NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA

Koczka Ferenc

Felsőoktatási rendszerek védelmi kérdései

Doktori (PhD) Értekezés

Témavezető:

Dr. Krasznay Csaba

.....

BUDAPEST, 2023

Tartalomjegyzék

1. Bevezetés

A modern oktatási intézmények egyre szélesebb körben vesznek igénybe informatikai eszközöket és szoftvereket. Az informatika az iskolában az oktatás tárgyaként jelent meg, de rövid idő elteltével az oktatás eszközévé vált. Az "informatizálódás" az oktatási tevékenységek szinte teljes vertikumában megkerülhetetlen követelménnyé vált, az oktatásban a tanulók életkori sajátosságaira és a különböző tárgyak jellegzetességeire alapozva iskolai alkalmazások tömkelege jelent meg a nyelvtanulástól a matematikán át zeneoktatásig. Eleinte a fejlesztések főként a felsőoktatási intézményekben indultak el, különféle alkalmazásokba integrálva a meglevő szakmai és kutatási tapasztalatokat. Közben az iskolák működési feladataik támogatására is megkezdődött a informatikai eszközök alkalmazása, és bár a mindennapi tevékenységeik támogatásában ezek a rendszerek nagy szerepet vállaltak, jelentős mértékűvé tették az infrastruktúrától való függésüket. Az IT szerepe az elmúlt évek Covid19 következtében kialakult helyzetben ugrásszerű fejlődést hozott a szektorban, a távolléti oktatás azonnali bevezetésének kényszere alatt az intézmények szinte hetek alatt oly mértékben reformálták meg az oktatást, amely a járvány nélkül éveket igényelt volna.

Az informatikai rendszerek alkalmazása azonban nagyfokú kitettséget is magával hozott. Magyarország Nemzeti Kiberbiztonsági Stratégiája kiemeli, hogy az informatikai kiszolgáló rendszerek kompromittálásának, azok adattartalmának jogosulatlan személyek számára történő megismerésének megakadályozása stratégiai fontosságú minden nemzetállam számára [1]. Ebben a kérdésben elsősorban a kritikus infrastruktúrákat, a gazdasági-, banki- és a kormányzati szférára szereplőit szokás kiemelten kezelni, meggyőződésem szerint ez dolgozatom célterületére, a felsőoktatási rendszerekre is érvényes.

A magyar felsőoktatási intézmények informatikai védelmi területen meglehetősen heterogén képet mutatnak, működésük nem egységes, összehangolatlan, védelmi rendszereik egyediek és eltérők, szabályzataik azonos feladatot ellátó rendszerelemeket különbözőképp kezelnek. Ezek gyökerei végsősoron az ágazat számára szabad döntéseket biztosító és megengedő jogszabályi környezetre vezethetők vissza.

Az akadémiai szféra intézményei működésük során számos különböző informatikai rendszert alkalmaznak, melyek elsődleges feladatai az oktatási és kutatási tevékenység ellátása, valamint a gazdasági, működési és adminisztrációs folyamatok támogatása. Bár az elmúlt években a kormányzat részben centralizálta az egyetemek gazdasági működését biztosító rendszerét és ko-

moly lépéseket tett a tanulmányi rendszerek egységesítésének irányába is, a felsőoktatási intézmények működését biztosító infrastruktúra többségében az intézmények saját üzemeltetésében van.

Magyarországon az elmúlt években az egyetemek és kutatócsoportok jelentős szervezeti átalakulásokon mentek keresztül, és a kutatóintézmények egy része is megváltozott feltételek mentén működik tovább. Dolgozatom írásakor még öt budapesti és egy vidéki egyetem állami fenntartású, a továbbiak az elmúlt időszak összevonásai és átszervezései után vagyonkezelői alapítványként, kisebb részben pedig egyházi fenntartásban működnek tovább. Ezek a folyamatok az informatikai rendszerek átkonfigurálását, bonyolult migrációs és átalakítási eljárásokat követeltek meg, melynek során egyes szakrendszereket egyesítettek, másokat szétválasztottak, az átadandó adathalmazokat a fogadó fél adatbázisaiba másoltak úgy, hogy az adatszolgáltatási kötelezettség ellátása érdekében a korábbi állapot archívumainak fenntartása is követelmény maradt. A fúziók eredményeként hazai viszonylatban korábban nem látott méretű intézmények jöttek létre, melyek az oktatói- és hallgatói adatok tekintetében jelentős átfedést tartalmazva, hatalmas mennyiségű adatot kezelnek, melyekben olyan személyes adatok is rendelkezésre állnak, melyek tulajdonosai soha nem álltak kapcsolatban velük. Az intézmények gyors átalakítására szabott szoros határidők az informatikai védelem szempontjából bizonytalan helyzeteket teremtettek, melyet a jogszabályi környezet megengedő jellege sem tett könnyebbé.

Nem csak az átalakulási folyamatok nehezítik meg a felsőoktatás informatikai üzemeltetési feladatait. Az akadémiai környezet számos ponton eltér a gazdasági társaságok és kormányzati fenntartású szervezetekétől, ezért a felsőoktatás üzemeltetési feladatai rendszerint egyéni utak mentén valósultak meg. Az informatikai rendszerek megtervezését és kialakítását, a szoftverkörnyezet kiválasztását jellemzően az üzemeltetésért felelős szervezeti egységek végzik, a biztonságos működtetés anyagi hátterének biztosítása pedig azon múlik, hogy képesek-e meggyőzni az intézményi vezetőket vagy a fenntartót annak szükségességéről. A bizonytalan anyagi háttér, főként a saját erőből történő beruházások helyett a pályázati forrásoktól várt fejlesztések csak néhány egyetem esetében teszik lehetővé egy többéves fejlesztési terv alapján működő, garantált és tervezhető finanszírozású rendszer koncepciójának kidolgozását és végrehajtását. Ugyanakkor az egyetemi informatikai rendszerekben tárolt adatvagyon mennyisége, azok jellege, az azokat ért incidensek száma, a technikai és humán oldalon is kimutatható mértékű sebezhetőségeik mennyisége és speciális jellege, a védelem eltérő megszervezése és annak betartása egyaránt felveti a felsőoktatási intézmények vezetőinek és az informatikai rendszerek üzemeltetőinek felelősségi kérdéseit.

1990 óta tanítok főállású oktatóként vagy óraadóként a felsőoktatásban, emellett több, eltérő területen szereztem tapasztalatokat az informatikai fejlesztés, üzemeltetés és vezetés területén. Dolgoztam rendszermérnökként a gazdasági szférában, részt vettem állami fenntartású szervezetek, főként önkormányzatok informatikai rendszereinek kialakításában és működtetésében. Több szervezetben láttam el informatikai vezetői feladatkört, tudományos munkám alapkérdéseit azonban főleg azok a problémák inspirálták, melyekkel kilenc éven át az egy magyar egyetem informatikai osztályvezetőjeként majd igazgatójaként találkoztam. A különböző területek üzemeltetési ismeretei alapján felismertem, hogy a feladatkörből, a működés finanszírozásából és a jellegzetes intézményi kultúrából adódóan egy komplex egyetemi informatikai vezetői munka körülményei több és hangsúlyos ponton térnek el a gazdasági ágazatban megszokottaktól.

Amellett, hogy lehetőségem volt megismerni egyetemem mindennapi életének informatikai aspektusait, centralizáltam az azt fenntartó csoportot, annak feladatait és racionalizáltam működését. Tudományos konferenciákon és egyéb szakmai rendezvényeken betekintést nyertem más magyar és külföldi egyetemek informatikai rendszereibe, valamint üzemeltetési kérdéseibe és azt tapasztaltam, hogy annak ellenére, hogy alapfeladataik nemzetközi viszonylatban is azonosak, köztük számos eltérés áll fenn.

Kutatásom számára kivételes lehetőséget nyújtott a tény, hogy informatikai vezetőként lehetőségem nyílt egy középméretű magyar egyetem teljes informatikai rendszerének üzemeltetési szempontú adatelemzésére[1], továbbá ki tudtam alakítani egy olyan mérési környezetet, amelyet egy kutató számára valószínűleg egyetlen egyetem sem tenne lehetővé. Adatgyűjtési módszereim kiválasztásakor mindig szem előtt tartottam a kutatásetikai követelményeket és a jogszabályok betartását. Több éven át erős felsővezetői támogatást kaptam az üzemeltetésben, így ismereteim szerint a magyar felsőoktatásban egyedüliként végezhettem olyan méréseket, mely során a teljes munkavállalói kör adathalászatra adott válaszreakcióit, vagy hamisított weboldalon tanúsított viselkedését, valamint teljeskörű sérülékenységvizsgálat eredményeit tanulmányozhattam. Ezért ezúton is szeretnék köszönetet mondani egykori munkatársaimnak, akik jelentős segítséget nyújtottak az ezekhez szükséges informatikai környezet műszaki megvalósításában.

[1] Az elemzett adatok körébe nem tartoznak bele az egyetem szakrendszereiben tárolt személyes, gazdasági vagy kutatási adatok és eredmények, kizárólag az informatikai rendszerek működéséhez szükséges, az infrastruktúrához, a felhasználókhoz és az informatikai biztonsághoz köthető adatok feldolgozásával végeztem kutatásokat.

1.1. A tudományos probléma megfogalmazása

A magyarországi felsőoktatási intézmények informatikai rendszereire, adatkezelési folyamataira csak általános jogszabályok vonatkoznak. E szektor működését nem határozzák meg az állami szervek működését keretek közé helyező törvények és rendeletek, nem tartoznak a 2013. évi L. törvény, valamint a 41/2015-ös BM rendelet hatálya alá sem [2] [3]. Az informatikai rendszereik tervezésében, felépítésében, kialakításában, üzemeltetésében és kivezetésében nincsenek a szektorra specializált jogszabályok által előírt kötelezettségek. Ennek következményeként a gyakorlatban az informatikai üzemeltetést ellátó szervezeti egységekben – jó esetben szabványok, jógyakorlatok figyelembevételével – a meglevő preferenciák, szaktudás és anyagi háttér hármasa determinálja a rendszerek megtervezése során alkalmazott stratégiát és a felépítésük, üzemeltetésük során meghozott döntéseket.

A felsőoktatási intézményekre az állami és önkormányzati szervezetekre vonatkozó jogszabályokat összevetve megállapítható, hogy az informatikai rendszerek üzemeltetését meghatározó követelmények nem következetesek. Az elmúlt években az önkormányzati ASP kifejlesztésével és bevezetésével az önkormányzatok saját hatáskörben, saját infrastruktúrán kezelt adatainak mennyisége számottevően csökkent, mivel az adatkezelő rendszereket az állami fenntartású, központilag felügyelt és professzionális rendszerekkel védett környezetbe vitték át. Ellentmondásos helyzet alakult ki azzal, hogy az önkormányzatok rendszereinek működését továbbra is a már említett jogszabályok határozzák meg, miközben az egyetemek esetenként több nagyságrenddel nagyobb mennyiségű és érzékenységű adatot tartalmazó rendszerei nem tartoznak a hatályuk alá. A szakirodalom általánosságban három fő területen határozza meg a felsőoktatási intézmények adatvagyonát.

A személyes adatok meghatározásakor az Európai Unió Általános Adatvédelmi Rendeletét (GDPR) vettem alapul, mely ezeket két kategóriába sorolja: a személyre vonatkozó adatok mellett meghatározza a különleges adat fogalmát is, melynek főbb elemei a vallási, egészségügyi és biometrikus, valamint a politikai és világnézeti adatok [4]. Az egyik legnagyobb adatkört a hallgatók, valamint oktatók, kutatók és egyéb munkakörben dolgozók személyes adatai teszik ki, a jogszabályi előírások következtében olyan személyeké is, akik már nem rendelkeznek aktív jogviszonnyal az adott intézményben. A felsőoktatás informatikai rendszerei különleges adatokat leginkább a különféle munkajogi kedvezmények igazolásaként, vagy sérült hallgatók egészségügyi igazolásainak dokumentálása, és az azzal járó kedvezmények érvényesíthetősége céljából tartalmaznak. Ezektől eltérő különleges adatok az általánosan használt felsőoktatási

rendszerekben meglehetősen ritkák, eltekintve azoktól az intézmény által működtetett levelezési vagy egyéb feliratkozást igénylő csoportlistáktól, melyek szervezeti tagságra, vagy valamilyen személyes irányultságra engednek következtetni. Kivételt az orvosképzés egyetemei jelentenek, ahol a munkatársak és hallgatók meghatározott köre betegadatokhoz férhet hozzá.

A személyes adatok védelme az egyetemek nagy mérete, szerteágazó, és gyakran gyenge kapcsolatban levő szervezeti egységei következtében gyakran sérül. Sudrastawa és szerzőtársai 2019-es mérésük során elemezték a felsőoktatási intézmények információs rendszerének weboldalain közzétett érzékeny személyes adatok típusait és azok megoszlását. Ennek során 72.522 vizsgált esetből 189.358 érzékeny személyes adatot gyűjtöttek, melynek 87,7%-át minősítették a tulajdonos azonosítására alkalmasnak, ezek a legtöbb esetben a születési helyre, születési dátumra, lakcímre, telefonszámra, az e-mail címre, arcképre, vallásra vonatkozó adatok voltak, de számos esetben jutottak munkavállalói azonosító számokhoz is [5].

A kutatási és fejlesztési adatok köre az intézmények sajátosságaiból adódóan önálló terület, ahol az egyes intézmények közt jelentős különbségek állnak fenn: a tudományegyetemek esetében ezek mennyisége és minősége általánosságban meghaladja az alkalmazott tudományok egyetemeit és a főiskolákét. A kutatási eredmények és hozzájuk kötődő adatok mennyisége az Európai Unió pályázatai támogatásainak felhasználása következtében 2020-ig erősen emelkedő tendenciát mutatott. Az egyetemek önálló kutatási egységeket hoztak létre, komplex projektjeikbe más, nem oktatási területek stratégiai fontosságú adatai is beépültek. Ezek kezelését az egyetemi dolgozók és kutatók az általános jogszabályok keretein túl saját döntésük alapján végezték. Személyes tapasztalataim szerint a kutatók nem feltétlenül vannak tisztában az adatkezelés szabályaival, így előfordulhat szabálytalan kezelésük. A szigorú adatkezelési előírások fellazítására irányul az egyetemek tradicionálisan nyílt működése, mely a kutatóintézetek jellemzője is. Amellett, hogy az új eredmények publikálása a kutatómunka szerves részét képezi, emellett a személyes minőségértékelésük alapja is, így az alkotók az informatikai biztonsági előírások lazítására irányuló intézkedéseket várják el. Ezért a védelem kérdésének vizsgálatakor kiemelten fontos szempontnak tartom a szellemi vagyon (intellectual property) mellett a kutatók személyazonosságának, kutatási- és szakterületeivel kapcsolatos adatainak védelmét, tekintettel arra, hogy ez az adatkör kiemelt értéket jelenthet a gazdasági szereplők számára, így a kiberkémkedés potenciális célpontjai. Megítélésem szerint a felsőoktatási intézmények ezeket az adatokat jelenleg nem részesítik értékarányos védelemben.

Az egyetemi önállóság, az oktatók és kutatók szabadságának, útkeresésük támogatási feladatai az egyetemi informatikai üzemeltetőktől a köz- és gazdasági szférától helyenként eltérő módszereket igényelnek, melyeket a védelmi kérdések megközelítésekor is figyelembe kell venni.

Néhány felsőoktatási intézményre, vagy azok kiemelt jelentőségű szervezeti egységeire viszont szigorúbb szabályzás vonatkozik. A 2009/2015. (XII. 29.) Kormányhatározat a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről jelenleg a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Debreceni Egyetem, a Dunaújvárosi Egyetem, a Pécsi Tudományegyetem és a Szegedi Tudományegyetem egyes kutatóintézeteit főként kutatási területük érzékenysége okán [6, p. 1.38], a Nemzeti Közszolgálati Egyetemet pedig teljes egészében nemzetbiztonsági védelem alá helyezi [6, p. 1.60].

A témára irányuló nemzetközi gyakorlat áttekintésekor nem találtam kifejezetten a felsőoktatás védelmi rendszereinek működését szabályzó komplex törvényi előírásokat.

A működési vagy gazdasági területen az elmúlt évek változásai alapján világosan kirajzolódik az informatikai rendszerek központosítási folyamata. A gazdasági rendszereket már részlegesen centralizálták, és a jelenleg még intézményi hatáskörben levő tanulmányi rendszer és iktatás is kötelező egységesítési folyamaton ment keresztül. Ez csökkenti az üzemeltetési feladatok mennyiségét és az intézmény felelősségi szintjét is: a centralizált gazdasági rendszerekkel kapcsolatban minden központi feladatot az azt működtető szervezet végez el, a helyi informatika szerepe kimerül a munkaállomások és a védett kapcsolatok biztosításában. Hasonló a helyzet a felelősségi körök terén is: nem találtam olyan intézményt, amely rendelkezne a központi szolgáltatásként igénybe vett gazdasági rendszer adatainak mentésével, vagy kivonási stratégiája lenne. Emellett kijelenthető, hogy a felsőoktatásban az infrastruktúra méretét, komplexitását és inhomogenitását tekintve az informatikai rendszerek teljes életciklusát lefedő üzemeltetési feladatait ellátó informatikai szakemberek létszáma a szükségesnél alacsonyabb. Szakmai konferenciákon szerzett tapasztalataim szerint a védelmi szempontokat magas prioritású kérdésként kezelik, de abban a számukra kiemelt fontosságú rendszerek mellett olyan elemek is működhetnek, melyek védelmi szintje az elvárható minimum alatt van. Az egyetemi autonómia ellenére az informatikai környezetet az akadémiai szféra és a fenntartói érdekei mentén saját hatáskörben tervezik meg és alakítják ki. Az adminisztratív védelmet meghatározó dokumentumok előállítása szintén így történik, és kötelező érvényű jogszabályi keretek nélkül a védelmi intézkedések kikényszerítése csak erős anyagi támogatás és vezetői felelősségvállalás mellett valósulhat meg, az ehhez szükséges eszköz- és szaktudás megszerzését és szinten tartását az elmúlt

évek gazdasági és munkaerőpiaci folyamatainak változásai pedig rendszerint negatívan befolyásolták.

Az informatikai üzemeltetés számára a hálózati kapcsolatokat és az évek során egyre apadó mértékű szakmai támogatást a KIFÜ biztosítja, melynek korábbi elődintézményei már az 1990-es évektől komoly szakmai támogatást nyújtottak a felsőoktatás és a kutatóintézetek számára. A KIFÜ jelenleg más feladatkört is ellát, így a felsőoktatás számára hálózati védelmet csak kisebb arányban biztosít, a korábbi évek szakmai támogatása, a rendszeres oktatások és közös egyetemi projektek megszűntek. Üzemeltetési szempontú szigorú törvényi kötelezettségei ennek a szervezetnek sincsenek. A Nemzetbiztonsági Szakszolgálat feladatkörébe nem tartozik bele az egyetemek informatikai védelme, és bár a gyakorlatban elvárja a nyomozati tevékenységek támogatásához, vagy forenzikus vizsgálatok lefolytatásához szükséges, az egyetem informatikai rendszereiben rögzített adatok rendelkezésre állását, annak hiányát jogszabályi kötelezettség hiányában nem szankcionálja. A Kibervédelmi Intézet szerepvállalása is hasonló: csak abban az esetben kerül kapcsolatba a felsőoktatási intézményekkel, ha a hatáskörébe tartozó szervezetek informatikai incidensei során kapcsolat merül fel velük.

Kutatási témám a felsőoktatási rendszerek informatikai rendszerének védelmi kérdéseinek vizsgálata, melynek középpontjában azok sérülékenységvizsgálati mérések során gyűjtött adatok elemzése és azokból levont következtetések állnak. Hipotéziseimet olyan feltételezések alapján választottam meg, melyeket eddigi vezetői feladatköröm ellátása során szerzett gyakorlati tapasztalataim során alakítottam ki, célom ezek tudományos értékű bizonyítása.

1.2. Kutatási célkitűzések

Kutatásom elsődleges célja a magyar felsőoktatás adatvagyonának feltárása, majd bizonyítása, hogy informatikai rendszereik nem csak belső informatikai incidenseket szenvednek el, hanem különböző célok elérésében motivált kibertámadók célpontjai is. Kimutatom, hogy a magyar egyetemek azonos szakrendszereinek biztonsági besorolása eltérő.

Esettanulmányokból kiindulva bizonyítom, hogy rendszereikben számottevő mennyiségű sérülékenység deríthető fel, és bizonyítom azok általános jellegét. Kimutatom az egyes rendszerek általánosságait, lehetséges eltéréseit, végül módszertani útmutatást és javaslatot adok a felsőoktatási informatikai rendszerek belső adatkapcsolatain és sérülékenységeinek monitorozásán alapuló pontosabb, dinamikus besorolására. Vizsgálataim dokumentálása során törekszem azok megismételhetőségre és az időbeni változások által megkívánt továbbfejlesztések támogatására,

valamint adaptálhatóságukat lehetővé tevő információk megadására. Ennek érdekében az alábbi részcélokat fogalmazom meg:

1. A magyar felsőoktatási rendszerek adatvagyonának felmérése, a veszélyeztetettségük kimutatása és rendszereik biztonsági besorolási különbségeinek bizonyítása. Jelenleg nem áll rendelkezésre a magyar felsőoktatási intézmények adatvagyonát leíró részletes és hiteles forrás. Tekintettel arra, hogy erről az intézmények nem szolgáltatnak adatokat, meghatározásuk lehetséges forrásai az informatikai-, vagy informatikai biztonsági szabályzataik lehetnek. Ezek többségükben listázzák az egyes informatikai rendszereket és feltüntetik az intézmény által meghatározott biztonsági osztályt is. Elemzésük lehetőséget ad a rendszerek számbavételére és a besorolások összehasonlításra, ugyanakkor várhatóan nem nyújtanak információt adattartalmukra és a köztük fennálló adatkapcsolatokra. Célom a rendszerek azonosítása, tárolt adataik jellegének, érzékenységének, amennyiben lehetséges, azok mennyiségének meghatározása. Bizonyítani kívánom, hogy a szférában működő különböző, helyi üzemeltetésű rendszerek nagy mennyiségű érzékeny adatot tartalmaznak, melyek más rendszerek számára periodikusan átadásra kerülnek vagy kerülhetnek, vagy közvetlen adatkapcsolat révén folyamatosan elérhetők lehetnek.

Nemzetközi és hazai adatok alapján bizonyítom a felsőoktatási rendszerek támadásának valós veszélyét, megállapítom azok trendjeit, motivációit és jellemző eszközkészletét. A gazdasági szféra jellemzőivel történő összehasonlítással és elemzésével meghatározom, hogy a felsőoktatási rendszereket milyen módszerekkel, mértékben és arányban érik kibertámadások így támpontot adok egy, a szférára specializált védelmi eljárás kidolgozására. Bizonyítom, hogy léteznek azok a motivációk, amelyek a felsőoktatási rendszerek feletti kontroll megszerzését, működésük befolyásolását és adattartalmuk bizalmasságának, sértetlenségének és rendelkezésre állásának megsértését célozzák. Dokumentumelemzés módszerére alapozva felkutatom az egyes egyetemek informatikai rendszereit, összehasonlítom azok besorolásait, és felkutatom különbözőségeiket. Végül bizonyítom, hogy az azonos feladatot ellátó rendszerek besorolási szintjét az intézmények eltérően állapítják meg.

2. A magyar felsőoktatási informatikai rendszereinek sérülékenységi állapotának mérése és elemzése. Ennek során kidolgozom a sérülékenységvizsgálat egy lehetséges metodikájának részleteit, esettanulmányokon keresztül bizonyítom a sérülékenységek létét, bemutatom a mérések elméleti hátterét és metodikáját, és a sikeres esettanulmányok alapján indukció, vagy további mérések alapján általánosítom eredményeimet. Az eredményeinek elemzésével kimuta-

tom, hogy a felsőoktatási informatikai rendszerek elemei nagyszámú sérülékenységet tartalmaznak, és elemzem ezek jellegét. Ezzel bizonyítom a rendszerek kitettségét a belső és külső támadók számára, mely alapján megállapítom, hogy jelen helyzetben a felsőoktatási rendszerek védelme csak részleges. Áttekintem a támadások korai jelzésének lehetőségeit.

3. A magyar felsőoktatási informatikai rendszerek biztonsági besorolására szolgáló, azokra specializált metodika kidolgozása. Dolgozatom záró hipotézisének bizonyításához feltárom az egyes rendszerek közt fennálló és lehetséges adatkapcsolatokat és a korábbi megállapítások során feltárt helyzetkép alapján ajánlást adok a felsőoktatási intézményekben működő informatikai rendszerek besorolásának megnövelt pontosságú, rövid periódusú kiszámításának metodikájára.

1.3. Kutatási hipotézisek

H1. A magyarországi felsőoktatási rendszerek adminisztratív szabályzásai heterogén tartalmúak és azonos feladatkört ellátó rendszereket eltérő besorolással kezelnek.

H2. A magyarországi felsőoktatási informatikai rendszerek központi területeken üzemeltetett rendszerelemein kisebb számú sérülékenység mérhető, mint a perifériális telephelyeken működőkén.

H3. A magyarországi felsőoktatási információs rendszerek sérülékenységeiről jelentős mennyiségű, egy évnél régebben ismert technikai információ gyűjthető össze, melyek túlnyomórészt hibás konfigurációs beállítások eredményei.

H4. A magyarországi felsőoktatási informatikai rendszerekre megadható egy specializált, kockázaton alapuló besorolási metodika.

1.4. Kutatási módszerek

Kutatásom során primer és szekunder kutatási módszert alkalmaztam. A szakirodalom felkutatása során számos jogszabályt, szabványt, ajánlást és jógyakorlatot tanulmányoztam, melyeket összevetettem a felsőoktatási környezettel, valamint saját vezetői, üzemeltetői, fejlesztői, és oktatói tapasztalataimmal azért, hogy megvizsgáljam érvényességüket a felsőoktatási rendszerekben, és feltárhassam eltéréseiket.

Az egyes intézmények informatikai rendszereinek számbavételére és biztonsági besorolásuk összevetésére az informatikai biztonsági szabályzataikon végzett dokumentumelemzést, az el-

térések megállapítására összehasonlító kritikai elemzést alkalmaztam. Az objektivitás érdekében lehetőség szerint számszerű adatok gyűjtésére törekedtem, melyeket statisztikai módszerekkel dolgoztam fel.

Különféle mérőeszközök alkalmazásával sérülékenységvizsgálati-, biztonsági események és konfigurációs hibák felderítésére irányuló méréseket végeztem, melyek alapján az összefüggések megállapítása érdekében statisztikai számításokat végeztem. A valós helyzetkép megállapítása érdekében az információbiztonság mérésének módszere az interjúk alkalmazása helyett a kísérlet volt. Mérési eredményeim számítógépes feldolgozását táblázatok átalakításával, adatbáziskezelő rendszerre alapozott SQL lekérdezésekkel, saját adatbázisok készítésével, és többségében saját programokkal végeztem. A dolgozatban szereplő diagramokat részben saját fejlesztésű programokkal állítottam elő.

Az egy intézményben végzett méréseket esettanulmányként azonosítottam [7, pp. 129-156], általános érvényességüket indukció útján, azokat más egyetemek informatikai rendszereinek reprezentatív mintáján azonos környezeti feltételek mellett elvégezve igazoltam.

A kutatási adatok összegyűjtésére közérdekű adatigénylést, valamint interneten elérhető statisztikák felkutatását alkalmaztam. Meglevő fejlesztési tapasztalataim alkalmazásával a Hackmageddon adatfájljainak feldolgozását MySql adatbázisba konvertálás után dolgoztam fel, az adatok kiértékelésére Python nyelvű programokat és Unix shell scripteket készítettem.

Tekintettel arra, hogy a kutatás megkezdésekor adataim és azok összefüggései még ismeretlenek voltak, azok összegyűjtésére és elemzésére, valamint az egyes informatikai rendszerek lehetséges adatkapcsolati térképének létrehozására a grounded theory módszerét alkalmaztam [7, pp. 83-128].

A munkatársak információbiztonság-tudatossággal kapcsolatos viselkedési mechanizmusainak esettanulmánya során interjúk helyett az akciókutatás módszerét alkalmaztam annak érdekében, hogy megállapításaim egy adott helyzet elvárt válaszai helyett valós környezetben mért reakciókon alapuljanak [8, pp. 440-456].

A kitűzött célok elérése érdekében vettem részt tudományos és szakmai konferenciákon, melyek során feldolgoztam, elemeztem és értékeltem más intézmények informatikai rendszereiről, környezetéről, valamint az azokban alkalmazott megoldásokról szerzett tapasztalatokat. Információt gyűjtöttem a felsőoktatás azonos területein dolgozó kollégáktól és szakemberektől. Annak érdekében, hogy minél pontosabb képet kapjak a felsőoktatási informatikai rendszereket ért incidensekről, elsősorban másodlagos forrásból folyamatosan gyűjtöttem a rájuk irányuló kibertámadások aktualitásait, folyóiratok, mértékadó szakfolyóiratok és tudományos kiadványok cikkeit, valamint nyílt és zárt internetes közösségek szakmai konzultációit.

Kutatási eredményeimet különböző folyóiratokban publikáltam, több szakmai és tudományos konferencián ismertettem azokat, emellett törekedtem további szakmai ismeret megszerzésére és az azonos területen dolgozó munkatársak közös munkába való bevonására.

2. Adatvagyon a magyar felsőoktatási rendszerekben

Az arányos és költséghatékony védelem kialakításának első lépése az informatika rendszerekben tárolt védendő értékek azonosítása. Magyarországon eddig nem történt meg az egyetemi adatvagyon tudományos igényességű vizsgálata, ezért következtetések levonásához saját tapasztalataimat és külföldi forrásokat vettem alapul. Sajnos a témát tárgyaló nemzetközi tudományos szakirodalom sem túl széles. Ulven és Wangen 2021-es szakirodalmi áttekintésében 18 tudományos igényű cikket, és 14 egyéb forrást (fehér könyveket, műszaki jelentéseket, szakdolgozatokat, szakmai weboldalakat) kutatott fel [9]. 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 konferenciaelőadások voltak, melyek közül csak hat volt publikusan is elérhető. A hivatkozott források közt egyetlen magyar sem volt, továbbá utalás sem szerepelt a hazai egyetemekre [10]. Bár a hazai és nemzetközi összehasonlításban számos azonosság állapítható meg meg, melyet a linzi székhelyű Johannes Kepler Universität-en végzett tanulmányutam során készített interjú 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, az azt működtető rendszerek sebezhető pontjait, továbbá azokat a tényezőket, amelyek következtében a védelmi megoldások szükségszerűen eltérnek más területekétől.

2.1. Jogszabályi és szervezeti háttér

A magyar kiberbiztonsági keretrendszer aránylag jól meghatározott, és lefedi azokat a jogi és szervezeti területeket, amelyek a kibervédelem ellátásához szükségesek. A stratégiai háttér alapját a Nemzeti Biztonsági Stratégia [11] és a Nemzeti Kiberbiztonsági Stratégia [1] adja. Ezt a 2013-as kormányrendeletet az informatika gyors fejlődése okán, az EU hálózati és információs rendszerek biztonságáról szóló irányelvével való szoros összhang, és a 2022-ben kialalkult háborús helyzet által jelentett magasabb kockázat következtében célszerű lenne rövidebb időközönként aktualizálni.

Magyarország Nemzeti Biztonsági Stratégiája kiemelten foglalkozik a magyar kibertér védelmével, a kibertérből érkező támadásokkal, azok negatív hatásainak elkerülésével. Katonai szempontú megközelítése összhangban van a NATO stratégiai koncepciójával és nemzetközi gyakorlattal, mely a kiberteret az ötödik műveleti térként határozza meg, melyen keresztül a

jelentős anyagi károkozására képes képességeket fegyverként definiálja. Feladataként határozza meg a magyar honvédség kiberképességeinek fejlesztését és a nemzetközi együttműködést. Kiemelten védendő szektorként nevezi meg az e-közigazgatást, közműszolgáltatást, stratégiai vállalatokat és a létfontosságú rendszerelemeket. A kibertámadások jellemző elkövetői körét a szervezett bűnözők csoportjaiban, nemzetközi terrorszervezetekben, szélsőséges vallási közösségekben, magán biztonsági cégekben, kiberbűnözői körökben és egyéb transznacionális hálózatokban határozza meg. Kiemeli kibertámadások intenzitásának erősödését, az erre irányuló kutatások fontosságát, valamint kitér a felhasználói információbiztonság jelentőségére, [11], melyet számos egyéb kutatás is megerősít [12] [13].

Magyarország Nemzeti Kiberbiztonsági Stratégiájának fő célja a döntéshozó politikai és szakmai irányítók figyelmének felhívása a kiberbiztonsági problémák létezésére és kezelésére [1]. A stratégia igazodik a Cyber Security and Defence 2012/2096(INI) [14] ajánlásaihoz, a NATO 2010-es stratégiai koncepciójához [15], a 2011-es kibervédelmi politikájához és a Szövetség kibervédelmi elveihez és céljaihoz [16]. Sem a Nemzeti Biztonsági Stratégia, sem a Nemzeti Kiberbiztonsági Stratégia nem tesz említést felsőoktatási intézményekről.

A magyar kibervédelem szervezeti hierarchiájának csúcsán a Miniszterelnöki Kabinetiroda áll. Az állami és önkormányzati szervezetek felügyeletét a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el, mely több szakmai területet fed le. A kibertérből érkező fenyegetettségek, illetve támadásokra specializált szervezet a nemzeti CSIRT.

Az elektronikus információs rendszerek biztonságának felügyeletéért felelős hatóság feladata a jogszabályok érvényesítése. A Nemzeti Infokommunikációs Szolgáltató Zrt. a törvény hatálya alá tartozó szervezetek mellett államigazgatási szervek és országos hatáskörű intézmények számára biztosít központosított infrastruktúrát és kapcsolódó szolgáltatásokat.

A fenti szervezetek nem nyújtanak szolgáltatásokat az akadémiai szféra számára. A katonai Nemzetbiztonsági Szolgálat (KNBSZ) kizárólag a Honvédelmi Minisztérium Katonai Nemzetbiztonsági Szolgálatán belül működik. A GovCert tevékenysége a felsőoktatásban csak másodlagosan jelenik meg. Tapasztalatom szerint a Kibervédelmi Intézet az önkormányzati és kórházi rendszerek sérülékenységeit rendszeresen vizsgálja, azokat célszoftverekkel elemzi és jelzi az érintett szervezetek vezetői számára a feltárt problémákat. Ezirányú tevékenységüket előre jelzik az üzemeltetők számára, de azok az eseménynaplók ellenőrzésekor egyértelműen nyomon követhetők. A felsőoktatás számára ezek a szervezetek sem nyújtanak ilyen szolgáltatást, így néhány kivételtől eltekintve csak az onnan kiinduló spam tevékenység jelzése során kerülnek kapcsolatba velük. Az elhárítási tevékenység terén még rosszabb a helyzet. A magyar CSIRT-eknek (Computer Security Incident Response Team) szintén nem célja a felsőoktatás védelme,

ilyen tevékenységet nem végeznek. Ugyanakkor ezek a szervezetek tevékenysége jogi szempontból is korlátozott, nem minősülnek nyomozóhatóságnak, és egy támadás érzékelése esetén aktív ellentevékenység végrehajtására sincsenek jogosítványaik.

A felsőoktatás számára két szervezet láthat el CSIRT feladatokat, a Hun-CERT és a KIFÜ (Kormányzati Informatikai Fejlesztési Ügynökség) CSIRT-je. Az előbbi deklarált célja a teljes magyar internetes közösség számára nyújtott szakmai és hálózati biztonsági szaktanácsadás nyújtása. A KIFÜ az ITM irányításával működő szervezet, melynek többek közt a magyar köznevelés, felsőoktatási és kutatási intézmények, valamint közgyűjtemények informatikai infrastruktúrájának fejlesztése és az arra épülő szolgáltatások nyújtása, emellett a már említett KIFÜ CSIRT működtetése. Ennek díjmentesen igénybe vehető fő szolgáltatásai a kiberbiztonság támogatása, incidensek megelőzése és elhárítása, valamint rendszeres tájékoztatók nyújtása.

Sajnos egyik CSIRT számára sem elsődleges feladat a felsőoktatás védelme. A KIFÜ feladatköre az elmúlt években kibővült a középfokú oktatási intézményekkel, melyekben lényegesen több informatikai védelmi feladat jelentkezik, mint a felsőoktatásban, ezért a rendelkezésükre álló erőforrások erre a területre koncentrálódnak. Sajnos a kezdeti pozitív kilátások ellenére nem terjedtek el sem a CSIRT-re alapozott szolgáltatások, sem a felsőoktatási intézményekre irányuló rendszeres sérülékenységvizsgálatok.

A kutatóintézetek és a kutatási eredmények védelme sem általános hatályú jogszabályok mentén történik. A nemzetbiztonsági védelem alá tartozó intézmények esetében a Nemzetbiztonsági Szakszolgálat ellátja az információbiztonsági feladatkörben a kibertérből érkező fenyegetésekkel szembeni védelmet, valamint szigorúbb adatvédelmi eljárások betartására kötelezi az érintett szervezeti egységeket, de ez nem fedi le a magyar kutatási intézmények teljes palettáját.

A nemzetközi gyakorlatban sem találtam példát kifejezetten oktatási intézményekre szabott szabályzásra, ugyanakkor egyes országokban elindultak olyan folyamatok, melyek a felsőoktatási intézményeket is érintik. Az Egyesült Államokban, Kalifornia Államban 2003. júniusától hatályos a Civil Code 1798-as jogszabálya a 82. paragrafusában előírja, hogy „a mások számára számítógépes adatokat kezelő vállalkozásoknak értesíteniük kell az adatok tulajdonosait, ha azok jogosulatlan felhasználó birtokába jutnak” [17]. Az incidensek emelkedő száma és a kiszivárgott adatok riasztó mennyisége miatt néhány év alatt hasonló törvény lépett életbe az ország más államaiban is, ami rávilágított arra, hogy számos incidens történik az oktatási rendszerekben is. 2011-től Ausztrália, Kanada, India, Olaszország, Pakisztán, az Egyesült Király-

ság, Norvégia, Új-Zéland, Belgium, Mexikó és Marokkó esetében is regisztráltak ilyen eseteket, melyek a bejelentési kötelezettség általános terjedése felé mutatnak, és világossá teszik a szabályzás szükségességét.

Ausztrália Belügyminisztériumának Kritikus Infrastruktúra Központja 2020-ban közreadott tervezete a felsőoktatási intézményeket ért támadások megnövekedett száma miatt a kritikus infrastruktúrák körébe sorolná azokat, vállalva a velejáró műszaki fejlesztések finanszírozási kötelezettségeit is [18, pp. 3-4].

A magyar jogszabályi környezet tehát nem rendelkezik közvetlenül a felsőoktatás informatikai védelmi szabályzásáról. A 2011. évi CCIV. törvény a nemzeti felsőoktatásról keretbe foglalja a felsőoktatási intézmények működését és említést tesz informatikai vonatkozású elemekről is, de semmilyen, az informatikai rendszer üzemeltetési szempontú szabályzására vonatkozó kitételt nem említ [19].

A 2012. évi C. törvény XLIII. fejezete rendelkezik a tiltott adatszerzésről és az információs rendszerek elleni bűncselekményekről, a XXXVI. fejezet az információs rendszer felhasználásával elkövetett csalásról, rendszer-, és adatsértésről valamint azok büntetési tételeiről. Védelmi feladatokat a törvény egyáltalán nem definiál [20].

Az Európai Unió Általános Adatvédelmi Rendelete az Európai Unió és az Európai Gazdasági Térség területén élő valamennyi személy adatvédelméről és a magánéletének védelméről szóló uniós jogi szabályozás. E rendelet célja, hogy az adatvédelmi jogszabályokat egységesítse az EU-n belül, és hatálya alá tartozik minden olyan szervezet, amely az EU-n belül élők adatait kezeli függetlenül a kezelő székhelyétől. A GDPR jogot biztosít a magánszemélyek számára a személyes adataikhoz való hozzáféréshez, azok helyesbítéséhez vagy törléshez. Korlátozhatják az adataik felhasználását, a profilalkotást, valamint az őket érintő automatizált döntéshozatalt is [4].

Annak ellenére, hogy a nemzetközi gyakorlat nem sok területen különbözik a magyartól, egyes országokban felismerték a szféra adatvédelmének fontosságát. Számos ország esetében fogalmaznak meg ajánlásokat a kritikus infrastruktúrák számára [21], amelyet más szervezetek is alkalmazhatnak a saját működésük biztonságossá tételére, ez elérhető és ajánlható az akadémiai szféra számára is. Az egyik ilyen figyelmet érdemlő ajánlást az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST) adta ki NIST Roadmap for Improving Critical Infrastructure Cybersecurity címmel, melynek fő célja a költséghatékonyság szem előtt tartásával a köz- és magánszféra, valamint a társadalmi, gazdasági és iparági szereplők számítógépes kockázatainak csökkentésére irányuló védelmi célú szabványok, iránymutatások, módszerek és jógya-

korlatok biztosítása. Az ajánlás három részből épül fel: a keretrendszerből, a végrehajtási szintekből és a keretprofilokból [22]. A végrehajtási szintek tulajdonképpen a szervezet érettségét írják le, vagy annak elérését tűzik ki célul a kockázatkezelési folyamat, az integrált kockázatkezelési program és a külső szervezetek részvétele szempontjából, a részlegestől az adaptív szintig. A keretrendszer segítségével felépíthető a szervezeti profil, amely tartalmazza, hogy melyek az adott szervezetre vonatkozó kockázati területek, azonosítja azok követelményeit, valamint rögzíti a kockázatviselési tolerancia szintjét. Ebben rejlik a NIST keretrendszer rugalmassága: a védendő informatikai rendszer függvényében minden szervezet egyénileg szabhatja testre a védelmi stratégiáját [21].
A keretrendszer felépítése és az ajánlott metodika alkalmazása esetén a szervezet információs rendszerének és adatvagyonának védelmi rendszere a szervezet szükségleteinek és a vállalható anyagi kondícióknak megfelelően építhető fel, az ajánlás rendszeres frissítésének és aktualizálásának követése biztosítja annak érvényességét a jövőben is.

A felsőoktatási intézmények jogszabályi környezetében várhatóan a 2023 januárjában megjelent NIS2 irányelv hoz változást [23]. 2016-os elődjének célja a kiberbiztonság javításával kapcsolatos jogszabályi környezet javítása volt, melyet az informatikai rendszereket ért incidensek számának akkori jelentős növekedése indokolt. Amellett, hogy a NIS hatályba lépését követően az egyes tagállamok eltérően értelmezték az abban foglaltakat, az azóta megszaporodó zsarolóvírus támadások, a Covid 19 helyzet tanulságai, az informatikai rendszerek orosz-ukrán háborús konfliktus következtében megnövekedett kitettsége, valamint (feltehetően) a mesterséges intelligencia ugrásszerű fejlődése indokolták az irányelv újra alkotását az érintett szervezetek körének kiterjesztésével, a kiberbiztonsági incidensek kezelésének és jelentési kötelezettségének szigorításával, továbbá a személyes felelősség bevezetésével. A felülvizsgálat szükségszerűségét indokolta a kiberbiztonsággal kapcsolatos információk központi kezelésének elégtelensége mellett a közös válságkezelés hiánya és tagállamonként történő eltérő kezelése is.
A NIS2 számos új követelményt fogalmaz meg, miközben a korábbiak szigorítását javasolja, és jelentősen bővíti az érintett intézmények körét is. Míg a NIS elsősorban a kritikus infrastruktúrákra (energia, közlekedés, vízellátás, egészségügy stb.) és digitális szolgáltatókra (elektronikus kereskedelem, felhőszolgáltatók stb.) koncentrált, a NIS2 hatálya lényegesen szélesebb körre terjed ki úgy, hogy az adott ágazat érvényben levő jogszabályaival koherens módon alkalmazható maradjon. A kiemelten kritikus ágazatok közt a digitális infrastruktúra, az internet- és felhőszolgáltatás mellett kiemeli a DNS szolgáltatás meghatározó szerepét, és előírja a re-

gisztrációs és adatszolgáltatási kötelezettségüket, mely alapján az ENISA létrehozza ezen szervezetek nyilvántartását. Az irányelv szándéka szerint a központi bankok, az igazságszolgáltatás, a bűnüldözés, a nemzetbiztonság és a közbiztonság kivételével minden közepes- és nagyméretű szervezet a hatálya alá tartozik, függetlenül az általuk kezelt adatok mennyiségétől vagy érzékenységétől. Ezzel a NIS2 magyar jogrendbe való beépülése magával hozza a nagyobb létszámú felsőoktatási- és kutatóintézmények kötelezettségeinek szigorítását is.

Az érintett szervezeteknek a korábbinál sokkal magasabb szintű informatikai biztonsági követelményeknek kell megfelelniük. Fel kell mérniük az őket fenyegető kibertámadások lehetséges hatásait, kockázatelemzést kell végezniük, melyeknek koherens módon kell megjelennie az informatikai szabályzatokban is, az utóbbinak előírásokat kell tartalmazniuk az alkalmazott biztonságos protokollokra, a kriptográfiai és hitelesítési eljárásokra. Tesztelt incidensmegelőzési tervekkel kell rendelkezniük, kockázatkezelési folyamataikat a lehetséges veszélyhelyzetekre adaptálva kell kialakítaniuk. Rendelkezniük kell üzletfolytonossági tervvel és katasztrófa utáni helyreállítási tervvel is, ezekkel kapcsolatban az irányelv külön kiemeli az adatmentések fontosságát. A dokumentum külön kitér a kiberbiztonsági képzések és kiberhigiéniai gyakorlatok jelentőségére is.

További szigorítások jelennek meg a tájékoztatási kötelezettségekkel kapcsolatban, az incidenst elszenvedő szervezeteknek 24 órán belül jelenteniük kell azokat a biztonsági eseményekre reagáló csoportok vagy az arra kijelölt hatóságok számára, akik segítséget nyújtanak azok kezelésében. A NIS2 a tagállamok számára előírja egy koordinációs szervezet kijelölését, mellyel megerősíti a hatóságok együttműködését nem csak az incidensek kezelésében, hanem az azzal kapcsolatos adatok megosztásában is; így egy fenyegetésre a jövőben várhatóan nem csak helyi, hanem Európai Uniós reakció is adható. Emellett a jogalkotó a jelentéktelen incidensek bejelentési kötelezettségeinek újra gondolásával észszerűbbé teszi a védekezés összehangolását, és meghatározza a jelentős incidensek körét, melynek lényeges pontjai a szolgáltatási képesség megzavarására vagy annak lehetőségére, a jelentős pénzügyi vagy nem vagyoni kár okozására vagy annak képességére irányulnak.

A NIS2 a végrehajtásban kiemeli a vezetői támogatás fontosságát. 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 bevételével arányos, nagy összegű bírság kiszabásának lehetőségét írja elő.

Az irányelv magyar jogszabályi környezetbe történő beépítése dolgozatom írásakor még nem történt meg, erre a hatályba lépését követően 21 hónap áll rendelkezésre. Hatása kiterjed majd

más jogszabályokra is, feltehetően változni fog az infotv., a 2013 évi L. törvény és a kapcsolódó 41/2015 BM rendelet is. Az irányelv alapján módosuló jogszabályok várhatóan komoly szigorításokat hoznak majd a felsőoktatási intézmények számára is, és hatással lehetnek a jelenleg még szabadon elvégezhető sérülékenységvizsgálatokra is.
Ki kell emelni az irányelv megvalósításának a szervezetek költségvetésére gyakorolt hatását: az informatikai eszközök naprakész állapotban tartása, a támogatás nélküli szoftverek kivezetése, a felügyeleti eszközök beszerzése és működtetése, a munkatársak és üzemeltetők képzése, valamint a szabályzati és dokumentációs feladatok ellátása az intézmények büdzséjét jelentős mértékben megterhelheti.

2.2. Értékek a felsőoktatásban

A 2013. évi L. törvény (Ibtv.) az állami fenntartású szervezetek és önkormányzatok számára előírja a szervezeti egységeik biztonsági szintekbe, valamint az informatikai rendszereik biztonsági osztályokba sorolását. Ennek részletes végrehajtásához a 41/2015-ös BM. rendelet nyújt konkrét és részletes szakmai útmutatást [3]. Az akadémiai szféra intézményei általánosságban nem tartoznak e jogszabályok hatálya alá, így nem is kell az említett feladatokat elvégezniük, ugyanakkor alkalmazása kiváló alapot adhatna a védelmi mechanizmusok kialakítása mellett a szabályzatok egységesítésére is. A kötelezettség hiánya ellenére az egyetemek informatikai biztonsági szabályzatai részben megkísérlik e jogszabály alkalmazását, többé-kevésbé azonosítják rendszereiket, és egy besorolást is adnak. A szervezeti egységek besorolásának meghatározására viszont csak két egyetem esetében találtam példát.

Annak ellenére, hogy a besorolás meghatározására a 2013 évi L. törvény és a 41/2015-ös BM rendelet részletes útmutatást nyújt, rendszereiket az egyetemek eltérően osztályokba sorolják. Ennek fő oka nem csak a jogszabályokban leírtak rugalmasságában gyökerezik, hanem abban is, hogy ezt a tevékenységet rendszerint informatikai munkatársak végzik, melynek során listázzák az egyes informatikai alrendszereket (például elektronikus levelezés, hallgatói nyilvántartás, VPN-kapcsolatok, hálózati szolgáltatások stb.) és saját szempontjaik alapján választják ki a biztonsági osztályt. E módszertan alkalmazása jól érzékelhető a magyar egyetemi szabályzatok áttekintése során. Ez eszköz- és funkcióközpontú meghatározást eredményez, amely rendszerszintű információ hiányában csak részlegesen veszi figyelembe az intézmény valódi céljait, így attól jelentősen eltérhet. A mérnöki szemléletű informatikai munkatársak és az intézményi vezetők pedig valószínűleg teljesen máshová helyezik a súlyponti kérdéseket.

Az értékek azonosítása az intézmények eltérő szervezeti felépítése következtében különböző területi vezetők felelőssége, amelynek során meghatározzák az intézmény számára értékes adatok körét, az előállításukat megkövetelő célokat és azok elérésükhöz szükséges fő követelményeket. Szinte minden egyetem esetében ilyen a hallgatói létszám növelése, az oktatás színvonalának emelése, a tudományos publikációk mennyiségi vagy minőségi javítása, valamint az intézmény által kiadott diplomák értékének szakmai körökben vagy közvéleményben történő elismertetése. Ez számos feltételt támaszt, szolgáltatást és egyéb támogatást igényel, amelyek számszerűsítésére a kulcsfontosságú teljesítménymutató (*Key Performance Indicator,* KPI) alkalmazható. A KPI-k azonosítása a célok eléréséhez szükséges elemeket mérhetővé teszik, így leírhatóvá és összehasonlíthatóvá válnak. A KPI-k azonosítása nem csak informatikai szempontból lényeges. Valójában számos olyan létezik, amelynek nincs informatikai vonatkozása, de meghatározásuk az intézményi informatikai folyamatok súlyának azonosításában jelentős szerepet játszanak. A felsőoktatási KPI-k képzésére Ballard doktori disszertációja nyújt példát, melyben az Amerikai Egyesült Államok 34 felsőoktatási intézményének 2139 különböző kulcsfontosságú teljesítménymutatóját vizsgálta, amit 24 kategóriába sorolt be, és azonosította azon adatok és folyamatok körét, amelyek az intézményi célok eléréséhez szükségesek [24]. Kutatása alapján a felsőoktatási rendszerek általános értékei személyes, oktatási, kutatási és működési adatokat tartalmazó csoportokba sorolhatók.

2.3. Személyes adatok

Az egyetemek egyik legértékesebb adatköre személyes adatokból áll. A McDonald Hopkins fehér könyve az amerikai egyetemek esetében nemcsak hallgatók, oktatók és kutatók személyes adatait említi, hanem adományozók, kurátorok, igazgatósági tagok, öregdiákok, diákok, szülők, jelentkezők, személyzet, betegek mellett fogyasztók és eladók adatait is [25]. Ezek egy része a magyar egyetemek esetében kulturális, működési és finanszírozási különbségek miatt nem áll rendelkezésre vagy nem is értelmezhető (például hazánkban a végzett hallgatók támogató szerepének jóval kisebb hagyománya van, 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 a hallgatói nyilvántartást nevezte meg a legfontosabb adatforrásként egy ghánai egyetemen [26]. A magyar elektronikus tanulmányi rendszer[2] kifejezetten nagy mennyiségű személyes adatot tartalmaz, a hallgatók általános adatai mellett a felvételi információit, korábbi iskoláik, nyelvvizsgáik részletes adatait, a teljes

[2] Tanulmányi rendszerként a magyar felsőoktatásban jogszabályi okokból kizárólag a Neptun alkalmazható, melyet elsőként 1997-ben a Budapesti Műszaki Egyetemen vezettek be.

tanulmányi történetüket, ösztöndíj és tandíj adatokat, és olyan, rendszerint valamilyen csökkent képességet leíró egészségügyi adatokat is, amelyeknek a tanulmányok során szerepe lehet[3].
A tanulmányi rendszer nem csak hazai, hanem nemzetközi viszonylatban is nagy mennyiségű és érzékeny adatokat tartalmaz. Egy olyan incidens, amely az ebben tárolt adatok sérülését vagy nyilvánosságra kerülését eredményezné, az adott egyetem reputációját is jelentős mértékben gyengítené, mely akár az oda jelentkező hallgatók számának csökkenésében is megnyilvánulna. Egy jelentős adatszivárgás következménye a GDPR-ban meghatározott súlyos büntetési tétel kiszabása lehetne, mely a legtöbb magyar egyetem esetében komoly anyagi forrásvesztést eredményezne, akár működési zavart is okozhatna. Bár ilyenre Magyarországon eddig nem volt példa, dolgozatom írásakor az általános- és középszintű oktatási intézmények tanulmányi rendszerét, a Krétát érintő, nagy mennyiségű adat szivárgásával járó incidens vizsgálata még nem zárult le.
A tanulmányi rendszer adatainak végleges elvesztése a legsúlyosabb következményekkel járna egy felsőoktatási intézmény számára. A tanulmányaikat folytató hallgatók tantárgy- és vizsgaeredményeinek elvesztése lehetetlenné tenné a követelmények teljesítésének ellenőrzését, körülményesen lennének kiadhatók a korábbi diplomák, és nehézkessé válna az államilag támogatott félévek elszámolása is. A rendelkezésre állást érintő incidensek elsősorban a tárgyfelvételi- és vizsgaidőszakban okoznának komolyabb működési problémákat, melyek végső soron a tanulmányi vagy vizsgaidőszakok rendjét is negatívan befolyásolhatnák. Bár a rendszer adai részben más forrásból pótolhatók (például a befizetett tandíjak esetében) a tanulmányi rendszert ért végzetes incidens az adatvesztés az intézményen belül nem oldható meg, így szintén komoly reputációs kárt okozna.
A nagy mennyiségű adat megfelelő kezelése különleges felelősséget ró az akadémiai szférára is, miközben ismertek ezzel kapcsolatos jogsértések is. A Nemzeti Adatvédelmi és Információs Hatóság (NAIH) több jogellenes adatkezeléssel kapcsolatos eljárást indított egyetemek hibás adatkezelési gyakorlata miatt [27] [28]. Az informatikai incidensekkel kapcsolatos valós kép megismerését nagyban nehezíti, hogy a bejelentési kötelezettség ellenére az a gyakorlatban az ritkán történik meg.

2.4. Oktatási- és kapcsolódó rendszerek

A jelenléti oktatás fellazítására egyre több egyetem törekszik. A Covid19 következtében, 2020-ban bevezetett kényszerintézkedések egyértelművé tették, hogy az egyetemi kurzusok bizonyos

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

területein az IKT-eszközökre alapozott távolléti rendszerű oktatás további fenntartása csökkentheti a hagyományos kontakt órák számát, miközben a hallgatók rugalmas időbeosztását is lehetővé teszi. Ugyanakkor a távolléti oktatás hatékonyságát többen is megkérdőjelezik. Butnaru és társai 2021-ben vizsgálták a távolléti oktatás különböző aspektusait. A Covid19 által kikényszerített változást átmenetinek jósolták, és úgy vélték, annak végén az oktatási tevékenységek formája visszatér az eredeti állapotába. A Covid helyzet alatti körülményeket ideiglenesnek tekintik, nem pedig egy új oktatási rendszer létrehozásaként, ezért annak lezárultával az online képzési mód kivezetésére törekszenek [29].

A felsőoktatás oktatói számára a tananyagok elektronikus formára alakítása és LMS *(Learning Management System)* rendszerekbe adaptálása a járvány előtt is gyakran alkalmazott lehetőség volt, ezek alkalmazása az elmúlt években viszont tömegessé vált. Ezeken a területeken jól érzékelhető, hogy az egyetemek a pandémia végével nem tértek vissza teljes egészében az oktatásszervezés korábbi, jelenléti formájához. Az Eszterházy Károly Katolikus Egyetemen a felnőttoktatásban és a levelező képzésben az elektronikus oktatási módok alkalmazásban maradtak, és más intézményekkel együtt a távolléti oktatási forma további alkalmazása mellett döntöttek, míg az Nemzeti Közszolgálati Egyetem az online oktatás lehetőségének minimalizálására törekszik. A korábban általános szóbeli vizsgák helyét egyre inkább a gépi számonkérések vették át, melyekkel kapcsolatban általános kritikaként merült fel, hogy néhány terület kivételével[4] nem voltak képesek a vizsgázó tudásának korábbi színvonalú mérésére, és a hangsúlyt az összefüggések felismeréséről és alkalmazásáról az egyes részletek felidézésére helyezték át. Az online vizsgák hatékonyságát tovább rontotta a mesterséges intelligencia alapú nyelvi modellek ugrásszerű fejlődése, mely egyetemi vizsgakérdéseket is képes eredményesen megválaszolni [30]. Bár az LMS rendszerek adattartalma és más rendszerekkel történő adatcsere folyamatai egyetemenként is eltérők, egy alkalmas sérülékenység kihasználásával a gyakorlati- és vizsgaeredmények módosítása lehetségessé válhat, így az ilyen támadások egyértelmű motivációt jelenthetnek belső és külső támadók számára [31].

Az LMS rendszerek mellett általános a szakmai gyakorlatok menedzselését ellátó szakrendszerek működése is. Ezek működésére nincs általános ajánlás, és gyakran saját fejlesztésként kerülnek megvalósításra. Kialakításuktól függően számos személyes adatot tartalmazhatnak, adatkapcsolataik révén más rendszerek adataihoz is hozzáférhetnek.

[4] A magyar online akkreditációval rendelkező nyelvvizsgák sikeresen működtek a járványhelyzet alatt is.

2.5. Kutatási adatok

A tudományos kutatás az akadémiai szféra intézményeinek egyik elsődleges tevékenysége. Kutatási adataik körébe a nyers és feldolgozott kutatási adatok, tudományos ismeretek, elemzések eredményei és tudományos publikációk tartoznak [32]. A FireEye tanulmányában kulcsfontosságúként minősíti a vállalati, kutatási és harmadik féltől származó adatokat, például az ipari együttműködések során az intézmények számára átadott adatokat [33]. Giszczak kutatásában olyan projektekre is kitér, amelyekben egyetemi kutatások kormányzati együttműködésből származó adatokat használnak fel [25].

A tudományos eredmények ma már nem jöhetnek létre informatikai háttértámogatás nélkül. A kutatási adatok eltérő értékűek, kibervédelmi szempontból viszont kiemelt figyelmet érdemelnek azok, amelyek gazdasági, ipari vagy pénzügyi területen olyan eredményeket állítanak elő, amelyek az azt birtokló gazdasági élet szereplőit előnyös helyzetbe hozhatják. A felsőoktatás kiemelt védelme nemzetközi viszonylatban is megjelenik, az ausztrál kormányzat tervei szerint az ország felsőoktatási intézményeit elsősorban a kutatási feladatokban vállalt kiemelkedő fontosságú szerepük miatt a kritikus infrastruktúra-elemek közé sorolja, és kötelezi őket a besorolásnak megfelelő informatikai védelem kialakítására [18].

2.6. Működési adatok

Az egyetemek magas költségvetésű intézmények, amelyek gazdasági tevékenysége az átláthatóság biztosítása érdekében nagyrészt nyilvános. A pénzügyekkel kapcsolatos feladatokat a legtöbb intézmény esetében önálló szervezeti egységek, akár teljes 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, amelyek hosszan sorolhatók a vegyszerek raktározásának nyilvántartásaitól a tűzjelző berendezések ellenőrzésének jegyzőkönyveiig. A gazdasági terület legfontosabb elemei a munkaügyi-, bér- és gazdasági folyamatokat kezelő szoftverek, melyek ma részben egy állami fenntartású rendszerben működnek függetlenül attól, hogy a fenntartó az állam, valamilyen alapítvány vagy egyház. Az ezekben tárolt adatok biztonságát kizárólag adminisztratív, arra az üzemeltetővel szerződésben meghatározott garanciák biztosítják. Az egyetemek kitettségét ezen a területen fokozza, hogy legtöbbjük nem rendelkezik kivonási stratégiával, az abban tárolt adatokról nem készíthetők helyi másolatok, de ha még volna is erre lehetőség, az azt kezelő szoftverrendszer hiányában nem 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 vezetésének, és a helyi informatikai személyzet felelőssége másodlagossá válik.

2.7. Összegzés

A fejezetben bemutattam a magyar felsőoktatási rendszerekben található adatvagyon fő csoportjait és a védelmüket meghatározó legfontosabb aspektusokat. Összefoglaltam a jogszabályok és az intézmények szervezeti kereteit és kapcsolódó szervezeteit, melyek az adatvagyon kezelésében meghatározó szereppel bírnak. Szakirodalmi kutatás alapján feltártam a szektor fő értékeit és megmutattam, hogy személyes adatok mellett elsősorban a gazdasági-működési, valamint tudományos adatok védelme elsődleges cél. A nemzetközi szakirodalmi források elemzése bizonyítja, hogy a magyar és a külföldi felsőoktatási intézmények adatbiztonságát befolyásoló tényezők csak részben azonosak, köztük számos különbség lelhető fel.
A magyar felsőoktatás adatvagyonának jellege, fő jellemzőinek és környezetének feltárása dolgozatom hipotéziseinek kidolgozásához nélkülözhetetlen.

3. A felsőoktatás informatikai szabályzatainak elemzése

H1. hipotézis bizonyításához elsőként megmutatom, hogy a felsőoktatási rendszereket érik kibertámadások, összehasonlítom azokat más szektorokkal, elemzem az alkalmazott támadási módszereket és a támadások motivációit. Eredménye támpontot nyújt a védelem megtervezéséhez és kialakításához, az elemzések periodikus ismétlése esetén azok finomhangolásához. Az intézmények informatikai szabályzatainak elemzése során meghatározom adatvagyonukat, és bizonyítom, hogy az informatikai rendszereiket heterogén módon sorolják be.

3.1. Kiberfenyegetettségek a felsőoktatásban

Számos egyetem szenvedett már el különböző informatikai incidenst, melyekről hazai viszonylatban leginkább kibervédelmi híradásokból, és egyetemek informatikai üzemeltetőinek beszámolóiból alkothatunk képet [34]. Tudományos források a felsőoktatási intézmények adatszivárgásainak emelkedő számát mutatják [35], mely az adatbiztonságra irányított figyelem hiányával is párosul: a Joint Information Systems Committee (JISC) felmérésében a hallgatók 39%-a rendelkezett valamilyen ismerettel arról, hogy egyetemük hogyan tárolja és használja fel személyes adataikat, emellett az intézmény adatvédelmi szintjét csak 15%-uk értékelte 80%-nál magasabbra. Chapman 2019-es kutatása szerint az adathalász támadások egyre kifinomultabb módszerekkel irányulnak az ösztöndíj vagy tandíj be- és kifizetések folyamatának megzavarására. Ugyanez a forrás említi az emelkedő számú whaling-et[5], valamint a legegyszerűbb, lándzsás adathalászatot is: utóbbi alkalmazásával a JISC egy egyetem legértékesebb adataihoz 2 órán belül fért hozzá [36]. A magyar felsőoktatási intézmények érintettségének megállapításához, a bekövetkező incidensek számának és súlyosságának meghatározásához, valamint statisztikai módszerekkel történő elemzésükhöz konkrét adatokra van szükség.

Nemzetközi viszonylatban több, elsősorban amerikai adatforrásra támaszkodhatunk. Az ottani tendenciákból vonhatunk le következtetéseket a várható hazai változásokra is, de azok nem alkalmazhatók a különbségek figyelembevétele nélkül. Sajnos a különböző forrásokból származó adatok eléggé eltérő képet rajzolnak ki. Az Open Security Foundation szerint az összes biztonsági incidens 35%-a a felsőoktatásban történik, ezt személy szerint túlzónak tartom [33]. Giszczak kutatása szerint 2016 első felében 50%-kal nőtt a felsőoktatási adatokkal kapcsolatos jogsértések száma. Munkájában bemutatja, hogy a reputációs veszteség megjelent a kutatási

[5] Bálnavadászat. Az adathalászat egy speciális formája, amelyben a támadók célzottan, adott pozícióban lévő munkatársat vagy vezetőt támadnak vagy igyekeznek megtéveszteni. Céljuk általában bizalmas információk megszerzése, vagy pénzügyi tranzakciók végrehajtása.

támogatások és az adományok megszerzésekor, amelynek kárértékét kiszivárgott rekordonként hozzávetőleg 300 dollárban határozta meg [25].

A Verizon 2022-es „Data Breaches in Education" riportjának az oktatási szférát elemző fejezetének főbb pontjai szerint az USA-ban 1.241 incidens történt, ebből 282-t erősítettek meg több forrásból. A rendszerekbe történő belépés, alapvető webes alkalmazások támadása és egyéb hibák a jogsértések 80%-át tették ki. A betörések 25%-át belső szereplők, 75%-ukat külső támadó kezdeményezte, melyek célja 95%-ban volt anyagi haszonszerzés, és csak 5%-ban fűtötte valamilyen kémkedési szándék. Az incidensek 63%-a személyes, 41%-a hitelesítő, 23%-a egyéb, 10%-a pedig belső adatok megszerzésére irányult. A jelentés összegzésében a szerzők kiemelik: „Az oktatási szolgáltatások kísértetiesen hasonló tendenciát követnek, mint a többi iparág többsége; drámaian megnövekedett a ransomware-támadások száma, mely a jogsértések több mint 30%-át teszi ki. Ezen túlmenően ennek az iparágnak meg kell védenie magát az ellopott hitelesítő adatokkal és az adathalász támadásokkal szemben, amelyek potenciálisan felfedhetik az alkalmazottak és diákok személyes adatait" [37].

A hackmageddon.com[6] 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 adataiban kiválaszthatók az oktatási intézményeket érintő incidensek és azok részletei is[7]. Ezek elemzése céljából felvettem a kapcsolatot a site üzemeltetőjével, aki kutatási célú hozzáférést biztosított az adatok különféle szerkezetű Excel táblázatokban tárolt nyers forrásaihoz, így azokból célirányosan kigyűjthettem az oktatási intézményekre irányuló eseményeket és elvégeztem azok elemzését. A munka során a táblázatokat azonos formátumúra alakítottam, adatait tisztítás után adatbázis táblákba töltöttem és SQL lekérdezéseket alkalmazva készítettem el a következtetések alapjául szolgáló kimeneteket. Megjegyzem, hogy sem ez az adathalmaz, sem a későbbiekben hivatkozott Privacy Rights Clearinghouse[8] (PRC) adatbázisa nem tesz különbséget az oktatási intézmények egyes típusai közt, így az ez alapján levont következtetések nem felsőoktatás-specifikusak, hanem a teljes oktatási szférát jellemzik.

[6] Hackmageddon. Lásd: www.hackmageddon.com/2021/01/13/2020-cyber-attacks-statistics/
[7] A forrás harmadik normálformába alakítása az eredeti adatsorok számának növekedését eredményezte. A közölt adat a folyamat végén keletkezett rekordok száma.
[8] https://privacyrights.org/data-breaches

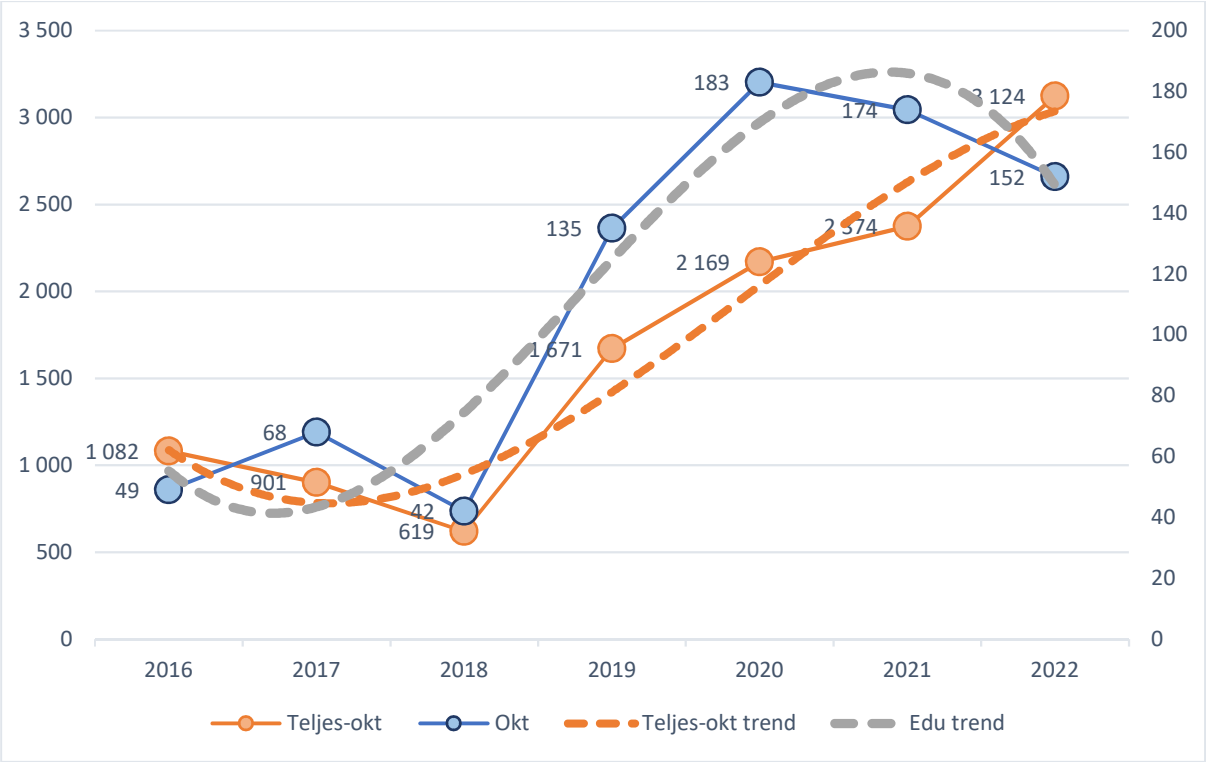
A trend meghatározhatósága érdekében elsőként az oktatási intézményeket ért incidensek számát évekre bontva gyűjtöttem ki. A *NemOkt* oszlopban az adott évben ismertté vált, nem oktatási intézményekre irányult adatsértések száma szerepel, melyet az adott év oktatási szférát érintő incidensek száma követ (Okt). A két adat százalékos aránya évről évre mutatja az az oktatási intézményekre 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	**4,5%**	9,1%	6,1%
2017	901	68	**7,5%**	7,5%	8,5%
2018	619	42	**6,8%**	5,2%	5,2%
2019	1.671	135	**8,1%**	14,0%	16,8%
2020	2.169	183	**8,4%**	18,2%	22,8%
2021	2.374	174	**7,3%**	19,9%	21,7%
2022	3.124	152	**4,9%**	26,2%	18,9%
Összesen	11.940	803	**6,7%**	100%	100%

1. táblázat. Az oktatási szektort ért támadások összevetése a támadások teljes számával éves bontásban. Forrás: a hackmageddon.com adatai alapján saját szerkesztés.

Az adatok alapján megállapítható, hogy az oktatási intézményeket érő adatsértések aránya a vizsgált időszakra nézve összességében 6,7%, mely az egyes években 4,5-8,4% között változott. Az évről évre emelkedő számú támadások mellett az oktatási szektorra irányulók száma 2021-ben megtorpant, majd csökkenni kezdett.

A trend igazolására mindkét adatsort egy diagramban ábrázoltam, melynek pontjait a tendencia láthatóvá tételének érdekében összekötöttem (a két pont közötti értékek változásairól 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 mutat, az oktatási szektor esetében ez a trend 2021-ben megfordult, és csökkenő számú eseményt jelez. Megjegyzendő, hogy 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 bevezetett, 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 megtagadást okozó támadások következtében alakultak ki [38]. A 2022-es évben mért csökkenés egyik valószínűsíthető oka pedig a kibertámadások kivitelezésére képes erőforrások áthelyezése az orosz-ukrán háború célpontjaira.

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[9]. 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 okta-

[9] Néhány adat besorolása hiányzott, vagy nem volt egyértelmű, ezeket a táblázatban nem tüntettem fel.

tási szférát ért támadásokat túlnyomórészt a kiberbűnözés, főként az anyagi előnyök megszerzése motiválja. A kiberkémkedésként minősített esetek kivétel nélkül célzott támadások voltak, melyek többségében a tanulók befolyásolására, vagy kutatóintézeti adatok megszerzésére irányultak. Egy példa erre a 2022.09.01-jén 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 adatbázis egyetlen Cyber Warfare besorolású esete szintén az orosz-ukrán háborúhoz kötődik: a jelentés szövege szerint *„a Wordfence kutatói az orosz megszállás kezdete 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 a forrás nem a Cyber Warfare-be, hanem Hacktivizmusba sorolta. Ezek előfordulása 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: a hackmageddon.com adatai alapján saját szerkesztés.

A motivációk elemzését érdemes az oktatási szektoron kívül eső intézményekre is megvizsgálni és azokkal 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 motivációs bázisú támadások ellen ebben a szférában lényegesen hatékonyabb védekezést kell folytatni.

	2016	2017	2018	2019	2020	2021	2022	Összesen	%
CC	762	681	500	1.380	1.840	1.971	2.310	9.444	81,2%
CE	48	143	81	205	236	267	396	1.376	11,8%
CW	168	31	19	56	44	41	125	484	4,2%
H	3	1	19	26	32	33	219	333	2,9%
Összesen	981	856	619	1.667	2.152	2.312	3.050	11.637	100,0%
%	8,4%	7,4%	5,3%	14,3%	18,5%	19,9%	26,2%	100,0%	

3. táblázat. A nem oktatási szektort érő incidensek motivációinak évek szerinti megoszlása. Forrás: a hackmageddon.com adatai alapján saját szerkesztés.

A motivációk ismerete befolyásolhatja a védendő rendszerek azonosítását, a védelmükre szolgáló módszerek és eszközök kiválasztását. Ez alapján az oktatási intézményeknek elsősorban azokra a rendszerekre kell koncentrálniuk, melyek a támadóik számára anyagi haszonszerzés elsődleges vagy másodlagos lehetőségét kínálják, tehát érzékeny adatok megszerzésére, ransomware aktiválásra irányulnak.

Az adatbázis elemzésével az alkalmazott módszerek is azonosíthatók. A támadók által használt eljárásokat 29 támadási technikába sorolják be, melynek több mint felét a vizsgált időszakban csak egyszer alkalmazták. Az adatok első áttekintése után egyértelműen leolvasható, hogy csak néhány típust érdemes mélyebben vizsgálni. Az esetleges trendek megállapítása érdekében szintén éves bontást alkalmaztam. Mivel az adatbázis azonos típusú módszerekre nem minden esetben alkalmazta ugyanazokat a megnevezéseket, ezért ezeket indokolt esetben összevontam. 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 maradt a támadási technikák közel negyede, melynek trendje is erősödött az elmúlt években, ráadásul a támadások egyre nagyobb részét is ez a típus teszi ki. Az account hijacking során ellopják vagy átirányítják egy személy valamilyen hozzáférését és az így végrehajtott identitáslopás során megszerzett adatokat más, olyan jogosulatlan tevékenységek végrehajtásához használják fel, melyek jogtalan anyagi haszonszerzésre vagy csalásra irányulnak. Annak ellenére, hogy legnagyobb anyagi hasznot a célzott támadások kivitelezésével lehet elérni, azok száma elenyésző, és erre irányuló releváns változás nem is fedezhető fel a vizsgált időszakban. A Covid19 alatt alkalmazott, a távolléti oktatást segítő szoftverek hibáinak kihasználására az átálláshoz rendelkezésre álló rövid idő okozta zűrzavart igyekeztek kihasználni a támadók. Ez jelenik meg pl. a 2020 és 2021-es évek Zoom bombing technikájában, mely során a meetingek képzési algoritmusának nyilvánosságra

kerülésével képezhető volt a belépéshez szükséges csatlakozási link, majd a belépési eljárás gyengeségét is kihasználó támadók ellehetetlenítették azok lebonyolítását. Annak ellenére, hogy egy-egy tanóra vagy meeting megzavarásán túl nagyobb kár nem következett be, ezek az incidensek aláásták a szolgáltatás megbízhatóságába vetett hitet.

A további technikák arányai az előzetes feltételezéseimet messze alulmúlták. A sérülékenységek általános kihasználását ezek az adatok alig támasztják alá, és kis számban detektáltak a szektorral szemben kezdeményezett túlterheléses támadást is. Az SQL injection elenyésző kihasználása is meglepő egy olyan szektorban, ahol a feladatokat részben komoly szakmai tapasztalattal nem rendelkező munkatárs végzi el, vagy hallgatói munka keretében kerülnek megvalósításra: a komolyabb szoftverfejlesztési gyakorlat nélkül készített web-alapú rendszerekben a biztonsági kérdések kezelése rendszerint másodlagos [39]. Ugyanakkor ez a támadási forma valószínűsíthetően a szoftverfejlesztési technikák és biztonságosabb keretrendszerek következtében ma már aligha használható ki hatékonyan. A lista utolsó helyén megjelenő jelszófeltörési eljárás alkalmazását összesen három esetben regisztrálták.

Megjegyzendő, hogy ezek az értékek hirtelen megváltozhatnak, amennyiben a szektorban tömegesen alkalmazott szoftver (esetleg hardver) sérülékenysége kerül nyilvánosságra. Magyar viszonylatban ilyen incidens volt a már említett eKréta elleni támadás, mely során egy megtévesztő levél alkalmazásával, rendszerben többszörösen jelenlevő konfigurációs hibák kihasználásával végül magyar tanulók adatai nagy mennyiségben szivárogtak ki. Az eset példa nélküli volt, az 1. sz. mellékletben szereplő közérdekű adatigénylés tanúsága szerint a Nemzeti Adatvédelmi Hatóság felé 2018. február és 2023. március között jelentett 124 esetből 62 ír le ezzel kapcsolatos adatsértést, 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%

4. táblázat. Az oktatási szektort ért releváns támadási technikák évek szerinti eloszlása. Forrás: a hackmageddon.com adatai alapján saját szerkesztés.

Ahhoz, hogy a Hackmageddon adatbázisának hazai vonatkozásai is megállapíthatók legyenek, megvizsgáltam az adatok forrásának ország szerinti eloszlását. Megállapítottam, hogy annak 90%-a összesen hat országból származik, magyar vonatkozású adatokat pedig egyáltalán nem tartalmaz. Ennek következtében a magyar oktatási szféra kitettségének mértékéről ez az adatbázis nem nyújt információt, így az indukció módszerének alkalmazása lászik célszerűnek: az eddig tett megállapítások érvényességének kiterjesztése magyar viszonylatra is. Az indukció alkalmazására az egyes országok eltérő sajátosságai, a rendszereikben tárolt adatok mennyisége és érzékenysége következtében nem állíthatók fel egyértelmű kritériumok, így érvényességük a hazai intézmények esetében kritika nélkül nem tehető meg. Tekintettel arra, hogy a magyar oktatási rendszerek kevesebb, azonnali anyagi előnyt biztosító adatot tartalmaznak, feltehetően a hazai oktatási intézményeket kisebb számban érik olyan támadások, melyek komolyabb károkat eredményeznek.

#	Ország	Rekordok száma
1	US	579
2	UK	75
3	CA	29
4	AU	18
5	IN	13
6	IE	9

5. táblázat. A Hackmageddon adatforrásai ország szerint.
Forrás: a hackmageddon.com adatai alapján saját szerkesztés.

A Hackmageddon adatbázisának vizsgálata alapján tehát megállapítható, hogy az elsősorban amerikai, továbbá angol, kanadai, ausztrál, indiai és ír források által szolgáltatott adatok alapján az oktatási intézmények fenyegetettsége 7% körüli, mely kismértékű ingadozás mellett 2016 óta jelentős mértékben nem változott. A támadók előszeretettel alkalmaznak malware-ekre alapozott támadási módszereket és lehetőség szerint igyekeznek megszerezni és felhasználni a felhasználók különböző hozzáféréseit. A 2022-től folyó háború ellenére ezeknek az intézményeknek a kiberhadviselésben nem látszik számottevő szerepük. A támadók tevékenysége elsősorban a kibertérre vagy ott elkövetett bűncselekményekre alapozott, így feltehetően az anyagi haszon megszerzésére irányul.

A hackmageddon.com eredményeinek validálása céljából egy másik, a PrivacyRights.org (PRC) által működtetett adatbázisának elemzését is elvégeztem. Ez 2021 októberében 9.015

incidens adatait tartalmazta[10]. Adatbázisuk szintén kategóriákba sorolja az incidenseket elszenvedő szervezeteket és az incidensek típusát is, mely részben eltér a hackmageddon által alkalmazottól. A PRC is önálló kategóriába sorolja az oktatási intézményeket, így lehetővé teszi összehasonlításukat. A szervezetek csoportosítása és a hozzájuk tartozó megnevezések és rövidítéseik 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

A PRC rendszerében szereplő incidensek típusai rámutatnak egy alapvető eltérésre a hackmageddon.com adataival: míg az utóbbi esetében az adatbázis kifejezetten a támadási célú eseményeket, addig a PRC az egyes szervezetek saját munkatársai által elkövetett hibák következtében megvalósulókat is rögzítik – ezt indokolhatja a két forrás alapján megállapított adatok eltéréseit. Az alkalmazott osztályozás az alábbi:

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, így azok összevethetők más szektorokéval. Az összehasonlíthatóság érdekében elkészítettem a

[10] Az adatbázis adatai letölthetők voltak a https://privacyrights.org/data-brokers URL-ről, az adatbányászatot lehetővé tevő forrásadatok letölthetőségét később nem tették lehetővé.

szektorok és incidens típusok mátrixát, amit a 6. táblázat tartalmaz. A PRC adatai alapján az összes incidens 9,4%-a fordul elő oktatási intézményben, amivel a szektor a korábbiakkal szemben magasabb, harmadik helyen szerepel, megelőzve ezzel a biztosítási szolgáltatókat, és a kormányzat és hadsereget is. Bár ez az érték határozottan nagyobb a hackmageddon.com bázisán kimutatottnál, az incidensek már említett különbözősége, és az egyéb, pl. a munkatársak által elkövetett adatsértések, elveszített adathordozók és számítástechnikai berendezések folytán bekövetkező incidensek magyarázatot adnak a magasabb értékekre.

	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
Összesen										9015	100,00

6. táblázat. A PRC incidenseinek szektoriális eloszlása. Forrás: saját szerkesztés.

3.2. Hazai incidensek

Az amerikai felsőoktatási intézmények 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[11]. A magyar egyetemek általánosan alkalmazott rendszereiben jelenleg nem tárolnak bankkártya adatokat, és mivel a személyi szám is csak korlátozott ügytípusok esetén alkalmazható, a személyes adatok kiszivárgásának hazánkban kevesebb esetben voltak súlyos, a sértett személy(ek) számára közvetlenül érzékelhető anyagi következményei. Ugyanez nem mondható el a célzott támadások és a belső munkatársak által okozott adatsértésekről, valamint a reputációs veszteségekről. Informatikai vezetői gyakorlatom alatt több alkalommal kellett az egyetemet

[11] Az Amerikai Egyesült Államokban az SSN-t egy csaló számos módon használhatja fel. Alkalmazható a személyazonosság ellopására pl. hitelszámla megnyitásakor, kölcsön igénylésekor, de ismeretében állami szolgáltatások is igénybe vehetők, akár adóbevallás is benyújtható. Az SSN birtokában munkaviszony létesíthető, az állami juttatások igénybevétele során a személyazonosság igazolható. Birtokában egy támadó szolgáltatási hozzáféréseket igényelhet, hozzáférhet már meglevő szolgáltatói adatokhoz, és ugródeszka lehet más rendszerekben tárolt személyes adatok eléréséhez. Pótlása bonyolult, és nyilvánosságra kerülése pedig egyes esetekben komoly kárt is okozhat tulajdonosának.

érintő célzott megtévesztéses incidens kezelésében részt vennem, ezek teljes kárértéke meghaladta a 100M Ft-ot. Különleges incidens volt egy olyan célzott támadás, mely egy megtévesztő levél helytelen kezelésével indult, s melynek következményeként a gazdasági szervezeti egység egy munkatársa módosította egy szolgáltató bankszámlaszámát a gazdasági rendszerben. A csaló kampánynak több magyar egyetem is célpontja volt, mely következtében ezek az intézmények hónapokon át milliós nagyságrendű havi számlákat egyenlítettek ki ismeretlen csalók számlaszámaira.

Egy másik, nagy kárértékű incidens forrása egy ügyintéző által megvalósított bűncselekmény volt, aki a tanulmányi rendszer manipulálásával közel tíz éven át utalt hallgatói tandíjakat saját bankszámlájára. Kisebb kárértékű, de nagyobb reputációs veszteségű esetek több alkalommal is történtek: 2008-ban a Veszprémi Egyetemről 1.717 hallgató adatainak szivárgását jelentették, amelyek a Google-keresésekben is megjelentek [40]. A Pázmány Péter Katolikus Egyetem (PPK) tanulmányi rendszerét 2020-ban egy zsarolóvírus tette átmenetileg elérhetetlenné [41].

A PRC adatbázisa sem tartalmaz hazai adatokat, így ebből is csak néhány, elsősorban a fejlett ország nemzetközi helyzetére lehet következtetni. A magyar felsőoktatást ért incidensekről nagyon kevés adat áll rendelkezésre, és ezek sem rendszerezettek, a Központi Statisztikai Hivatal (KSH) sem tesz közzé ilyen forrást. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) archívumában fellelhető egy NAIH/2018/7420/2/Z számú adatigénylés és az arra adott válasz, mely a 2018 május 25. és december 18. között a szektorban történt adatsértések listáját tartalmazza [42]. A dokumentum 239 bejelentett esetet sorol fel, melyben összesen öt felsőoktatási intézmény érintett, és minden incidens esetében a bizalmasság sérülése állt fenn.

Bejelentő	Érintettek száma	Incidens jellege
Pécsi Tudományegyetem	1	bizalmas jelleg sérülése
Pécsi Tudományegyetem	1	bizalmas jelleg sérülése
Bács-Kiskun Megyei Kórház SZTE Orvostudományi Kar Oktató Kórháza	797	bizalmas jelleg sérülése
Pécsi Tudományegyetem	6160	bizalmas jelleg sérülése
Magyar Tudományos Akadémia	N/A	bizalmas jelleg sérülése

7. táblázat. A NAIH felé jelentett adatvédelmi incidensek.
Forrás: saját szerkesztés.

Mivel az adatszolgáltatásban foglalt időszak kevesebb, mint hét hónapot ölel fel, ezért a kutatásom szempontjából releváns adatok megszerzése szintén egy közérdekű adatigénylés kezdeményezésével történt, melynek tárgya a NAIH felé „az oktatási intézmények és kutatóintézetek részéről bejelentett informatikai és adatvédelmi incidensek listája, mely tartalmazza az érintett

szervezet nevét, az érintettek számát és az incidens jellegét". Az adatokat a NAIH 2018 február és 2023 márciusa közötti időszakra gyűjtötte ki és adta át[12].

Az adatok vizsgálata során megállapítottam, hogy az 5 évet lefedő adatszolgáltatásban mindössze a 30 felsőoktatási intézményt érintő eset szerepelt. Az ezekben előforduló incidenseket hét kategóriába soroltam és kigyűjtöttem az előfordulásuk számát.

Jelleg	Darabszám	Százalék
Adatok nyilvánosságra kerülése	18	58%
Adathalászat	4	13%
Ransomware támadás	3	10%
Spam küldés	3	10%
Adatvesztés	1	3%
Csalás	1	3%
Deface	1	3%

8. táblázat. A felsőoktatási intézmények adatsértési jelentéseinek száma és jellege 2018–2023.03. között. Forrás: saját szerkesztés.

Az öt évre kimutatott harmincas esetszám irreális, mely arra enged következtetni, hogy a magyar felsőoktatási intézmények nem jelentik adatsértéseiket. A közölt esetek következményei túlnyomórészt elhanyagolható, súlyosságuk elenyésző, a téves címre kiküldött levelek, vagy az online oktatás anyagának közzététele nyilvános videomegosztó portálon minden valószínűség szerint nem okoztak komolyabb kárt az érintett intézmény működésében vagy reputációjában. A három említett sikeres ransomware támadás személyes ismereteim alapján biztosan nem fedi le a teljes incidens számot, a vizsgált időszakban több ilyen eseményről tudok. Az adathalász kísérletek rendkívül magas száma miatt egyáltalán nem tartom valószínűnek továbbá, hogy csak négy alkalommal lett volna sikeres, különös tekintettel arra, hogy a külföldi oktatók a helyi szokások gyenge ismerete és a hiányos magyar nyelvtudás miatt nehezen azonosítanak adathalászként egy magyar nyelvű levelet.

A jelentés alapján megállapítható, hogy a vizsgált időszakban a felsőoktatási intézmények csak részben tettek eleget az adatsértések jelentési kötelezettségének, és valószínűsíthetően csak a már nyilvánosságra került, vagy jelentéktelen incidensek esetében tesznek eleget. A magyar felsőoktatási intézményeket ért támadások száma ennél fogva ismeretlen, így a további vizsgálataimban a nemzetközi tendenciák alapján kimutatott adatokat és trendeket veszem alapul.

[12] Az átadott adathalmaz első dátumát minden bizonnyal elírták, az nem 2019-re, hanem 2018-ra vonatkozott.

3.3. A felsőoktatási rendszerek adatvagyona

Kutatásom első részében bizonyítottam, hogy a felsőoktatási intézményeket érik támadások, és elsősorban külföldi adatok alapján meghatároztam ezek nagyságát. A kutatási téma indokoltságának kimutatása érdekében ebben a fejezetben igazolom, hogy a magyar felsőoktatási intézmények jelentős mennyiségű és értékes adatvagyonnal rendelkeznek, így bizonyítom védelmük szükségességét.

A felsőoktatási rendszerek adatvagyonának felméréséhez nem sok publikusan elérhető forrást találtam. A személyes adatok mennyiségének és érzékenységének meghatározását az Oktatási Hivatal (OH) által üzemeltetett Felsőoktatási Információs Rendszerre (FIR) alapoztam. A felsőoktatási intézmények az aktuális hallgatói és oktatói létszámaikat havi rendszerességgel jelentik az OH felé, ezek forrása az intézményben működő tanulmányi rendszer, technikailag a folyamatot ennek egy modulja bonyolítja le. A FIR adatait az OH nyilvánosan is elérhetővé teszi[13], a hallgatókra és oktatókra vonatkozó adatok megismerhetők. A FIR 2022 októberében a táblázat szerinti bontásban, közel 2,3 millió személyes adatot tartalmazott.

A magyar felsőoktatásban résztvevő hallgatók száma összesen	2.017.565 fő
Hallgatói jogviszonnyal rendelkezők száma	291.251 fő
A felsőoktatásban dolgozók száma összesen	83.825 fő
A felsőoktatásban dolgozók száma	28.835 fő

9. táblázat. A FIR-ben tárolt személyes adatok száma 2022 októberében.
Forrás: saját szerkesztés.

Az adatok értelmezése során figyelembe veendő, hogy a FIR adatrekordjainak száma a felsőoktatási intézmények rendszereiben tárolt rekordok összessége, így abban a több egyetemmel is hallgatói jogviszonnyal rendelkező hallgatók és dolgozók többszörösen jelennek meg, így valójában 2.017.565 főnél kevesebb személy adatait tartalmazza. A hallgatók és dolgozók száma azonban ennek ismeretében is kimagaslónak mondható, így dedukció útján megállapítható, hogy az intézmények tanulmányi rendszereiben tárolt adatok személyes- és különleges adatok mennyisége országos viszonylatban is jelentős, tehát kiemelkedően védendő adathalmazt jelent.

A teljesség kedvéért meg kell említeni a többszörös adattárolás egy másik okát, melynek forrása felsőoktatási intézmények átszervezése során végzett adatmigráció. A jogutódlásból következő jogszabályi kötelezettség okán egy intézmény beolvadása, áthelyezése vagy önállóvá válása

[13] https://firgraf.oh.gov.hu/intezmenyi-adatok

során kialakult gyakorlat szerint a fogadó intézmény tanulmányi rendszerébe a korábbi intézmény teljes adatállományának migrációja történik. A rendszeres átszervezések következményeként így egy intézmény tanulmányi rendszere olyan hallgatói adatokat is tartalmazhat, melylyel soha nem álltak közvetlen jogviszonyban[14].

A kutatásaim során a FIR adatbázisán kívül nem leltem fel más, a felsőoktatás adatvagyonára vonatkozó statisztikai adatot, így a további vizsgálatokat saját gyűjtésű adatok elemzésére alapoztam. Mivel a saját egyetemem nem rendelkezik a kezelésében levő adatok komplex nyilvántartásával, és néhány más egyetemi vezetővel folytatott személyes konzultációm során szerzett tapasztalataim alapján ilyen más egyetemeken sem áll rendelkezésre, ezért az intézmények informatikai biztonsági szabályzatainak elemzésével határoztam meg az intézmények adatvagyonának főbb elemeit és azok értékét.
A módszer alkalmazhatóságát az alábbi két feltételezésre alapoztam:

1. Az intézmények a kiemelt fontosságú adataikat a törvényi kötelezettségük okán elektronikus úton tárolják, tehát alkalmaznak informatikai rendszereket.
2. Az informatikai védelemben kellően érett egyetemek nem csak technikai, hanem szabályzati úton is törekszenek a védelem hatékonyságának javítására. Amennyiben egy intézmény a szabályzatainak felépítése során figyelembe vették a 2013 évi L. törvény ajánlásait, és elvégezték a rendszereik biztonsági osztályba sorolását, az tükrözi az azokban tárolt adatok mennyiségét, értékét és valószínűsíthetően érzékenységét is.

A kutatást dokumentumelemzés módszerével végeztem [43]. Bár alkalmazása számos előnyt kínál, a potenciális hibák elkerülése érdekében felmértem annak hátrányait is. Yin összefoglaló táblázata alapján a dokumentumelemzés potenciális gyengeségei esetemben az alábbiak lehetnek [44]:

1. Jelentős kockázatot jelenthet, hogy a biztonsági szabályzatokat nem kutatási célú adatszolgáltatáshoz készítették, így annak tartalma hiányos lehet, vagy abból téves következtetés vonható le.
2. A dokumentumok kiválasztásakor megjelenő esetleges elfogultság az adatok szelektív gyűjtését eredményezi, melynek torzító hatása lesz az azokból levont következtetésekre.
3. A dokumentumok hozzáférésének tiltása akadályozó tényező az elemzés elvégzésében.

[14] A Gyöngyösi Károly Róbert Főiskola 2003-ig a Gödöllői Agrártudományi Egyetem Mezőgazdasági Főiskolai Karaként működött. 2016-ban olvadt be az egri Eszterházy Károly Egyetembe, majd 2020-ban a Szent István Egyetembe. 2021-től a Magyar Agrár- és Élettudományi Egyetem campusaként működik.

Személyes tapasztalatom, hogy az informatikai vezetők nem értenek egyet az informatikai szabályzatok publikus hozzáférhetőségével.

Az egyes torzító tényezőket az alábbi módszerek alkalmazásával küszöböltem ki:

- Megállapításaimat kizárólag a szabályzatokban közölt adatok alapján tettem meg, a nem közölt adatokat ismeretlennek feltételeztem, azok hiányát nem vettem figyelembe. A szabályzatok eltérő kora magában foglalja az azokban foglalt adatok esetleges érvénytelenségét, ezek valódiságáról más csatornákon próbáltam meggyőződni. Amennyiben egy szabályzat nem tett közzé releváns adatokat, vagy egy egyetem nem közölte azokat, helyette másikat választottam[15].
- Tekintettel arra, hogy 2013 februárjában a FIR nyilvántartásában 236 felsőoktatási intézmény szerepelt, és nem állt rendelkezésemre erőforrás, hogy a kutatást mindegyikre kiterjesszem, ezért az intézmények körét úgy szűkítettem, hogy a vizsgáltak reprezentálják a teljes egyetemi kört. A szabályzatokat így a reprezentatív mintavételezés szabályainak megtartásával választottam ki, ennek érdekében meghatároztam azokat a szempontokat, melyekkel a magyar egyetemek teljes spektruma lefedhető.
- Nem minden egyetem tette közzé a szabályzatait, ezért ezekben az esetekben személyes megkeresés útján szereztem be azokat. Ez a BGME és a PKE esetében állt fenn, ugyanakkor a kis egyetemek többsége nem helyezett hangsúlyt a minőségi szabályzatok készítésére. Helyettük más egyetemet választottam, de az alacsony hallgatói létszámmal rendelkezők osztályában alig találtam olyat, mely elfogadható minőségű szabályzattal rendelkezik.

A fentiek alapján tehát a törvényi kötelezettség mellett dokumentumelemzés módszerével gyűjthető információ az adatvagyon számottevő elemeiről, emellett azok biztonsági besorolásai is összehasonlíthatók, mely igazolhatja feltételezésemet.
Tekintettel arra, hogy nincs lehetőségem a teljes magyar felsőoktatási intézményi kör szabályzatainak elemzésére, ezért azok reprezentatív mintáját dolgozom fel, majd az adatgyűjtést és elemzést erre a körre szűkítve végzem el. A reprezentativitás biztosítja, hogy az így kapott eredmények a teljes adathalmaztól való eltérése nem lesz jelentős.

[15] A Debreceni Egyetem informatikai biztonsági szabályzata kiemelkedő részletességgel és magas színvonalon készült, ugyanakkor minimális olyan információt tartalmaz, amelyből az informatikai rendszer belső viszonyaira lehetne következtetni.

A reprezentativitás alapját az egyetemek csoportosítása képezi, melynek meghatározása után minden csoporthoz hozzárendelésre kerül legalább három, a csoport meghatározásának feltételeit kielégítő intézmény. Első lépésként ezért szempontokat definiáltam, amelyek alapján kiválasztható az egyetemeknek az a legszűkebb halmaza, mely vizsgálata után az indukció módszerével megalapozott általánosítás végezhető. A csoportok képzésének szempontjait az alábbiakban határoztam meg:

Az intézmény mérete

Egy intézmény méretének meghatározásakor nem csak az elmúlt években jellemző összevonások és átszervezések következtében létrejött létszám- és adatvagyon változásokat kell figyelembe venni, hanem a különböző képzések időszakos támogatásából, vagy éppen azok megszűnéséből adódó hallgatói- és oktatói létszámokat is. Mivel idősoros adatforrás nem állt rendelkezésemre, ezért a méret osztályt a hallgatói és oktatói létszám alapján határoztam meg, amihez a jelenlegi (tehát nem az intézmény teljes életciklusa alatt mért összesített) hallgatói létszámot használtam fel. Ez pontosabban írja le egy egyetem aktuális állapotát, melyben nem érvényesül valamilyen múltbéli tényező befolyásoló hatása. A pontossága ugyanakkor néhány ponton megkérdőjelezhető, mivel a már említett, az egyetemek átszervezése során létrejött új intézmények annak ellenére, hogy jelenleg nagy számú hallgatót képeznek, a fiatal koruk következtében alacsonyabb hallgatói létszámot mutatnak.

Egy egyetem mérete nem csak a hallgatói, hanem a dolgozói létszám alapján is mérhető, ezért azt is megvizsgáltam, hogy ezen a téren mekkora eltérések tapasztalhatók. A dolgozói létszám figyelembevételének érdekében kiszámítottam az egy hallgatóra jutó számukat (a FIR nem különbözteti meg a kinevezéses munkaviszonyú oktatókat az óraadóktól) és kimutattam, hogy arányuk az intézmények profiljának függvényében jelentős eltérést mutat. Az oktatói és hallgatói arány számos művészeti és a hittudományokhoz kötődő egyetemek esetében magas, míg az általános intézmények esetében többségében inkább alacsony. Az oktatói, illetve a hallgatói létszámok alapján csak a Dunaújvárosi Egyetem mutatott szignifikáns eltérést, így esetében a hallgatói létszámot vettem alapul.

A jelenlegi hallgatói létszám alapján három méret osztályt határoztam meg. Mivel a létszámadatokban 18.559-nél egy határozott ugrás tapasztalható, az első csoportba (Cs.1.) a 18.000 hallgató feletti, a középsőbe (Cs.2.) az 5.000 és 17.999 közé eső, a harmadikba pedig (Cs.3.) az 5.000 fő alatti hallgatói létszámmal rendelkező intézményeket soroltam be.

Fenntartó

A vizsgálandó intézmények kiválasztásának másik szempontjaként a fenntartó jellegét választottam. Az egyes intézmények fenntartóinak meghatározásához szintén az OH által közzétett lekérdezési felületet[16], valamint a felsőoktatási törvény 1. mellékletét használtam [19]. Az egyetemek típusait és hallgatói létszámát az alábbi táblázatban foglaltam össze.

Fenntartó típus	Darab	Összes hallgató
Alapítvány (ALAP)	4	788
Magyar állam (ALLM) [17]	6	65.346
Egyházi jogi személy (EGYH)	27	29.536
Gazdasági társaság (GAZD)	6	12.214
Közalapítvány (KALA)	1	218
Külföldi szervezet (KSZE)	7	540
Vagyonkezelő alapítvány (KEKVA) (VALA)	21	182.609
Összesen	**72**	**291.251**

10. táblázat. A magyar felsőoktatási intézmények csoportosítása és összesített hallgatói létszámaik fenntartóik alapján. Forrás: saját szerkesztés.

Az elemzésből kizártam azokat az intézményeket, amelyek (még vagy már) nem működnek (Fudan Egyetem), az alacsony hallgatói létszámuk miatt a külföldi szervezeteket, és az egyszerű- és közalapítványok által fenntartottakat. Az intézmények számát ezzel 61-re csökkentettem úgy, hogy közben a vizsgált hallgatók köréből csak 851-et zártam ki. A hozzávetőleg két ezrelékes nagyságrendű redukció nem jelent lényeges változást, ezért az így előállított adathalmaz továbbra is reprezentatív.

A gazdasági társaságok által üzemeltetett egyetemek informatikai védelmi szempontú súlyát a Budapesti Metropolitan Egyetem kivételével nem ítéltem jelentősnek, ezért ebből a fenntartói körből csak ezt az egyetemet vontam be a vizsgálati körbe. A külföldi szervezetek esetében kizártam azokat, melyek nem működnek, hasonlóképp jártam el a működőként megjelölt, de jelenleg nulla hallgatói létszámú intézményekkel is. Vizsgálataim során megállapítottam, hogy a megmaradó intézmények vizsgálatát a magyarországi működésre vonatkozó szabályzataik hiányában nem tudom elvégezni, így végül azokat a már említett Budapesti Metropolitan Egyetem kivételével teljes egészében figyelmen kívül hagytam[18].

[16] https://firgraf.oh.gov.hu/prg/int.php?hatalyvalt=hatályosság+bekapcsolása

[17] Ezek a Budapesti Műszaki és Gazdaságtudományi Egyetem, az Eötvös Loránd Tudományegyetem, a Liszt Ferenc Zeneművészeti Egyetem, a Magyar Képzőművészeti Egyetem, a Nemzeti Közszolgálati Egyetem és az Eötvös József Főiskola.

[18] Ezek a következőK: Central European University, New York, École Supérieure des Sciences Commerciales d'Angers, FernUniversität in Hagen, Fudan University, McDaniel College, Mod'Art International, Stichting Maastricht School of Management, Universitatea de Medicină şi Farmacie Târgu-Mureş, Université Pantheton-Assas (Paris II), École d'Art Maryse Eloy.

A fenntartó, mint elemzési szempont kiválasztását azért tartottam fontosnak, mert meg kívántam vizsgálni, hogy felfedezhető-e összefüggés a fenntartó jellege és az intézményi szabályzatok minősége, az informatikai védelem érettségi foka, ebből következően az annak kialakítására tett operatív lépések között.
Felmerül a kérdés továbbá, hogy létezik-e összefüggés az intézmény fő profilja és az adatvagyon védelme, valamint az informatikai védelem között, és hogy egy informatikát nélkülöző képzési profilú, vallási vagy művészeti intézmény kisebb hangsúlyt helyez-e erre a területre. Ennek megválaszolására vettem fel a vizsgált intézmények sorába a Magyar Képzőművészeti Egyetemet.

Nemzetbiztonsági védelem

A már hivatkozott 2009/2015. (XII. 29.) kormányhatározat rendelkezik a magyar felsőoktatási intézmények és kutatóintézetek nemzetbiztonsági védelem alá eső köréről. Bár ebben jellemzően inkább az egyetemek egyes szervezetei érintettek (Pécs esetében a nemzetközi viszonylatban is jelentős Virológiai Nemzeti Laboratórium), ezért érdemesnek tartottam az ezeknek helyt adó egyetemeket a vizsgálati körbe bevonni. A Nemzeti Közszolgálati Egyetem a 2009/2015. kormányhatározat 1.60. pont alapján teljes egészében nemzetbiztonsági védelem alá esik, működését az Ibtv. határozza meg, így vizsgálata szintén az általánostól eltérő eredményt hozhat.
A kiválasztási szempontok alapján az alábbi táblázatban szereplő egyetemek különféle informatikai szabályzatait kutattam fel és töltöttem le. Az elnevezések nem voltak egységesek, az informatikai szabályzat mellett informatikai biztonsági szabályzatok is elérhetők voltak, esetenként mindkettő rendelkezésre állt. A DUE nyilvános szabályzatai közt egy katasztrófaelhárítási terv is fellelhető volt, melyet szintén bevontam a dokumentumelemzésbe. A szabályzatok jellegében további eltéréseket állapítottam meg: nem minden intézmény, főleg a kis egyetemek és főiskolák nem tették közzé vagy el sem készítették azokat, esetleg nem önálló formában voltak elérhetők, hanem más szabályzatokba integrálták azokat. Esetükben az adott felsőoktatási intézmény helyett másikat választottam, de a reprezentativitás megtartása érdekében a Tokaj-Hegyalja Egyetemet annak ellenére, hogy egyáltalán nem rendelkezett ilyen szabályzattal, másik alkalmas egyetem hiányában megtartottam[19].
Az elemzett intézményeket az alábbi táblázat sorolja fel, az ebben alkalmazott rövidítések azonosak az előző táblázatban is használt, az OH fenntartói adatszolgáltatásban alkalmazottal.

[19] A Wesley János Lelkészképző Főiskola vagy a Baptista Teológiai Akadémia nem tett elérhetővé ilyen szabályzatot.

Név	Fenntartó				Nemzetb. védelem	Hallgatói létszám		
	ALLM	VALA	EGYH	GAZD		Cs.1.	Cs.2.	Cs.3.
Eötvös Loránd Tudományegyetem	✓					✓		
Pécsi Tudományegyetem		✓			✓	✓		
Budapesti Műszaki és Gazdaságtudományi Egyetem	✓				✓	✓		
Pázmány Péter Katolikus Egyetem			✓				✓	
Eszterházy Károly Katolikus Egyetem			✓				✓	
A Tan Kapuja Buddhista Főiskola			✓					✓
Nemzeti Közszolgálati Egyetem	✓						✓	
Dunaújvárosi Egyetem		✓			✓			✓
Tokaj-Hegyalja Egyetem		✓						✓
Budapesti Metropolitan Egyetem				✓			✓	
Magyar Képzőművészeti Egyetem	✓							✓

11. táblázat. A vizsgálatban résztvevő egyetemek. Forrás: saját szerkesztés.

3.4. A szabályzatok elemzése

A dokumentumelemzés folyamatának első lépése kiválasztott szempontok definiálása és értékeik megfelelő kategóriákba történő sorolása. Ennek szakszerű elvégzése informatikai szabályzatok esetében lényegesen egyszerűbb, mint humán területeken történő alkalmazáskor, különösen kérdőívek esetén okozhat nehézséget az értékelés objektivitása. A kódolást nehezítő tényezők közt a kódolók eltérő szövegértelmezését vagy befolyásoltságát, valamint a válaszadók nem egzakt nyelvhasználatát emelik ki, ezért ezeket különös figyelemmel igyekeztem elkerülni.

Az informatikai szabályzatok elemzésének első lépése a kódolás megtervezése és paramétereinek meghatározása volt, melyet az alábbi kérdések megválaszolásának érdekében terveztem meg:

- Milyen informatikai rendszerek működnek az egyes felsőoktatási intézményekben?
- Van az egyetemnek publikusan elérhető informatikai vagy informatikai biztonsági szabályzata?
- Annak ellenére, hogy az egyetemek számára nem kötelező érvényű az 2013/L. tv. szerinti besorolások elvégzése, elvégezték-e a felsorolt rendszerek biztonsági besorolását?
- Ha igen, milyen besorolási módszertant és skálát alkalmaztak?

- Elvégezték a szervezeti egységek besorolását?
- A dokumentumelemzés során fellelhetők-e további, a grounded theory során alkalmazható újabb adatok vagy összefüggések? Amennyiben igen, ez alapján egy újabb iterációval kiterjeszthető az elemzés hatóköre?

A kódolási folyamat első lépéseként rögzítettem az intézmény nevét, az elemzett dokumentum nevét és korát. Következő lépésként elvégeztem a szöveg releváns részeinek kiválasztását, majd az egyes rendszereket leíró rész kiválasztása után ellenőriztem, hogy az abban felsorolt elemek szerepelnek-e már az elemzés már felépített rész-rendszerlistájában. Amennyiben igen, úgy rögzítettem az intézmény nevét, azonosítóját, besorolását és az alkalmazott skála adatait. Egy korábban még nem szereplő új rendszer fellelésekor azt új elemként rögzítettem, és a korábban már elemzett intézmények esetében rögzítettem a felsorolás hiányát. Esetenként a hasonló feladatot ellátó, vagy kisebb eltérést mutató rendszereket összevontam, ugyanígy jártam el a téma szempontjából önálló jelentőséggel nem bíró részterületek esetében is[20].

[20] Számos szabályzat sorolta fel az informatikai alap infrastruktúra egyes elemeit, pl. switcheket, routereket, wifi hálózatot.

Megnevezés	Eötvös Loránd Tudományegyetem	Pécsi Tudományegyetem	Budapesti Műszaki és Gazdaság-tudományi Egyetem	Pázmány Péter Katolikus Egyetem	Eszterházy Károly Katolikus Egyetem	A Tan Kapuja Buddhista Főiskola	Nemzeti Közszolgálati Egyetem	Dunaújvárosi Egyetem	Tokaj-Hegyalja Egyetem	Budapesti Metropolitan Egyetem	Magyar Képzőművészeti Egyetem
Publikus szabályzatok			Nem	Nem							
Nemzetvédelmi felügyelet		Igen					Igen	Igen			
Informatikai Szabályzat (ISZ) hatály	2007	2022	2009	N/A	-	-	-	-	-	-	2016
Informatikai Biztonsági Szabályzat (IBSZ) hatály	2007	2022	**2014**	N/A	-	-	2021		-	2019	-
Összevont szabályzat				N/A	2019	2017	-	2022	-	-	-
Szervezeti egységek besorolása		Igen					Igen				
Skála elemszáma	4	4	4	4	5	Nem alkalmaz	5	4	Nincs	Nem alkalmaz	4
Hivatkozás	5. oldal	44. oldal	7. oldal	4. oldal	IBSZ 6-7		62. oldal	IBSZ 8.o.			IBSZ 17.o.
Szakrendszerek konkrét megnevezése	Nem	Igen, IBSZ 44.o.	Igen, ISZ 6.o.	Igen, IBSZ 4.o.	Nem	Nem	Igen, 62.oldal.	Nem	Nem	Nem	Nem
Telefonkönyv			1								
VIR		3									
Kórházi Információs Rendszer		1									
Laboratóriumi információs rendszer		1									
Medbakter mikrobiológiai rendszer		1									
Egyéb orvosi rendszerek		2									
Medikai képtároló rendszer		2									
Központi tanúsítvány struktúra							2				
Nyomtatás											3
Technológiai rendszerek			2	2							
Nagios Infrastruktúra menedzsment		1						2			
Határvédelmi rendszerek		1		1							
Könyvtári rendszer		2					2				
Riasztó- és beléptető rendszerek		3						3			
HPC	3			3							
E-learning rendszerek		3					1	1			
Hallgatói laborok			3		4						3
Virtualizációs rendszerek			2	1				2			1
Egyetemi webszerver szolgáltatás		2	2	2							3
Telefonközpont			2	2	2						2
Kommunikációs rendszerek	2			1	2						2
Központi címtár			1	1	2			1			1
Telefonhálózat	2		2	1	2						2
Szerverek	3		3	3	3			2			
Authentikációs rendszerek	1	2	1	1				1			1
Kutatói rendszerek	3	3	3	3	3		2				
Központi tárhely kiszolgálók	1	2	1	1	2			1			1
Dokumentumkezelési/Iktatási rendszer	1	2		1	2		1	1			1
Számítógép hálózat	2	2	2	2	1			2			2
Middleware rendszerek (DNS)	2	2	2	2	3			2			1
Tanulmányi rendszer	1	1	1	1	1		1	1			1
Bér, és munkaügyi rendszer	1	1	1	1	1		2	1			1
Központi levelező kiszolgálók	1	2	1	2	2		2	1			1
Gazdasági/Gazdálkodási rendszer	1	2	1	1	1		2	1			1

Megállapítások. A 11 vizsgált egyetem közül 10 rendelkezik valamilyen önálló informatikai szabályzattal. 8 intézmény tett lépéseket az informatikai rendszerek besorolására, a szabályzataik a 2013 évi L. tv. szellemében készültek. Két esetben csak általános szabályzók kerültek megfogalmazásra, három esetben elkülönült informatikai biztonsági szabályzat is létezik. Csak az NKE és a PTE végezte el a szervezeti egységek besorolását is. A szabályzatok aktualizálása többségében azon egyetemek esetében történt meg, melyek fenntartója változott. Az EKKE, a PTE és a DUE szabályzatait az új környezetnek megfelelően újraírták vagy megújították. A jelenleg állami fenntartású Eötvös Loránd Tudományegyetem szabályzata 2007, az azonos státuszú Budapesti Műszaki és Gazdaságtudományi Egyetem szabályzata 2014 óta van hatályban.

Külön vizsgáltam, hogy az adott egyetem publikus szabályzatai milyen mértékben teszik lehetővé a nyílt forrású információszerzést. Emellett a dokumentumok jellegének és korának rögzítését is bevontam a vizsgálati körbe azért, hogy meg tudjam állapítani azok naprakészségét és szerkezetét is.

Megállapítások. Az OSINT információszerzést számos egyetem támogatta (dolgozatom későbbi fejezetében alapvető szerepet kap a munkavállalók adatainak, főként e-mail címeinek publikus elérhetősége is). A 11 vizsgált intézményből 6 publikus információkat közöl az informatikai rendszereiről, megnevezi azokat, vagy következtetni lehet az alkalmazott szoftverekre (ugyanakkor verziószámot egyetlen esetben sem közöltek). A képet valamelyest javítja, hogy a vizsgált egyetemek közül a Budapesti Műszaki és Gazdaságtudományi Egyetem és a Pázmány Péter Katolikus Egyetem szabályzatai publikusan nem voltak elérhetők, azokat az egyetem informatikai munkatársai bocsájtották rendelkezésemre, így a szakrendszerek megismeréséhez egy potenciális OSINT felderítőnek eggyel több lépést kell megtennie. Csak két esetben nem tartalmazott a szabályzat értékelhető információt a rendszer elemeiről. A publikus elérhetőség csak az általános és kötelezően használandó rendszerek esetében nem nyújt extra információt – a magyar felsőoktatási intézmények számára kötelező a Neptun tanulmányi rendszer alkalmazása, így ez nyilvános adat. Ugyanakkor, főleg az orvosképzést végző egyetemek esetében a szabályzatok tételes felsorolását adják olyan magas besorolású rendszereknek, amelyek különleges besorolású, tipikusan egészségügyi adatokat tartalmazhatnak. Bár a vizsgált körben csak a Pécsi Tudományegyetem szerepelt, a kontrollként elemzett Semmelweis Egyetem szabályzatában hasonlóan fellelhetők a konkrét egészségügyi rendszerek megnevezései.

A nemzetbiztonsági felügyelet alá eső kutatóintézettel rendelkező egyetemek esetében semmilyen különbség nem volt kimutatható. Mindegyikük publikusan elérhetővé tette a szabályzatait,

listázta a rendszereit és azok biztonsági besorolását, a Pécsi Tudományegyetem megnevezte az orvosi szakrendszereit is[21]. Az informatikai szabályzatok több esetben tartalmazták az alkalmazott rendszerek megnevezését. Ugyanakkor a védett kutatólaborokról semmilyen használható információt nem tudtam nyilvános forrásból felkutatni – a Pécsi Tudományegyetem Virológiai Nemzeti Laboratóriuma önálló szervezeti egység, mely az egyetem informatikai egységeitől teljesen elkülönítve működik. A Dunaújvárosi Egyetem esetében nem sikerült információt szerezni arról sem, hogy mely szervezeti egységük tartozik nemzetbiztonsági felügyelet alá. Összességében megállapítható, hogy a nemzetbiztonsági védelem alá tartozó szervezeti egységek esetében az OSINT alkalmazása lényegesen kevesebb eredménnyel járt.

Ugyanakkor a fenntartó alapján nem volt megállapítható szignifikáns különbség. A fenntartóváltások jogi folyamatai megkövetelik szabályzatok aktualizálását, ez indokolhatja, hogy a változatlan státuszú állami fenntartású egyetemek hatályos szabályzatai a legrégebbiek. Ezen a téren határozottan megfigyelhető a kis egyetemek elmaradása is.

H1. igazolásához azon intézmények esetében, ahol rendelkezésre álltak a szükséges adatok, összehasonlítottam az egyes rendszerelemek besorolásait.

Első lépésként meghatároztam, hogy melyek azok a védendő rendszerek, amelyeket minden egyetemnek működtetnie kell. Ezeket a besorolásukkor akkor is meglevőnek feltételeztem, ha azokat nem szerepeltették, vagy csak funkcióikat nevezték meg. Azokról, melyek ugyan jogszabályi kötelezettség, vagy életszerűség okán minden bizonnyal léteznek, de a besorolásuk nem volt feltalálható, nem rögzítettem adatokat. Megvizsgáltam továbbá, hogy a feltüntetett rendszerek besorolásában szerepelnek-e különbségek, és azok közt milyen eltérések mutathatók ki.

Az objektív értékelést megnehezítette, hogy a szabályzatokban az egyes rendszerek besorolásait egyes intézmények nem öt- hanem csak négyfokozatú skála alapján végezték el. Ezért az összehasonlíthatóság érdekében azokat az elemzés során azonos skálára konvertáltam. Mivel az intézmények túlnyomórészt a négyfokozatú skálát alkalmazták, ezért ezt tartottam meg. Az egyes rendszerek említési gyakoriságait, besorolásukat és a köztük levő eltérés nagyságát (Diff) az alábbi táblázat tartalmazza. Ebben sárgával jelöltem azokat a rendszereket, melyek besorolása nem egységes, piros háttérrel pedig azokat, amelyek esetében a besorolást két szint eltéréssel határozták meg.

[21] Kórházi Információs Rendszer, Laboratóriumi információs rendszer, Medbakter mikrobiológiai rendszer, Medikai képtároló rendszer.

Rendszerelem	Említés	Max	Min	Diff
Tanulmányi rendszer	100%	1	1	0
Bér, és munkaügyi rendszer	100%	1	2	1
Központi levelező kiszolgálók	100%	1	2	1
Gazdasági/Gazdálkodási rendszer	100%	1	2	1
Dokumentumkezelési/Iktatási rendszer	88%	1	2	1
Központi tárhely kiszolgálók	88%	1	2	1
Számítógép hálózat	88%	1	2	1
Middleware rendszerek	88%	1	3	2
Authentikációs rendszerek	75%	1	2	1
Kutatói rendszerek	75%	2	3	1
Központi címtár	63%	1	2	1
Telefonhálózat	63%	1	2	1
Szerverek	63%	2	3	1
Virtualizációs rendszerek	50%	1	2	1
Egyetemi webszerver szolgáltatás	50%	2	3	1
Telefonközpont	50%	2	2	0
Kommunikációs rendszerek	50%	1	2	1
E-learning rendszerek	38%	1	3	2
Hallgatói laborok	38%	3	4	1
Technológiai rendszerek	25%	2	2	0
Nagios Infrastruktúra menedzsment	25%	1	2	1
Határvédelmi rendszerek	25%	1	1	0
Könyvtári rendszer	25%	2	2	0
Riasztó- és beléptető rendszerek	25%	3	3	0
HPC	25%	3	3	0
Telefonkönyv	13%	1	1	0
Vezetői információs rendszer	13%	3	3	0
Kórházi Információs Rendszer	13%	1	1	0
Laboratóriumi információs rendszer	13%	1	1	0
Medbakter mikrobiológiai rendszer	13%	1	1	0
Egyéb orvosi rendszerek	13%	2	2	0
Medikai képtároló rendszer	13%	2	2	0
Központi tanúsítvány struktúra	13%	2	2	0
Nyomtatás	13%	3	3	0

12. táblázat. A vizsgált egyetemek IT rendszereinek besorolásai. Forrás: saját szerkesztés.

Következtetések. Az elemzés adatai bizonyították, hogy az egyetemek a tanulmányi rendszert tekintik elsődleges és legfontosabb informatikai rendszerüknek. Ezt a rendszert minden szabályzat említi, és egységesen a legmagasabb szintbe sorolták.

A bér- és munkaügyi rendszereket egyes szabályzatok az alkalmazott rendszerek függvényében együtt vagy különálló rendszerként említették, vagy az önálló kategóriába sorolt gazdasági rendszerekbe integráltként feltételezték. Említésük szintén teljeskörű, bár az NKE egyiket sem sorolta a legmagasabb, 1-es szintbe, így megítélése e rendszernek sem egységes.
A dokumentumkezelő és iktatási rendszerek besorolása szintén nem azonos szempontok mellett történik. Ezek a rendszerek nagymennyiségű személyes adatot tárolnak, a különféle szerződések és megbízások mellett az egyetemek számtalan hivatalos dokumentumát tartalmazzák, ezért bizalmasságuk és sértetlenségük, valamint rendelkezésre állásuk létfontosságú az intézmények számára. Ennek ellenére csak 88%-ban említették, és eltérő, 1-es és 2-es szintbe sorolták őket. Figyelmet érdemel a központi levelező kiszolgálók és a dokumentumkezelő/iktatási rendszerek összehasonlítása: az elektronikus levelezés besorolását minden szabályzat megtette, és 1-es vagy 2-es szintbe sorolta.
A szabályzatok 34 különböző területet soroltak fel, melyből 29 jelenléte általános a magyar egyetemeken. Ebből 11 besorolását végezték el egymástól függetlenül azonos módon. Kizárólag a tanulmányi rendszer, a határvédelmi rendszerek és a telefonkönyv kaptak azonos és 1-es szintű besorolást, utóbbi említése viszont csak 13%-os, így ez nem tekinthető relevánsnak. A további 9 azonos besorolású rendszer nem kritikus, és említésük aránya sem kiemelkedő.
Kétpontos különbség tapasztalható az E-Learning és a middleware rendszerek besorolásában. Az utóbbi értelmezése nem egységes a szabályzatokban, feltehetően ez okozza a besorolások nagy eltérését. A middleware-eknek számos különböző formája létezik, a leginkább közismertek a Java engine, domain name system vagy a webes API szolgáltatások [45]. Céljuk a legtöbb esetben olyan háttérszolgáltatások nyújtása, amelyek lehetővé teszik az alkalmazások kommunikációját, integrációját vagy koordinációját.
Az E-Learning rendszerek csak három szabályzatban, nagy besorolási eltéréssel kerültek említésre, mely valószínűsíthetően a szoftverek eltérő személyes adat tartalmából adódik: az NKE és a Dunaújvárosi Egyetem ezt 1-es szintre, míg a PTE csak a 3-asba sorolta. A Covid19 korlátozásai következtében az E-Learning rendszerek jelentősége minden felsőoktatási intézményben megnőtt és azok alkalmazása jelenleg is általános, így adattartalma várhatóan évről évre növekszik. Bár az általánosan elterjedt Moodle alaprendszere minimális személyes adatot tartalmaz a regisztrált/rögzített hallgatókról és oktatókról, számos felsőoktatási intézmény integrálta azt más, tipikusan a tanulmányi, és video kommunikációs rendszerével. Az így létrehozott adatkapcsolatok révén a ezekbe a rendszerekbe ismétlődő importálási eljárás során, vagy folyamatos adatkapcsolat révén tömegesen tárolt vagy valós időben elérhető személyes adatok révén

az egyes rendszerek érzékeny adat tartalma tehát eltérő lehet, mely indokolhatja a kétpontos eltérést. Ennek bizonyítása azonban további vizsgálatot igényel.
A könyvtári rendszereket csak két intézmény említette, illetve végezte el besorolását annak ellenére, hogy a kölcsönzési rendszereik személyes adat tartalma valószínűsíthetően magas. Az ügyviteli folyamat egyszerűsítésének érdekében elfogadott gyakorlat az első évfolyamos hallgatók adatainak teljes importálása a tanulmányi rendszerből, melyet az intézménnyel jogviszonyban nem álló „külsős" olvasók adatai tovább növelnek, az általános gyakorlat szerint pedig a végzett hallgatók törlése helyett azok inaktív állapotba helyezését végzik el.
Az elemzés kimutatta, hogy a magyar felsőoktatási intézmények esetén olyan, feltehetően nagy mennyiségű személyes adatot tartalmazó informatikai rendszerek besorolása sem egységes, mint a gazdasági-, bér- és munkaügyi rendszerek, valamint az eltérő besorolásból adódóan a védelmükre fordított erőforrások is feltehetően eltérők. **Ezzel igazoltam H1. hipotézist: A magyarországi felsőoktatási rendszerek adminisztratív szabályzásai heterogén tartalmúak és azonos feladatkört ellátó rendszereket eltérő besorolással kezelnek.**

3.5. Következtetések

A felsőoktatási informatikai rendszerekkel 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 nem találtam.
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 eltérések mutathatók ki, 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 sem. Komolyabb eltérés van a károkozásra közvetlenül alkalmas adatelemek terén: az amerikai SSN-hez hasonló érzékenységű adatelemek, bankkártyaadatok a hazai rendszerekben sokkal kisebb mennyiségben fordulnak elő így a közvetlen anyagi haszonszerzés elemei a hazai rendszerekben nem relevánsak. 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 az alkalmazható tanulmányi, és egy szűkebb kör számára a gazdasági és iktatási rendszert.

Az oktatói és kutatói terület speciális jellege következtében fennálló védelmi problémák a szakirodalmi hivatkozások alapján közel azonosnak.

A kiberfenyegetések azonosítására nem állt rendelkezésre olyan mennyiségű magyar adat, amely lehetővé tenné a nemzetközi összehasonlítást. Ezért főként amerikai adatok alapján kimutattam, hogy az oktatási szektor az informatikai incidensek 6-9%-ában érintett terület, és megállapításokat tettem az egyes incidenstípusok gyakoriságára is. 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.

A fejezetben bizonyítottam, hogy a felsőoktatás informatikai rendszereiben nagy mennyiségű érzékeny és személyes adat található. Védelmükre nem készültek a szférára adaptált konkrét jogszabályi keretek, így az üzemeltetésük nem egységes szabályok mentén történik. A változó fenntartói kör, a rendszeres átalakítások negatív hatást gyakorolnak e rendszerek biztonságára, melyet az egyetemi szabályzatok gyakran lassan követnek.

A védendő adatok körét és az azokat kezelő rendszereket az informatikai szabályzatok dokumentumelemzés módszerével azonosítottam, feltártam azok különbségeit, bizonyítottam inhomogenitásukat, mely indokolja a felsőoktatási rendszerekre adaptált egységes besorolási rendszer kidolgozásának szükségességét.

"If you can not measure it, you can not improve it."
Lord Kelvin

4. Felsőoktatási intézmények sérülékenységvizsgálaton alapuló vizsgálata

Dolgozatomban kimutattam, hogy a magyar felsőoktatási intézmények informatikai rendszereiben nagymennyiségű érzékeny adat található, és azok eltérő biztonsági besorolásúak. Ennek következtében valószínűsíthető, hogy működtetésüket is különböző védelmi eljárások alkalmazásával végzik. A rendszereket alkotó szoftver és hardver eszközök sérülékenységei növelik a tárolt adatok illetéktelen hozzáférésének kockázatát, melynek növekedésével egy informatikai incidens bekövetkezési valószínűsége is megemelkedik. H2. és H3. hipotézisek bizonyítását ezért egy sebezhetőségvizsgálaton alapuló esettanulmányra, majd annak a magyar felsőoktatási intézmények reprezentatív mintáján elvégzett megismételt mérésekkel általánosságban is igazolom. Hangsúlyozni kívánom, hogy dolgozatom e fejezetének nem célja a védekezési eljárásokra vonatkozó megállapítások megtétele, kizárólag a rendszerek sérülékenységeire vonatkozó mérések elemzéséből és összevetéséből következő kockázatnövekedés bizonyítása.
A felsőoktatási intézmények informatikai rendszereinek vizsgálatakor nem szabad figyelmen kívül hagyni, hogy jogi szabályzásuk, működési rendjük, az intézményen belüli folyamataik, a felelősségi körök, a vezetők kiválasztásának szempontjai, valamint a nyitott működés és az oktató- és kutatói szabadság más szféra működéséhez képest komoly eltéréseket eredményez.

4.1. A felsőoktatási rendszerek jogi szabályozása

A felsőoktatási rendszerekkel szemben támasztott védelmi követelmények szoros szabályzása nemzetközi viszonylatban sem jellemző, a szakirodalom csak néhány törekvést említ ennek megváltoztatására. Az Amerikai Egyesült Államokban nem létezik átfogó, a felsőoktatásra szabott jogi környezet, az informatikai rendszerekkel kapcsolatos szabályzást több, különböző területet lefedő jogszabály valósítja meg úgy, hogy azok államonként is eltérhetnek. A tanulói/hallgatói adatok védelme ott az európai gyakorlatnál sokkal régebbre nyúlik vissza: az USA Oktatási Minisztériuma a Family Educational Rights and Privacy Act-ben (Családi oktatási jogok és adatvédelmi törvény, FERPA) szabályozza a tanulói adatkezeléssel kapcsolatos előírásokat. Ennek hatálya kiterjed minden olyan általános, középiskolai vagy felsőoktatási intéz-

ményre, valamint minden olyan állami vagy helyi oktatási intézményre, amely az Egyesült Államok Oktatási Minisztériumának valamely programja keretében anyagi erőforrást kap. Azok az iskolák, amelyek nem tartják be a FERPA szabályait, a szövetségi finanszírozás elvesztését kockáztatják [46].

Magyarországon nincs kifejezetten felsőoktatásra szabott szektorspecifikus jogszabályi keret, így az informatikai működést pusztán az általános szabályzók mentén kell biztosítani. A személyes adatok védelméről szóló általános szabályzás, a GDPR mellett a legfontosabb a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, de a szektorra nézve relevánsak a Btk. vonatkozó részei is [20] [47].

A 2011. évi CXII. törvény határozza meg a személyes adat fogalmát, mely egy "azonosított vagy azonosítható természetes személyre (’érintett’) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható" [4]

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 áll fenn 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, s melyet leginkább az egyetemi kultúra által határoz meg.

4.2. 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, de személyes tapasztalataim is egybeesnek ezzel [48]. A FireEye fehér könyve [33] a biztonsági eszközök korlátozó hatását emeli ki, amely akadályozza az információhoz történő hozzáférést. Az oktatók és kutatók a biztonsági intézkedések fellazítása érdekében nyomást gyakorolnak az egyetemi vezetésre, ugyanakkor egy esetleges incidens esetén az felelősséget az üzemeltetésre igyekeznek hárítani. Ezt a jelenséget Adams már 2003-ban megfogalmazza, és a kultúrák összecsapásának *(clash of cultures)* nevezte [48].

Az informatikai védelem gyengítését célzó törekvések számos olyan ponton jelennek meg, melyek a gazdasági szférában jórészt ismeretlenek. A jelszóképzési szabályokkal történő szembefordulás, a körülményes *secure printing* kötelezettsége alóli kibújás személyes tapasztalataim szerint olyan belső szervezeti egységeknél is megjelenik, amelyek nagy mennyiségű bizalmas dokumentumot kezelnek, éppen azok egy részénél, amelyek védelme érdekében a biztonságos rendszereket bevezették. A távoli munka biztosítása érdekében bevezetett bonyolultabb felhasználói interakciót igénylő VPN-kliensek alkalmazási kényszere számos kritikát kap. Tipikus a kutatási feladatok ellátására pályázati forrásból beszerzett szerverek fizikai birtoklási vágya, amelyeket egyszerű irodákban, megfelelő fizikai védelem nélkül, helyi, a megfelelő informatikai biztonsági ismereteket nélkülöző rendszergazdákkal üzemeltetnek, és a külső adatcserék érdekében az internet irányában minél szélesebb kör számára elérhetővé tesznek. A saját tulajdonú eszközök alkalmazása a felsőoktatásban szintén általános, ezek a legfeljebb részlegesen felügyelt, esetenként a családtagokkal közös használatú gépek a belső hálózatban 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 szervezeti hierarchia alapján magukra nézve ne tekintsék szigorúan kötelezőnek az informatikai munkatársak vagy szabályzatok előírásait. Az egységes informatikai koncepció és üzemeltetés különösen nehezen tartható fenn azokon az egyetemeken, amelyek lehetővé teszik a különböző szervezeti egységek számára önálló informatikus foglalkoztatását, mivel ők csak laza kapcsolat mentén működnek együtt a többi üzemeltetővel. Megítélésem szerint amennyiben a szeparáció elengedhetetlen, legalább a hierarchikus modell kialakítása a kívánatos.

A nyilvánosság azonban nem csak az egyetemi kultúra sajátossága. A közintézmények esetében megkövetelt átláthatóság a nyílt forráskódú felderítés (*Open Source Intelligence,* OSINT) aranybányája, amely nagyban javítja egy célzott támadás sikeres megtervezésének és kivitelezésének esélyét. A nyílt elérésű adatok közt gyakran szerepelnek szabályzatok, szerződések, beszállítók és számos más olyan információ, amelyet egy potenciális támadó az intézmény belső működésének, eszközparkjának felderítésére használhat fel.[22] Amennyiben egy célintézmény eszközparkja ismert, egy nyilvános sérülékenységi adatbázis alapján már alapvető szakmai kompetenciák birtokában is képes lehet azonosítani azok támadható pontjait, ami a behatolás sikerességét sokkal valószínűbbé teszi.

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

4.3. Információbiztonsági tudatosság

Egy hagyományos szervezettel szemben a felsőoktatási intézmények hallgatósága évről évre változik. A végzett hallgatók elhagyják az intézményt, és helyüket új évfolyam váltja fel. A belépő hallgatók számára szolgáltatások tömegét kell biztosítani, miközben azok nyilvános hozzáférhetősége biztonsági kockázatot jelent. Al-Janabi és Al Shourbaji kutatásában a közel-keleti oktatási intézmények hallgatói körében meglevő információbiztonsági hiányosságokra mutatnak rá [49]. Fő okként a biztonsági követelmények betartásának elmulasztását, az általános ismeretek hiányát, a felhasználók kockázatos viselkedését és meggyőződéseit, valamint a technológia helytelen használatát jelölték meg.

A jelszavak alkalmazása a felsőoktatási rendszerekben a legelterjedtebb hitelesítési módszer annak ellenére, hogy az ipari szereplők és egyes tudományos kutatások és is azt jósolták, hogy az hamarosan elavult technológiává válik [50] [51]. Adams és Sasse [52] megállapították, hogy a felhasználók számára nem elfogadható jelszószabályok elégedetlenséget váltanak ki, így azok kontraproduktívak lesznek. A jelszavakkal kapcsolatos hatékonyság javításának egyik leghatékonyabb eszköze a felhasználók meggyőzése [53], ugyanakkor nagy figyelmet kapnak az alkalmazásukat helyettesítő, a memorizálást megkönnyítő módszerek [54] [55]. Bonneau kutatásában megállapította, hogy ezek a módszerek sem tökéletesek, a vizsgálatában résztvevők egyetlen, a jelszavak helyett alkalmazható alternatív megoldást sem tartottak teljes körűen elfogadhatónak [56].

A social engineering (SE) támadások egyetemi környezetben is sikeresnek bizonyultak [57]. Wangen és szerzőtársai egy egyetemi felmérésben naponta regisztráltak sikeres SE biztonsági incidenst. A felmérésében résztvevők 48%-a tapasztalt már személyre szabott támadást, és 22%-uk jelezte, hogy tudomása van olyan esetről, amikor valaki ilyen incidens áldozatává vált [57]. Eltérő metodikával magyar egyetemi környezetben végeztem sikeres adathalász támadást, mely igazolja, hogy a módszer hazai környezetben is hatékony [58]. A szerzők az alacsony információbiztonság-tudatossági szint okait az informatikai eszközökhöz való viszonyulásban, következményeit pedig a folyamatosan visszatérő jelszósértések és alapvető adatbiztonsági tevékenységek elmulasztásában állapították meg.

4.4. Erőforrások és vezetői támogatás

A FireEye fehér könyvében rámutat arra is, hogy az egyetemi rendszergazdák számára komoly kihívást jelent egy több kampuszra kiterjedő nagy méretű hálózat fenntartása és védelme [33]. A szakirodalmi utalások és a saját tapasztalataim alapján feltételezem, hogy ennek okai csak

részben felsőoktatás-specifikusak. Az informatikai rendszerek széleskörű elterjedésével és szinte minden területre kiterjedő alkalmazásával annak kielégítő védelmét nem lehet megfelelő célszoftverek és menedzsment eszközök nélkül biztosítani, így a legnagyobb problémát feltételezhetően a rendelkezésre álló erőforrások hiánya jelenti. 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, intézményi szintű, koncepcionális fejlesztés megvalósítására alig van mód annak ellenére, hogy a kutatások pályázati támogatása is az informatikai rendszerek működőképességén, a pályázati adatok védelme az informatikai rendszerek biztonságán alapul. Ezen a téren a NIS2 magyarországi bevezetése hozhat változást, ennek szövege alapján várható a felsőoktatási intézmények informatikai védelmének megerősítése, mely csak a szükséges erőforrások rendelkezésre állása mellett valósítható meg.

Az informatikai eszközpark mellett az üzemeltetést végző személyzet rendelkezésre állása és esetleges alacsony szintű 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. Megfigyelhető, hogy egyre kevesebben tartják ideális munkahelynek a felsőoktatás intézményeit, nagyban csökken az ott munkát keresők száma, ami hosszú távon az üzemeltetés szakmai kiüresedéséhez vezet. Míg a végfelhasználók és munkaállomásaik támogatását biztosító munkatársak alkalmazása és megtartása viszonylag könnyebb feladat, a szerver- és hálózatüzemeltetést ellátó, speciális szakrendszerekben jártas kollégák a piaci elszívó hatással szembeni hosszú idejű megtartása már minden felsőoktatási intézmény számára megerőltető feladatot jelent. Jellemző, hogy a szakemberek a második gazdaságban egészítik ki jövedelmüket, munkaerejüket csak részben fordítják az egyetemi feladatok ellátására.

Az anyagi erőforrások hiányának következménye a saját, gyakran kényszerű megoldások kifejlesztése. Ezek a rendszerint webalapú szoftverek erősítik az egymással nem, vagy dokumentálatlanul kommunikáló, szigetszerű rendszerek elburjánzását, így hosszabb távon több kockázatot is magukban hordoznak. Mivel általános, hogy ezeket az adott szakterület valamelyik munkatársa díjazás nélkül, szabadidejében fejleszti, minőségük kétséges, és a fejlesztő távozásával támogatásuk megszűnik. Személyes tapasztalataim szerint nem elhanyagolható az amatőr programozók szerepvállalása, ugyanakkor megoldásaik alapvető biztonsági követelményeket hagyhatnak figyelmen kívül. Rendszereik felülvizsgálata során annak ellenére találtam példát jelszavak titkosítás nélküli tárolására, hogy annak kockázataira Robert Morris és Ken Thompson már 1979-ben felhívták a figyelmet [59]. A távoli hozzáféréssel elérhető alkalmazásaik a belső

informatikai hálózat egészére nézve jelenthetnek kockázatot, miközben a szervezeti hierarchiában gyakran alattuk elhelyezkedő informatikai üzemeltetés nem tudja megakadályozni alkalmazásaik üzembe helyezését. Hasonló kockázati elemet jelent az alacsony szintű tervezés és kontroll során 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.

A magyar egyetemek komplex informatikai rendszerei nagymennyiségű adatot tárolnak olyan környezetben, amelynek szisztematikus biztonsági elemzésének elvégzéséről a szabályzataik nem rendelkeznek. Ugyanakkor egy komplex informatikai rendszer működőképességének fenntartása és egy esetleges adatszivárgás megakadályozásának alapvető feltétele, hogy abban ne legyen ismert vagy kihasználható sérülékenység. Ehhez több okból sem elégséges csupán a szoftver támogatója által közzétett javítások rendszeres elvégzése. A gyártó által kibocsájtott frissítéseknek csak egy része tartalmaz biztonsági javításokat, a kisebb új funkciók bevezetése is ilyen formában érkezhet. Ugyanakkor ezek az update-ek az informatikai védelemnek csak az alsó szintjét jelentik, és nem adnak javítást azokra a konfigurációs hibákra, melyeket maguk a rendszermérnökök vagy rendszergazdák okoznak. A sérülékenységek számának minimálisra csökkentése érdekében szükséges azok feltérképezése, amelyre több módszer is ismert. A technikai eljárások a potenciális támadók által is alkalmazhatók, mely során képet kaphatnak egy rendszer aktuális állapotáról. Vizsgálatom szempontjából az alábbiak a leginkább relevánsak:

1. *Vulnerability Assessment (Sebezhetőségi vizsgálat).* Ebben az eljárásban egy rendszer ismert sebezhetőségeit kutatják fel, amely a megfelelő szoftver alkalmazásával magában foglalja az egyes sérülékenységek azonosítását, értékelését és kihasználhatóságát is. A vizsgálat elvégezhető rendszeresen vagy alkalomszerűen, automatizált, és manuális úton is. Számos, e célra kifejlesztett célszoftver van forgalomban, melyek kezelhetőség és funkcionalitás terén erős eltérést mutatnak.
2. A *Behatolásvizsgálat* (penetrációs teszt) olyan tesztelési eljárás, amelynek során a rendszer tulajdonosa által megbízott szolgáltató a sebezhetőségi vizsgálatok eszköztárán túl-

mutató módszerek alkalmazásával törekszik a vizsgált rendszer kompromittálására. Ennek célja azoknak pontoknak a meghatározása, amelyek lehetőséget nyújtanak a rendszerbe történő belépésre, adataihoz történő hozzáférésre, a CIA alapelvek megsértésének elérésére. A vizsgálat végrehajtását követően hozott intézkedéseknek a feltárt eljárások további alkalmazásának lehetőségét ki kell zárniuk. Különböző változatai ismertek, melyek elsősorban a vizsgált rendszerre vonatkozó előzetes ismerthalmaz rendelkezésre állásában különböznek, eszközkészletük pedig jellemzően előzetes sebezhetőségi vizsgálaton alapul, az adott rendszerre irányuló, egyedi támadási módszerek kidolgozását igényli.

3. A *kódelemzés* célja sérülékenységek azonosítása egy szoftver forráskódjának felülvizsgálatával. A nyílt forráskódú szoftverek esetében ez a potenciális támadók által is könnyen alkalmazható, míg zárt forráskód esetén alternatív módszerek alkalmazhatók a hibák felderítésére, melyek kihasználásával egy adott rendszer működése megzavarható. Egyetemi környezetben és más, közbeszerzésre kötelezett intézmények esetén a nyilvánosság érdekében közzétett beszerzési eljárások, szállítók, a beszerzett eszközök, valamint a jogszabályban előírt szoftverek megismerésével egy támadási forgatókönyv hatékonysága jelentősen növelhető. A mesterséges intelligencia napjainkban tapasztalható fejlődése várhatóan ezen a téren komoly áttörést hozhat.

Egy rendszer állapotának felmérése nem technikai megközelítéssel is lehetséges.

1. *Kockázatértékelés.* Az eljárás magában foglalja a rendszert fenyegető kockázatok azonosítását, értékelését, az előfordulás valószínűségének és hatásának súlyosságát. A kockázatkezeléshez szorosan kapcsolódik a kezelés rendjének kidolgozása, és a vállalt kockázat meghatározása.
2. *Biztonsági ellenőrzés.* A biztonsági ellenőrzés az informatikai rendszerben alkalmazott biztonsági intézkedések átfogó felülvizsgálata. Ez tartalmazza a biztonsági irányelvek, eljárások és konfigurációk felülvizsgálatát hatékonyságuk biztosítása és az iparági szabványok követelményeinek biztosítása érdekében.
3. A *fenyegetés modellezése* – hasonlóan a kódelemzéshez – egy-egy rendszer konfigurációjának elemzésével kezdődik, melyet a lehetséges fenyegetések és azok következményeinek meghatározása követ. A kockázatok elemzése után a konfigurációk módosításával további, például határvédelmi eszközök telepítésével vagy szabályzási úton meghozott védelmi intézkedések bevezetésével csökkentők az egyes incidensek bekövetkezésének valószínűségei. A számítógépes hálózatok kiemelt szereppel bírnak, esetükben

hálózatbiztonsági elemzést alkalmazzák, mely a hálózati infrastruktúra biztonságos működésének analízisét célozza, beleértve a fizikai eszközöket, azok konfigurációit és az alkalmazott hálózati protokollokat is.

4. Az *adatbiztonsági elemzés* során az egyes rendszereken belül tárolt adatok biztonságának értékelése mellett azok rendszerek közti megosztása, továbbításának és hozzáférési módjai kerülnek elemzésre.

Az arányos védelem kialakításához önmagában a fent felsoroltak egyike sem elegendő, így ezek költségarányos kombinációját kell alkalmazni, figyelembe véve, hogy egyes módszerek rendkívül magas anyagi ráfordítást igényelhetnek.

Az üzemeltetéséret felelős szervezeti egység számára a belső folyamatok ismerete, a rendelkezésre álló dokumentációs háttér és a szállítói támogatás hatékonyabb védelmi eljárások kidolgozását teszi lehetővé, ugyanakkor egy támadó különböző (pl. OSINT) technikákkal kombinálva ezek számottevő részét megismerheti. Egyetemi és más, közbeszerzésre kötelezett intézmények esetén a nyilvánosság érdekében közzétett beszerzési eljárások, szállítók, a beszerzett eszközök, valamint a jogszabályban előírt szoftverek megismerésével[23] egy támadási forgatókönyv hatékonysága jelentősen növelhető.

Az arányos védelem kialakításához önmagában a fent felsoroltak egyike sem elegendő, így ezek költségarányos kombinációját kell alkalmazni, figyelembe véve, hogy egyes módszerek rendkívül magas anyagi ráfordítást igényelhetnek. H2 és H3. hipotézisek bizonyításához szükséges adatforrást sebezhetőségi felméréssel állítottam elő, melynek eredményéből vontam le a következtetéseimet. Az ehhez szükséges eszközrendszer meghatározását a Mitre Att&ck mátrixa alapján végeztem [60]. Ez egy „konkrét fenyegetettségi modellek és módszerek kidolgozásának alapjául szolgáló" keretrendszer, mely strukturálja egy informatikai rendszer kompromittálásának lehetséges fázisait, az azokban alkalmazható módszereket és technikai megvalósításait. A sérülékenységvizsgálat elemeit a Felderítés (Reconnaissance) oszlop tartalmazza, melyből adatgyűjtési eljárásaim során az alábbiakat megvalósító technikai eszközöket használtam fel:

- *Szervezeti információk összegyűjtése*, melynek során magyar egyetemek IP címtartományait gyűjtöttem össze azért, hogy az általuk birtokolt hálózati címtartományokat meghatározzam.
- *Aktív hálózati szkennelés*. A módszer célja minél több, elsősorban szolgáltatási vagy

[23] A magyar felsőoktatási intézmények tanulmányi rendszere kötelezően a Neptun, a gazdasági rendszer pedig számos esetben egy SAP alapokon működő centralizált rendszer.

kapcsolódási információ összegyűjtése egy hálózati eszközről vagy azok halmazáról. A szkennelés eredménye alapján további cél felderített hálózati szolgáltatás sérülékenységének feltárása és lehetőség szerinti kihasználása.

- *További információk gyűjtése egy hálózati szolgáltatáshoz tartozó hozzáférésről*, melynek során általános vagy jelszó nélkül történő belépési lehetőségek jelenlétét vizsgálata történik meg. Kutatásetikai és a vizsgálatok jogszerű keretek közti végrehajtása érdekében ezt kizárólag a saját intézményem eszközein alkalmaztam, annak eredményeit nem általánosítottam.
- *Az adathalászat* módszerével a felhasználók információbiztonság-tudatosságát mértem le. Ennek eredményét dolgozatomban nem használtam fel, mivel nem álltak rendelkezésemre az általánosításhoz szükséges további mérések.
- *Nyílt technikai adatbázisok felderítésével és tartalmuk kinyerésével* elsősorban az intézményi e-mail címek és egyéb személyes adatok összegyűjtését, valamint a különféle pozíciókban dolgozó munkatársak azonosítását végeztem.

4.5. A sérülékenységek felderítése és mérési metodikája

Egy szervezet informatikai rendszerében jelenlevő sérülékenységek azonosítása elengedhetetlen egy jól működő védelmi stratégia kidolgozásához. Az intézkedések ideális sorrendjének meghatározásához és az annak érdekében alkalmazott eszközök vagy módszerek működőképességének ellenőrzésében elengedhetetlen egy metrika kialakítása és az az alapján végzett folyamatos mérés. Nagyobb szervezetek esetén szinte lehetetlen minden sérülékenységre azonnali és helyes választ adni, és lehetetlen a rendszer összes elemén minden elérhető javítást azonnal érvényre juttatni, figyelembe véve, hogy számos szervezet előírja a módosítások következményeinek előzetes vizsgálatát. Ilyen esetekre az informatikai menedzsmentnek rendelkeznie kell az egyes veszélyhelyzetek kezelésére vonatkozó stratégiával melyre H4. hipotézis ad egy, a felsőoktatási rendszerekre kidolgozott metodikát.

A sérülékenységek kezelése során a nagyobb kár okozására képes veszélyhelyzet előidézésére vagy okozására alkalmasakat magasabb prioritással kell kezelni. Így a tervezés alapfeltétele az egyes sérülékenységek fennállása következtében megjelenő kockázat súlyosságának helyes megítélése, mely megköveteli azok összehasonlíthatóságát, így egy egzakt mérési metrika meghatározását. A mérések alapját egy, a sérülékenységek katalogizálásával előállított adatbázis jelenti.

A cél elérését más megoldások is támogatják. Az IDS (Intrusion Detection System) rendszerek működése a hálózati forgalom folyamatos analizálásán alapul, melyben az elemzést végző eszköz a különböző támadásokra jellemző mintákat próbál azonosítani. Az eredmények alapján generált riportok kimutatják az egyes rendszerelemek forgalma alapján megállapított *lehetséges* érintettséget, így jelentős támogatást nyújthatnak az incidensek kezelésében és támogatják a korai előrejelzést is. Az IDS-ek modern változatai jelenleg elsősorban az adatbázisukban rögzített, már ismert támadásokra és sérülékenységekre jellemző minták alapján működnek, ugyanakkor a mélytanulásban elért tudományos eredmények alkalmazhatóságát számos kutatás vizsgálja [61] [62, p. 2]. Az IDS-ek alkalmazásának fő hátrányaként a hálózatban megjelenő támadó minták detektálása és az azokat tartalmazó csomagok célpontjai közti kapcsolat hiányát tartom. Egy ilyen rendszer beüzemelése során egy magyar egyetem internet átjáróján mért forgalmának analízise legnagyobb számban Log4J sérülékenység kihasználására irányuló forgalomról számolt be, miközben az egyetemi informatikai rendszer nem tartalmazott olyan komponenst, amely erre érzékeny lett volna.

Egy az IDS kiterjesztéseként működő IPS (Intrusion Prevention System) egy támadó minta azonosítása esetén képes megszakítani a kommunikációban részvevő számítógépek forgalmát is, a detektáláson túl tehát védelmi funkciója is van. Az IPS alkalmazása esetén bekövetkező téves riasztások viszont már komolyabb következményekkel járhatnak, mivel a kapcsolatok indokolatlan blokkolása a rendszer rendelkezésre állását nagyban leronthatja [63].

Az IDS és IPS rendszerek adatbázisainak adatai gyakran különféle csapdarendszerek (honeypot, sandbox stb.) adatainak elemzéséből származnak. Ezek a „mézesbödönök” olyan preparált rendszerek, melyek rossz konfigurációval, hibás védelmi beállításokkal vagy ismert sérülékenységekkel teszik lehetővé a rendszer megtámadását, mely során folyamatosan nyomon követik és naplózzák a támadók lépéseit. Feng megfogalmazásában a honeypotok alkalmazása a passzív IDS/IPS rendszereket integrált aktív eszközökké változtatják [64, p. 231]. Magyarországon a már említett Hun-Cert tervezett és működtet Raspberry PI alapú honeypot gépeket, ezek számos magyar szervezet hálózatában működnek és gyűjtenek támadási adatokat elsősorban levelezési, távoli bejelentkezési és webszolgáltatásokkal kapcsolatban.

Mind az IDS, mid az IPS rendszerek alkalmasak lehetnek forenzikus vizsgálatok elvégzésének támogatására is.

4.6. Sérülékenységi adatbázisok

A sérülékenységek nyilvántartására és jellemzőik leírására a Massachusetts Institute of Technology Research and Engineering (MITRE) 1999-ben indított közösségi programot, melynek

célja a Common Vulnerabilities and Exposures (CVE) adatbázis létrehozása volt [65]. Ebben az adatbázisban olyan hibákat tartanak nyilván, melyeket a gyártójuk elismert vagy dokumentált, és más hibáktól függetlenül javíthatók. Az adatbázisban az így ismertté vált sebezhetőségeket egységesített azonosítóval, rövid leírással és megjegyzések rögzítésére alkalmas mezővel látták el. Lényeges, hogy az adatbázis nem tartalmaz sérülékenységekre vonatkozó technikai adatokat és annak lehetséges hatásaira vagy a javítására vonatkozó információkat sem. Ezek – amennyiben léteznek – részben a gyártók által fenntartott listákban, részben pedig más adatbázisokban, például az Amerikai Egyesült Államokban a National Vulnerability Database-ben[24] (NVD), vagy a CERT/CC Vulnerability Notes-ban találhatók meg. Emellett más, nyilvános közzétételi források is léteznek, többek közt a szoftvergyártók saját megoldásaiban, vagy olyan nyílt közösségi fórumokon, mint amilyen a BugTraq volt.

A CVE azonosítókat a CVE Numbering Authority szervezete (CNA) kezeli, melynek e sorok írásakor 35 országban 260 informatikai cég volt tagja, s melyek a legnagyobb számban az USA vállalatai közül kerülnek ki. Az adatbázis bármilyen forrásból fogad sérülékenységi adatokat, melyeket kivizsgálásuk után CVE azonosítóval lát el.

Az NVD a CVE-re épülő adatbázis, mely további adatokkal egészíti ki azt. Az NVD „egy átfogó kiberbiztonsági sebezhetőségi adatbázis, amely integrálja az összes nyilvánosan elérhető amerikai kormányzati sebezhetőségi forrást, és hivatkozásokat biztosít az ipari forrásokra, a CVE-listával szinkronizált, és [működése] azon alapul. Az NVD tartalmazza a biztonsági tartalom automatizálási protokoll (SCAP) leképezéseit is a CVE azonosítókhoz. A SCAP egy olyan módszer, amely meghatározott szabványok felhasználásával lehetővé teszi a sebezhetőségek automatizált kezelését, mérését és a szabályoknak való megfelelés értékelését (pl. FISMA-megfelelés).” [66]

Mind a CVE, mind az NVE nyilvánosan elérhető, és minkettő felügyeletében a részt vesz az Amerikai Egyesült Államok Belbiztonsági Minisztériumának részeként működő Cybersecurity and Infrastructure Security Agency (CISA)[25]. A CVE-NVD adatait számos egyéb szervezet alkalmazza a saját adatbázisában, és látja el saját jelölésével – így pl. a CVE-2016-1546 sérülékenység megtalálható apache-httpd-cve-2016-1546 néven is.

Bár a sérülékenységi adatbázisokat a nyilvánosságra hozott kiberbiztonsági sebezhetőségek védelmi célú azonosítására, meghatározására és katalogizálására hozták létre, sajnos az így közzétett publikus információk egy azonosított rendszerelem ellen indított támadás tervezési fo-

[24] Egyesült Államok Nemzeti Sebezhetőségi Adatbázisa, melynek elérhetősége: https://nvd.nist.gov.
[25] Kibervédelmi és Infrastruktúra-biztonsági Ügynökség.

lyamatában annak eredeti céljával ellentétesen is felhasználhatók. A sérülékenységi adatbázisokra alapozva egy potenciális támadó a kompromittálni kívánt célrendszer verziószámának ismeretében pontos információt kap annak ismert sérülékenységeiről, majd az exploit adatbázisok[26] valamelyikéről letöltött kész támadó eszköz alkalmazásával célirányosan támadhatja azt. A zero-day, és más, javítással még nem rendelkező sérülékenységek esetében a támadók informálásának elkerülése érdekében ezért a CNA elvégzi ugyan egy új azonosító hozzárendelését, de a rendszerben való láthatóságát korlátozza arra az időre, amíg a hibajavítás el nem készül. A sebezhetőségi adatbázisok ilyen irányú kihasználásával számos kutatás foglalkozik. Arora és társai 2006-ban kimutatták, hogy a közzétett sebezhetőségre vonatkozó javítások elérhetővé tétele után a vizsgált munkaállomásaik naponta 0,17 támadást szenvedtek el, míg a sebezhetőségek publikálása kb. 0,11 támadást eredményez minden munkaállomásra nézve. Megállapításuk szerint nyilvánvaló, hogy a sérülékenységek javítására szolgáló információk közzététele a támadók számára előnyt jelent. Úgy tapasztalták, hogy a munkaállomások hibajavításának késése és a patch-ek által nyújtott hasznos információk javítják a támadási esélyeket, ezért az azon alapuló támadások száma kibocsájtásukkor jelentősen megnő. Eredményük azt is sugallja, hogy a közzétett és a javított sebezhetőségeket valószínűleg jobban kihasználják, mint azokat, amelyeket még nem publikáltak [67].

4.7. A sérülékenységek számszerű meghatározása

A kockázatelemzés során alkalmazható módszertanok, az azokat támogató szabványok és jógyakorlatok gyakran nem adnak lehetőséget a kockázat becsléséhez. Egyes szervezetek különböző sebezhetőségi pontozási keretrendszereket definiáltak a kockázat minőségi[27] vagy mennyiségi értékelésére[28]. A sérülékenységi metrikák megkerülhetetlen szereplője a Forum of Incident Response and Security Teams, Inc. (FIRST) nonprofit szervezet által birtokolt és kezelt Common Vulnerability Scoring System (CVSS) keretrendszer, de több más, hasonló célú rendszer is ismert [68]. Johnson és társai egy Bayes-módszeren alapuló kutatásban összehasonlították az NVD, X-Force, OSVDB CERT-VN és a Cisco hasonló célú rendszereit, és bár különböző területeken eltérő eredményeket kaptak, összességében néhány dimenzió kivételével a CVSS megbízhatóságát jónak találták [69]. Ennek első változata 2005-ben jelent meg, melyet azóta többször is továbbfejlesztettek, és jelenleg is több különböző verziója van használatban.

[26] Ilyen forrás érhető el pl. a https://www.exploit-db.com/ oldalon.
[27] A Microsoft a kockázatokat kritikus, fontos, közepes és alacsony súlyossági skála alapján sorolja be.
[28] A Cybersecurity and Infrastructure Security Agency (CISA) pontozási rendszere az incidensekre irányul, melynek leírása a https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System oldalon érhető el.

Használatát az Amerikai Egyesült Államok kormányzata számos állami vagy a kritikus infrastruktúra elem, többek között bankkártyák és orvosi eszközök gyártói számára teszi kötelezővé. A CVSS emellett számos különféle határvédelmi rendszerbe és sebezhetőségi vizsgálatokat végző szoftverbe is beépítésre került, melyek egy része jelenleg is a korábbi, a 2.0-s verzióra épül.

Annak ellenére, hogy jelenleg a 3.1-es változat a legfrissebb, a kutatásomban a 3.0-s változattal dolgoztam, melynek legfőbb oka a rendelkezésemre álló sérülékenység-detektáló szoftverek 3.1-es implementációjának hiánya volt. Megállapításaim bizonyításában a 3.0-s verzió alkalmazásának az alábbi szempontok alapján nincs számottevő negatív hatása:

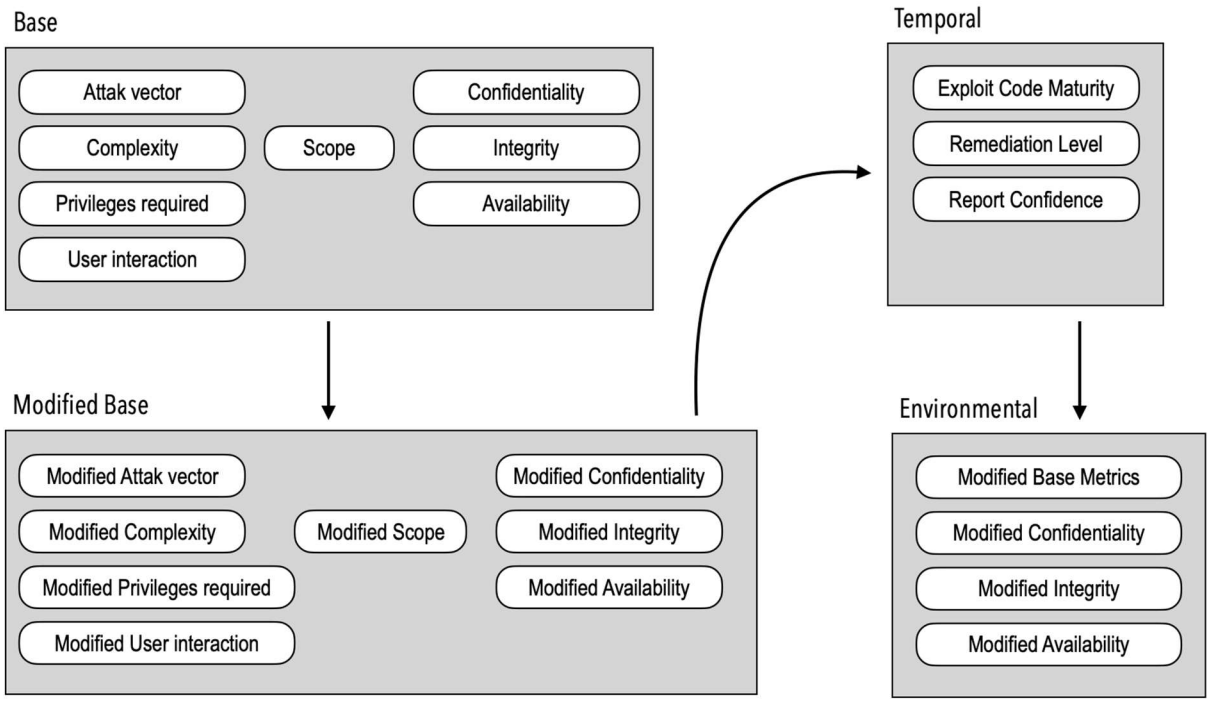
- Az új sérülékenységekre az NVD adatbázisban 2019. szeptember 10-én kezdték meg a 3.1-es változat szerinti értékelést, ekkor indult a korábbi rekordok visszamenőleges újraértékelése is.
- Murray 2020-as vizsgálatában kimutatta, hogy 2019-ben az NVD adatbázisának csak 18%-a tartalmazott CVSS 3.1-es értékelést, azok túlnyomó részben a 2019-es sérülékenységekre korlátozódtak, és az értékelésük pontszáma pontosan megegyezett a 3.0-s verzióban előállított értékekkel. A legnagyobb eltérést a CVE-2019-1010241 sérülékenységnél találták, melyben a 3.1-es verzió szerinti érték a korábbi 8,8-ról 6,5-re esett vissza, tehát egy korábban súlyosabb minősítést gyengített meg [70].

A CVSS elsődleges célja a sérülékenység által jelentett potenciális veszély számszerű kifejezése[29]. Ennek elérése érdekében egy adott sérülékenység súlyosságát meghatározó tényezők összességét a CVSS három fő metrikacsoportba sorolja, melyek a *Base (alap),* a *Temporal (időbeni)* és az *Environmental (környezeti)* besorolást kapták. Az alapérték meghatározásában olyan komponensek vesznek részt, melyek a sérülékenység teljes életciklusa alatt változatlanok maradnak, a *temporal* pontértékek alapját az időben változó elemek adják, a környezetiek pedig korrekciós lehetőséget biztosítanak a végső pontszám súlyozása érdekében, egy, a rendszert ért incidens következményeinek lehetséges hatásai alapján. A továbbiakban az érték gyors kiolvasását lehetővé tevő ún. *vectorstring* érthetőségének érdekében, mely a metrikacsoportok képzésében résztvevő egyes komponenseket és annak értékeit rövidített formában tartalmazza, a tulajdonságok angol neveit fogom használni.

[29] https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf

A metrika előállításának módszertanában a sérülékenységet három metrikacsoport pontszámának együtteséből képzett érték írja le, melynek kiszámításához a FIRST meghatározta az alkalmazandó formulákat is. Az egyes csoportok pontszámai együttesen adják sérülékenység végső pontszámát, amely végül egy [0-10] zárt intervallumba eső valós szám, ahol a magasabb pontszám az adott területen magasabb fokú veszélyt jelent. Végül, ezen metrikák együttese alapján határozható meg a CVSS pontszám, a sérülékenység részleteinek rövidített leírására pedig a *vectorstring*.
Az egyes komponensek meghatározásának kritériumait a CVSS 3.0 dokumentációja szintén meghatározza. Ebben a munkafolyamatban később érdemes meggondolni a 3.1-es verzió ajánlásait, melyek a legtöbb esetben a korábbi változat pontosításai.
Az NVD CVSS pontozási rendszere eltér a fentiektől, annak részhalmazaként tekinthető. Annak ellenére, hogy az NVD pontszám kalkulátorában mindhárom említett metrikacsoport megjelenik, valamint támogatja a CVSS 2.0, 3.0 és 3.1-es változatait is, az NVD az egyes sérülékenységek pontozását csak a *base* osztály alapján képezi. Tekintettel arra, hogy az NVD esetében nincs mód sem az érintett szervezetek egyéni sajátosságainak alapján környezeti módosítók meghatározására, sem időbeni módosulások érvényesítésére, kizárólagos alkalmazása az érintett szervezeteket hátrányosan érinti, mivel nincs lehetőségük a reális pontozási érték alkalmazására.

A CVSS 3.x verziójában a *base* metrikacsoport értékének kiszámításában azok a komponensek vesznek részt, melyek függetlenek az érintett rendszer sérülékenységének lehetséges következményeitől (azaz a környezeti jellemzőktől) és a sérülékenység életciklusa során nem változnak meg. Egy sérülékenység értékelése során a base metrikacsoporthoz ezért három almetrikát kell kiszámítani, melyek a confidentiality (kihasználhatóság), a scope (hatókör) és az impact (hatás) mérőszámai. A kihasználhatóság meghatározásában azokat a jellemzőket kell figyelembe venni, amelyek meghatározzák, hogy az adott sebezhetőség milyen könnyen, milyen technikai feltételek mellett használható ki.



2. ábra. A CVSS 3.0 metrika felépítése. Szerkesztette a szerző.

A base metrikacsoportot négy, időben állandó komponensegyütteséből alkotott érték határozza meg. Kiszámításukkor és az általuk jelentett kockázat kiértékelésekor a metodika feltételezi, hogy a támadó ismeri a megtámadni kívánt rendszer belső felépítését, és rendelkezik annak működéséről a számára szükséges adatokkal. Így a kihasználhatóságot lehetővé tevő körülmények meghatározása során feltételezi, hogy az a támadó számára ideális környezetben történik. Paul Karger és Roger Schell már 1974-ben leírták, hogy milyen nehéz védekezni egy olyan támadó ellen, aki rendelkezik a megtámadni kívánt rendszer egy példányával, és képes minden rétegének offline vizsgálatára [71]. Bár ez a követelmény épp a CVSS-szel szembeni egyik leghangsúlyosabb kritika alapja, melynek következménye a sebezhetőségek túlértékelésének lehetősége, a megfelelő módon kezelve azokat a besorolás minősége javítható.

4.8. A CVSS pontszám meghatározása

Az attack vector (AV) mérőszáma a támadó és a sérülékeny rendszer között megkövetelt távolságot írja le. Magas fenyegetettséget jelent, ha egy célpont nagy kiterjedésű hálózati kapcsola-

tán, tipikusan egy meglevő internetkapcsolaton keresztül támadható. Az ilyen besorolású sérülékenységek értékét a Zerodium Bounty programjának ártáblája[30] is alátámasztja: a legnagyobb értékű kifizetéseket a cég az ún. zero click sérülékenységekért kínálja [72]. Az AV további értékei az Adjacent, mely a kistávolságú hálózatokat, tipikusan bluetooth kapcsolatokat definiál, a helyi (Local), mely pl. egy konzol hozzáférést, a fizikai (Physical) pedig közvetlen hozzáférést követel meg. Utóbbit igénylő támadások jellemző példái egy rendszert tartalmazó háttértár kiszerelése és egy más rendszerben, a védelmi eljárások megkerülésével történő olvasása, esetleg live OS indításán alapuló, a különféle CD/USB háttértárakból indított hozzáférési technikák, de ebbe sorolandók a különféle *evil maid* típusú támadások is[31]. Tereshkin tanulmányában rámutatott, hogy a megfelelő környezeti feltételek mellett a fizikai hozzáférés abban az esetben is lehet eredményes, ha egy számítógép merevlemeze teljes egészében erős titkosítással van ellátva [73].

Az *attack vector* meghatározása nem minden esetben egyértelmű, és bizonyos esetekben mélyebb szakmai ismeretet igényel. A problémára Murray ad egy jól érthető példát: ebben egy olyan attack vector besorolásának problémáját veti fel, melynek kihasználásához az egérkurzor mozgatása szükséges. Ennek besorolásakor téves annak feltételezése, hogy a támadónak fizikailag hozzá kell férnie az egérhez, figyelembe véve, hogy az egérkurzor mozgatása tisztán szoftveres úton is lehetséges [70].

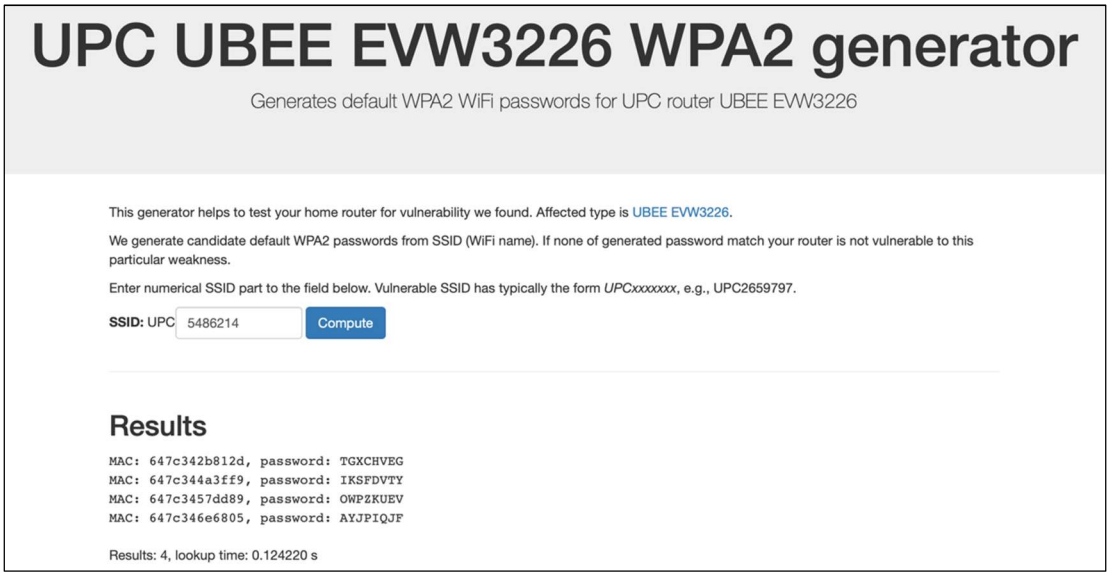
Az Attack Complexity (AC) mérőszáma a sérülékenység kihasználásának bonyolultsági fokát definiálja. gyakorlati lehetőségét írja le. Egy man in the middle típusú támadás megvalósítása komolyabb előkészületet követel meg, míg egy kész exploit alkalmazása alapszintű felhasználói ismeretek mellett is végrehajtható [74].

A Privileges Required (PR) értékét az adott sérülékenység kihasználásához szükséges előzetes jogosultság követelménye határozza meg. Magyar példaként a UPC internetszolgáltató egyes végberendezéseinek nevezetes sérülékenysége szolgálhat, amely során a hozzáférési jelszavakat az általuk használt SSID-iből generálták, így az adott eszközhöz tartozó jelszó legfeljebb egy 16 lépéses eljárással képezhető[32].

[30] A Zerodium egy kiberbiztonsági szakértő vállalkozás, mely a korábban ismeretlen sérülékenységeket vásárol meg. Feltételezhető, hogy ezeket kiberfegyverek vagy más, támadó jellegű alkalmazások építésében használják fel, vagy értékesítik.

[31] Ez a támadás a hotelszobákban felügyelet nélkül hagyott számítógépek manipulálásával, fizikai elemeinek kompromittált változatra történő cseréjével megvalósított metodikák. A szakszolgálatok az ilyen típusú támadások elkerülésére javasolják a kisméretű, állandóan személyes felügyelet alatt tartható adathordozók alkalmazását, valamint a potenciális célszemélyek számára a külföldi utak során mindenfajta személyes adatot nélkülöző, ideiglenes használatú informatikai eszközök használatát.

[32] Forrás: https://ubee.deadcode.me.



3. ábra. Egy UPC router alapértelmezett jelszavának feltörése.

A User Interaction (UI) értékét valamilyen felhasználói cselekmény követelménye határozza meg (pl. egy levél mellékletében küldött kártékony program elindítása), a scope metrika azt mutatja meg, hogy egy adott sérülékenység hatása kiterjedhet-e olyan területre is, amely eredetileg nem tartozott annak hatókörébe. A hatás mérőszámait az adott sérülékenység kihasználása esetén a bizalmasság, a sértetlenség és a rendelkezésre állás területén várható következmények alapján képezik.

Mivel a base metrikacsoport értékét nyolc, egymástól független érték határozza meg, ezért annak tömör leírására a napi gyakorlatban a már említett vectorstringet alkalmazzák, amely az alábbi alakú :

CVSS:3.0/AV:N|A|L|P/AC:H|L/PR:H|L|N/UI:L|N/S:C|U/C:H|L|N/I:H|L|N/A:H|L|N

A base score kiszámításához a metrika besorolásonként egy-egy számértéket definiál, mely azonban nem minden rendszer esetében helytálló. Amennyiben egy rendszer konfigurációja eltér attól, amit az eredeti értékelést végzők az adott komponens alapértelmezett vagy ajánlott konfigurációjának ismeretében meghatároztak, az adott metrika értékét a megváltozott konfigurációjú környezetnek megfelelően újra kell értékelni, és megfelelően módosítani. Az értékelendő komponens jogosultságai, vagy esetleges sérülékenységéből származó hatókör megváltozásának függvényében ez egyaránt jelenhet szigorítást vagy könnyítést is.

Az egyes sérülékenységek lehetséges hatásai különböző környezetekben is lehetnek eltérők, így, amennyiben egy szervezet az incidenskezelésben azt alkalmazni kívánja, figyelembe kell

vennie az érintett rendszerek fontosságát is. A CVSS-ben ezért a környezeti (environmental) mérőszámok alkalmazásával lehetőség van a pontszám korrekciójára a bizalmasság, a sértetlenség és a rendelkezésre állás területén. Az így korrigált értékek a módosított bizalmasság, módosított sértetlenség és módosított rendelkezésre állás elnevezést kapták. Meghatározásukban olyan tényezők kapnak szerepet, mint a sebezhető eszközök hozzáférhetősége a támadók számára, a sebezhetőség típusa, a támadható eszköz alkalmazásának célja, adattartalmának, vagy az általa biztosított szolgáltatások értéke vagy elvesztése következtében keletkezett kár stb. Alkalmazásukkal érvényesíthető a különbség egy, csak oktatási vagy gyakorlási célokat szolgáló szerver, és a tanulmányi rendszer kiszolgálóit egyaránt érintő sérülékenység között: míg az előbbit ért sikeres támadás következményei nem jelentősek, a legmagasabb védelmi szintbe sorolt alkalmazások szerverei esetében ugyanez egy rendkívüli incidens lehetséges forrásaként kerül meghatározásra. Végül a CVSS a sérülékenységet az összesített pontszám alapján a None, Low, Medium, High és Critical szintek valamelyikébe sorolja be.

4.9. Sérülékenységvizsgálati eszközök

A sérülékenységek feltárása jellemzően sérülékenységvizsgálati szoftverekkel történik, melyek célja adott informatikai környezet biztonsági állapotának felderítése, valamint az abban található sérülékenységek, hibák, gyenge pontok feltárása, mely során azonosíthatóvá válnak azok a potenciális biztonsági rések vagy sebezhetőségek, amelyeket kihasználva támadók jogosulatlan hozzáférést vagy kihasználást érnek el. Működésük és felhasználásuk alapján több csoportba sorolhatók.

A sérülékenységvizsgálati rendszerek ismert sérülékenységek adatbázisára épülnek, és általában több technikát integrálnak. Egyes változataik csak egy-egy adott részterületre koncentrálnak[33], mások általános célú keretrendszert alkotnak, melyek szabadon bővíthetők[34]. A hálózati forgalom analizálásán alapuló eszközök a rajtuk átfolyó forgalom elemzésével azonosítják a kártékony adatforgalmat és jelentéseket készítenek (IDS) vagy válaszlépéseket tesznek (IPS). A log analizátorok a rendszerek eseménynaplóinak folyamatos ellenőrzésével végeznek vizsgálatokat. A hálózati sérülékenységvizsgálati eszközök a hálózaton keresztül kihasználható ismert sérülékenységeket és konfigurációs hibákat tárják fel[35].

[33] A Nikto, az Arachni és az OWASP ZAP webalkalmazások sérülékenységeinek felkutatására szolgál.
[34] A Metasploit egy közismert, nyílt forráskódú, kifejezetten a penetration testing és az exploit fejlesztés céljaira kifejlesztett keretrendszer.
[35] A Nessus és a Nexpose ismert kereskedelmi, a közösségi OpenVAS szabadon elérhető szoftver ebben a kategóriában.

A Security Information and Event Management (SIEM) rendszerek általános biztonsági felügyeletet biztosítanak: lehetővé teszik rendszernaplók, események és egyéb biztonsági információk gyűjtését, feldolgozását, elemzését és megjelenítését egy központi konzolon[36]. Fontos megemlíteni, hogy a felsorolt példák csak részben fedik le a sérülékenységvizsgálat teljes eszközrendszerét.

4.10.A CVSS hiányosságai

A CVSS alkalmazásával szemben számos kritika merül fel. Bár az egyes sérülékenységek pontértékének összehasonlíthatósága ideális lehetőségnek tűnik egy a kockázatelemzési eljárás kidolgozása során, általános szabály, hogy az önmagában nem alkalmazható. A *base* pontszámai nem veszik figyelembe a sebezhetőség kihasználhatóságának időbeni változásait, így például azt sem, hogy a gyártó biztosított-e már javítócsomagot, hogy a sérülékenység milyen régóta áll fenn, és hogy az adott környezetben egyáltalán kihasználható-e.

A CVSS-szel szembeni másik kritika az alkalmazott formulákon alapul. Bozorgi és társai [75, p. 2] így írnak erről: „While we have little doubt that these scoring metrics were carefully considered and of great value when FIRST developed, we suspect that any single fixed equation, such as eq. 1 is unlikely to provide a robust and lasting model of vulnerability severity."[37]

Egyes kutatások arra irányulnak, hogy informatikai rendszerek incidenseit összekapcsolják a biztonsági eseményekkel és az általuk jelentett kockázatokkal, Allodi és Massacci pedig egy kutatásban bizonyítják, hogy a legnagyobb kockázatcsökkentést a feketepiacon megjelenő exploitokra adott gyors reakció eredményezi [76]. Ezen a ponton jelenik meg a CVSS-szel szembeni egyik legtöbbet hangsúlyozott alkalmazási hiba, a CVSS pontérték és a kockázat közötti szoros összefüggés feltételezése.

Annak érdekében, hogy egy adott sérülékenység kihasználásának valószínűsége is meghatározható legyen, további módszerek alkalmazása szükséges. Egy lehetséges megoldást azon szoftverek rendszernaplóinak elemzése jelenthet, melyek egy hálózaton áthaladó forgalmat analizálják és rögzítik az egyes sérülékenységeket kihasználó minták megjelenését. Az így mért adatok feldolgozására szintén Allodi és Massacci ad tudományos módszertant [77]. Tipikus típusai a már említett IDS vagy a felismert minták alapján a hálózati forgalom szabályozására is képes

[36] Egy ingyenes és jól használható SIEM rendszer a Wazuh.

[37] Bár nincs kétségünk afelől, hogy ezeket a mérőszámokat alaposan átgondolták és a FIRST fejlesztése komoly értéket képvisel, azt gyanítjuk, hogy egyetlen rögzített egyenlet, mint például [a base score értékének kiszámítását végző formula], nem valószínű, hogy a sebezhetőség súlyosságának robusztus és tartós modelljét nyújtja.

IPS rendszerek [78]. A kockázat mértékét a gyakorlatban ezt a sérülékenységvizsgálati szoftverekbe épített Exploit Prediction Scoring System (EPSS) algoritmus teszi lehetővé [79], mely az említett rendszernaplók elemzése során egy [0,1] intervallumba eső valószínűségi szorzót definiál, melyre alapozva egy tanulási fázis eltelte után meghatározza a sérülékenység kihasználásának következő harminc napban bekövetkező valószínűségét[38]. Az EPSS az érték kiszámításának bemenő paramétereiként több adatforrást használ fel:

- A CVE adatbázis publikus információi, valamint az azokban található szöveges leírások elemzése. A valószínűség kiszámításában paraméterként szerepel a publikálás óta eltelt napok száma.
- Gyártói jelentések.
- Az NVD által közzétett CVSS v3 vektorok szerinti besorolás a pontozási táblázat alkalmazása nélkül.
- Biztonsági szkennerszoftverek riportjait,[39] melyek az eddig említett forrásokon túl számos más, elsősorban konfigurációs hiba felderítését is végzik, nyitott portok detektálásától a szolgáltatások nyers erővel történő támadásán át címtárak tartalmának megszerzéséig.
- Ismert forrásokból[40] származó, az egyes sérülékenységek kihasználáshoz szükséges kész kódok alkalmazhatóságát.
- Biztonsági cégek napi jelentéseit a sérülékenységek megjelenéséről, valamint aktivitásuk változásáról.

Bár a rendszernapló-elemzésen alapuló behatolásvizsgálat terén a mesterséges intelligencia alkalmazhatóságát már bizonyították [80], az EPSS rendszerekbe építésére még konkrét szakirodalmi hivatkozást még nem találtam, bár az a későbbiekben minden bizonnyal megjelenik [81]. Az utóbbi két elem az EPSS előrejelzési modelljében játszik szerepet, mely jelentősen befolyásolhatja az incidensek megelőzésére tett intézkedések sorrendjét és a hozzájuk allokált erőforrások helyes megválasztását. Alkalmazásával a szervezetek képesek lehetnek a javítást célzó intézkedések sorrendjének optimalizálásra, akár azt is feltételezve, hogy lesznek olyanok, amelyek e stratégia mentén sohasem kerülnek sorra. Így egy EPSS-t alkalmazó szervezetnek vár-

[38] A kiszámítás módját a FIRST a https://www.first.org/epss/model oldalon publikálta.
[39] Ilyen szoftver pl. a Sn1per vagy a Nuclei.
[40] A legismertebb változatok a Metasploit vagy az ExploitDB.

hatóan kisebb számú sebezhetőséget kell javítania, mint a klasszikus CVSS-re alapozott, pontszám szerinti döntésen alapuló stratégiát alkalmazónak, miközben a védelmének szintje várhatóan emelkedni fog.
Az EPSS sem kezelhető önmagában kockázati pontszámként, mivel értékét az adott szervezet egyéni működési környezete jelentősen módosíthatja. A legjobb eredményt a CVSS-szel történő együttes értékeléssel lehet elérni.
Megítélésem szerint az EPSS korrekcióval meghatározott értéke sem alkalmazható mérlegelés nélkül kockázati pontszámként, mivel ez is számos, a veszélyeztetettség szempontjából lényeges paramétert hagy figyelmen kívül. Ebben sem jelenik meg egyes eszközök hozzáférhetősége egy külső vagy belső támadó számára, csakúgy, mint az eszköz által ellátott szolgáltatás célja és annak súlya az azt működtető szervezetben. Egyedül az EPSS-re alapozva nem határozható meg helyes védelmi stratégia.

4.11. Egy egyetemi rendszer sérülékenységvizsgálati elemzése

Személyes szakmai tapasztalataim alapján feltételezem, hogy az egyetemi informatikai rendszerek üzemeltetői a központi informatikai berendezések karbantartását és védelmét magasabb prioritással kezelik, így azok üzemeltetési feladatait nagyobb időkeretben és magasabb prioritással végzik el. Ebből következően a perifériális elemek védelmének feladatai másodlagos feladatkört jelentenek, ezért az azokban tárolt adatokkal kapcsolatos közvetett kockázat magasabb, mint a központi infrastruktúra esetén. Ennek bizonyítását H2. hipotézisben fogalmaztam meg: **A magyarországi felsőoktatási informatikai rendszerek központi területeken üzemeltetett rendszerelemein kisebb számú sérülékenység mérhető, mint a perifériális telephelyeken működőkén**. H3. hipotézist szintén üzemeltetési tapasztalataim alapján állítottam fel, melynek lényege a programhibák okozta sérülékenységek magas száma, valamint a hibás konfigurációs beállítások következtében sérülékennyé vált rendszerek támadhatósága: **a magyarországi felsőoktatási információs rendszerek sérülékenységeiről jelentős mennyiségű, egy évnél régebben ismert technikai információ gyűjthető össze, melyek túlnyomórészt hibás konfigurációs beállítások eredményei**.

Mindkét hipotézis igazolását valós körülmények közt, egy egyetemi informatikai rendszer állapotának felmérésével és elemzésével végeztem, melynek alapfeltétele releváns adatok tervszerű gyűjtése, valamint a hipotézisek igazolásához szükséges csoportosítás kialakítása. Mindkét hipotézis bizonyításának első lépése egy-egy esettanulmány volt, további intézmények vizsgálatát csak ezek teljesülése esetén terveztem lefolytatni.

Bár egyes források a belső személyzet által végzett sérülékenységvizsgálati eljárások hatékonyságát kétségbe vonják [82, p. 48], megfelelő erőforrások hiányában ezeket önállóan végeztem. A szükséges adatok összegyűjtését egy vulnerability scanner szoftverre alapozva terveztem, melyeknek számos különböző megvalósítása létezik. Szolgáltatáskészletük és áruk elemzése alapján végül az alábbiak alkalmazását mérlegeltem [83].

- A Nessus széles körben elterjedt szkenner szoftver, mely működését elsősorban a sebezhetőségek különböző adatbázisaira, többek közt a már bemutatott CVE-re alapozza. Ez alapján képes számos sérülékenység azonosítására, feltünteti azok súlyossági szintjét, tartalmazza a CVSS vectorstringet és elemeit, és képes a CVSS pontszám meghatározására. Rendszerkonfigurációs hibák azonosításának képessége az informatikai rendszerek auditja során szinte nélkülözhetetlenné teszi. Működése automatizálható, egy ezzel felügyelt rendszer állapota folyamatosan nyomon követhető, továbbá integrálható más rendszerekkel – képes a detektált sérülékenységeket valamely SIEM rendszer számára átadni, vagy abból hibajegyet készíteni. A folyamatos frissítések és a gyártó által fejlesztett és naprakészen tartott adatbázisa következtében a szoftver ára meglehetősen magas. Kipróbálható változata teljes funkcionalitással csak 7 napon át, maximum 16 IP címre működik.
- A Nexpose a Nessus szolgáltatási köréhez hasonló funkcionalitású termék, hozzávetőleg 50 további szoftver integrációjának lehetőségével, melyben a Metasploit is szerepel[41]. Bár fő funkcióiban, a mérési adatok összegyűjtésében alig különbözik a Nessustól, néhány különbség felfedezhető, melyek közül az egyik legfontosabb a CVSS kihasználhatósági pontszámok előállítása. Ez a virtuális gépként is letölthető szkenner szintén több adatforrás használ fel, a kipróbálható változat egy hónapon át nyújt teljes szolgáltatási kört 500 IP címre.
- Az Open Vulnerability Assessment System (OpenVAS) egy nyílt forrású szoftver, melyet 2002 óta fejlesztenek. Alkalmazását elsősorban rendszerüzemeltetőknek szánják, így beállítása és működtetése, felügyelete nagyobb szakértelmet kíván. Ez a keretrendszer is elsősorban a sebezhetőségek felderítését célozza, és bár szintén nagy sérülékenységi adatbázissal rendelkezik, annak mérete elmarad a Nessusétól [84, pp. 52-58]. Mivel ingyenes szoftver, hosszú távon is működtethető szemben a kereskedelmi szoftverekkel,

[41] A szoftverek részletes szolgáltatási körének összehasonlító táblázata a https://sourceforge.net/software/compare/Nessus-vs-Nexpose-vs-OpenVAS/ címen érhető el.

melyek alapára is meglehetősen magas, s a kiegészítő modulok licenszeivel az többszörösére is emelkedhet.

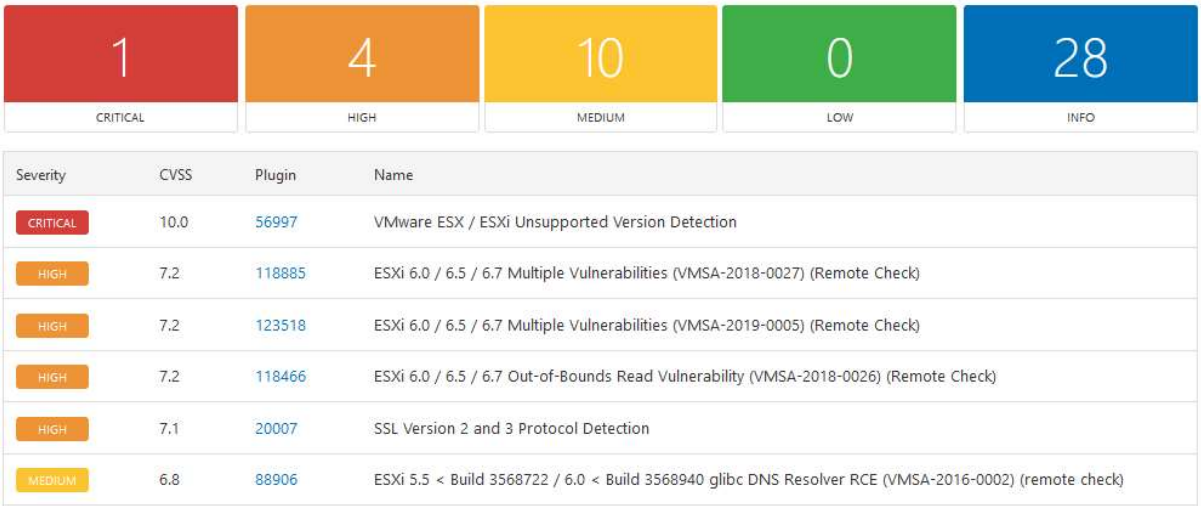
- A szintén nyílt forráskódú Wazuh egy szabadon felhasználható SIEM rendszer, mely elsősorban a biztonsági incidensek felismerésében és kezelésében használható. Funkciói közt nem csak a sérülékenységi riportok generálása, hanem javasolt konfigurációs beállítások széles gyűjteménye található meg. A szoftver az eddig ismertetekkel szemben a felügyelt gépekre kliensprogram telepítését követeli meg, ezért bár kiválóan alkalmazható egy rendszer biztonságának javításához és fenntartásához, általános célú szkennerként a kutatásban nem volt alkalmazható [85].

A sebezhetőségi vizsgálatok első szakaszát a magyar felsőoktatási intézmények számára szolgáltatásként tervezett Nessus riportjainak alapján, 2021. május 21-én végeztem el. Az első mérésen túl 2022. február 1-jén egy második, megismételt adatgyűjtés is történt, melynek adatait kontrollként használtam fel. Tekintettel arra, hogy egy külső site-on működő mérőeszköz számára csak a határvédelmi rendszerek által engedélyezett forgalmi kapcsolatok hozzáférhetők, az abban szereplő adatok csak a publikus internet irányából érkező támadások elemzése során tekinthetők relevánsnak. A Nessus alkalmazásával adataim teljes szolgáltatási körrel rendelkező, korlátozás nélküli, frissítések rendszeres letöltésére képes szkennerből származtak.
A sérülékenységvizsgálatok legális elvégzése felveti a jogszerűség kérdését is. Szakmai körökben általánosan vitatott egy hálózat sérülékenységeinek illetékesség nélküli megállapítására irányuló adatgyűjtési eljárás legalitása, illetve törvényes keretek közt történő lefolytatása. Az eljárással szembeni fő kritikát a módszer rosszindulatú alkalmazási gyakorlata jelenti, mely során egy rendszer lehetséges behatolási pontjai meghatározhatók. Bár nemzetközi viszonylatban találhatók eltérések, a kutatásban alkalmazott mérés elvégzését a magyar jogszabályok nem tiltják. A Btk. szellemisége nem akadályozza meg a sérülékenységek tudományos célú gyűjtését, a tiltott adatszerzés megvalósulásának feltételeként a személyes adat, magántitok, vagy üzleti titok megszerzésére irányuló tevékenységeket, valamint a levéltitok megsértésének különféle formáit definiálja. Egy információs rendszer adatsértéséhez a rendszerekbe történő belépésnek, vagy adattartalmának megváltoztatásának (ideértve új adat bevitelét, módosítását vagy törlését), vagy az információs rendszer működését befolyásoló cselekmények kell megvalósulnia, melyek egy mérés során nem valósulnak meg. Gyakran említik korlátozó tényezőként a 2013. évi L. törvény 18. paragrafusát, mely a sérülékenységvizsgálat elvégzésére jogosult személyek és szervezetek körét és a velük szemben támasztott feltételeket határozza meg. A felsőoktatási

intézmények azonban nem tartoznak e törvény hatálya alá. A mérés során nem történik személyes adat kezelése sem, így sem a GDPR, sem az Infotv. nem korlátozza annak elvégzését.

Az esettanulmányban vizsgált egyetem több telephellyel rendelkezik, ezekben eltérő méretű informatikai eszközpark található. A legnagyobb informatikai bázis a „C" campus, ebben két nagy szerverteremben száz feletti fizikai és virtuális kiszolgáló működik, emellett itt üzemel a legnagyobb informatikai hálózat is. A vizsgált egyetem működését biztosító fő infrastruktúrán található az intézmény adatvagyonának jelentős része. Kutatásomban a központi informatikai helyszín a „C" campuson található. A „J" és „S" campusok nagyobb földrajzi távolságban, más régióban helyezkednek el, és kizárólag a saját működésükhöz szükséges informatikai infrastruktúrával rendelkeznek, a központi rendszert WAN összeköttetésen keresztül érik el. Ezeken a helyszíneken egy-egy informatikus látja el helyi támogatási feladatokat, feladatkörük a munkaállomások és munkatársak informatikai támogatása. A „J" és „S" campusok szerepe kiszolgáló informatikai infrastruktúra területén perifériális.

A Nessus riportjai előre meghatározott IP tartományok elemeinek egyszeri vizsgálata alapján készültek, mely során a szkenner cím szerint listázta a vizsgált hostokat. A szoftver elvégezte a megtalált sérülékenységek Critical, High, Medium, Low és Info osztályokba történő besorolását, és minden egyedi címre megadta ezek számát és egyéb jellemzőit. A riport részletesen közölte a nem Info osztályú sérülékenységek CVSS 2.0-s pontszámait is, melyek alapján további vizsgálatok végezhetők (az Info osztályba tartozó elemel nem rendelkeznek ilyen pontértékkel).



1	4	10	0	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
CRITICAL	10.0	56997	VMware ESX / ESXi Unsupported Version Detection
HIGH	7.2	118885	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)
HIGH	7.2	123518	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)
HIGH	7.2	118466	ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.8	88906	ESXi 5.5 < Build 3568722 / 6.0 < Build 3568940 glibc DNS Resolver RCE (VMSA-2016-0002) (remote check)

4. ábra. A Nessus riportjának egy részlete. Forrás: saját szerkesztés.

A Nessus riportjai html formátumúak, így a leíró statisztikai adatok kinyeréséhez rövid shell scripteket készítettem, melyekkel a html forrásból kigyűjtöttem a kutatás szempontjából releváns adatokat. Ezeket strukturáltam, majd egy MySQL adatbázisba töltöttem. Az így kapott 5.976 rekord különböző összefüggéseit alkalmas SQL lekérdezések megírásával állapítottam meg.

Mivel a Nessusból származó riportok CVSS 2.0 és 3.0-s besorolást is tartalmaznak, ezért a két pontozási eljárás különbözőségeinek megállapítására megvizsgáltam ezek eltéréseit. 458 rekordban áll rendelkezésre mindkét pontszám, és nem szerepelt olyan, amelyben csak az egyik érték lett volna ismert.

Mivel a kutatásom későbbi fázisában méréseimet a Nexpose-ra alapozva folytattam, mely a sebezhetőségek besorolására csak egy hármas osztályt tartalmaz (Critical, Severe, Low), a mért eredmények összehasonlíthatóságának érdekében létre kellett hoznom az egységes besorolási szempontok tábláit és kapcsolódásukat biztosító kulcsait. Ennek eléréséhez a Nexpose saját értékeinek helyettesítésére előállítottam egy másodlagos skálát, melyben pontosan alkalmaztam a First által ajánlott értékhatárokat [68]. A besorolás kiszámításakor a CVSS 3.0 értékeket használtam fel, a CVSS 2.0 alkalmazását a továbbiakban ezzel elvetettem. A CVSS 2.0 és 3.0 közti pontértékek eltérése ellenére a súlyosság besorolása az eredetitől csupán két olyan típus esetén mutatott különbséget, melyek a vizsgált környezetben előfordultak:

- a 15 esetben megtalált *„SSL Version 2 and 3 Protocol Detection”* eredeti besorolása a CVSS pontérték 9,8-as értéke mellett csak High, melyet a Critical-ra módosítottam annak ellenére, hogy a NIST 2030-ig ad időt a kivezetésére [86].
- A „HP iLO 3 < 1.93 / HP iLO 4 < 2.75 / HP iLO Superdome 4 < 1.64 / HP iLO 5 < 2.18 / HP Moonshot/Edgeline iLO 5 < 2.30 Ripple20 Multiple vulnerabilities” a 10-es CVSS pontérték ellenére eredetileg szintén csak High minősítésű, amit szintén Critical-ra módosítottam. Tekintettel a sérülékenység jellegére, és a First ajánlásában szereplő kitételre, mely szerint „egy sebezhetőség értékelésekor a rendszer egyéb környezeti körülményeit nem szabad figyelembe venni”, az eredeti besorolást tartom helytelennek. A Hewlett Packard szervereibe épített iLO (Integrated Lights-Out) távoli menedzsmentet és monitorozást biztosít, melynek segítségével a kiszolgáló távolról is elérhető és menedzselhető. Sérülékenysége akár egy virtuális gépeket futtató kiszolgáló teljes kontrolljának elvesztésével is járhat.

Az alábbi táblázat a campusokra és a módosított besorolás szerinti osztályokra bontva tartalmazza a sérülékenységek számát, valamint a CVSS 3.0 pontszámait:

Besorolás	Campus „C” (102 host)		Campus „C” #2 (138 host)		Campus „S” (7 host)		Campus „J” (13 host)	
	pontszám	darab	pontszám	darab	pontszám	darab	pontszám	darab
Critical	210	21	230	23	0	0	59,3	23
High	118,8	16	155,7	21	0	0	29,4	21
Medium	875,2	163	1249,5	231	0	0	110,7	231
Low	83,2	32	148,2	57	0	0	0	57
Info	0	2327	0	2819	0	63	0	2819

13. táblázat. A publikus sérülékenységek összesített pontszáma és az azonosított hostok száma campusonként. Forrás: saját szerkesztés.

A tesztelést végző rendszer az első mérés során a központi campuson a 102 interfészt ért el, melyben a riport összesen 21 kritikus minősítésű sérülékenységet mutatott ki. Ezek túlnyomó részt valóban kritikus hibák voltak, főként lejárt támogatású operációs rendszerekre, a virtualizációs rendszerek kritikus támadhatóságára, és a már említett iLO hozzáféréssel kapcsolatos hibákra mutattak rá. A „C” Campus nyolc hónappal későbbi megismételt jelentésében az elérhető gépek száma közel 30%-kal nőtt, ennek megfelelően a hibák száma is minden kategóriában emelkedett: kettővel a magas kockázatú hibák mennyisége, mely mellett a magas, közepes és alacsony kockázatúakon túl a mérés 21%-kal több info besorolású hibát mutatott ki. Ebből azonban nem következik a sérülékenységi szint általános növekedése: a pontszámok és darabszámok hányadosával képzett arány a két campus esetében elhanyagolható eltérést mutat. H2. bizonyításában „C” campus esetében az első adatsort vettem alapul, mivel a további campusokra a későbbi, kontrollként alkalmazni kívánt mérés elvégzésére már nem volt lehetőségem: „S” campus későbbi, belső vizsgálatára a felsőoktatási intézmények átszervezése következtében már nem volt lehetőségem. Tekintettel arra, hogy a „C” campus 8 hónappal később, kontrollként indított második mérése nem mutatott releváns különbséget, ez feltételezhetően a sokkal kisebb és kevésbé változó perifériális campusok esetében sem történt volna másképp.

Az egyes sérülékenységi csoportok elemzése során először a rendelkezésre álló CVSS 3.0-s mérőszámok összehasonlítását végeztem el. Ebben természetes a központi informatikára eső magasabb pontszám, hiszen az itt működő kiszolgálók száma lényegesen nagyobb. Ezért a campusok összevetését nem csak a gépek száma, hanem a CVSS pontszámok szerinti arányosításban is elvégeztem. Az alábbi táblázatban az adott campus esetén az egy gépre jutó pontszámot S/I-vel, a súlyossági pontértékének és az abban érintett gépek számának hányadosát pedig R-rel jelöltem.

Besorolás	Campus „C” (102 host)		Campus „C” #2 (138 host)		Campus „S” (7 host)		Campus „J” (13 host)	
	S/I	R	S/I	R	S/I	R	S/I	R
Critical	2,1	10,0	1,7	10,0	0,0	0,0	4,6	9,9
High	1,2	7,4	1,1	7,4	0,0	0,0	2,3	7,4
Medium	8,6	5,4	9,1	5,4	0,0	0,0	8,5	5,5
Low	0,8	2,6	1,1	2,6	0,0	0,0	0,0	0,0
Info	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0

14. táblázat. S/I és R értéke campus és a sérülékenységek súlyossági értékének bontásában. Forrás: saját szerkesztés.

Mivel „S” campuson az internet irányából elérhető interfészek száma minimális volt, és azon a helyszínen csak elenyésző számban működtek publikus szolgáltatások, így arra vonatkozó megállapítás kellő mennyiségű adat hiányában nem adható.

Az R értékét vizsgálva tehát nem mutatható ki releváns különbség az egyes campusok sérülékenységei közt. A kritikus besorolású sérülékenységek értéke a „J” és a „C” campus esetében is megközelítőleg 10. A további osztályok esetében a „J” és „C” campusokon mért sérülékenységek R értékeinek összehasonlítása során megállapítható, hogy különbségük az Low osztály elemeinek kivételével nem haladja meg a 0,2-t, mely a gyakorlatban azt jelenti, hogy jellegükben ugyanazok a sérülékenységek fordulnak elő mindkét campuson, arányuk megközelítőleg azonos.

Ez alapján nem igazolható, hogy a magyarországi felsőoktatási intézmények perifériális informatikai rendszerei kisebb számú, az internet irányából elérhető sérülékenységet tartalmaznak. A H2. hipotézis megcáfolásával a további intézményi vizsgálatok elvégzése szükségtelen.

4.12. Sérülékenységek jellegének és korának vizsgálata

A kutatás első fázisában a sérülékenységek vizsgálata külső forrásból végzett adatgyűjtés alapján történt, mely során csak azok a szolgáltatási/sebezhetőségi pontok voltak mérhetők, melyek hozzáférését a határvédelmi rendszerek lehetővé tették. Mivel a Verizon jelentésében 25%-ra teszi az oktatási intézmények belső támadóinak arányát [37], a hatékony védelem szempontjából lényeges szempont a rendszer belső kitettségének vizsgálata is, hiszen annak elemeit nem csak a külső, hanem a belső támadókkal szemben is védeni kell. Egy ilyen típusú mérés lebonyolítása egy már működő infrastruktúra esetén bonyolult műszaki problémát jelent, mivel biztosítani kell a szkenner hozzáférést a hálózat minden vizsgálandó eleméhez, melynek során az

eszközök kommunikációját nem akadályozhatják tűzfalak vagy virtuális hálózat (VLAN) szeparációk.

A H3. hipotézis igazolását megalapozó esettanulmány során a külső mérés adatait a belső hálózatban lefolytatott méréssel is összevetettem, melynek másodlagos célja a részletesebb kép kialakítása az egyes szakterületek állapotáról és a nagy számú, hálózatba kötött számítástechnikai eszközről. A szakterületi felbontás csoportjainak kialakításához a publikus internet irányába nyitott rendszerelemek szétválasztása mellett a belső, szegmentált hálózatok elemeit is önálló elemként kezeltem. A H2. bizonyításához alkalmazott mérési eszközrendszer ebben az esetben csak akkor lett volna alkalmazható, ha a határvédelmi eszközök konfigurációinak módosításával az első fázisban alkalmazott szkenner számára lehetőséget nyílik a belső hálózati elemekkel történő kommunikációra. Az elérésükhöz szükséges útvonalak kialakítása követelménye az egyetemi tűzfalak konfigurációinak jelentős módosítása, mely a gyakorlatban szinte biztosan hálózati üzemzavarokat okozott volna. A mérés során sem ezt, sem egy harmadik fél számára egy esetleges hozzáférést biztosító, az intézmény belső hálózati sérülékenységeinek detektálására képes eszköz elhelyezésének kockázatát nem kívántam felvállalni. Ezért a mérések folytatását egy új, a belső tűzfalrendszer mögött már létező alkalmas pontra telepített új szkenner gépre alapoztam. Tekintettel arra, hogy az első mérésben alkalmazott Nessus beszerzésére nem állt rendelkezésemre a megfelelő anyagi háttér, ezen egy hasonló funkcionalitású Nexpose futott. A szkenner felügyelete teljes egészében az intézmény saját kezelésében volt, megfelelt a vizsgálat kritériumainak, és a már említett korlátozásokat tartalmazó szkenner szoftver futtatásával a sérülékenységek vizsgálata a határvédelmi eszközök védelmi funkcióinak módosítása nélkül volt elvégezhető.

A belső hálózatot további bontásban vizsgáltam, melynek alapját az intézmény hálózatának VLAN felosztása nyújtotta. Mivel ez a hasonló területek esetében is több csoportot alkotott (pl. különböző tanszékek, a gazdasági hivatal egyéb szervezeti egységei) az eredetileg 55 különböző VLAN által meghatározott területet azok szerepköre alapján csoportosítottam, és kiválasztottam azokat, amelyeket a továbbiakban részletesen vizsgálni kívántam. Emellett azonosítottam azokat a területeket, amelyekhez nem áll rendelkezésre elegendő adat, vagy kutatásom jelen fázisában szerepük nem volt releváns. Az eredeti VLAN-okhoz a felosztás alapján szakterületeket rendeltem, melyeket a Nexpose adatbázisának bővítésével, a lekérdezések végrehajtásának érdekében a rendszerben tároltam. Az infrastrukturális elemeket ezzel hét csoportba soroltam:

1. Akadémiai szféra *(academy)*. Ebbe a csoportba tartoznak az oktatási egységek általános

célú számítógépei, az oktatásban alkalmazott, hálózatra kapcsolt laborberendezések, valamint az oktatók munkaállomásai, laptopjai. Műszaki szétválaszthatóság hiányában ide soroltam be az oktatók és hallgatók kezelésében levő, de nem a kutatásokra dedikált számítógépeket, melyek közt földrajz és kémiai kutatások szerverei is szerepeltek. Speciális felhasználási területet jelentenek a tanszéki adminisztrátorok munkaállomásai, melyek besorolása nem végezhető el egyértelműen: ezeken a helyi feladatok ellátása mellett a menedzsment kliensprogramjai, illetve a menedzsment szolgáltatásainak hozzáférései is megtalálhatók. Ugyanebbe a csoportba soroltam be az egyetemi könyvtár nyilvános számítógépeit, és minden más olyan informatikai berendezést, mely az egyetemi polgárok számára nyújtanak szolgáltatásokat.

2. Az informatikai hálózat és szolgáltatás eszközeinek csoportjába *(IT)* azok a berendezések tartoznak, amelyek az informatikai alap infrastruktúrát nyújtják, beleértve a központi hálózati eszközöket (határvédelmi eszközök, routerek, switchek, VPN végpontok, WiFi berendezések), azok menedzsment eszközei, emellett minden olyan szerver számítógép, amely az informatikai üzemeltetés hatókörébe tartozik, továbbá azok az egyéb informatikai berendezések, munkaállomások, mobil eszközök, kamerarendszerek, melyek az alap infrastruktúra IP tartományában kaptak helyet – például a rendszergazdák és rendszermérnökök munkaállomásai.
3. A Menedzsment *(management)* csoportba a gazdasági szervezeti egységek, valamint az egyetem vezetésének hálózati eszközeit soroltam be, melyek fő részterületei az egyetem felsővezetői körének kiszolgálása mellett a jogi-, gazdálkodási-, projekt-, anyaggazdálkodási-, beszerzési-, műszaki igazgatási-, bér- és HR egységei. Ugyanebben a csoportban kaptak helyet a tanulmányi ügyekért felelős szervezeti egységek, valamint az egyetem kiadója is.
4. A publikus internet *(pubnet)* számítógépei és informatikai infrastruktúrája az eltérő címosztályok alkalmazása következtében jól megkülönböztethetők, és mivel ezen berendezéseknek az internet irányból történő láthatósági vizsgálata a határvédelmi eszközök kontrollja mellett bárki számára megismételhető, egy önálló mérési osztályba soroltam őket. Az eredmények értékelésekor figyelembe vettem, hogy a csoport sebezhetőségeinek felderítésekor a mérést végző szoftvert esetemben (ellentétben egy internet irányból érkező támadással) nem korlátozták az említett határvédelmi berendezések. Ezt a tényezőt azonban a CVSS értékelési szabályrendszere alapján figyelmen kívül hagytam, arra az értékelési eljárás során megfogalmazott követelményre való tekintettel, hogy a sérülékenységek besorolása során az annak kihasználására szolgáló környezetet kedvező

konfigurációjúnak kell tekinteni.

5. Kutatási terület *(research)*. Ennek tagjai azok szervezeti egységek, amelyek elsődleges feladata a tudományos kutatás, és az ott keletkezett eredmények mellett a kutató egységek által előállított adatok tárolása és közzététele. Ez a terület más magyar tudományegyetemekkel összevetve a vizsgált adatkörben kifejezetten alacsony számú elemet tartalmaz.
6. Kollégiumok *(dormitory)* csoportba a kollégiumi hálózatok elemeit soroltam be. Ezen a téren meglehetősen kevés mérési adat áll rendelkezésre, mivel a vizsgált hálózatban nem állnak rendelkezésre olyan eszközök, amellyel a kollégiumok hálózati átjárója mögötti infrastruktúra elemei megkülönböztethetők lettek volna. Tekintettel arra, hogy a kollégiumok munkaállomásai nem egyetemi tulajdonúak és azok konfigurációira az egyetemi IT üzemeltetésnek minimális hatása van, ezen hálózatok elemeire semmilyen bizalmi szabályt nem érvényesítettünk, azokat közel nyilvános gépekként kezeltük. Mivel a vizsgált egyetem számára nem állt rendelkezésre olyan hálózati infrastruktúra, mellyel a kollégiumok gépei is vizsgálhatók lettek volna, így azok szerepe a kutatás során inkább csak formális.
7. A külső szervezeti egységek csoportjába *(external)* azok a berendezések és hálózatok tartoznak, melyek az egyetem regionális központi feladatkörének ellátása okán kapcsolódnak az egyetem hálózatához, ezért az azokban fellelhető sérülékenységek nincsenek közvetlen hatással az intézmény saját infrastruktúrájára. Ennek a csoportnak az elemei azok az iskolák, és egyéb intézmények, melyek internetkapcsolata az egyetemen keresztül került kialakításra, továbbá ebbe tartoznak a fenntartó, az oktatási feladathoz csak részlegesen köthető egyéb hálózatai. Ugyanebbe a csoportba tartoznak azok a külső tulajdonú eszközök, melyek idegen tulajdonúak, és üzemeltetésüket nem az egyetem végzi (pl. a különféle hálózati kommunikációt igénylő reklámtáblák).

Az alkalmazott területi bontás az általam ismert magyar felsőoktatási intézményekre változtatás nélkül alkalmazható, speciális képzési profilú intézményekben pedig szükség esetén akár több önálló területtel is bővíthetők[42].

H3. bizonyításához a Nexpose egy hónapon át működő változatát használtam fel, mely egy időben 500 számítógépben limitálta a számítógépek számát. Ennél hozzávetőleg másfélszer több interfész vizsgálatára nyílt lehetőség, mivel az egyes hálózatok gépeit eltérő időpontokban

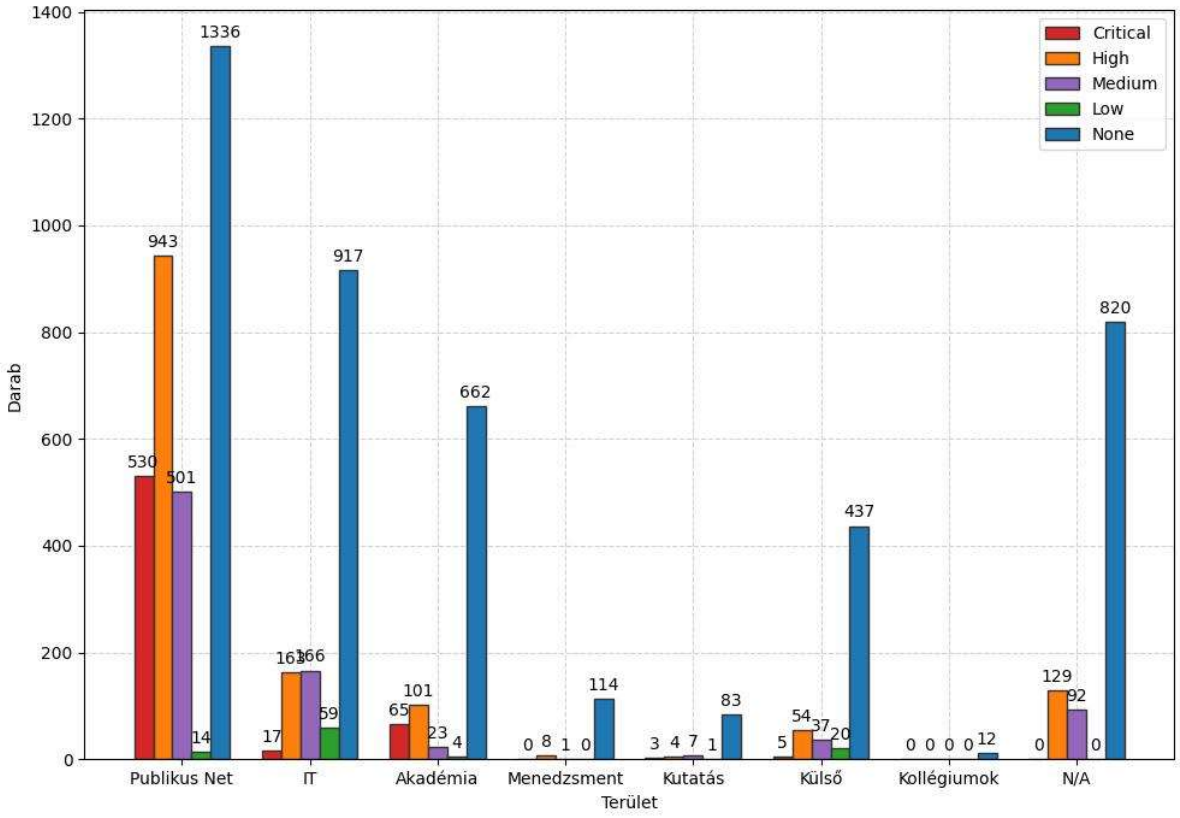
[42] Ilyenek lehetnek az orvosi egyetemek kórházi ellátással összefüggő informatikai infrastruktúráinak azon elemei, melyek az egyetem üzemeltetésébe, vagy felelősségi körébe tartoznak.

tartották bekapcsolva, így az említett korlát a számítógépek más-más halmazára érvényesült. Munkaidőben a dolgozók munkaállomásai voltak nagyobb számban szkennelhetők, míg azon kívül a kiszolgáló, illetve más 7/24 működésű berendezések voltak vizsgálhatók. A szoftver periodikus ellenőrzési beállításain keresztül ezek a vizsgálatok ennek a körülménynek megfelelően optimalizálhatók voltak.

A Nexpose két különböző adatbázisban is képes rögzíteni a mért adatait. Egy viszonylag egyszerű felépítésű MySQL adatbázist alkalmaz az áttekintő adatok tárolására, és egy PostgreSQL alatt működő data warehouse-ban tárolja részletes működési adatait. Kutatási eredményeimet ez utóbbi nagyobb mennyiségű és sokkal részletesebb adathalmaz feldolgozásával kaptam.

Elsőként az egyes területeken mért sérülékenységek számát elemeztem, és megállapítottam, hogy míg az internet irányából 102 gépen 2.559 sérülékenység volt azonosítható, a belső hálózatban 745 hoston 38,2%-kal több, 7.382 került azonosításra. Bár a két szoftver eltérő adatbázissal rendelkezik, egyértelmű, hogy a határvédelmi eszközök védelmi funkciói számos, a publikus internet irányából érkező sérülékenység felderítését (és kihasználhatóságát) akadályozták meg. Míg az internet irányából 21 kritikus sérülékenység volt kimutatható, a belső hálózatból 530-at azonosítottam, mely 623,8%-kal magasabb értéket jelent.

A további osztályokba tartozó sérülékenységek hasonlóan nagy eltérést mutatnak. A magas kockázatú sérülékenységek száma 16-ról 943-ra, a közepes besorolásúak 163-ról 501-re emelkedett. Az alacsony kockázatú sebezhetőségek számát viszont csak kis mértékben mértem alacsonyabbnak, melynek lehetséges oka a belső és külső mérés közt eltelt idő is lehetett. A legmagasabb számban előforduló Info típusú sérülékenységek (melyet a Nessus None-ként azonosít) száma viszont 2.327-ról 1.336-ra csökkent.



5. ábra. A sebezhetőségek száma és súlyossága szakterületi felosztásban.
Forrás: saját szerkesztés

A diagram alapján a H3. alapjául szolgáló esettanulmány igazoltnak tekinthető. Az Info/None besorolású rekordok nem rendelkeznek sem CVSS 3.0 pontszámmal (értékük az adatbázisban NULL volt), sem pedig CVE azonosítóval. **Ezek tehát nem CVE szerinti sebezhetőségek, hanem olyan beállítási hibák**, amelyek önmagukban ugyan nem jelentenek sérülékenységet, de egy potenciális támadót közvetett úton segítenek egy alkalmas stratégia kidolgozásában. Az ilyen típusú információforrások a szisztematikus és automatizált felderítést végző alkalmazások számára is értéket jelentenek, mert ezeket kihasználva képesek felfedni a kívánt verziójú szoftver jelenlétét vagy az azokat futtató kiszolgálókat, munkaállomásokat, vagy épp felderíteni az általuk alkalmazott vagy elfogadott titkosítási protokollokat. Az ilyen típusú hibákat az egyértelműség kedvéért a továbbiakban *konfigurációs hibának* nevezem. Ezek a vizsgált rendszerben nagy számban fordulnak elő, elsősorban emiatt jelentenek kockázatot.

A belső és külső mérések konfigurációs hibáinak mennyiségét és arányát az alábbi táblázat tartalmazza. Ebben a Kh/n oszlopban az egy számítógépre jutó hibák számát tüntettem fel, mely az adott campusban felderített konfigurációs hibák és hostok számának hányadosa (azaz az egy gépre jutó hibák száma).

	Hostok száma	Rekordok száma	Info típus darabszáma	Info típus aránya	Kh/n
„C” campus a publikus internet felől	102	2559	2327	0,91	22,81
„C” campus belső hálózatból	745	7382	4381	0,59	5,88
„J” Campus a publikus internet felől	13	203	171	0,84	12,15
„S” Campus a publikus internet felől	7	63	63	1,00	9

15. táblázat. Konfigurációs hibák mennyisége és aránya az egyes campusokon. Forrás: saját szerkesztés.

A mért adatok alapján megállapítható, hogy az internet irányából mért konfigurációs hibák aránya a „J” campus esetben a legalacsonyabb, 84%, a „C” campuson 91%, az „S” campus esetében pedig 100%. A konfigurációs hibák száma a rendszer elemeinek számával növekedett, és ezek jelentős részét a helyesen konfigurált határvédelmi eszközök a publikus internet irányából eltakarták. A konfigurációs hibák mennyisége nagy számú szolgáltatás esetén meghaladja a kisebb központok, tipikusan a perifériális campusokban mért értéket. Figyelemre méltó tény, hogy az Internet felé összesen 7 interfészen nyújtott Campus „S” szolgáltatási köre is 63 konfigurációs hibát tartalmazott úgy, hogy abban egyetlen CVSS pontozású sérülékenység sem volt kimutatható.

A fenti táblázat alapján tehát **egy felsőoktatási intézmény esetében bizonyítottam, hogy sérülékenységeiről jelentős mennyiségű technikai információ gyűjthető össze, melyek túlnyomórészt hibás konfigurációs beállítások eredményei.**

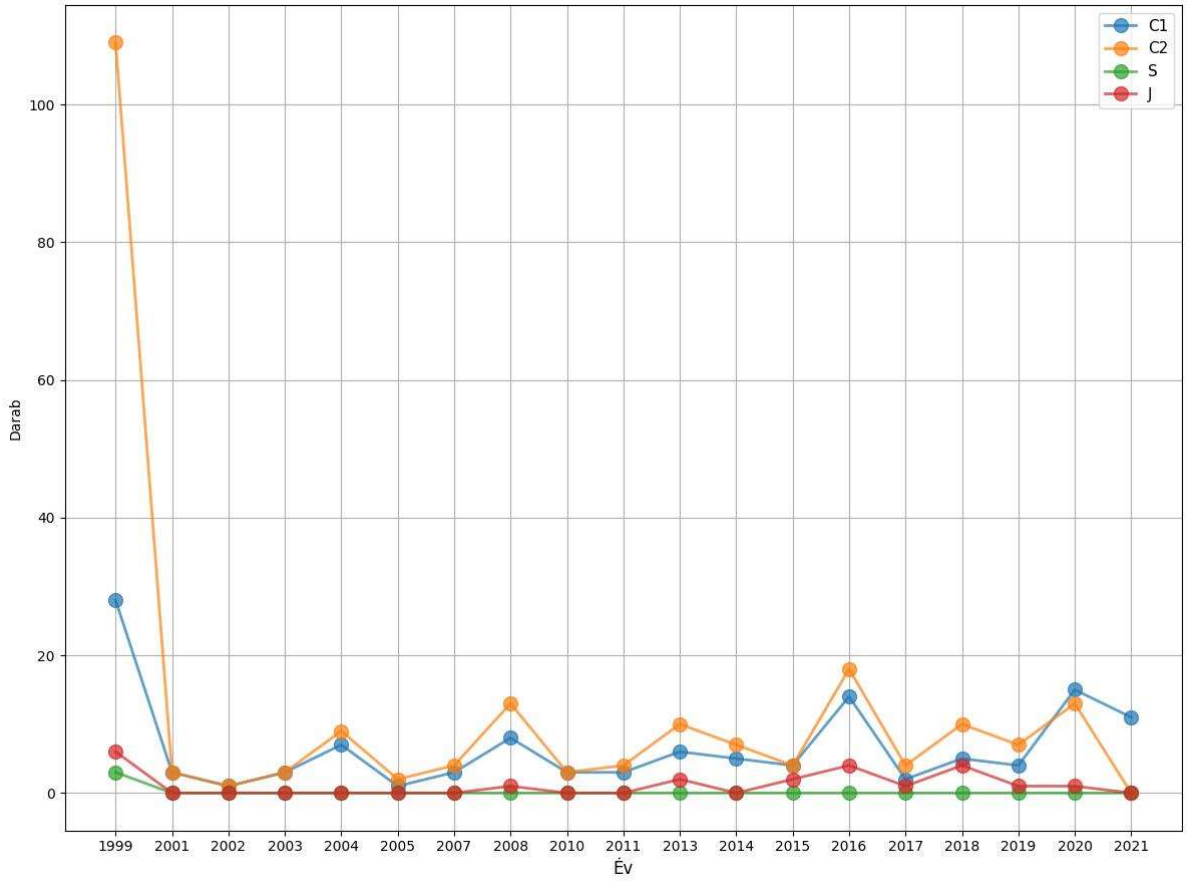
Az esettanulmányra vonatkozóan ugyanezen adathalmaz alapján vizsgálható meg H3. hipotézis sérülékenységek korára vonatkozó részállítása. Az egyes sérülékenységek ismertté válásának évszáma több módon is meghatározható, a legegyszerűbb megoldás a CVE adatbázis nevezéktanának alkalmazása volt. Tekintettel arra, hogy a sérülékenységek azonosítóinak kötelező eleme a regisztráció éve, így a már ismertté vált sérülékenységek kora egyszerűen kinyerhető. A konfigurációs hibák csak minimális számban rendelkeznek CVE azonosítóval, annak hiányában nem köthetők évszámhoz. H3. hipotézis korra vonatkozó állításának igazolásakor így kizárólag azokat használtam fel, melyek tartalmaztak évszámra vonatkozó információt.

Az alábbi táblázatban kor szerinti bontásban összesítettem az azonosított sérülékenységek számát. Bár H3. hipotézis igazolásában a belső hálózatból indított mérési eredmények nem vesznek részt, kutatásom jelentős melléktermé ke az ebből a forrásból azonosított sérülékenységek magas száma és kora.

Év	Mérés		
	Belső hálózatból	Belső hálózatból Info típus nélkül	Publikus internetről Info nélkül
1970	6	0	0
1990	29	0	0
1995	289	0	0
1996	80	0	0
1997	713	0	0
1999	33	0	146
2000	13	0	0
2001	0	0	6
2002	117	0	2
2003	7	0	6
2004	192	0	16
2005	151	0	3
2006	25	0	0
2007	225	11	7
2008	74	0	22
2009	280	0	0
2010	166	0	6
2011	307	0	7
2012	78	0	0
2013	213	42	18
2014	962	77	12
2015	577	84	10
2016	565	565	36
2017	384	331	7
2018	367	367	19
2019	485	485	12
2020	192	188	29
2021	835	835	11
2022	17	16	0
Összesen	**7382**	**3001**	**375**

16. táblázat. A publikus forrásból elérhető nem Info besorolású sérülékenységek kor szerinti eloszlása. Forrás: saját szerkesztés.

Az így redukált adathalmaz elemeit campusonként összesítve készítettem el az alábbi diagramot, mely az esettanulmányban szereplő egyetem internet irányából elérhető sérülékenységeit tartalmazza.



6. ábra. A publikus forrásból elérhető nem Info besorolású sérülékenységek kor szerinti eloszlása. Forrás: saját szerkesztés.

Ebben leolvasható, hogy a 2021-ben végzett mérés során feltárt adatok nagy számban tartalmaztak olyan, a publikus internet irányából elérhető sérülékenységet, melyek már 1999-ben már ismertek voltak, és néhánytól eltekintve minden évből maradt hátra olyan sérülékenység, melyet az üzemeltetők nem javítottak.

Az eredmények az 1999-es évhez rendelt sérülékenységek számának kivételével hozzávetőleg egyenletes eloszlást mutatnak, a kiinduló év kivételével nagy kiugrás nem figyelhető meg. Az 5.976 rekordból csak 375 rendelkezett CVE azonosítóval (6,2%), ami 55 különböző sérülékenységet írt le. A képet tovább árnyalja, hogy 130 esetben (34,6%) fordult elő az 1999-ben regisztrált *ICMP Timestamp Request Remote Date Disclosure* sérülékenység, mely – mivel elsődleges felhasználása adatgyűjtésre, és nem egy rendszer megsértésére irányul – alacsony kockázati besorolást kapott. Ez a sebezhetőség lehetővé teszi a támadó számára, hogy megismerje az állomáson lévő időt és dátumot, mely segítheti a támadót az időalapú hitelesítési eljárások megtévesztésében [87, p. 61]. A további sérülékenységek operációs rendszerekhez vagy szerverszoftverekhez kötődnek, de előfordulnak firmware sérülékenységek is (pl. *HP iLO Ripple20 Multiple vulnerabilities*). Egy másik, szintén 1999-re datált, 9 alkalommal előforduló beállítási

hiba az SNMP protokollhoz fűződik. Bár a CVE-1999-0517 azonosítójú, *SNMP Agent Default Community Name (public)* sebezhetőséget inkább konfigurációs hibaként azonosítottam, beállításával egy támadó képes lehet egy SNMP szerver által menedzselt eszközbe bejelentkezni, annak konfigurációjához hozzáférni, adott körülmények közt akár az abban tárolt adatokat módosítani is. A további, rendkívül régi hibák elavult webszervereket, titkosítási protokollokat vagy azok gyenge algoritmusait, különféle szerver szolgáltatások SSL hibáit írják le, de már ezekben az években ismert és később kiemelt támadási ponttá váló Remote Desktop (RDP) hibák is azonosíthatók voltak.

A kor szerinti eloszlás vizsgálatát a belső hálózatra is elvégeztem és megállapítottam, hogy az ott azonosított sérülékenységek kora az előzőtől lényegesen eltérő képet mutat. A Nexpose mérései 1970-ig nyúlnak vissza, ez minden bizonnyal csak technikai dátum. Az 1995-re datált találatok tanúsítványok 30 napon belüli lejártát jelzik, ennek jelzését ebben a rendszerben nem tartom indokoltnak. A további eredmények azonban számos konfigurációs hibára és kritikus sérülékenységekre mutattak rá, és felvetik a kérdést, hogy miképpen lehetséges, hogy ilyen régi sebezhetőségek kihasználása nem történt meg ennyi éven át.

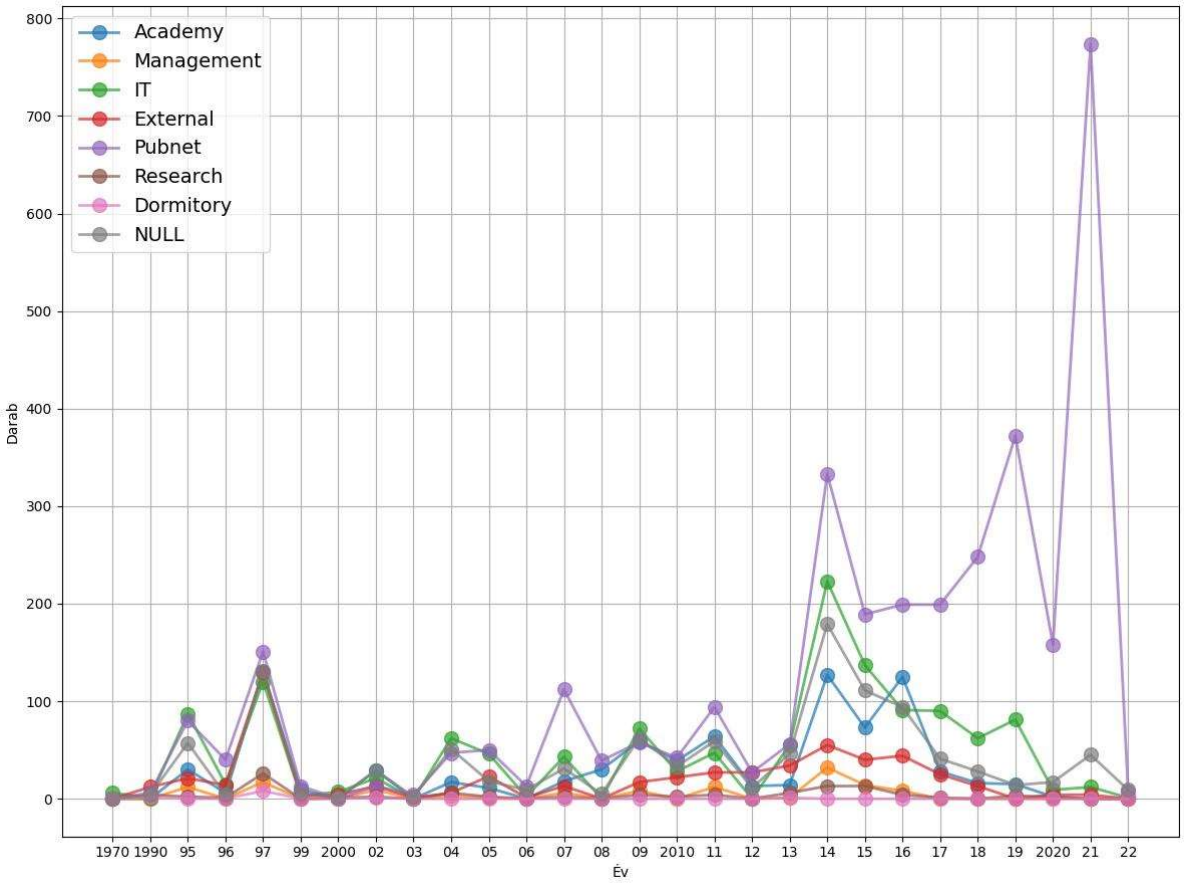
A diagramban több évben is határozott kiugrások figyelhetők meg, valamint egy lassabb lefutású csúcs is kirajzolódik 2013-ban. Ahhoz, hogy ezek megjelenése magyarázható legyen, valamint az egyes szervezeti egységek kitettségének azonosítása érdekében áttekintettem a kiugró szakaszokban fellehető sérülékenységeket:

- 1997: a már említett *„ICMP timestamp response" és „Default or Guessable SNMP community names: public"* megjelenése. Elsősorban a publikus internet gépei, az IT eszközei és a kutatók számítógépei és eszközei érintettek, melyből 335 valamilyen Linux variáns, 96 Canon nyomtató, és 40 feleletti a Cisco IOS operációs rendszer érintettsége.
- 2007: a kiugró értékeket több PHP és néhány DNS sebezhetőség megjelenése mellett számos *„X.509 Certificate Subject CN Does Not Match the Entity Name"* típusú hiba okozza, melyek szintén a publikus internet irányába nyitottak. Az érintett rendszerek többsége továbbra is Linux operációs rendszert futtató kiszolgálók (136), valamint a Canon nyomtatók (34).
- 2014: az informatikai csoport létszáma ebben az évben bővült, és a szerveroldali szolgáltatások száma jelentősen megnövekedett. Kialakításra került az egyetemi címtár, melyet számos más szolgáltatásba integráltunk. A hibák túlnyomó részét a „TLS Server Supports TLS version 1.0/1", valamint az SSH kapcsolatokban más, elavult protokollok

jelenléte jelentette, melyek javítására több, erős algoritmust dolgoztak ki [88]. Az érintettek ebben az esetben is a publikus internetszolgáltatások és az IT, valamint a szolgáltatásokat igénybe vevő akadémiai szféra berendezései, operációs rendszereik Linux (512), MS Windows (115), VMWare ESXi (85) és a már említett Canon nyomtatók (68) mellett a Cisco IOS (35) voltak.

- A 2020-as évet három, az Apache webszerverhez, az Exim MTA-hoz és a MySQL-hez kötődő hiba domainálta. Az érintettek ebben a szakaszban is az egyetem publikus internet elérésű gépei, melyek főként Linux rendszerű gépek voltak (182 sérülékenység).

A legmagasabb pontszámot elért gép egymaga 463 különböző sérülékenységet tartalmazott, melyből 123-hoz exploit is elérhető volt, melyet egy olyan NAS követett, amit az IT hatásköre és engedélye nélkül üzemeltettek egy tanszéken. Ez 130 kritikus, 224 közepes és 20 nem súlyos sérülékenységgel, valamint a feltöréséhez rendelkezésre álló 59 exploittal foglalta el a legsérülékenyebb informatikai eszközök listájának második helyét.



7. ábra. A belső hálózatban detektálható sérülékenységek kor szerinti eloszlása szakterületenkénti bontásban. Forrás: saját szerkesztés.

Az alábbi táblázat a „C1” campus mérésének összesítését a 2020-as évet megelőző és az azt követő bontásban tartalmazza, mely alapján H3. sérülékenységek korára vonatkozó állítása az esettanulmányban vizsgált egyetemre bizonyítható.

	Mérés					
	Belső, teljes	%	Belső, nem Info	%	Külső, nem Info	%
Egy évnél régebbi	6.338	83,5%	1.962	47,0%	335	88,1%
Egy évnél fiatalabb	1.044	16,5%	1.039	53,0%	40	11,9%
Összesen	7.382	100,0%	3.001	100,0%	375	100,0%

17. táblázat. Az egyes sérülékenységek száma 2020 előtt és után. Forrás: saját szerkesztés.

A 2021-ben végzett mérés idején a publikus internet irányából mért nem Info típusú sérülékenységek száma 375 volt. Ebből 11-et 2021-ben, 29-et 2020-ban regisztráltak. A fennmaradó 335 sérülékenység CVE azonosítója 2020 előtti regisztrációról tanúskodik, mely aránya 88,1%. Ugyanezt az értékelést a belső hálózatból indított mérési adatokra is elvégeztem, itt a nem Info típusú sebezhetőségek száma 3.001 volt, melyből 1.039-et 2020-ban vagy korábban regisztráltak. A fennmaradó 1.962 sérülékenység 2020 előtt került be a CVE adatbázisába, eszerint a hibák 47%-a 2020 előtti. Az esettanulmányban szereplő egyetemi hálózat esetében tehát a publikus internet irányából jelentős számban voltak kimutathatók egy évnél régebben ismert sérülékenységek.
Amennyiben évszámként a szkenner adatbázisába való bekerülés évét tekintjük alapul, a teljes belső hálózaton végzett mérés adatain is igazolást nyer a hipotézis erre vonatkozó része: ekkor a 2020 előtti sérülékenységek és nyilvántartásba vett konfigurációs hibák aránya 83,5%, ami szintén jelentős.

Az esettanulmány eredményének általánosítása az indukció mellett a magyar egyetemek reprezentatív mintáján elvégzett azonos mérések elemzése útján végezhető el. Az indukció alkalmazhatósága mellett és ellen több érv és ellenérv hozható. Az egyetemek azonos feladatköre, a kötelezően alkalmazandó rendszerek, az azonos jogszabályi környezet és a közösen alkalmazható megoldások alapján feltételezhető, hogy H3. hipotézis a magyar felsőoktatás jelentős részére érvényes. A szabadon megválasztható eszközpark és szoftverek, az eltérő fenntartói kör és finanszírozás, a geolokációs eltérések viszont arra utalnak, hogy a szféra egyes intézményei közt is jelentős eltérések állhatnak fenn. Ezért H3. bizonyítását az egyetemek reprezentatív mintáján elvégzett további mérések alapján folytattam le, mely során technikai okokból az első

fejezetben meghatározott reprezentatív mintától kis mértékben eltértem. Az Eötvös Loránd Tudományegyetem és a Budapest Gazdasági és Műszaki Egyetem a lehetőségeimhez képest túl nagy hálózati címtartományt birtokol, mely vizsgálatához nem állt rendelkezésemre megfelelő technikai erőforrás. Ezért helyettük a Semmelweis Egyetemet vizsgáltam, mely oktatói- és hallgatói létszáma alapján a reprezentativitás nem sérül. A Metropolitan Egyetemhez rendelt hálózati címtartomány pedig külső szolgáltató kezelésében van, így annak szkennelésétől a lehetséges jogsértések elkerülése érdekében eltekintettem.

H3. hipotézis bizonyításához így az alábbi egyetemek esetében végeztem el az esettanulmányban alkalmazott módszer szerinti méréseket, mely során 14.912 sérülékenységet azonosítottam. Az alábbi táblázatban a vizsgált egyetemek neve és az IP tartományukban mért sérülékenységek súlyossági foka mellett feltüntettem azok összegét és az azonosított konfigurációs hibák százalékos arányát is.

Egyetem	Info	Low	Med	High	Crit	Összesen	Info%
A Tan Kapuja Buddhista Főiskola	2.734	46	229	19	13	3.041	89.9%
Dunaújvárosi Egyetem	730	10	68	6	10	824	88,6%
Eszterházy Károly Katolikus Egyetem	1.765	24	119	11	12	1.931	91.4%
Nemzeti Közszolgálati Egyetem	810	0	5	0	0	815	99,4%
Pázmány Péter Katolikus Egyetem	2.395	11	55	4	9	2.474	96,8%
Pécsi Tudományegyetem	3.669	40	529	80	42	4.460	84,2%
Semmelweis Egyetem	1.227	11	118	10	6	1.372	89,4%
Tokaj-Hegyalja Egyetem	92	0	1	1	1	95	96,8%
Összesen	13.422	142	1.124	131	93	14.912	
Arány	90,0%	1,0%	7,5%	0,9%	0,6%		

18. táblázat. Magyar egyetemek informatikai rendszereinek publikus forrásból azonosítható sérülékenységeinek száma és aránya. Forrás: saját szerkesztés.

A táblázatból leolvasható, hogy a konfigurációs hibák minimális aránya a JPTE-n volt mérhető, melynek értéke 84,2% volt. Összességében a vizsgált egyetemek rendszereiben mért Info típusú hibák átlagos mértéke ennél magasabb, 92,1%, és csak két esetben nem érte el a 90%-os értéket. Ez az arány megközelítőleg azonos az esettanulmányban mérttel, ezért H3. hipotézis részleges bizonyítása megtörtént.

A sérülékenységek korát az esettanulmányban alkalmazott módszer alkalmazásával, a fenti egyetemek rendszereiről gyűjtött adathalmazokra alkalmazva mutattam ki, melyet az alábbi táblázatban foglaltam össze.

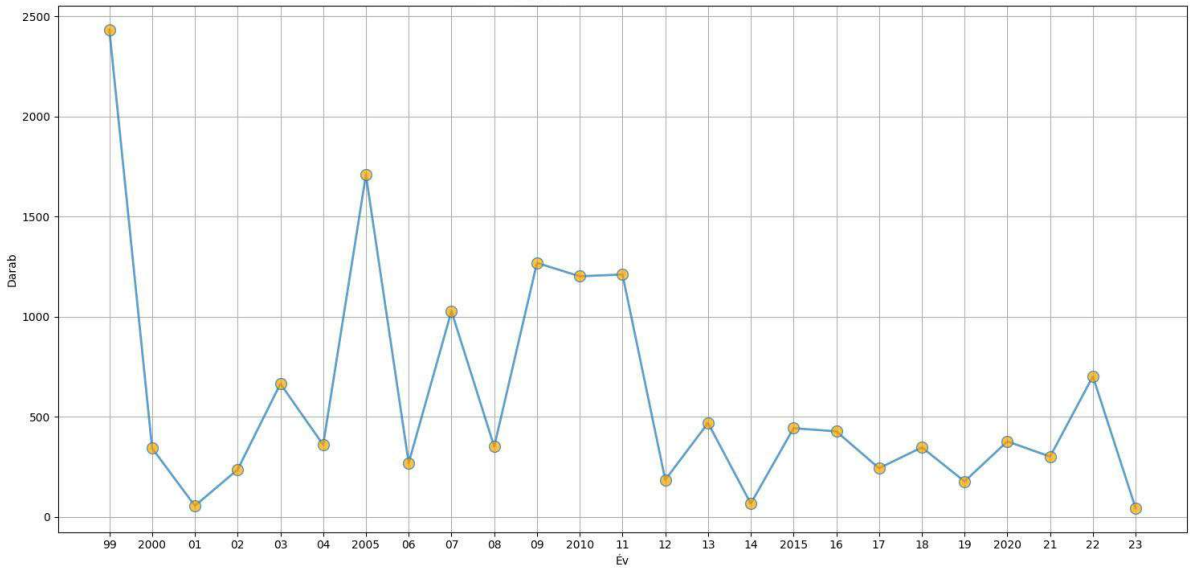
Egyetem	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010

A Tan Kapuja Buddhista Főiskola	393	48	24	54	190	49	164	61	199	89	333	271
Dunaújvárosi Egyetem	125	26	1	14	32	19	78	16	64	22	71	71
Eszterházy Károly Katolikus Egyetem	283	41	7	37	95	39	143	39	161	54	184	166
Nemzeti Közszolgálati Egyetem	143	31	0	2	39	28	139	18	58	19	79	56
Pázmány Péter Katolikus Egyetem	869	37	2	31	43	19	781	14	99	28	88	101
Pécsi Tudományegyetem	455	126	20	83	183	160	267	88	327	104	394	394
Semmelweis Egyetem	140	33	1	15	70	46	122	32	117	34	111	135
Tokaj-Hegyalja Egyetem	26	1	0	0	13	0	15	1	3	1	9	8
Összesen	2434	343	55	236	665	360	1709	269	1028	351	1269	1202
Százalék	16,3 %	2,3%	0,4%	1,6%	4,5%	2,4%	11,5 %	1,8%	6,9%	2,4%	8,5%	8,1%

Egyetem	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
A Tan Kapuja Buddhista Főiskola	324	53	103	19	94	107	54	79	41	89	60	139	4
Dunaújvárosi Egyetem	64	4	36	3	26	21	17	20	12	16	19	43	4
Eszterházy Károly Katolikus Egyetem	176	13	82	2	50	46	31	67	28	43	56	87	1
Nemzeti Közszolgálati Egyetem	81	8	5	0	16	35	1	6	0	18	0	33	0
Pázmány Péter Katolikus Egyetem	70	5	49	1	23	38	8	55	10	22	47	34	0
Pécsi Tudományegyetem	357	84	148	39	182	125	122	84	73	142	84	291	28
Semmelweis Egyetem	131	18	44	2	50	53	10	36	13	46	35	74	4
Tokaj-Hegyalja Egyetem	8	0	2	0	2	2	0	0	0	1	0	1	2
Összesen	1211	185	469	66	443	427	243	347	177	377	301	702	43
Százalék	8,1%	1,2%	3,1%	0,4%	3,0%	2,9%	1,6%	2,3%	1,2%	2,5%	2,0%	4,7%	0,3%

19. táblázat. Magyar egyetemek informatikai rendszereinek publikus forrásból azonosítható sérülékenységeinek száma kor szerinti eloszlásban. Forrás: saját szerkesztés.

A táblázatból kiolvasható, hogy az egy évnél fiatalabb sérülékenységek aránya kevéssel 5% alatti, a sérülékenységek korának összesített értékeit az alábbi diagram ábrázolja. A korábbi évekhez tartozó értékek egyértelműen bizonyítják, hogy a vizsgált egyetemek esetében számos, egy évnél korábban ismert sérülékenység volt kimutatható.



8. ábra. Magyar egyetemek reprezentatív mintáján végzett publikus forrásból azonosítható sérülékenységek száma. Forrás: saját szerkesztés.

Ezzel igazoltam H3. hipotézist: a magyarországi felsőoktatási információs rendszerek sérülékenységeiről jelentős mennyiségű, egy évnél régebben ismert technikai információ gyűjthető össze, melyek túlnyomórészt hibás konfigurációs beállítások eredményei.

4.13. Összegzés

A fejezetben bemutattam a felsőoktatási rendszerek informatikai védelmi kérdéseinek irodalmi áttekintését, kitértem az egyetemi szféra informatikai működtetési feladatainak és környezetének különbözőségeire más szektorokéval szemben. Megmutattam, hogy az egyetemi informatikai rendszereket érik támadások, és összegyűjtöttem legjellemzőbb motivációit. Sorra vettem az IT biztonság elemzésének elterjedt módszereit, és sérülékenységvizsgálaton alapuló részletes vizsgálat megvalósítását, és eredményeinek elemzését tűztem ki célul.

Az informatikai rendszerek sebezhetőségeinek leírására képes metrika alkalmazása jelentős támogatást nyújt az informatikai üzemeltetés szereplői számára. Az alkalmazott módszertan szerinti szoftveres háttértámogatással a sérülékenységek azonosíthatók, és különféle stratégiák mentén azok kártékony hatásainak elkerülésére hozott lépések időben elvégezhetők. A mérések rendszeres elvégzésével a rendszermérnökök feladatai pontosan meghatározhatók, így az ad-hoc döntéseket egy tervezett és ellenőrzött munkafolyamat válthatja fel. A rendszeres mérések

az egyes szervezetek IBF-jei számára is biztosítják az IT rendszer gyenge pontjainak azonosítását és a megfelelő stratégia alkalmazása mellett azok megerősítését anélkül, hogy a részletes műszaki tartalmukat mélységében kellene ismerniük.

Az ezt támogató rendszerelemek közül bemutattam az esettanulmányban résztvevő egyetem mérési eredményeit, hasznosíthatósági korlátait és tapasztalatait, majd H2. és H3. igazolásához szükséges technikai hátteret: a CVE és kapcsolódó adatbázisait, valamint az informatikai rendszerek sérülékenységeinek mérésére szolgáló de facto szabványt, a CVSS metrikát, annak fogalmait, az értékelés módját és kapcsolódó területeit. Kitértem a CVSS kritikájára és lehetséges továbbfejlesztési módszereire.

A fejezet második részében egy magyar egyetem sérülékenységvizsgálatának esettanulmányát követően annak eredményeiből levonható további következtetéseket tártam fel. Bemutattam a sérülékenységek mérésének két gyakorlati alkalmazását, azt ezt végző szoftverek néhány típusát. Az eredmények egy részének értékeléséhez saját adatbázist építettem, melyet más forrásból származó adatokkal egészítettem ki a mérést végző szoftver funkcionalitásának bővítése érdekében. A mérés első fázisában ismertettem néhány helyi kirívó, negatív példát, majd a mért adatok elemzésével kimutattam, hogy H2. hipotézis nem igazolható.

A belső rendszer vizsgálata során bemutattam az annak kiépítéséhez szükséges műszaki követelményeket, melyek más egyetemek esetében is alkalmazhatók. A részletes elemezhetőség érdekében kialakítottam az egyetemeket jellemző szakterületi felosztást annak érdekében, hogy különbözőségeik megállapíthatók legyenek, és bemutattam azt a műszaki hátteret, melyre alapozva ez egy mérési szoftverbe átvihető. Részletesen elemeztem az egyes területek sérülékenységeinek számát és jellegét, megállapításaimat a publikus internet irányából és a belső hálózatból, a határvédelmi eszközök védelme nélkül detektálható sérülékenységekre külön-külön tettem meg. Megmutattam, hogy a feltárt sérülékenységek nagyrészt konfigurációs hibák következményei, és azok jelentős számban már a mérést megelőző *legalább* egy évvel korábban is ismertek voltak. Megmutattam, hogy az informatikai rendszer egyes elemei rendkívül régi, 1999-ben is ismert hibákat tartalmaznak. Végül szakterületi bontásban megvizsgáltam a sérülékenységek számának kiugrásait, és a konkrét sérülékenységek vizsgálásával elemeztem azokat.

A felsőoktatási rendszerekben elvégzett mérés alapján indokoltnak tartom a konfigurációs beállítások szigorítása mellett azok rendszeres ellenőrzését, és azok szükséges minimum szint alatt tartását. Emellett szabályzati vagy automatikus sérülékenységvizsgálati rendszer bevezetésével el kell érni, hogy a perifériális szolgáltatások, vidéki campusok, kutatóállomások informatikai infrastruktúrájának védelme a központi rendszerek magasabb prioritásának árnyékában

hátrányt szenvedjen. Hangsúlyt kell fektetni az említett konfigurációs hibák számának tervszerű csökkentésére, valamint ki kell dolgozni azokat az üzembe helyezési gyakorlatokat, melyek megakadályozzák újabbak megjelenését. A bemutatott eredmények feltehetően nem csak a felsőoktatás területén relevánsak, így célszerűnek tartom vizsgálatok végzését más szektorokban is, és az eredmények összevetésével szakterületi profilok kialakítását.

A fejezet tapasztalatai alapján az egyetemi informatikai rendszerekben sokkal nagyobb hangsúlyt kell fordítani az End-of-Life eszközök kivezetésére. A feltárt sérülékenységek jórésze egyértelműen a már nem támogatott operációs rendszerek, virtualizációs környezetek következménye, de nem ritka a régi weboldalak korai változatú, már nem frissíthető futtatási környezetinek leválthatatlansága. Ezek lecserélése egyes szoftverek újraírását követelné meg, melyhez a megfelelő szakmai és anyagi erőforrás nem áll rendelkezésre – ma a legtöbb felsőoktatási intézmény számára mindkét terület problémát jelent. Ugyanakkor a konfigurációs hibák elemzésével megállapítható, hogy egyes területeken nagyobb gondossággal célszerű eljárni, ki kell dolgozni azokat a belső szabályokat, amelyek meghatározzák és fenntartják az egyes rendszerelemek hardening követelményeit – legalább a publikus internet irányában elérhető eszközök tekintetében. Ezek feltérképezéséhez és naprakészen tartásához szükséges egy szkenner szoftver folyamatos működtetése, rendszeres időközönként generált jelentések készítése és elemzése, valamint a feltárt sérülékenységek és konfigurációs hibák prioritás szerinti kezelése. A riportok alapján nem csak ellenőrizhető az IT munkatársak feladatkörének ellátása, hanem felderíthetők az intézményben megjelenő, hálózatba kötött, nem intézményi tulajdonú eszközei is – mellyel hatékony lépés tehető a shadow informatika felszámolása felé is.

5. Ajánlás a felsőoktatási rendszerek besorolására

A dolgozatom harmadik fejezetében dokumentumelemzéssel bizonyítottam, hogy a magyar felsőoktatási rendszerek adminisztratív szabályzásai heterogén tartalmúak és azonos feladatkört ellátó rendszereket eltérő besorolással kezelnek. H4. hipotézis a felsőoktatási intézmények profiljának hasonlósága alapján az informatikai rendszerek besorolására az általános szempontokon alapuló eljárásra épülő, az egyes rendszerek közti kapcsolatok, és folyamatos sérülékenységvizsgálatok eredményei alapján finomított, a változásokra gyorsan reagálni képes metodika kialakítását célozza:

H4. a magyarországi felsőoktatási informatikai rendszerekre megadható egy specializált, kockázaton alapuló besorolási metodika.

A hipotézis igazolását egy, a szektor egészére alkalmazható ajánlás felépítésével bizonyítom, mely az általános besorolási szabályok mellett figyelembe veszi a speciális intézményi tevékenységeket, az alkalmazott szoftverek alapján azok adottságait, adattartalmukat. A metodika alapvető eleme az egyes rendszerek állandó vagy rendszeres adatkapcsolatait leíró mátrix, változásait pedig egy rendszeres sérülékenységvizsgálaton alapuló felülvizsgálat során feltárt sérülékenységek vagy konfigurációs hibák indokolják. A metodika alkalmazásával meghatározott biztonsági besorolások pontosabbá válnak, így az ideális védelmi eljárások meghatározása a rendszerrel szemben támasztott módosított bizalmassági, sértetlenségi és rendelkezésre állási besorolás változása alapján módosítható. A metodika alkalmazásának további előnye a kapcsolódó rendszerek érintettségének gyors feltárása és a kapcsolat jellegétől függő gördülő felülvizsgálata. Alkalmazása így túlmutat a sérülékenységekre adott válasz adott rendszerre irányuló megoldásán, az egyes rendszerek kapcsolati gráfjainak bejárásával az érintett rendszerek azonnal meghatározhatók, és akár többszörös iterációval mentén a további rendszerek védelme is aktualizálható.

Az ajánlás alapját az ibtv. alap besorolási ajánlásán túl az egyes informatikai rendszerek kapcsolatai jelentik, így kidolgozása során az érintett rendszerek minél szélesebb körének feltérképezése érdekében a korábban reprezentatív mintaként kiválasztott 11 intézmény mellett továbbiak szabályzatainak releváns részeit is áttekintettem és felhasználtam. Ennek során a grounded theory módszertanát alkalmaztam: a kutatási adatok folyamatos gyűjtése és a köztük fennálló kapcsolatok elemzésének többlépéses iterációja folyamatosan pontosították a rendszerek adatait, és juttattak el a kutatási eredményhez. A módszer az adatkapcsolatok elemzése során ide-

ális metodikának bizonyult, mivel nem követelte meg a tudományos eredmény előzetes felállítását, annak részletei a kutatás folyamata során folyamatosan rajzolódtak ki, és jelölték ki a annak további irányát.

A felsőoktatási rendszerek biztonsági besorolásakor az állami és önkormányzati szervekre kidolgozott 41/2015 BM rendelet 1-es melléklete szerint célszerű az egyetemek informatikai rendszereinek biztonsági besorolását elvégezni. A szabályzatok elemzése során megállapítottam, hogy az egyetemek szabályzataikban túlnyomórészt A-D jelölésű négyfokozatú skálát alkalmaztak, javaslatom a rendelet öt biztonsági osztályának használatát szorgalmazza. A rendelet általános elvei valamelyest szűkíthetők ha azok célterületeként csak a néhány területen az általánostól eltérő sajátosságokkal rendelkező felsőoktatási intézményeket jelöljük ki, ezért az kis módosításokkal a célterület számára testre szabható. Ennek meghatározásakor a rendelet besorolási szempontjaiból a nem releváns részeket elhagytam, másokat pedig a szektorhoz alakítottam. A metodikában szereplő alap besorolások meghatározásakor az egyes rendszerek ibtv. szerinti besorolásakor az alábbi módosított kritériumrendszert alkalmaztam.

1. 5-ös biztonsági osztályba sorolandók azok a rendszerek, amelyek az intézmény működésében létfontosságúak, vagy melyek sérülése vagy elvesztése esetén az alapvető funkciók ellátása lehetetlenné válik, az intézmény költségvetéséhez mérten komoly anyagi kár keletkezik, vagy melynek következtében az intézmény reputációja komoly kárt szenved. Ugyancsak ebbe az osztályba sorolandók azok, melyek az intézmények működésével vagy ügymenetével kapcsolatos nagy mennyiségű adatot tartalmaznak, melyek bizalmasságának és sértetlenségének megőrzése az intézmény működése vagy reputációjának fenntartása érdekében kiemelt fontossággal bírnak. Hasonlóan ide sorolandók be a jelentős mennyiségű személyes, gazdasági, vagy más, érzékeny adatot tartalmazó rendszerek, a hallgatói, oktatói, kutatói vagy dolgozói adatokat, valamint az intézmény alapfunkcióinak működőképességét fenntartó rendszerek. Az orvosképzést végző intézmények esetében ez kiegészül a különleges, pl. egészségügyi adatokat tartalmazó szakrendszerekkel. Értéküktől függően e biztonsági osztályba sorolandók az intézményben folyó kutatásokkal összefüggő, tudományos vagy üzleti eredmények elérését támogató rendszerek. Amennyiben az intézményben vagy annak szervezeti egységében működik kritikus infrastruktúrához kapcsolódó alrendszer, annak besorolását jelen ajánláson kívül, a vonatkozó jogszabályok alapján kell elvégezni. Kiemelt területként kell kezelni az oktatás és kutatás folyamatát, valamint a gazdasági folyamatok zavartalan működését

meghatározó elemeket.

2. 4-es biztonsági osztályba sorolandók azok a rendszerelemek, melyek kiesésének esetén az intézmény működésében jelentős zavar áll be, valamely alapfunkciót támogató rendszer működése áll le vagy szenved el jelentős funkcióvesztést. A működés vagy az ügymenet során keletkezett bizalmas adatok, nagy mennyiségű személyes vagy különleges adat kerül nyilvánosságra vagy vész el. A rendszer kiesésének vagy sérülésének következtében elszenvedett kár jelentős, annak következményei a nyilvánosság számára ismertté válnak így az intézmény megítélése is kárt szenved.
3. 3-as biztonsági osztályba sorolandók azok a rendszerek, melyek kiesése vagy hibás működése zavart okoz, különleges adat sérülése nem, de kisebb mennyiségű személyes adat bizalmassága vagy sértetlensége csorbul. Anyagi kár keletkezése esetén az az adatokért felelős nagyobb szervezeti egység (pl. egy igazgatóság) saját költségvetésében kezelhető, viszont az intézmény külső reputációja nem sérül, és az incidens saját hatáskörben kezelhető.
4. A 2-es osztályba sorolandó minden olyan rendszer, mely nem tárol bizalmas, az intézmény működésében jelentős információt, minimális mennyiségű személyes adatot tartalmaz, vagy az azokban tárolt információk jogszerű felhasználás mellett más, publikus forrásól is elérhetők. A rendszerrel kapcsolatos problémák az intézményen belül kezelhetők, azoknak nincs negatív hatása az intézmény reputációjára. Az esetleges anyagi kár az adatokért felelős szervezeti egység saját költségvetésében kezelhető.
5. Az 1-es osztályba sorolt rendszerek nem tartalmaznak semmilyen érzékeny adatot, a bekövetkező káresemény jelentéktelen, és működési rendellenességeik, kiesésük az intézmény működésében nem okoz számottevő problémát.

Megítélésem szerint kockázatos egy egyetemi informatikai rendszer bármelyik elemének 1-es szintbe sorolása és csak indokolt esetben célszerű az alkalmazása. A szint meghatározása kizárólag az adattartalomra koncentrál, miközben nem veszi figyelembe a berendezések lehetséges kapcsolatait. A csoport tipikus elemei a számítógépes laborok és nyilvános könyvtári számítógépek, melyek az intézményi határvédelmi berendezések első vonala mögött helyezkednek el, így kompromittálásuk ugródeszkát jelenthet a hálózat további eszközeinek megtámadásakor. Ezért védelmük érdekében a gyakorlatban legalább a 2-es osztály előírásainak érvényesítése javasolt.

A H4. hipotézis bizonyítására felépített, a felsőoktatási rendszerek besorolási metodikájának alapját az ibtv. szerinti javasolt besorolás módosítása képezte, mely jogszabályban meghatározott konkrét, vagy jogszabályi kötelezettség okán működtetett rendszerek esetében egyértelműen meghatározható, kiszámításában az OVI táblák nyújtanak gyakorlati segítséget. A H4. bizonyítására kidolgozott metodika ezt veszi alapul, és a fenti módosításokkal határozza meg az egyes rendszerek besorolásának minimális értékeit, melyet a kapcsolati mátrixban tüntettem fel.

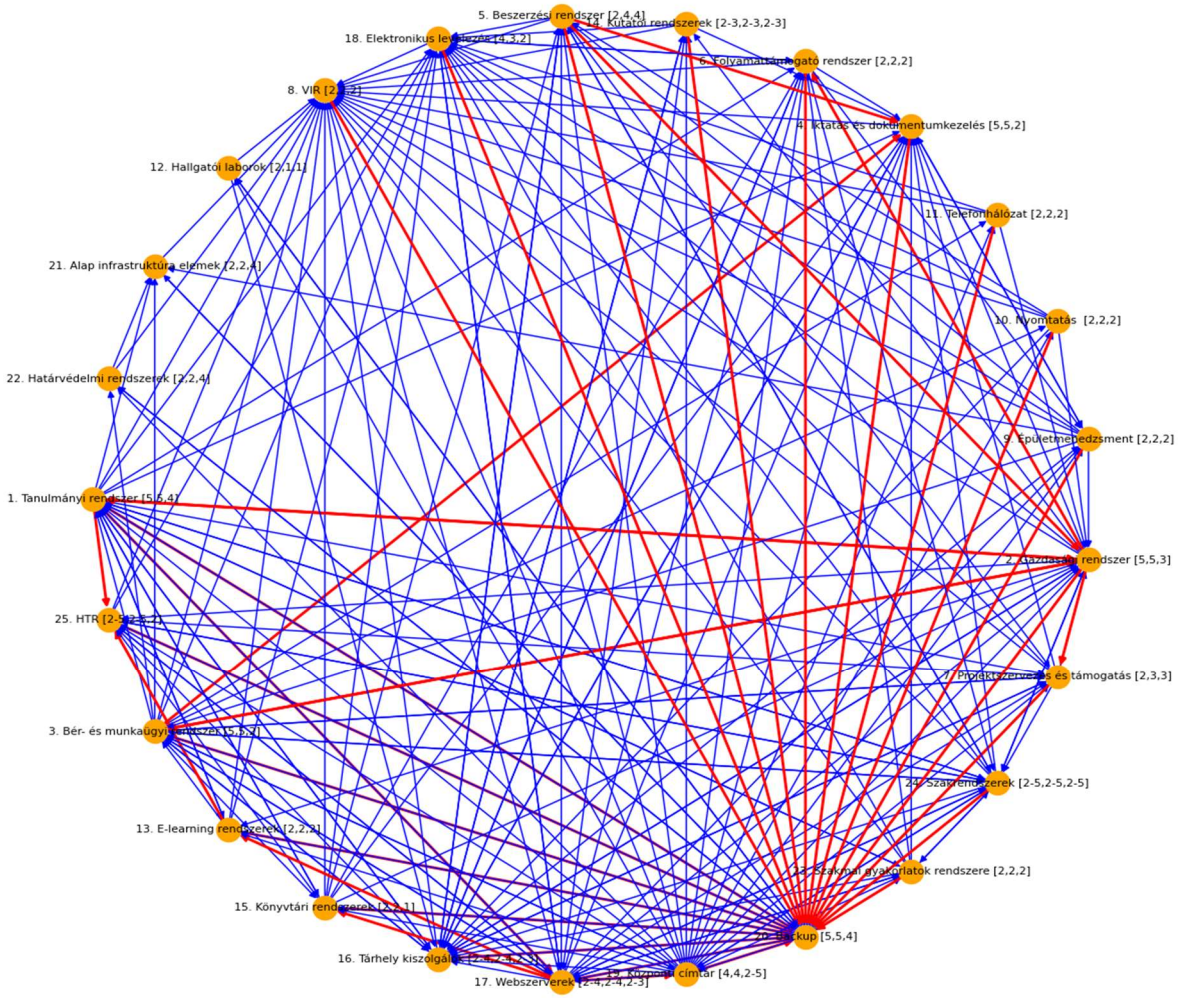
A 41/2015 BM rendelet meghatározza, hogy „a (biztonsági osztályba) sorolást ... kockázatelemzés alapján kell elvégezni.” [3, p. 17702], melynek meghatározó eleme egy rendszer pillanatnyi sérülékenységi állapota is. A jogszabály besorolást meghatározó szempontjai a fentiek alapján ugyan általánosak, ugyanakkor módosításukra vagy saját besorolás kialakítására is lehetőéget ad. H4. metodika a CVSS 3.0 metrika „hatás” mutatójához hasonlóan kitér azokra a rendszerekre, melyekkel az osztályba sorolandó rendszer valamilyen, annak adat-, vagy működési biztonságára hatással levő kapcsolatban áll. Tipikus kapcsolati típusok az alkalomszerű vagy rendszeres, manuális vagy automatikus adat átadási műveletek, import vagy export folyamatok, de ide tartoznak a jellemzően API hívásokkal megvalósított külső rendszerhívások is. Egyes rendszerek tipikus kapcsolati útjai szinte minden intézményben kiépítésre kerültek, míg mások jelenléte csupán opcionális. A metodika szerinti alap besorolás ezek alapján bővítendők, melyet a kapcsolati mátrix alapján kell elvégezni. A mátrix minden egyes rendszer esetén páronként írja le lehetséges kommunikációs kapcsolataikat, valamint feltünteti azok irányát is. A mátrix sorai és oszlopai tartalmazzák az egyes rendszerelemeket, azok alap besorolási javaslatát, metszéspontjukban pedig azok lehetséges kapcsolatait. Az irányt a táblázatban feltüntetett nyilak jelzik: az adatkapcsolatok az oszlopoktól a sorok felé irányulnak. A kapcsolati mátrix elemeinek lehetséges értékei:

- N: nincs az adott oszlopban szereplő rendszerből induló, működést befolyásoló kommunikáció és nem történik adat átadása a sorban meghatározott rendszer felé.
- AK: az adott oszlopban szereplő rendszerből annak működését befolyásoló kommunikáció vagy adat átadása történik a sorban szereplő rendszer felé.
- N/AK: az oszlopban szereplő rendszer kezdeményezhet adat átadást vagy egyéb, a célrendszer működését befolyásoló kommunikációt a sorban meghatározott rendszer felé.

		IBTV szerinti javasolt besorolás	Irány	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25		
				Tanulmányi rendszer	Gazdasági rendszer	Bér- és munkaügyi rendszer	Iktatás és dokumentumkezelés	Beszerzési rendszer	Folyamattámogató rendszer	Projektszervezés és támogatás	VIR	Épületmenedzsment	Nyomtatás	Telefonhálózat	Hallgatói laborok	E-learning rendszerek	Kutatói rendszerek	Könyvtári rendszerek	Tárhely kiszolgálók	Webszerverek	Elektronikus levelezés	Központi címtár	Backup	Alap infrastruktúra elemek	Határvédelmi rendszerek	Szakmai gyakorlatok rendszere	Szakrendszerek	HTR	AK Darab	N/AK Darab
				↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	Tanulmányi rendszer	5,5,4	←		AK	N/AK	N	N	N	N	N	N	N	N	N	N/AK	N	N/AK	N/AK	N/AK	N	N/AK	N/AK	N	N	N/AK	N/AK	N	1	9
2	Gazdasági rendszer	5,5,3	←	AK		AK	N	AK	N	N/AK	N	N/AK	N/AK	N/AK	N	N	N	N/AK	N/AK	N/AK	N	N/AK	N/AK	N	N	N	N/AK	N	3	10
3	Bér- és munkaügyi rendszer	5,5,3	←	N	AK		N	N	N	N/AK	N	N/AK	N	N	N	N/AK	N	N	N/AK	N/AK	N	N/AK	N/AK	N	N	N	N/AK	N	1	8
4	Iktatás és dokumentumkezelés	5,5,2	←	N/AK	N/AK	AK		AK	N/AK	N/AK	N	N/AK	N	N	N	N	N/AK	N/AK	N/AK	N/AK	N	N/AK	N/AK	N	N	N/AK	N/AK	N	2	13
5	Beszerzési rendszer	2,4,4	←	N	N/AK	N	N		N	N	N	N/AK	N/AK	N	N	N	N	N/AK	N/AK	N/AK	N	N/AK	N/AK	N	N	N	N/AK	N	0	9
6	Folyamattámogató rendszer	2,2,2	←	N/AK	AK	N	N	N		N	N	N	N	N	N	N	N	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N	N	N/AK	N	N	1	8
7	Projektszervezés és támogatás	2,3,3	←	N/AK	AK	N/AK	N	N/AK	N		N	N	N	N	N	N	N	N	N/AK	N/AK	N	N/AK	N/AK	N	N	N	N	N	1	7
8	VIR	2,2,2	←	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK		N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	0	24
9	Épületmenedzsment	2,2,2	←	N	N	N	N/AK	N	N/AK	N	N		N	N	N	N	N	N	N/AK	N/AK	N	N/AK	N/AK	N	N	N	N	N	0	6
10	Nyomtatás	2,2,2	←	N	N	N/AK	N	N	N	N	N	N		N	N	N	N	N	N	N	N	N/AK	N/AK	N	N	N	N	N	0	3
11	Telefonhálózat	2,2,2	←	N	N	N/AK	N	N	N	N	N	N	N		N	N	N	N	N	N	N	N/AK	N/AK	N	N	N	N	N	0	3
12	Hallgatói laborok	2,1,1	←	N	N	N	N	N	N	N	N	N	N	N		N	N	N	N	N	N	N/AK	N/AK	N	N	N	N	N	0	2
13	E-learning rendszerek	2,2,2	←	N/AK	N/AK	N	N	N	N	N	N	N	N	N	N		N	N	N	AK	N	N/AK	N/AK	N	N	N	N	N/AK	1	5
14	Kutatói rendszerek	2-3,2-3,2-3	←	N	N/AK	N	N	N	N	N	N	N	N	N	N	N		N	N/AK	N	N	N/AK	N/AK	N	N	N	N	N	0	4
15	Könyvtári rendszerek	2,2,1	←	N/AK	N	N/AK	N	N	N	N	N	N	N	N	N	N	N		N	AK	N	N/AK	N/AK	N	N	N	N	N	1	4
16	Tárhely kiszolgálók	1-5,1-4,1-3	←	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N/AK	N	N	N/AK	N	N/AK	N	N/AK	N		N/AK	N	N/AK	N/AK	N	N	N/AK	N/AK	N/AK	0	16
17	Webszerverek	2-5,2-5,2-4	←	AK	N	N/AK	N	N	N	N	N	N	N	N	N	N	N/AK	N	N		N/AK	N/AK	N/AK	N	N	N/AK	N/AK	N/AK	1	8
18	Elektronikus levelezés	4,3,2	←	N/AK	N/AK	N/AK	N	N/AK	N/AK	N/AK	N	N/AK	N/AK	N/AK	N	N/AK	N/AK	N/AK	N	N/AK		N/AK	N/AK	N	N	N/AK	N/AK	N/AK	0	18
19	Központi címtár	4-5,4-5,2-5	←	N	N	N/AK	N	N	N	N	N	N	N	N	N	N	N	N	N	AK	N		N/AK	N	N	N	N/AK	N	1	3
20	Backup	2-5,2-5,2-5	←	AK	AK	AK	AK	AK	AK	AK	AK	AK	AK	AK	N/AK	AK	AK	AK	AK	AK	AK	AK		N/AK	N/AK	AK	AK	AK	21	3
21	Alap infrastruktúra elemek	2,2,4	←	N/AK	N	N/AK	N	N	N	N	N	N/AK	N	N	N	N	N	N	N	N	N	N	N/AK		N/AK	N	N	N	0	5
22	Határvédelmi rendszerek	2,2,4	←	N	N	N/AK	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N/AK	N/AK	N		N	N	N	0	3
23	Szakmai gyakorlatok rendszere	2,2,2	←	N/AK	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N/AK	N	N/AK	N/AK	N	N		N/AK	N	0	5
24	Szakrendszerek	2-5,2-5,2-5	←	N/AK	N/AK	N/AK	N	N/AK	N/AK	N/AK	N	N	N	N	N	N	N	N	N	N/AK	N	N/AK	N/AK	N	N	N/AK		N/AK	0	11
25	HTR	2-5,2-5,2	←	AK	N/AK	N	N	N	N	N/AK	N	N	N	N	N	AK	N	N/AK	N	N/AK	N	N/AK	N/AK	N	N	N	N/AK		2	7
	AK Darab		←	3	5	3	1	3	1	1	1	1	1	1	0	1	1	1	1	4	1	1	0	0	0	1	1	1		
	N/AK Darab		←	9	13	15	5	8	7	8	2	9	7	5	4	6	7	9	12	16	5	20	21	3	3	8	11	6		

A mátrix tartalmát a bevezetést követően az intézmény informatikai rendszerének megfelelően az N/AK tartalmú cellák áttekintésével N-re vagy AK-ra történő módosításával úgy kell aktualizálni, hogy az az intézmény rendszereinek aktuális kapcsolatait írja le. A mátrix nem feltételezett speciális adatkapcsolatainak aktualizálására az eredetileg N-nel jelölt cellát értékét is felül kell vizsgálni, és el kell végezni az így feltárt kapcsolatokat dokumentálását. Új rendszer bevezetésekor azt azonos sor- és oszlopszámmal a mátrixban rögzíteni kell, valamint meg kell határozni minden, a mátrixban már szereplő rendszerrel fennálló, annak működését befolyásoló kapcsolatait. A meglevő rendszerek változásai során a kapcsolati mátrix elemeit frissíteni kell, egy meglevő rendszer kivezetésekor az a kapcsolati mátrixból törölhető.

A 41/2015 BM rendelet a 3.3.5.3. bekezdésben kitér a sérülékenységvizsgálati eszközök alkalmazásának lehetőségére is [3, p. 17736], melynek eredménye beépíthető a biztonsági besorolás folyamatába úgy, hogy az érintett rendszer mellett annak kapcsolódási útjai figyelembevételével más rendszerekre gyakorolt lehetséges hatásait is figyelembe veszi.



9. ábra. A felsőoktatási rendszerek közötti adat- és kommunikációs kapcsolatok.

Forrás: saját szerkesztés.

Egy rendszer biztonsági besorolásának alapját tehát az ibtv. szerinti módosított besorolás adja, mely felülvizsgálandó a rendszer változása, vagy az azt működtető infrastruktúrában megjelent, vagy javított sérülékenység esetén is alkalmazni kell oly módon, hogy a mátrixban szereplő, a szóban forgó rendszerrel kapcsolatban levő rendszerek kockázatának megváltozása alapján annak biztonsági osztályát módosítani kell. Az érintett rendszer felülvizsgálatát követően minden kapcsolódó rendszer esetén el kell végezni a sérülékenység lehetséges hatásának elemzését és amennyiben szükséges, azok besorolását is módostani kell. A besorolás során a CIA alapelvek mindegyikét vizsgálni kell, és a sérülékenység lehetséges hatásainak elemzésével elsőként meg kell határozni a rendszerrel kapcsolatos kockázatok változásait és a kapcsolódó rendszerek érintettségét. Amennyiben a kapcsolódó rendszer érintettsége megállapításra kerül, az eljárást iteratív úton minden kapcsolódó rendszere érvényesíteni kell.
A kapcsolati mátrix gráfban történő ábrázolása meglehetősen összetett képet nyújt, ezért az egyes rendszerek leírása során ennek irányított részgráfjait tüntettem fel. Az ezt alkotó kék színnel jelölt vektorok a lehetséges, a pirossal kirajzoltak az intézmények többségében érvényes kapcsolatokat jelölik. A gráf csomópontjaiban a rendszerek megnevezése mellett a bizalmasság, sértetlenség és rendelkezésre állás mérőszámai is feltüntetésre kerültek.

Egy rendszer általános leírását az alábbi szerkezetben adtam meg:
Az IBTV szerinti javasolt besorolás tartalmazza az adott rendszer alap besorolását, melynek meghatározása az ibtv., módosítása alapján, az VI tábláka alkalmazásával, elsősorban a rendszer által tárolt adatok jellege és mennyisége alapján történt. Ebben feltüntetésre kerülnek a bizalmasság, sértetlenség és a rendelkezésre állás mérőszámai mellett a rendszer normál állapota szerinti biztonsági besorolása.

A leírás a rendszer jellemzőinek rövid leírását, kezelt adatainak és főbb funkcióinak felsorolását tartalmazzák.

A kockázatok a bizalmasságot, sértetlenséget és rendelkezésre állást meghatározó, az adott egyetem működési környezete és sajátosságai által meghatározott tényezők.

A *bejövő adatok és hozzáférések* azon rendszerek felsorolását tartalmazzák, ahonnan érzékeny adatok érkezhetnek, vagy onnan olyan, a szóban forgó rendszer működést befolyásoló rendszerhívás kezdeményezehető, mely kihat a célrendszer működésének biztonságára.

A *kimenő adatok és hozzáférések* azon rendszereket sorolja fel, melyekbe az adott rendszer adatokat küld, azzal alkalmi, vagy folyamatos kapcsolatot tart fenn, melyek az adott rendszer adattartalmát vagy működési módját oly módon befolyásolhatja, mely kihat a célrendszer működésének biztonságára.

A be- és kimenő adatkapcsolatok a kapcsolati mátrix alapján kerültek meghatározásra és a sérülékenységek bekövetkezésekor vizsgálandó további rendszerelemek meghatározásában van szerepük. Egy adott sérülékenység CVE adatbázisba kerülésekor a CVSS pontszám mellett annak súlyossági besorolását is megadják. Amennyiben egy rendszerben kritikus vagy súlyos minősítésű sérülékenység jelenik meg, a kapcsolódó rendszerek védelmi szintjének felülvizsgálatát a legrövidebb időn belül el kell végezni. Ugyancsak felülvizsgálatot igényelnek a kapcsolódó rendszerek abban az esetben, ha a CVSS *scope* értékei alapján további rendszerek is lehetnek érintettek, mely alapján a biztonsági besorolásukat ezzel arányosan változtatni kell. Egy adott rendszer biztonsági besorolásának aktualizálása mellett a kapcsolati mátrix által meghatározott további rendszerek védelmi szintjét is megfelelően változtatni kell, továbbá életbe kell léptetni azokat az elsődleges és másodlagos védelmi eljárásokat, melyek a megváltozott helyzetben képesek védelmet nyújtani az érintett rendszerek mindegyikére.

5.1. Általános rendszerek

Az egyes rendszerek adatkapcsolatainak feltárása során több azonos jellegű, elsősorban általános, vagy adott részfeladat ellátásáért felelős kapcsolatot azonosítottam, mely számos rendszer számára kínál szolgáltatást, szerepük és védelmi szempontjaik is rendszerenként megközelítőleg azonosak. Az ismétlődések elkerülése érdekében elsőként ezeket ismertetem, az esetleges eltérések az egyes rendszereknél feltüntetésre kerülnek.

Központi címtár

IBTV szerinti javasolt besorolás: *Bizalmasság: 4-5 sértetlenség: 4-5, rendelkezésre állás: 2-5. Biztonsági osztály: 4*

A központi címtár elsődleges feladata általános azonosítási szolgáltatás nyújtsa további rendszerek számára, mely megvalósítására az egyszerű bejelentkezési név és jelszó páros mellett számos egyéb megoldás (pl. kétfaktoros azonosítás) ismert [50] [89]. A címtárak emellett tartalmazhatnak engedélyezési információkat különféle szolgáltatások igénybevételéhez is. A szolgáltatásra alapozva központi felhasználói adatbázis és ahhoz kapcsolódó jogosultsági rendszer alakítható ki, mely hozzájárul a teljes informatikai rendszer átláthatóságához és lehetővé

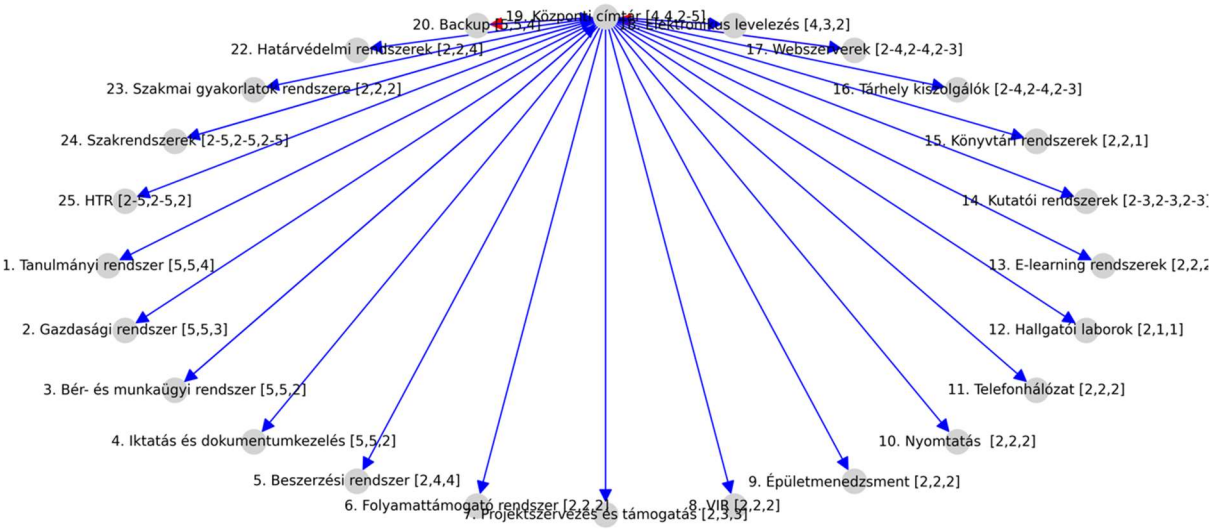
teszi központi kezelhetőségét. A fejlesztések során a legtöbb intézmény törekszik a címtár alapú azonosítás minél szélesebb körben történő bevezetésére. Ennek hatása van a jelszóbiztonságra: az egy ponton történő azonosítás megkíméli a munkatársakat a különböző rendszerekhez tartozó jelszavak memorizálásának kényszerétől, csökkenti az azonos jelszavak használatát különböző rendszerekben, így kisebb valószínűséggel írják fel azokat [90]. A jelszavak használhatóságával kapcsolatban számos tanulmány fogalmazott meg kritikákat, ugyanakkor más azonosítási módszerek alkalmazása nehézkes, a személyazonosság biometrikus[43] igazolása pedig csak indokolt esetben alkalmazható [91]. A címtárszolgáltatáson alapul a több egyetemi informatikai szabályzat által külön említett intézményi telefonkönyv vagy tudakozó is.

Bizalmasság. A címtárszolgáltatás centralizált jellege és az abban tárolt nagymennyiségű adat különösen érzékennyé teszi a szolgáltatást, mely sérülékenysége esetén az összes olyan rendszer hozzáférési adatainak szivárgásának lehetőségével kell számolni, mely az azonosítási szolgáltatást igénybe veszi. A jelszó adatbázisok ellen számos támadás ismert, [92] [93] [94] [95], az internetről milliárdos nagyságrendben tölthetők le jelszó adatbázisok [96]. A belépési adatok visszafejtésének megakadályozását az alkalmazott kriptográfiai eljárások sem képesek minden esetben megakadályozni [97] [98], ezért a címtárakat kifejezetten magas kockázatú rendszerként kell kezelni. Az alkalmazott algoritmusok ellenállóképességét rendszeresen felül kell vizsgálni, és azokat modern, akár kvantumszámítógépi algoritmusoknak is ellenálló megoldásra kell cserélni [99]. A címtárak bizalmassági besorolásának értékét azt alkalmazó rendszerek bizalmassági besorolásának maximuma adja, mely a felsőoktatási rendszerek esetén 5.

Sértetlenség. Azonos szabály érvényesül a sértetlenség besorolásakor is. A címtárszolgáltatás adatainak rosszindulatú módosítása, az abban tárolt jelszavak, hozzáférési jogosultságok megváltoztatásának következményei minden, a szolgáltatást igénybe vevő rendszerre kihathatnak, így sérülékenysége esetén azonnali beavatkozás szükséges.

Rendelkezésre állás. A rendszer szolgáltatás kiesésének következményei a kapcsolódó rendszerek rendelkezésre állási követelményeinek függvényében változnak, és szintén a legmagasabb rendelkezésre állási igényű szakrendszer szerint kell meghatározni. Az általános felsőoktatási rendszerek esetében ennek értéke 4.

[43] A biometrikus adat az Általános Adatvédelmi rendelet 4. cikkelye alapján: „egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat”



10. ábra. A címtárszolgáltatás lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A címtár adatainak változásai a rendszer üzemeltetői által használt saját adminisztrációs felület mellett a munkaügyi rendszerből, illetve más irányból is érkezhetnek. Az informatikai egységek mellett a munkaügyi rendszer adatkapcsolati mechanizmusai is elvégezhetik a címtár adminisztrációs feladatait új dolgozó felvételekor, munkakörének változásakor vagy egy munkaviszony megszűnésekor. Alkalmazhatók web alapú adminisztrációs felületek, esetükben a webszerverek felől kell olyan kiinduló kapcsolattal számolni, mely a címtár adatainak módosítását eredményezheti.

Kimenő adatok és hozzáférések: tetszőleges, a központi címtárszolgáltatást igénybe vevő rendszerek köre.

A címtárszolgáltatásban megjelenő sérülékenység esetén tehát minden olyan rendszer érintettségét felül kell vizsgálni, mely annak szolgáltatásait igénybe veszi, és a módosult kockázat alapján a besorolását felül kell vizsgálni. A címtárszolgáltatás adatainak módosítására képes rendszerek sérülékenysége esetén annak javításáig a köztük fennálló adatkapcsolatot meg kell szakítani, és a rendszer működtetését az üzletfolytonossági tervben, alternatív úton elvégezni.

Backup

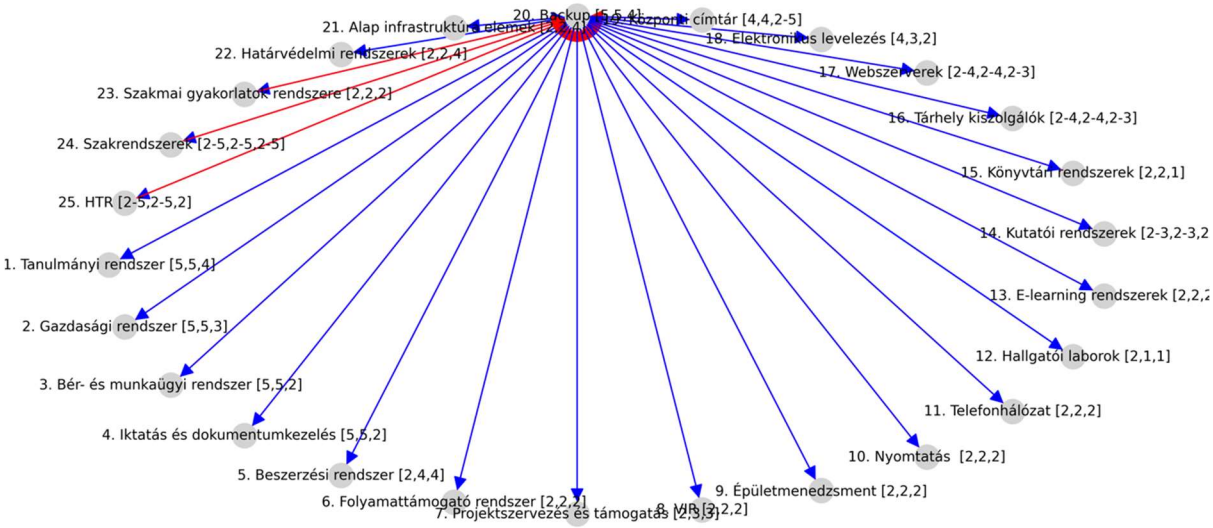
IBTV szerinti javasolt besorolás: *Bizalmasság: 2-5, sértetlenség: 2-5, rendelkezésre állás: 2-4. Biztonsági osztály: 2-5*

Egy mentési rendszer az egyetemi informatikai környezet egy vagy több adatforrásából vagy komplex rendszeréről automatizált másolatképzését végző, rendszerint központosított megoldás, mely az egyes másolatokat képes több verzióban, akár teljes mérföldkövek megőrzésével is megtartani. Elsődleges célja sérült vagy hiányzó fájlok vagy komplex rendszerek korábbi állapotának lehetőség szerint gyors és konzisztens helyreállítása.

Bizalmasság. Egy mentési rendszer szivárgásának következményei azonosak a forrásrendszerével, ezért bizalmasságának besorolási értéke az abban legmagasabb bizalmassági besorolású rendszer évél egyezik meg.

Sértetlenség. Tekintettel arra, hogy a mentési rendszerekben tárolt adatoknak szinte kizárólag a forrásrendszert ért incidens esetében van szerepe, annak sértetlensége a normál működés során másodlagos. Ugyanakkor egy nehezen kivédhető támadási forma egy teljes mentett rendszer kompromittálása, vagy annak adatainak megváltoztatását követő helyreállítási folyamat során az eredetibe való visszatöltése, ezért a sértetlenség besorolását a legmagasabb besorolású mentett rendszerével azonosként kell meghatározni.

Rendelkezésre állás: A sértetlenséghez hasonlóan ennek mértéke is a mentett rendszer besorolásának függvénye, mely a felsőoktatási rendszerek esetében az ajánlás szerint legfeljebb 4. A rendelkezésre állással szembeni maradványkockázat vállalásának mértékét meghatározza a rendszerek mentési frekvenciája, mely az egyetemi rendszerekben általában egy nap.



11. ábra. A mentési rendszer lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

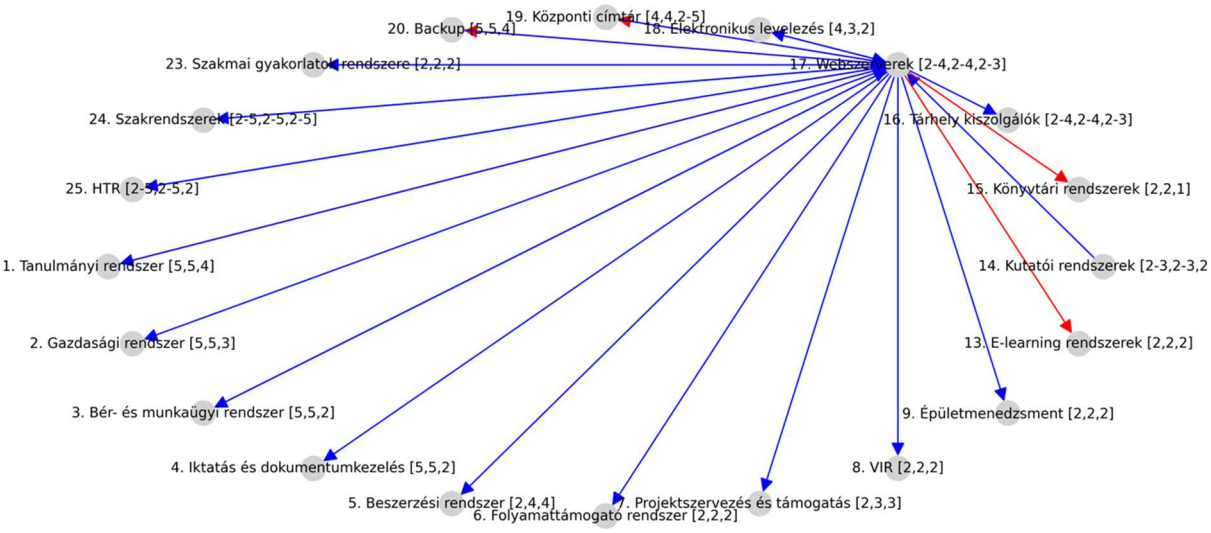
Bejövő adatok és hozzáférések. A mentési rendszerek az intézmény bármely információs rendszerének adatát, vagy az informatikai struktúra konfigurációját tartalmazhatja, így adatforrásként szinte minden rendszer megjelölhető. Amennyiben a mentési infrastruktúrához az egyes rendszerek önálló hozzáféréssel rendelkeznek, a mentést ők kezdeményezik, úgy sérülékenységük esetén a mentési rendszer egészére irányuló kockázatelemzéssel kell meghatározni annak új besorolási szintjét, és az ahhoz rendelt védelmi intézkedéseket.
Kimenő adatok és hozzáférések. Egy incidenst követő helyreállítási folyamat alapjául szintén a mentési rendszer adatai szolgálnak, így a kapcsolódó adatforrások a bejövő adatforrásokkal egyeznek meg. Amennyiben a mentési eljárásokat a backup rendszer kezdeményezésével, a mentendő rendszerhez történő kapcsolódás során végzi, a mentési rendszerben megjelenő sérülékenység az összes, mentendő rendszerre kihatással lehet. Ebben az esetben az összes olyan rendszer felülvizsgálatát el kell végezni, melyhez a mentési rendszer hozzáférési jogosultsággal bír.
Emellett mentési rendszerben fennálló sérülékenység kockázata az abban tárolt adatok szivárgása, így annak fennállása esetén minden, a mentésben szereplő rendszer érintettségét vizsgálni kell abban az esetben, ha az abban tárolt adatok helyreállítása szükségessé válik. A kockázat nagyban csökkenthető a mentési eljárás során alkalmazott titkosítási eljárásokkal.

Webszerverek

IBTV szerinti javasolt besorolás: *Bizalmasság: 2-5 sértetlenség: 2-5, rendelkezésre állás: 2-4. Biztonsági osztály: 2-5*

A webszerverek virtuális tárhelyszolgáltatásuk révén számos website kiszolgálását egyidőben képesek ellátni, melyet besorolásuk során kiemelet szempontként kell kezelni.
Bizalmasság. Amennyiben egy website csak saját kezelésben levő adatok alapján működik, bizalmassági besorolása az ibtv. szerinti ajánlás alkalmazásával egyszerűen elvégezhető. A kockázat meghatározása során ugyanakkor fel kell térképezni az adott webszerver által kiszolgált további webhelyeket is, ugyanis azok sérülése vagy konfigurációs hibája minden más site-ra is kihatással lehet. Egy ilyen esetben a szerver által kezelt teljes adattartalom szivárgásával számolni kell, emellett lehetséges adatkapcsolatai mentén további rendszerek adattartalma is sérülhet. Ezért a webszerverek besorolásait minden új web tárhely kialakítása során el kell végezni, és annak változását minden más érintett rendszerre tovább kell görgetni.
Sértetlenség. Egy webszerver sértetlenségének besorolását a már ismertetett okok alapján az általa működtetett legmagasabb besorolású website adattartalma és kapcsolatai alapján kell meghatározni, és minden új website hozzáadásakor felül kell vizsgálni.

Rendelkezésre állás. Mértékét szintén a webszerver által kiszolgált rendszerek rendelkezésre állásának besorolási maximuma határozza meg.



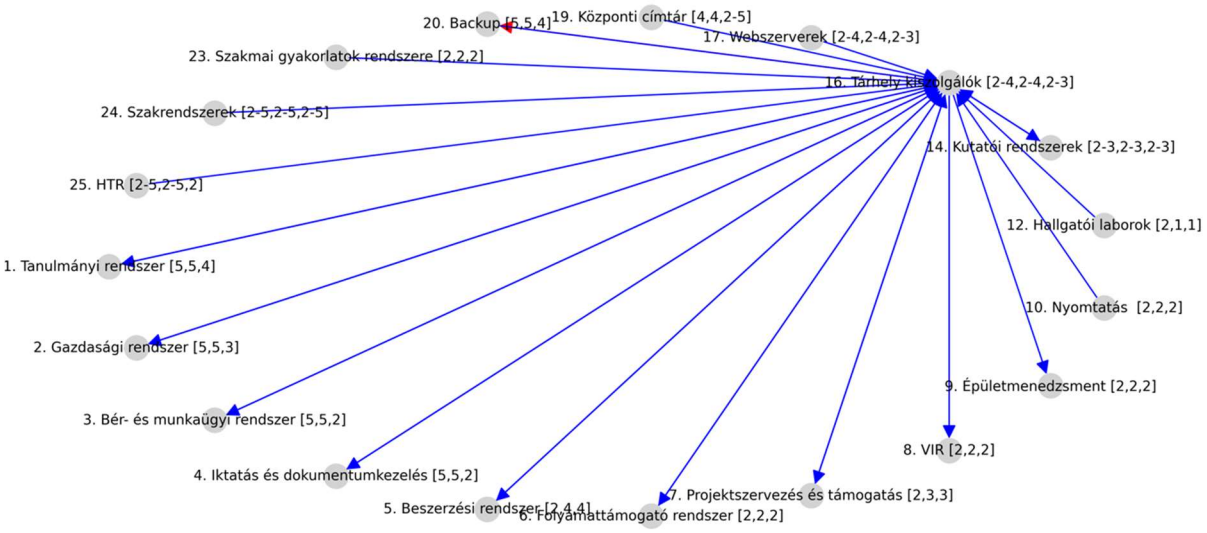
12. ábra. A webszerverek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő- és kimenő adatok, hozzáférések. Számos rendszer rendelkezhet webes felülettel. A tanulmányi rendszer hallgatói hozzáférési felülete, fájlszolgáltatások, bérjegyzékek lekérdezésének, beszerzési igények kezelésének, iktatás, a vezetői információs rendszer webes felületei csak néhány példa ezekre. A webszerverek lehetséges adatkapcsolatait leíró gráfban feltüntetésre kerültek azok a szakrendszerek, melyek rendelkezhetnek ilyen eléréssel. Az egyes intézmények esetén a kapcsolati gráfot a rendszereik felülvizsgálatával aktualizálni kell.
Sérülékenység esetén érintett rendszerek. A webszerver sérülékenységei befolyásolják minden kezelésükben levő webhely biztonságát. Amennyiben valamely rendszerhez kapcsolódó szolgáltatáshoz webes felület (is) elérhető, a kiszolgáló webszerver sérülékenysége az adott rendszerrel kapcsolatos kockázatok növekedését eredményezi, így szükséges annak felülvizsgálata. A kockázatok csökkentésére, a magas védelmi szintet megkövetelő webszerverek alacsony szinten tartására célszerű több kiszolgáló alkalmazása oly módon, hogy az azonos besorolású website-ok azonos besorolású webszerverekre legyenek szétválasztva.

Tárhely kiszolgálók

IBTV szerinti javasolt besorolás: *Bizalmasság: 1-5 sértetlenség: 1-4, rendelkezésre állás: 1-3. Biztonsági osztály: 1-4*

A tárhely kiszolgálók tipikus elemei fájlszerverek, illetve a különféle, az intézményi infrastruktúrán vagy felhőszolgáltatásban működő, általános célú, fájlok tárolására szolgáló megoldások. Ezek biztonsági besorolásának alapjául adattartalmuk szolgál. Azon kiszolgálók, melyek nem tartalmaznak az intézmény szempontjából releváns vagy személyes adatokat (pl. számítógépes hallgatói laborok fájlszerverei) a legalacsonyabb biztonsági osztályba sorolandók. Egyéb esetekben a bizalmasság és a rendelkezésre állás besorolását az adattartalom érzékenysége alapján kell meghatározni.



13. ábra. A tárhely kiszolgálók lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

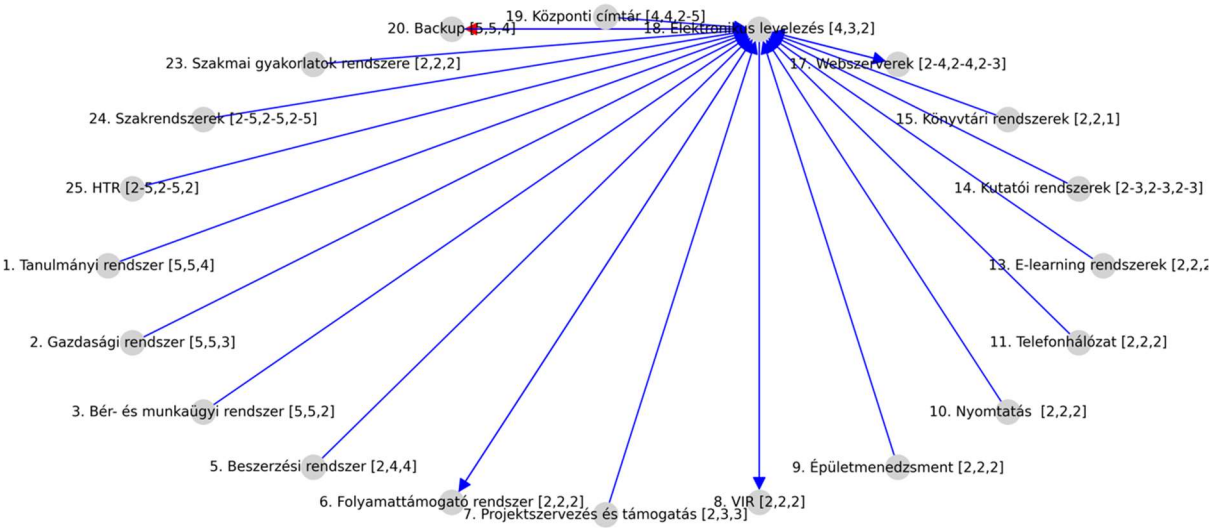
Bizalmasság. A tárhelykiszolgálók általános jellege következtében azok bizalmassági besorolásának mértékét az abban tárolt adatok bizalmassági szintjének maximumaként kell meghatározni. Számos rendszerből származhatnak olyan riportok, különböző adatigénylések során előállított export fájlok, melyek érzékeny adatokat tartalmaznak, így általános besorolásuk csak ezek elemzésével tehető meg. A tárolt fájlok érzékenységének szintje esetenként egyértelműen meghatározható, általános besorolásuk azonban nehézséget jelenthet. Amennyiben a tárhelykiszolgáló egy konkrét rendszer számára nyújt kiegészítő szolgáltatást (pl. szerződések dokumentumfájljainak tárolása), annak szivárgása esetén a bekövetkező káresemény a forrásrendszerével egyezik meg, ezért bizalmasságának besorolási értéke azt használó rendszerével azonos.
Sértetlenség. Amennyiben a tárhelykiszolgáló egy általános célú fájltároló, a sértetlenség besorolását szintén a tárolt fájlok várható tartalma alapján kell megállapítani. Egyéb más rendszer részére nyújtott szolgáltatás esetén a sértetlenség besorolását azzal azonos mértékűként kell meghatározni, többszörös szolgáltatás esetén pedig a legnagyobb értékkel kell megegyeznie.

Rendelkezésre állás. Amennyiben a tárhelykiszolgáló egy általános célú fájltároló, a rendelkezésre állás besorolását szintén a tárolt fájlok rendelkezésre állásával szemben támasztott igény határozza meg, azzal azonos lesz. Amennyiben az valamilyen egyéb rendszer részére nyújt szolgáltatást, a rendelkezésre állás besorolását azzal azonos értékűként kell megállapítani.
Bejövő és kimenő adatok és hozzáférések. A tárhely kiszolgálók kapcsolati gráfja alapján egy ilyen rendszer tetszőleges más rendszerrel állhat adatkapcsolatban, és a szolgáltatás természete következtében jellemzően nem áll fenn különbség a bejövő és a kimenő adatok forrásaként működő rendszerek közt. Egy tárhelykiszolgáló sérülékenysége elsősorban az abban tárolt fájlok bizalmasságát és sértetlenségét befolyásolhatja, amennyiben a kiszolgáló más rendszerek számára nyújt további szolgáltatást, azok bizalmasságának és sértetlenségének kockázatát is negatív módon befolyásolja, így azok felülvizsgálatát szintén el kell végezni.

Elektronikus levelezés

IBTV szerinti javasolt besorolás: *Bizalmasság: 4 sértetlenség: 3, rendelkezésre állás: 2. Biztonsági osztály: 4*

Az elektronikus levelezés adatainak érzékenysége a fájlszerverekhez hasonlóan széles skálán mozoghat. Tekintettel arra, hogy a szolgáltatás biztonsága titkosítás, illetve digitális aláírás nélkül meglehetően alacsony, ezért érzékeny adatok továbbítására inkább más módszer javasolt. Ugyanakkor elterjedt gyakorlat az egyes rendszerekből küldött automatizált levelek, értesítések, jelentések küldése, melyek tartalmazhatnak érzékeny adatokat.
Bizalmasság. Az elektronikus levelezés biztonsági besorolása annak adattartalma alapján határozható meg, és feltételezhetően az egyetemek e-mail forgalma összességében csak kis számban tartalmaz érzékeny adatot. Ugyanakkor az elektronikus levelekben vagy azok mellékleteiben bármely szakrendszerekből származó riport, jelszóemlékeztető, kétfaktoros azonosítási- vagy egyéb bizalmas adat szerepelhet, valamint az intézményi e-mail címek önmagukban is személyes adatnak minősülnek, az elektronikus levelezés bizalmasságának javasolt besorolása magas, legalább 4. A besorolás pontosságának javítása érdekében fel kell térképezni az érzékeny adatok küldését vagy fogadását végző rendszereket, azonosítani kell az általuk küldött és fogadott adatköröket, és meg kell határozni azok érzékenységét és mennyiségét.



14. ábra. Az elektronikus levelezés lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Sértetlenség: az elektronikus levelezés sértetlenségével szembeni elvárás intézményenként szintén eltérő lehet. A besorolás pontos meghatározásához rendszerenként meg kell határozni az e-mail rendszerbe kerülő adatok módosításának vagy elvesztésének kockázatát, melyek közül a legmagasabb adja a sértetlenség besorolását.

Rendelkezésre állás: az elektronikus levelezés rendelkezésre állásának besorolása szintén a küldött és fogadott adatok függvénye, és adott időszakban az átlagosnál akár magasabb is lehet. A rendelkezésre állás besorolását ezért szintén az intézményben működő rendszerekhez kapcsolódó folyamatok által megszabott határidők alapján kell meghatározni.

Sérülékenység esetén érintett rendszerek. A levelezési rendszer sérülékenysége esetén, amennyiben a levelek bizalmasságának sérülése feltételezhető, az adatok forrásául szolgáló rendszerek levélküldési funkciójának átmeneti leállítása indokolt. A levelező rendszer működési biztonságára a központi címtár és az esetleges webes levelező felület, valamint a postafiókok adminisztrációját biztosító felület sérülékenysége van kihatással. Ezek hibái esetén a levelezési rendszerrel kapcsolatos kockázat növekedése a védelmi eljárások megerősített szintre emelésével, a szolgáltatás elérhetőségének korlátozásával, végső esetben átmeneti felfüggesztésével érhető el.

Vezetői Információs Rendszer (VIR)

IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2*

A Vezetői Információs Rendszer (VIR) az egyes rendszerekből származó statisztikák előállításával segíti vezetői döntéstámogatást. Ideális működése során annak tartalma más szakrendszerek kumulált adatokat tartalmazó adatcsomagjai alapján épül fel, melyek rendszeres időközönként aktualizálásra kerülnek. A VIR rendszerek rendszerint nem tartalmaznak személyes adatokat. Az egyetemek jórésze közintézmény, melynek adatai az állampolgárok számára pl. egy közérdekű adatigénylés formájában megismerhetők, így a VIR-ben minimális mennyiségű érzékeny adat jelenik meg. Egy VIR sérülésekor fellépő kockázat leginkább a vezetői döntések támogatásának ellehetetlenülésében nyilvánul meg, melynek kezelésére az üzletfolytonossági terv, vagy a szükséges információk manuális úton történő előállítása adhat útmutatást.

Bizalmasság. Egy VIR jellemzően nem tárol személyes adatot, ugyanakkor abban szerepelhetnek olyan, pl. költségvetésre, bevételes tevékenységre, pályázati adatokra vonatkozó összesítések, melyek nyilvánosságra kerülése az intézménynek nem érdeke és nem minősülnek közérdekű adatnak sem.

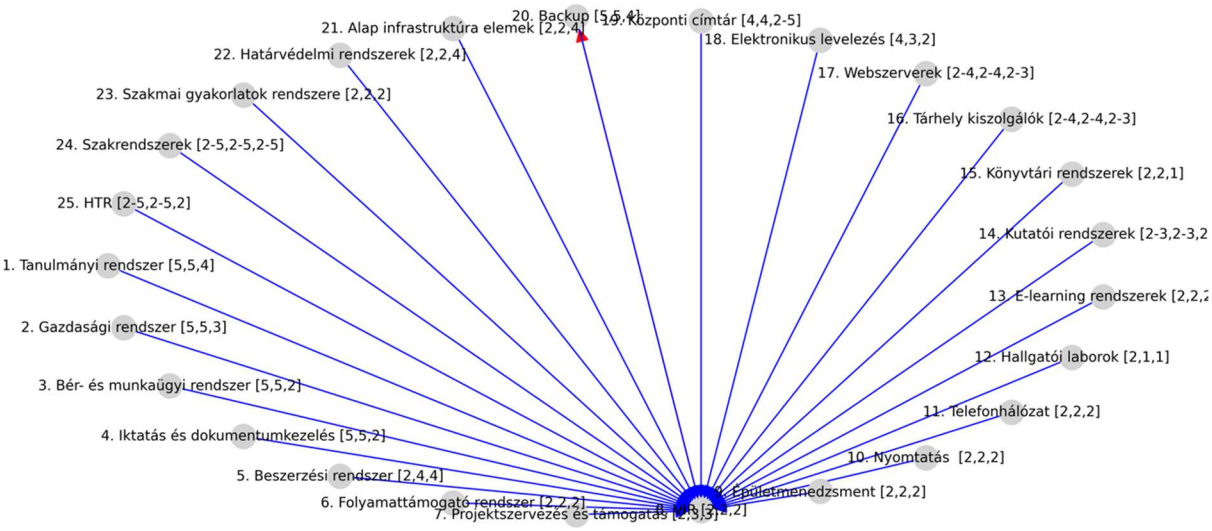
Sértetlenség. A VIR adatai jellemzően más rendszerekből származókon alapulnak, így azok újra előállíthatók. A rendszer adatainak rosszindulatú módosítása az eredeti adatok ismeretében felfedezhető, melynek támadói motivációja egy téves adatokon alapuló, ennél fogva helytelen vezetői döntés elérése lehet.

Rendelkezésre állás: a VIR rendszerek jellemzően nincsenek napi használatban, így kiesésük feltehetően nem gyakorol komoly hatást az intézmény működésére.

Bejövő adatok és hozzáférések. Egy VIR számos rendszerből fogadhat vagy kérhet le a statisztikák elkészítéséhez szükséges adatokat. Adatkapcsolatai korlátozódhatnak a már kumulált adatokból képzett jelentésekre, de előfordulhatnak olyan megoldások, melyben közvetlen hozzáférésük van az adatforrásként működő rendszerekhez, így kompromittálásuk során előfordulhat a VIR funkcionalitásától eltérő adatkezelés is. A VIR adatkapcsolatainak megvalósításának módja tehát alapvető az esetleges sérülése során fellépő kockázat mértékében, melyet az állandóan változó forrásrendszerek következtében szükséges módosítások is növelnek.

Kimenő adatok és hozzáférések. A VIR rendszerek jellemzően nincsenek kimenő adatkapcsolataik.

Sérülékenység esetén érintett rendszerek. Egy adatforrásként szolgáló rendszer sérülése a VIR aktualitása, esetleg érvényessége sérülésével járhat, melynek adatvédelmi szempontból valószínűleg nincs jelentős hatása.



15. ábra. A VIR lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Tanulmányi rendszer

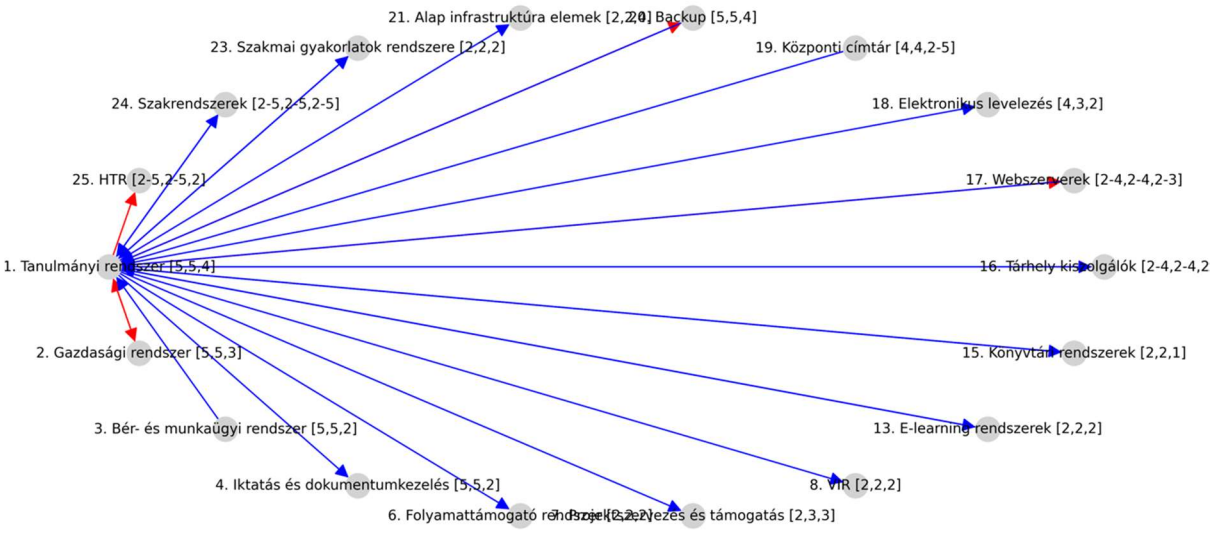
IBTV szerinti javasolt besorolás: Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 4. Biztonsági osztály: 5

A tanulmányi rendszer minden felsőoktatási intézmény esetében az SDA által fejlesztett és támogatott Neptun. Minden egyetem számára kötelező és nélkülözhetetlen rendszerelem, kiesése esetén számos jogszabályban előírt kötelezettség nem teljesíthető, sérül az állami támogatás elszámolásának folyamata, az alkalmazott modulok függvényében pedig meghiúsulhat a tandíjak befizetése, számlák kiállítása, küldése. Hiányában a FIR jelentések csak manuálisan lennének továbbíthatók, mely nagy mennyiségű plusz feladatot róna az intézmények tanulmányi ügyekekért felelős szervezeti egységeire. Kiesése esetén az intézmény csak az üzletfolytonossági tervben foglaltak szerint, manuális helyettesítő eljárásokkal képes ellátni fő profilja, az oktatás adminisztrációját, mely a szorgalmi időszakban kisebb, tantárgyfelvételi és a vizsgaidőszakban komolyabb fennakadást okoz. A rendszer hiányában nem adhatók ki igazolások a korábbi tanulmányokról és az intézmény részéről problémát jelent a kiadott diplomák igazolása is[44]. A tanulmányi rendszer az államilag támogatott félévek számának pontos meghatározásában is nélkülözhetetlen.

Bizalmasság. A rendszer bizalmasságának fenntartása alapvető elvárás minden felsőoktatási intézmény esetén. A rendszerben tárolt nagy mennyiségű személyes, és kisebb mennyiségű különleges adat az ibtv. szerinti alap besorolás alapján is a legmagasabb besorolást követeli meg.

[44] Az Oktatási Hivatal (OH) rendszeréből utóbbiak lekérdezhetők.

Sértetlenség. A rendszer sértetlenségének fenntartása szintén alapvető követelmény az intézmény számára. Bár adatainak egy része más szervezetek számára jelentések formájában átadásra kerül, jelentős részük csak a rendszerben áll rendelkezésre. A diplomák, vizsgaeredmények módosítására irányuló támadások csak elvétve fordultak elő, nemzetközi viszonylatban azonban ezek kimutatható motivációt jelentettek.
Rendelkezésre állás: a tanulmányi rendszer rendelkezésre állásának követelménye a különböző oktatási időszakokban eltérő, kiesése a tárgyfelvételi- és vizsga-, valamint a felvételi időszakban kevéssé tolerálható, míg a nyári időszakban, oktatási szünetekben akár több napos rendelkezésre állási problémák sem kritikusak.



16. ábra. A tanulmányi rendszer lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A rendszer számos forrásból fogadhat adatokat. A gazdasági rendszerhez a hallgatók különféle pénzügyi folyamatainak kezelése, ösztöndíjak, tandíjak, vizsgadíjak, kollégiumi díjak és egyéb befizetések fogadása mellett számos további ponton kapcsolódhat. A szakmai gyakorlatok teljesítésével kapcsolatos információk az erre a célra szolgáló rendszerből, az érdemjegyek, jelenléti adatok pedig az e-learning rendszerből érkezhetnek.
A szakrendszerekből változatos adatkör érkezhet. A Neptun fejlesztésének folyamata jól mutatja, hogy a fejlesztő törekszik minél több, az oktatáshoz kötődő feladatot lefedő modul kifejlesztésére, így az elmúlt évek oktatástámogatási funkciói mellett az e-learning modul kialakítása is napirenden van; ez a tendencia hosszú távon csökkenti a külső rendszerek kapcsolódási pontjainak számát így a Neptun a jövőben várhatóan egy jóval magasabb komplexitású rendszerré fejlődik.

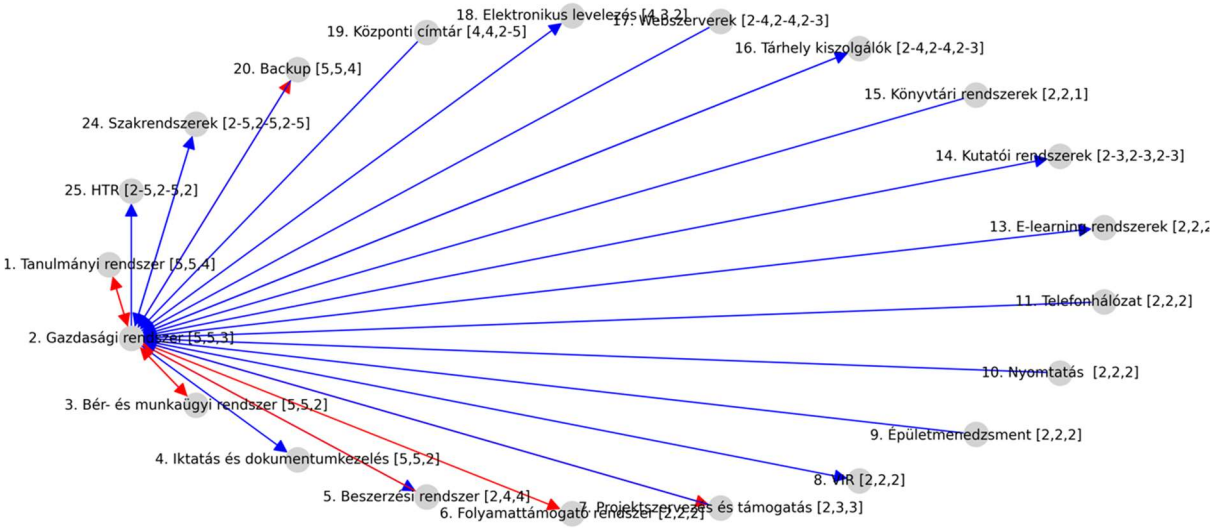
A bejövő kapcsolatok terén az kiemelt lehet a címtár szerepe az azonosítási feladatok, a webszerverek a hallgatói és oktatói feladatok ellátására, de a tárhelyszolgáltatási és mentési rendszerek kapcsolata is kulcsfontosságú a tanulmányi rendszer esetében.
Kimenő adatok és hozzáférések. Bár a Neptun üzemeltetése igénybe vehető egyfajta felhőszolgáltatásként is, számos egyetem inkább saját infrastruktúráján működteti azért, hogy azzal a rendszert működtető adatbázisra és a hozzá tartozó Application Programming Interface-re (API) épülő további szolgáltatásokat üzemeltessen. Ezek jellemzően a Neptun saját felhasználói bázisán alapuló azonosítási szolgáltatásokat kínálnak, de számos más rendszer számára adatforrásként működhetnek. Több egyetem hozott létre a hallgatói lemorzsolódás megelőzését célzó, különféle támogató rendszereket, vezetői információs rendszert, de a rendszer működésképtelensége több intézmény esetében megbénítaná az arra tervezett EduRoam és az EduID azonosítási funkcióinak működését a hallgatók számára. A távolléti oktatás menedzsmentjének támogatására több egyetem fejlesztett ki kommunikációs- és adatcsere interfészeket különféle LMS-ekkel (pl. a Teams és Moodle adminisztrációjának részleges automatizálására). A felsoroltak mellett a Neptun szoros adatkapcsolatban működik a felsőoktatásban általánosan alkalmazott, szintén az SDA által fejlesztett Poszeidon iktatási rendszerrel.
A tanulmányi rendszer elvesztése, vagy adatainak nyilvánosságra kerülése komoly reputációs problémát okozna az intézmények számára, ahogyan azt 2022-ben a szintén az SDA fejlesztésében levő Kréta rendszert ért incidens esete már megmutatta. A rendszer támadására már több alkalommal volt példa – a nyilvánosságra került esetek többnyire a rendszerbe épített üzenetküldési szolgáltatás támadásáról szólnak [100]. A rendszer nyitottsága a publikus internet felé, a tárolt adatok értéke és az ismert támadási motivációk a Neptunt a felsőoktatási rendszerek leginkább támadott célpontjává teszik. Feltörése vagy sérülékenysége adatkapcsolatai révén kihatna az adatkapcsolati gráfban szereplő további rendszerekre, az iktatástól a projekttámogatáson át a könyvtári rendszerekre és az e-learning-re is, melyek kockázatelemzését és biztonsági besorolását az új helyzetnek megfelelően felül kell vizsgálni.

Gazdasági rendszer

IBTV szerinti javasolt besorolás: *Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 3. Biztonsági osztály: 5*

A gazdasági rendszereket a dokumentumelemzés során vizsgált szabályzatok eltérően értelmezték. A gazdasági szervezeti egységek számos területből állnak, melyek munkáját különböző alrendszerek segítik, melyek közül a leggyakoribbak a beszerzési, szerződésnyilvántartó és folyamattámogató rendszerek, melyeket a személy- és bérügyi rendszerek kivételével a gazdasági

rendszerbe soroltam be. Jelenlegi működésük és központosításuk az intézmény fenntartójától függően eltérő. A vagyonkezelő alapítványok által fenntartott egyetemek többnyire külső szolgáltató által üzemeltetett, SAP alapú integrált rendszer központosított megoldását alkalmazzák. Kivonási terv vagy stratégia, lokális adatmentés, archívum vagy helyi tartalék rendszer nem áll az rendelkezésükre, viszont a rendszerrel kapcsolatos felelősségi szintjük is alacsonyabb. A magán- és állami egyetemeknek van mozgásterük a számukra megfelelő rendszer megválasztásában és dönthetnek arról, hogy milyen infrastruktúrán milyen felelősségi körök mentén üzemeltetik azokat.



17. ábra. A gazdasági rendszer lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bizalmasság. Az állami fenntartású egyetemek gazdasági és működési adatai nyilvánosak, közbeszerzésre kötelezettek, így a rendszer adatainak bizalmassági követelményszintje elmarad a gazdasági szférában érvényes szinttől, ugyanakkor a bér- és egyéb címen történő kifizetések adatai mellett személyes adatokat is tartalmaz, ezért a legmagasabb szintű bizalmassági kritériumoknak kell megfelelnie.

Sértetlenség: a rendszer sértetlensége elemi fontosságú, az intézmény gazdálkodásának, kifizetéseinek alapját képező rendszer adatainak módosítása a támadók számára konkrét gazdasági előnyt, pl. jogtalan kifizetéseket eredményezhet. Adatainak sérülése vagy elvesztése az intézmény számára komoly anyagi és reputációs veszteséget okozna.

Rendelkezésre állás: a rendszer kiesése vagy elvesztése esetén az intézmény működése komoly zavart szenved, nem tudja ellátni a bejövő és kimenő számláinak kezelését, nem tud eleget tenni

adatszolgáltatási kötelezettségeinek, és az állam felé irányuló kötelező adatközléseknek függetlenül attól, hogy az saját infrastruktúráján vagy szolgáltatásként működik. Így a gazdasági rendszer szerepe a felsőoktatási intézményekben kiemelt, kiesése legfeljebb minimális ideig tolerálható.

Bejövő adatok és hozzáférések elsősorban a tanulmányi, bér és munkaügyi, beszerzési, valamint a projektszervezés és támogatási rendszer irányából érkeznek. Opcionális kapcsolatot jelenthetnek az épületmenedzsment rendszer adatai a nagy mennyiségű javítási és karbantartási feladatok elszámolásának automatikus folyamatának támogatására. A nyomtatási rendszerből az egyes szervezeti egységek nyomtatási költségelszámolásának alapjául szolgáló elszámolási adatai kerülhetnek átadásra. Szintén elszámolási adatok érkezhetnek a telefonhálózat forgalomfigyelő rendszeréből, késedelmi, és egyéb díjakra vonatkozók a könyvtári rendszerekből. Általános adatkapcsolat működhet a tárhely kiszolgálókkal, webszerverekkel, azonosítási szolgáltatást vehet igénybe a központi címtártól, adatait a mentés során a backup rendszerbe mentik. A felsoroltakon túl az egyes szakrendszerekkel kialakított kapcsolata intézményenként eltérő lehet.

A gazdasági rendszer sérülékenysége, vagy egy azt ért incidens esetén az érintett rendszerek száma más rendszerekkel történő összevetésben meglehetősen magas. A rendszer adatkapcsolatot tarthat fenn a tanulmányi rendszerrel a már ismertetett pénzügyi és egyéb adatok átadása érdekében és a bér- és munkaügyi rendszerrel is. A folyamattámogatási, iktatási és projektszervezési rendszer adatkapcsolattal rendelkezhet vagy adatokat fogadhat a gazdasági rendszertől. További adatkapcsolatok valószínűsíthetők a beszerzési rendszerrel, valamint az e-learning és HTR rendszerekkel is. Amennyiben az intézmény működtet vezetői információs rendszert, annak egyik elsődleges adatforrása valószínűsíthetően a gazdasági rendszer, de az elektronikus levelezés, egyes szakrendszerek, valamint a kutatói rendszerