltételek mentén működik. E cikk írásakor öt budapesti és egy vidéki egyetem tartotta meg korábbi státuszát,[3] többségük összevonások és átszervezések után alapítványi, néhány pedig egyházi fenntartóval működik tovább. Az átalakítási folyamatokban az egyetemi informatikai rendszereket egyesítették, átadandó adataikat a fogadó fél adatbázisaiba másolták, közben a régi rendszerek archívumait is fenntartják. A fúziók eredményeként hazai viszonylatban korábban nem látott méretű intézmények jöttek létre, hatalmas mennyiségű adatot kezelve úgy, hogy rendszereikben olyan személyes adatok is megjelennek, amelyek tulajdonosai soha nem álltak kapcsolatban velük. Az intézmények gyors átalakítására szabott szoros határidők az informatikai védelem szempontjából bizonytalan helyzeteket hoztak, amit a jogszabályi környezet engedékenysége sem tett könnyebbé.

Nem csak az átalakulási folyamat nehezíti meg a felsőoktatás informatikai üzemeltetési feladatait. Az akadémiai környezet számos ponton eltér a gazdasági társaságok és kormányzati fenntartású szervezetekétől, ezért a felsőoktatás üzemeltetési feladatai mindig is egyéni utak mentén valósultak meg. Az egyetemi informatikai rendszerekben tárolt adatvagyon mennyisége, azok jellege, incidenseik száma, a technikai és humán oldalon is kimutatható sebezhetőségek mennyisége és speciális jellege, a védelem eltérő megszervezése és annak betartása felveti a felsőoktatási informatikai rendszerek védelmének általános újragondolását.

[2] A cikkben az akadémiai szféra intézményei alatt a főiskolákat, egyetemeket és kutatóintézeteket értjük.

[3] Új egyetemeként a Tokaj-Hegyalja Egyetem jött létre, önálló maradt a Budapesti Műszaki és Gazdaságtudományi Egyetem, az Eötvös Loránd Tudományegyetem, a Liszt Ferenc Zeneművészeti Egyetem, a Magyar Képzőművészeti Egyetem, a Magyar Táncművészeti Egyetem, a Nemzeti Közszolgálati Egyetem és a Testnevelési Egyetem.

Az arányos és költséghatékony védelem kialakításának első lépése a védendő értékek azonosítása. Magyarországon nem történt meg az egyetemi adatvagyon tudományos igényességű vizsgálata, ezért következtetések levonásához külföldi forrásokat kell alapul vennünk. Sajnos a témát tárgyaló nemzetközi tudományos szakirodalom sem túl széles. Ulven és Wangen 2021-es szakirodalmi áttekintésében[4] 18 tudományos igényű cikket, és 14 egyéb forrást[5] kutatott fel. Rahim és szerzőtársai[6] bibliometriai elemzésében az elmúlt tíz év online forrásból elérhető szakirodalmát vizsgálták. Ők ezekben 418 dokumentumot azonosítottak, amelyek többségükben nem tudományos igényű cikkek, hanem konferenciaelőadások voltak, közülük is csak hat volt publikusan is elérhető. A hivatkozott források közt egyetlen magyar sem volt, és utalás sem szerepelt a hazai egyetemekre. Bár a magyar és nemzetközi összehasonlításban számos közös pont valószínűsíthető, a szerző személyes tapasztalatai szerint a hazai felsőoktatás védelmi kérdéseinek vizsgálatakor jelentős különbségek kerülnének felszínre. Ezek azonosításához először fel kell térképezni a felsőoktatás értékeit, az őket érő informatikai incidenseket, sebezhető pontjaikat és azokat a tényezőket, amelyek következtében a védelmi megoldások szükségszerűen eltérnek más területekétől.

2. Értékek a felsőoktatásban

A 2013. évi L. törvény (Ibtv.) hatálya alá tartozó szervezeteknek szervezeti egységeiket biztonsági szintekbe, az informatikai rendszereiket pedig biztonsági osztályokba kell sorolniuk. Ennek végrehajtásához a 41/2015-ös BM rendelet nyújt konkrét és részletes szakmai útmutatást. Az akadémiai szféra intézményei általánosságban nem tartoznak e jogszabályok hatálya alá, így nem is kell az említett feladatokat elvégezniük. A kötelezettség hiánya ellenére az egyetemek informatikai biztonsági szabályzatai részben e jogszabályok szellemében készültek, ők valamilyen szinten azonosították rendszereik értékét és elvégezték a besorolásukat.

Az értékek meghatározására nem ismert általánosan alkalmazott metodika. Megalapozott módszertan nélkül a hivatkozott jogszabályok szerinti besorolást rendszerint informatikai munkatársak végzik, aminek során listázzák az egyes informatikai alrendszereket (például elektronikus levelezés, hallgatói nyilvántartás, VPN-kapcsolatok, hálózati szolgáltatások stb.) és saját szempontjaik alapján adnak szubjektív besorolást. E módszertan alkalmazása jól érzékelhető a magyar egyetemi szabályzatok áttekintése során. Ez a gyakorlat eszköz- és funkcióközpontú meghatározást eredményez, amely rendszerszintű információ hiányában csak részlegesen veszi figyelembe az intézmény valódi céljait, így attól jelentősen eltérhet. A technikai szemléletű informatikai munkatársak és az intézményi vezetők pedig valószínűleg teljesen máshová helyezik a súlyponti kérdéseket.

[4] Joachim B. Ulven – Gaute Wangen: Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet,* 13. (2021), 39. 1–40.

[5] Ezek a források fehér könyvek, műszaki jelentések, szakdolgozatok és szakmai weboldalak voltak.

[6] Nazahah Rahim – Zaleha Othman – Fathilatul Zakimi Hamid: Cyber Security and the Higher Education Literature: A Bibliometric Analysis. *International Journal of Innovation, Creativity and Change,* 12. (2020), 12.

Az értékek azonosítása az intézmény különböző területi vezetőinek feladata, amelynek során meghatározzák az intézmény értékeit, az érték előállítását szolgáló célokat és az ahhoz szükséges fő követelményeket. Szinte minden egyetem esetében ilyen érték a hallgatói létszám növelése, a tudományos publikációk mennyiségi vagy minőségi javítása, vagy az intézmény által kiadott diplomák értéke szakmai körökben, vagy a közvéleményben. Ezen értékek eléréséhez számos feltétel, szolgáltatás, körülmény szükséges, amelyek számszerűsítésére a kulcsfontosságú teljesítménymutató (*Key Performance Indicator,* KPI) alkalmazható. A KPI-k azonosítása a célok eléréséhez szükséges elemeket mérhetővé, így leírhatóvá és összehasonlíthatóvá teszik. A KPI-k azonosítása nem csak informatikai szempontból lényeges. Valójában számos olyan KPI létezik, amelynek nincs informatikai vonatkozása, de meghatározásuk az intézményi informatikai folyamatok súlyának azonosításában jelentős szerepet játszik. A felsőoktatási KPI-k képzésére Ballard[7] doktori disszertációja ad példát, amelyben 34 felsőoktatási intézmény 2139 különböző kulcsfontosságú teljesítménymutatóját vizsgálta, amit 24 kategóriába sorolt be, egyúttal azonosítja az adatok és folyamatok körét, amelyek az intézményi célok eléréséhez szükségesek.

A felsőoktatási rendszerek adatvagyona néhány fő területre koncentrálódik, ezek a személyes, kutatási és működési adatok.

2.1. Személyes adatok

Az egyetemek egyik legértékesebb adatköre személyes adatokból áll. A McDonald Hopkins fehér könyve[8] az amerikai egyetemek esetében nemcsak egyetemi hallgatók, oktatók és kutatók személyes adatait említi, hanem adományozók, kurátorok, igazgatósági tagok, öregdiákok, diákok, szülők, jelentkezők, személyzet, betegek mellett fogyasztók és eladók adatait is. Ezek egy része a magyar egyetemek esetében a kulturális, működési és finanszírozási különbségek miatt nem is értelmezhető, például hazánkban a végzett hallgatók támogató szerepe is jóval gyengébb hagyományokra tekint vissza, mint az amerikai magánegyetemek esetében. Ennek ellenére a személyes adatok jelentősége annak mennyisége és részletessége miatt is kiemelkedő az egyetemek esetében. Kwaa-Aido és Agbeko tanulmánya[9] a hallgatói nyilvántartást nevezte meg a legfontosabb adatforrásként egy ghánai egyetemen. A magyar elektronikus tanulmányi rendszer[10] kifejezetten sok személyes adatot tartalmaz, a hallgatók általános személyes adatai mellett a felvételi információit, korábbi iskoláik, nyelvvizsgáik részletes adatait, a teljes tanulmányi történetüket, ösztöndíj és tandíj adatokat,

[7] Paul J. Ballard: *Measuring Performance Excellence: Key Performance Indicators for Institutions Accepted into the Academic Quality Improvement Program (AQIP).* PhD-értekezés. Kalamazoo, MI, Western Michigan University, 2013.

[8] James J. Giszczak – Dominic A. Paluzzi: *Pass or Fail? Data Privacy and Cybersecurity Risks in Higher Education.* McDonald Hopkins, 2016. augusztus 13.

[9] Ephrem K. Kwaa-Aidoo – Mathias Agbeko: An Analysis of Information System Security of a Ghanaian University. *International Journal of Information Security Science,* 7. (2018), 2. 90–99.

[10] A magyar felsőoktatás kizárólag a Neptunt alkalmazza, amelyet 1997-ben elsőként a BME-n vezettek be.

és olyan, rendszerint valamilyen csökkent képességet leíró egészségügyi adatokat is, amelyeknek a tanulmányok során szerepe lehet.[11]

Magyar viszonylatban az oktatók és kutatók adatai is nagy mennyiségű érzékeny adathalmazt jelentenek. Egy olyan incidens, amely a tanulmányi rendszer adatainak sérülését vagy nyilvánosságra kerülését eredményezné, az adott egyetem reputációját is jelentős mértékben ronthatná. Amennyiben jelentős mértékű adatsértés történne, az valószínűleg magával hozná a GDPR-ban meghatározott büntetési tétel érvényesítését, ami a legtöbb magyar egyetem esetében működésképtelenséget eredményezne. A tanulmányi rendszer adatainak elvesztése a legsúlyosabb következményekkel járna egy felsőoktatási intézmény számára. A tanulmányaikat folytató hallgatók tantárgy- és vizsgaeredményeinek elvesztése lehetetlenné tenné a követelmények teljesítésének ellenőrzését, nem lennének kiadhatók a korábbi diplomák, és kétségessé válna az államilag támogatott félévek elszámolása is. Bár az adatok egy része más forrásból pótolható lenne (például a befizetett tandíjak esetében) a tanulmányi rendszert ért végzetes incidens komoly reputációs veszteséget okozna.

A magyar egyetemek hallgatói és az oktatói létszámát a Felsőoktatási Információs Rendszerben (FIR) tartják nyilván, amely az 1. táblázat szerinti bontásban, 2021 januárjában több mint 2,5 millió személyes adatot tartalmazott.

1. táblázat: A FIR-ben tárolt személyes adatok száma 2021 januárjában

A magyar felsőoktatásban részt vevő hallgatók száma összesen:	1 832 965 fő
Hallgatói jogviszonnyal rendelkezők száma 2021. január 14-én:	608 301 fő
A felsőoktatásban dolgozók száma összesen:	69 602 fő
A felsőoktatásban dolgozók száma jelenleg:	51 020 fő

Forrás: a szerző szerkesztése

A nagy mennyiségű adat kezelése különleges felelősséget ró az akadémiai szférára is. Több jogellenes adatkezeléssel kapcsolatos eljárás ismert,[12] amelyet a Nemzeti Adatvédelmi és Információs Hatóság (NAIH) indított az egyetemek hibás adatkezelési gyakorlata következtében.[13] Az informatikai incidensekkel kapcsolatos valós kép megismerését nagyban nehezíti, hogy annak ellenére, hogy azok bejelentése a NAIH felé kötelező, az a gyakorlatban ritkán történik meg.

[11] Az adatok részletes leírását a mindenkor adatkezelési tájékoztató tartalmazza. Egy példa: www.kth.bme.hu/document/2148/original/Neptun_adatkezelesi_tajekoztato.pdf

[12] NAIH/2020/54: *Rendszeres szociális ösztöndíjakkal kapcsolatos adatkezelés a Budapesti Műszaki és Gazdaságtudományi Egyetemen.*

[13] NAIH-6298-2/2021: *Állásfoglalás a koronavírus elleni védettség tényének felsőoktatási intézmény általi megismerhetőségéről, nyilvántarthatóságáról kollégiumi elhelyezés és egyetemi rendezvények kapcsán.*

2.2. Oktatási rendszerek

A jelenléti oktatás kiváltására egyre több egyetem törekszik. A Covid–19 következtében, 2020-ban bevezetett kényszerintézkedések világossá tették, hogy az egyetemi kurzusok bizonyos területein az IKT-eszközökre alapozott távolléti rendszerű oktatás további fenntartása csökkentheti a hagyományos kontaktórák számát, miközben a hallgatók rugalmas időbeosztását is lehetővé teszi. A felsőoktatás oktatói számára a tananyagok elektronikus formára alakítása és LMS- *(Learning Management System)* rendszerekbe építése a járvány előtt is gyakran alkalmazott lehetőség volt, ezek alkalmazása a szektorban tömegessé vált. Jól látható, hogy a pandémia visszaszorulásával az oktatási folyamat nem tért vissza teljes egészében a régi, jelenléti oktatáshoz. A felnőttoktatásban és a levelező képzésben az elektronikus oktatási forma alkalmazásban maradt, és egyes intézmények a távolléti oktatási módszerek további alkalmazása mellett döntöttek.[14] A korábban jellemző szóbeli vizsgák helyét egyre inkább a gépi vizsgák vették át, amelyek néhány terület kivételével[15] nem voltak képesek a vizsgázó tudásának korábbi színvonalú mérésére, és a hangsúlyt az összefüggések felismerésére és alkalmazására az egyes részletek felidézésére helyezték át. Az LMS-rendszerek sérülékenysége ugyanakkor lehetőséget ad a vizsgaeredmények módosítására, így azok motivációt jelenthetnek belső és külső támadók számára egyaránt.[16]

2.3. Kutatási adatok

A tudományos kutatás az akadémiai szféra intézményeinek egyik elsődleges tevékenysége. A kutatási adatok körébe a nyers és feldolgozott kutatási adatok, tudományos ismeretek, elemzések eredményei és a tudományos publikációk tartoznak.[17] A FireEye tanulmányában[18] a vállalati, kutatási és harmadik féltől származó adatokat, például az ipari együttműködések során az intézmények számára átadott adatokat minősíti kulcsfontosságúaknak. Giszczak kutatásában olyan projektekre is kitér, amelyekben egyetemi kutatások kormányzati együttműködésből származó adatokat használnak fel.

A tudományos eredmények ma már nem jöhetnek létre informatikai háttértámogatás nélkül. A kutatási adatok eltérő értékűek, kibervédelmi szempontból kiemelt figyelmet érdemelnek azok, amelyek főként gazdasági, ipari, pénzügyi területen olyan eredményeket tartalmaznak, amelyek a gazdasági élet szereplőit előnyösebb helyzetbe hozhatják. A magyar akadémiai szféra intézményeiben is folynak olyan kutatások, amelyek eredményeinek védelme nemzeti érdek, ezért egyes kutatási egységek nemzetbiztonsági védelem alatt állnak.[19] A felsőoktatás kiemelt védelme

[14] Pl. az Eszterházy Károly Katolikus Egyetem esetében.
[15] A magyar online akkreditációval rendelkező nyelvvizsgák sikeresen működtek a járványhelyzet alatt is.
[16] Wee Ling Loo: *Student Hacking into University's Learning Management System to Save His Grades: A Cautionary Tale.* Singapore Management University, 2016.
[17] *Unit-Department for ICT and Joint Services in Higher Education and Research.* Technical Report, 2019.
[18] FireEye Inc.: *Why Cyber Attackers are Targeting Higher Education, and What Universities Can Do about It.* White Paper. 2015.
[19] 2009/2015. (XII. 29.) Korm. határozat a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről.

nemzetközi viszonylatban is megjelenik, az ausztrál kormányzat az ország felsőoktatási intézményeit elsősorban a kritikus kutatási feladatokban vállalt szerepük miatt a kritikus infrastruktúra-elemek közé sorolja,[20] és kötelezi őket a besorolásnak megfelelő informatikai védelem kialakítására.

2.4. Működési adatok

Az egyetemek nagy költségvetésű intézmények, amelyek gazdasági tevékenysége az átláthatóság biztosítása érdekében nagyrészt nyilvános. A pénzügyekkel kapcsolatos feladatokat a legtöbb intézmény esetében akár egész igazgatóságok látják el. Emellett számos egyéb területet szabályoznak olyan törvényi előírások, amelyeket egységes elektronikus nyilvántartás hiányában nehéz kezelni. Ilyen rendszerek nélkül ezeket szigetszerű megoldásokra, saját fejlesztésű szoftverekre alapozzák, amelyeket hosszan lehetne sorolni a vegyszerraktárak nyilvántartásaitól a tűzjelző berendezések ellenőrzési jegyzőkönyvéig. A gazdasági terület legfontosabb rendszere, a HR- és gazdasági folyamatokat kezelő szoftver ma egy állami fenntartású változat. Az abban tárolt adatok biztonsága kizárólag adminisztratív, arra az üzemeltetővel szerződésben meghatározott garanciák érvényesek. Nem létezik kivonási stratégia, adatairól nem készíthetők helyi másolatok, de ha még volna is erre lehetőség, akkor sem lehetne azt mibe visszatölteni.

Egy centralizált rendszer alkalmazása ugyanakkor számos terhet vesz le az intézményről, a kommunikációs kapcsolat és a munkaállomás védelmének biztosításán túl a helyi informatikai személyzetnek nincs a rendszerrel kapcsolatos felelőssége.

3. Kiberfenyegetettségek a felsőoktatásban

Számos egyetem szenvedett már el különböző típusú informatikai incidenseket. A média kibervédelemmel foglalkozó híreit nyomon követve érzékelhető, hogy egyre gyakrabban olvashatunk a szférát ért támadásokról. Ezek mennyiségi és súlyossági besorolásához, valamint statisztikai módszerekkel történő elemzésükhöz konkrét adatokra van szükség.

Nemzetközi viszonylatban több, elsősorban amerikai adatforrásokra támaszkodhatunk. Az ottani tendenciákból vonhatunk le következtetéseket a várható hazai változásokra is, de azok nem lesznek alkalmazhatók a különbségek figyelembevétele nélkül. Sajnos a különböző forrásokból származó adatok nem ugyanazt a képet rajzolják ki. Az Open Security Foundation szerint az összes biztonsági incidens 35%-a a felsőoktatásban történik.[21] Giszczak kutatása szerint 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

[20] Australian Government Department of Home Affairs: *Security Legislation Amendment (Critical Infrastructure) Bill 2020. Explanatory Document.* (2020. november).

[21] FireEye (2015): i. m.

megszerzésében, amelynek mértékét rekordonként körülbelül 300 dolláros kárként azonosítja.

A hackmageddon.com[22] havi bontásban közöl statisztikákat a szerkesztő által gyűjtött incidensekről, amelyek adatforrása is elérhető és tovább elemezhető. Ez a forrás sem teljes körű, de 2021 szeptemberéig közel 2000 eseményt és 72 adatszivárgást dokumentált. Adataiban elkülöníthetők az oktatási intézményeket érintő események részletei is. Ennek 2020-as adatai szerint a kibertámadások 7,8%-a irányult a teljes oktatási szektorra, ebből a szerkesztő 178-at sorolt a kiberbűnözés, és csak 3-at a kiberkémkedés kategóriájába.

Az oktatási intézmények vonatkozásában a vizsgálat alapjául a Privacy Rights Clearinghouse (PRC) adatbázisát választottam, amely 2021 októberében 9015 incidens adatait tartalmazta.[23] Az adatbázis kategóriákba sorolja az incidenseket elszenvedett szervezeteket és az incidensek típusát is. A szervezetek csoportosítása és a hozzájuk tartozó kódok az alábbiak:

- MED: egészségügy, egészségügyi szolgáltatók és kapcsolódó biztosítások;
- BSO: egyéb üzleti szolgáltatók;
- EDU: oktatási intézmények;
- BSF: üzleti és biztosítási szolgáltatók;
- GOV: kormányzat és hadsereg;
- BSR: kis- és nagykereskedők, online boltok;
- UNKN: ismeretlen;
- NGO: nonprofit intézmények.

Az egyes incidenstípusok:

- HACK: feltörés vagy rosszindulatú szoftver alkalmazása;
- DISC: véletlen nyilvánosságra hozatal;
- PORT: elvesztett vagy kidobott eszköz (laptop, telefon CD/DVD stb.);
- PHYS: papíralapú dokumentum elvesztése, ellopása;
- STAT: nem hordozható számítógép elvesztése, ellopása;
- UNKN: ismeretlen;
- INSD: belső munkatárs által okozott incidens;
- CARD: nem internetes bankkártyacsalás.

A PRC adatainak elemzésével megállapítható az oktatási intézmények incidenseinek jellege, és azok összehasonlíthatók más szektorokéval. A 2. táblázat alapján látható, hogy az összes incidens 9,4%-a az oktatási intézményekben történik, amivel ez a szektor a harmadik helyen szerepel a gyakorisági listán, megelőzve a biztosítási szolgáltatókat, a kormányzatot és a hadsereget is.

[22] Hackmageddon. Lásd: www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/
[23] Lásd: https://privacyrights.org/data-breaches

2. táblázat: A PRC incidenseinek szektoriális eloszlása

	HACK	DISC	PORT	PHYS	STAT	UNKN	INSD	CARD	#N/A	SUM	%
MED	925	1072	463	1394	107	38	254	1	89	4343	48,20
BSO	618	116	137	61	22	23	63	5	0	1045	11,60
EDU	**290**	**239**	**138**	**61**	**48**	**45**	**26**	**1**	**0**	**848**	**9,40**
BSF	213	123	161	64	27	74	101	24	0	787	8,70
GOV	148	225	170	104	24	30	80	0	0	781	8,70
BSR	301	71	66	38	16	21	73	37	0	623	6,90
UNKN	0	0	0	0	0	469	0	0	0	469	5,20
NGO	38	15	37	11	5	4	9	0	0	119	1,30
SUM										9015	100,00

Forrás: a szerző szerkesztése

Az amerikai egyetemek a jogszabályi különbségekből adódóan a hazaitól eltérő adatkezelést valósítanak meg. A könnyen értékesíthető adatok körébe főleg a bankkártyák engedély nélküli felhasználásához kapcsolódó adatok és az SSN *(Social Security Number)* tartoznak. A magyar egyetemek többségükben nem tárolnak bankkártyaadatokat, és mivel a személyi szám is csak korlátozott ügytípusok esetén alkalmazható, a személyes adatok kiszivárgásának hazánkban kevesebb esetben voltak súlyos, a sértett személy számára közvetlenül érzékelhető anyagi következményei. Ugyanez nem mondható el a célzott támadások és a belső munkatársak által okozott adatsértésekről, valamint reputációs veszteségekről. A szerző gyakorlatában az egyik legnagyobb kárértékű példa egy célzott megtévesztő levél helytelen kezelésével indult, amelyet több egyetem munkatársa is valósnak vélt, és módosította egy beszállítójának banksámlaszámát a gazdasági rendszerében. Emiatt annak havidíjait később már a csalók számlájára utalták át. A legnagyobb anyagi kárt viszont egy ügyintéző okozta, aki a tanulmányi rendszer manipulálásával közel tíz éven át volt képes hallgatói tandíjak elsikkasztására. Kisebb kárértékű, de nagyobb reputációs veszteségű esetek több alkalommal is történtek: 2008-ban a Veszprémi Egyetemről 1717 hallgató adatainak szivárgását jelentették, amelyek a Google-keresésekben is megjelentek.[24] A Pázmány Péter Katolikus Egyetem (PPK) tanulmányi rendszerét 2020-ban egy zsarolóvírus tette átmenetileg elérhetetlenné.[25]

4. A felsőoktatási rendszerek különbözősége

A felsőoktatási rendszerekkel szemben támasztott védelmi követelmények szoros szabályozása nemzetközi viszonylatban sem jellemző, a szakirodalom csak néhány törekvést említ ennek megváltoztatására. Az Amerikai Egyesült Államokban sem létezik átfogó, a felsőoktatásra szabott jogi környezet, az informatikai rendszerekkel

[24] Vámosi Gergő: Ezerhétszáz hallgató adatait vesztette el a veszprémi egyetem. *Origo,* 2008. december 10.
[25] Zsarolóvírus-támadás érte a Pázmányt, leállt a Neptun. *HVG.hu,* 2020. április 24.

kapcsolatos szabályzást több, különböző területet lefedő jogszabály valósítja meg úgy, hogy azok államonként is eltérhetnek. A tanulói adatok védelme az európai gyakorlatnál sokkal régebbre nyúlik vissza: az USA Oktatási Minisztériuma a Family Educational Rights and Privacy Act-ben[26] (Családi oktatási jogok és adatvédelmi törvény, FERPA) szabályozza a tanulói adatkezeléssel kapcsolatos előírásokat. Ennek hatálya kiterjed minden olyan általános, középiskolai vagy felsőoktatási intézményre, valamint minden olyan állami vagy helyi oktatási intézményre, amely az Egyesült Államok oktatási minisztériumának valamely vonatkozó programja keretében pénzeszközöket kap. Azok az iskolák, amelyek nem tartják be a FERPA szabályait, a szövetségi finanszírozás elvesztését kockáztatják.

Magyarországon sincs kifejezetten felsőoktatásra szabott szektorspecifikus jogszabályi keret, így az informatikai működést pusztán az általános szabályzók mentén kell biztosítani. A személyes adatok védelméről szóló általános GDPR mellett a legfontosabbak a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,[27] de a szektorra nézve fontosak a Btk. vonatkozó részei is. A felsőoktatás általánosságban, néhány kutatási terület kivételével nem tartozik a 2013. évi L. törvény és annak végrehajtási rendeletének hatálya alá, a kezelt adatok mennyisége alapján így nehezen indokolható kontraszt érzékelhető egy vidéki önkormányzat és egy egyetem működési keretei között.

A szabályzás megengedő jellege mellett a felsőoktatás IT-rendszereit olyan speciális környezetben kell működtetni, amelyet szinte egyetlen más intézménytípusban sem találhatunk meg.

4.1. Egyetemi kultúra

Az egyetemi környezetet az oktatói és kutatói szabadság mellett a nyitottság jellemzi, amely esetenként konfliktust generál az informatikai üzemeltetést végző személyzet és az oktató-kutató munkatársak között. Dadkah a kutatókat érő kibertámadások vizsgálatával kapcsolatban tesz erről említést,[28] de a szerző személyes tapasztalatai is egybeesnek ezzel. A FireEye fehér könyve[29] a biztonsági eszközök korlátozó hatását emeli ki, amely akadályozza az információhoz való hozzáférést. Az oktatók és kutatók nyomást gyakorolnak az egyetemi vezetésre a biztonsági intézkedések fellazítása érdekében, ugyanakkor egy esetleges incidens esetén az üzemeltetést okolhatják. Ezt a jelenséget Adams már 2003-ban megfogalmazza, és a kultúrák összeütközésének *(clash of cultures)* nevezi.[30]

Az informatikai védelem gyengítését célzó törekvések számos ponton jelennek meg, amelyek hosszasan sorolhatók lennének. A jelszóképzési szabályok kritizálása, a körülményes *secure printing* kötelezettsége alóli kibújás olyan szervezeti egységeknél

[26] Lásd: https://studentprivacy.ed.gov/node/548/
[27] Lásd: https://njt.hu/jogszabaly/2011-112-00-00.29
[28] Anne Adams – Ann Blandford: Security and Online Learning: To Protect or Prohibit. In Claude Ghaoui (szerk.): *Usability Evaluation of Online Learning Programs.* London, Idea, 2003. 331–359.
[29] FireEye (2015): i. m.
[30] Adams–Blandford (2003): i. m.

is megjelenik, amelyek bizalmas dokumentumok tömegét kezelik. A távoli munka biztosítása érdekében bevezetett bonyolultabb VPN-kliensek alkalmazási kényszere is számos kritikát kap. Tipikus a kutatási feladatok ellátására pályázati forrásból beszerzett szerverek fizikai birtoklási vágya, amelyeket egyszerű irodákban, megfelelő fizikai védelem nélkül, helyi amatőr rendszergazdákkal üzemeltetnek, és a külső adatcserék érdekében az internet irányában elérhetővé tesznek. A saját tulajdonú eszközök alkalmazása a felsőoktatásban különösen jellemző, és ezek a legfeljebb részlegesen felügyelt, a családtagokkal közös használatú gépek különösen nagy kockázatot jelentenek.

Az informatikai üzemeltetés szervezeti felépítésben elfoglalt helye is meghatározó. Azok az egyetemek, amelyekben ezt a szervezeti egységet túl alacsony szintre helyezik, lehetővé teszik más egységek számára, hogy a hierarchia okán tekintse szigorúan kötelezőnek az informatikai szakemberek előírásait. Az egységes informatikai koncepció és üzemeltetés nehezen tartható fenn azokon az egyetemeken, amelyek lehetővé teszik a különböző szervezeti egységek számára önálló informatikus foglalkoztatását, mivel ők csak önkéntes alapon működnek együtt a többi üzemeltetővel. Amennyiben a szeparáció elengedhetetlen, inkább a hierarchikus modell kialakítására érdemes törekedni.

A nyilvánosság igénye nem csak az egyetemi kultúra következménye. A közintézmények esetében megkövetelt átláthatóság a nyílt forráskódú felderítés (*Open Source Intelligence,* OSINT) aranybányája, amely nagyban növeli egy célzott támadás megtervezését és sikerét. A nyílt adatok közt gyakran szerepelnek szabályzatok, szerződések, beszállítók és számos más olyan információ, amelyet egy potenciális támadó az intézmény belső működésének, eszközparkjának felderítésére használhat fel.[31] Amennyiben egy ilyen személy számára ismert a célintézmény eszközparkja, a már említett CVE-adatbázis alapján képes azonosítani azok sérülékenységeit, ami egy támadás sikerét sokkal valószínűbbé teszi.

4.2. Információbiztonsági tudatosság

Egy hagyományos szervezettel szemben a felsőoktatási intézmények hallgatósága évről évre változik. A végzett hallgatók elhagyják az intézményt, és helyüket egy új évfolyam váltja fel. Az új hallgatók számára szolgáltatások tömegét kell biztosítani úgy, hogy azok nyilvános hozzáférhetősége biztonsági kockázatot jelent. Al-Janabi és Al Shourbaji kutatásában[32] a közel-keleti oktatási intézmények hallgatói körében meglevő információbiztonsági hiányosságokra mutat rá. Ennek fő okai közt a biztonsági követelmények betartásának elmulasztását, az általános ismeretek hiányát, a felhasználók kockázatos viselkedését és meggyőződéseit és a technológia nem megfelelő használatát jelölték meg.

[31] Egy példa az intézmény által vásárolt eszközök nyilvánosságára: https://ekr.gov.hu/portal/kozbeszerzes/eljarasok/EKR000934752018/reszletek

[32] Samaher Al-Janabi – Ibrahim Al-Shourbaji: A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management,* 15. (2016), 1. 1650007.

A social engineering támadások az egyetemi környezetben is sikeresnek bizonyultak.[33] Wangen és szerzőtársai egy egyetemi felmérésben naponta regisztráltak sikeres social engineering biztonsági incidenst. A felmérésben részt vevők 48%-a tapasztalt már személyre szabott támadást, és 22%-uk jelezte, hogy tudomása van olyan esetről, amikor valaki ilyen támadás áldozatává vált. Eltérő metodikával magyar egyetemi környezetben is történt hasonló felmérés. Az Eszterházy Károly Egyetemen végzett tesztben az 1750 egyetemi dolgozó számára küldött megtévesztő levél csatolmányát két óra alatt 969-en töltötték le (55,3%), egy csaló jelszóellenőrző weboldalon 304-en (17,3%) adták meg a jelszavukat.[34] Az alacsony információbiztonság-tudatossági szint oka az informatikai eszközökhöz való viszonyulás, következményei pedig a folyamatosan visszatérő jelszósértések és alapvető adatbiztonsági tevékenységek elmulasztása voltak.

4.3. Erőforrások és vezetői támogatás

A FireEye fehér könyvében[35] rávilágít arra, hogy az egyetemi rendszergazdák számára komoly kihívást jelent egy több kampuszra kiterjedő nagy méretű hálózat fenntartása és védelme. A legnagyobb problémát talán a rendelkezésre álló erőforrások hiánya jelenti. Az informatikai rendszerek védelmét nem lehet megfelelő eszközök és szoftverek nélkül megoldani. A szűkös saját költségvetéssel rendelkező, többségében pályázati forrásokból építkező egyetemeknek nincs lehetőségük modern kiszolgáló eszközpark és védelmi megoldások beszerzésére. Bár egyes pályázatok költségvetése lehetővé teszi bizonyos rendszerelemek bővítését, de egyetemi szintű, koncepcionális fejlesztés megvalósítására csak ritkán nyílik lehetőség. Ez annak ellenére van így, hogy a kutatások pályázati támogatása is az informatikai rendszerek működőképességén, a pályázati adatok védelme az informatikai rendszerek biztonságán alapul.

Az informatikai eszközpark mellett az üzemeltetést végző személyzet rendelkezésre állása és szaktudása is komoly problémát jelent az egyetemek számára. A gazdasági szféra elszívó ereje, az alacsony bérek, a távolléti munkavégzés lehetősége nem teszi vonzóvá az akadémiai szférát. Általános a másodállások létesítése, saját vállalkozások indítása a hiányzó bevételek pótlására. Megfigyelhető, hogy egyre kevesebben tartják vonzó munkahelynek az akadémiai szféra intézményeit, nagyban csökken az ott munkát keresők száma, ami hosszú távon a szakértelem eltűnéséhez vezet.

Az anyagi erőforrások hiányának egy másik következménye a saját kényszermegoldások kifejlesztése. Ezek a rendszerint webalapú szoftverek erősítik az egymással nem kommunikáló, szigetszerű rendszerek elburjánzását, így több veszélyt is magukban hordoznak. Mivel egy részüket az adott terület valamelyik munkatársa díjazás nélkül, szabadidejében fejleszti, távozásával a támogatás is megszűnik. Esetenként ezek a munkatársak amatőr programozók, akik nem feltétlenül ismerik a védelmi

[33] Gaute Wangen et al.: *Unrecorded Security Incidents at NTNU 2018 (Mørketallsundersøkelsen ved NTNU 2018).* Bachelor's Thesis. Trondheim, Sweden, NTNU Open Gjøvik, 2019.

[34] Koczka Ferenc: Információbiztonsági teszt az Eszterházy Károly Egyetemen. In *Networkshop 2018 konferenciakiadvány.* Budapest, Hungarnet Egyesület, 2018. 4–14.

[35] FireEye (2015): i. m.

megoldásokat, így alapvető biztonsági követelményeket hagynak figyelmen kívül. Ennek következtében a távoli hozzáférést is biztosító rendszereik kockázatot jelentenek, miközben a hierarchiában esetleg alattuk elhelyezkedő informatikai üzemeltetés nem tudja megakadályozni a működésüket. Hasonló helyzeteket teremthet a hallgatói munka keretében fejlesztett szoftverek bevezetése is.

Az informatikai biztonság megvalósításában meghatározó szerepe van a vezetői akaratnak. Az informatikai incidensek felelősségét az intézmények vezetői viselik, így a védelem támogatása elemi érdekük. Több magyar egyetem számára az ehhez szükséges anyagi erőforrások biztosítása lehetetlen feladat, de az informatikai biztonság humán oldalának megvalósításában nyújtott támogatásuk kulcsfontosságú. Az akadémiai szféra intézményeiben ez a támogatás jelenleg különböző mértékben jelenik meg.

5. Összefoglalás

A felsőoktatási informatikai rendszerek informatikai kérdéseivel kapcsolatban kevés tudományos igényű szakirodalom áll rendelkezésre. Az egyetemek speciális informatikai környezetét főleg amerikai, norvég, maláj és kínai források tárgyalják, így megalapozott megállapítások főleg erre a régióra vonatkoztatva tehetők. Tudományos igényű magyar forrást a témában a szerző eddig nem lelt fel.

A tág értelemben vett informatikai védelem terén az egyetemek nemzetközi és magyar viszonylatban több hasonlóságot mutatnak, így a nemzetközi tendenciák változását valószínűleg a hazaiak is követik majd. Ugyanakkor több ponton is eltérések érzékelhetők, amelyekre vonatkozó megállapításaimat magyar szakirodalmi források hiányában személyes tapasztalataimra alapozva tettem meg. A magyar egyetemek esetében nem látszik jelentős különbség a kezelt adatok széles körében, a jogszabályi háttér viszonylagos megengedő jellegében és az egyetemekre szabott jogszabályok hiányában. Komolyabb különbség merül fel a károkozásra közvetlenül alkalmas adatelemek terén, SSN-típusú és bankkártyaadatok a hazai rendszerekben sokkal kisebb mennyiségben fordulnak elő. Nemzetközi viszonylatban a legnagyobb értéket és a legnagyobb kockázati tényezőt is a hallgatói és dolgozói adatok jelentik. Az alkalmazandó rendszerek terén a hazai előírások több megkötést tartalmaznak, a kormányzat meghatározza a gazdasági és a tanulmányi rendszert.

Az oktatói és kutatói terület által generált védelmi problémák viszont közel azonosnak tűnnek, amelyekre a szakirodalom is hivatkozik.

A kiberfenyegetések azonosítására nem állt rendelkezésre olyan mennyiségű magyar adat, amely lehetővé tenné a nemzetközi összehasonlítást. Főként amerikai adatok elemzésével kimutattam, hogy az oktatási szektor az informatikai incidensek területén a harmadik legveszélyeztetettebb terület, és megállapításokat tettem az egyes incidenstípusok jelenlétének gyakoriságára is.

A fejlett országokban a szféra fő problémái az egyetem nyitott kultúrája, az informatikai veszélyhelyzetek felismerésének hiánya, a vezetői támogatás problémái, a saját használatú eszközök és a finanszírozási kérdések köré csoportosulnak. A fejlődő országok egyetemei esetében ezek a problémák fokozottan jelentkeznek.

Összességében megállapítható, hogy a szféra kutatása magyar viszonylatban jórészt feldolgozatlan terület, amelyben számos kérdés merül fel, amelyekre nem született tudományos igényű válasz.

Felhasznált irodalom

Adams, Anne – Ann Blandford: Security and Online Learning: To Protect or Prohibit. In Claude Ghaoui (szerk.): *Usability Evaluation of Online Learning Programs.* London, Idea, 2003. 331–359. Online: https://doi.org/10.4018/978-1-59140-105-6.ch018

Al-Janabi, Samaher – Ibrahim Al-Shourbaji: A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management,* 15. (2016), 1. 1650007. Online: https://doi.org/10.1142/S0219649216500076

Australian Government Department of Home Affairs: *Security Legislation Amendment (Critical Infrastructure) Bill 2020. Explanatory Document.* 2020. november. Online: https://doi.org/10.31915/NWS.2018.1

Ballard, Paul J.: *Measuring Performance Excellence: Key Performance Indicators for Institutions Accepted into the Academic Quality Improvement Program (AQIP).* PhD-értekezés. Kalamazoo, MI, Western Michigan University, 2013.

FireEye Inc.: *Why Cyber Attackers are Targeting Higher Education, and What Universities Can Do about It.* White Paper. 2015.

Giszczak, James J. – Dominic A. Paluzzi: *Pass or Fail? Data Privacy and Cybersecurity Risks in Higher Education,* McDonald Hopkins, 2016. augusztus 23. Online: https://mcdonaldhopkins.com/Insights/August-2016/Pass-or-fail-Data-privacy-and-cybersecurity-risks

Koczka Ferenc: Információbiztonsági teszt az Eszterházy Károly Egyetemen. In *Networkshop 2018 konferenciakiadvány.* Hungarnet Egyesület, Budapest, 2018. 4–14. Online: https://doi.org/10.31915/NWS.2018.1

Kwaa-Aidoo, Ephrem K. – Mathias Agbeko: An Analysis of Information System Security of a Ghanaian University. *International Journal of Information Security Science,* 7. (2018), 2. 90–99.

Loo, Ling Wee: *Student Hacking into University's Learning Management System to Save His Grades: A Cautionary Tale.* Singapore Management University, 2016. Online: https://ink.library.smu.edu.sg/cases_coll_all/172/

NAIH-6298-2/2021: *Állásfoglalás a koronavírus elleni védettség tényének felsőoktatási intézmény általi megismerhetőségéről, nyilvántarthatóságáról kollégiumi elhelyezés és egyetemi rendezvények kapcsán.* Online: https://naih.hu/adatvedelmi-allasfoglalasok/file/417-allasfoglalas-a-koronavirus-elleni-vedettseg-tenyenek-felsooktatasi-intezmeny-altali-megismerhetosegerol-nyilvantarthatosagarol-kollegiumi-elhelyezes-es-egyetemi-rendezvenyek-kapcsan

NAIH/2020/54: *Rendszeres szociális ösztöndíjakkal kapcsolatos adatkezelés a Budapesti Műszaki és Gazdaságtudományi Egyetemen.* Online: https://naih.hu/hatarozatok-vegzesek/file/325-1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adat-

kezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemen-modositasokkal-egyseges-szerkezetben
Rahim, Nazahah – Zaleha Othman – Fathilatul Zakimi Hamid: Cyber Security and the Higher Education Literature: A Bibliometric Analysis. *International Journal of Innovation, Creativity and Change,* 12. (2020), 12. Online: www.ijicc.net/images/vol12/iss12/121282_Rahim_2020_E_R.pdf
Ulven, Joachim B. – Gaute Wangen: A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet,* 13. (2021), 39. 1–40. Online: https://doi.org/10.3390/fi13020039
Unit-Department for ICT and Joint Services in Higher Education and Research. Technical Report, 2019. Online: www.jstor.org/stable/pdf/26441233.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A5966892c9e805357cc27fd4374cc012d
Vámosi Gergő: Ezerhétszáz hallgató adatait vesztette el a veszprémi egyetem. *Origo,* 2008. december 10. Online: www.origo.hu/techbazis/20081210-1717-hallgato-adatait-vesztette-el-a-veszpremi-egyetem.html
Wangen, Gaute – Even Ø. Brodin – Bent H. Skari – Christopher Berglind: Unrecorded *Security Incidents at NTNU 2018 (Mørketallsundersøkelsen ved NTNU 2018).* Bachelor's Thesis. Trondheim, Sweden, NTNU Open Gjøvik, 2019.
Zsarolóvírus-támadás érte a Pázmányt, leállt a Neptun. *HVG.hu,* 2020. április 24. Online: https://hvg.hu/tudomany/20200424_pazmany_peter_katolikus_egyetem_zsarolovirus_neptun_tanulmanyi_rendszer_szakdolgozat_leadasi_hatarido

Jogi források

2011. évi CCIV. törvény a nemzeti felsőoktatásról
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
2009/2015. (XII. 29.) Korm. határozat a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről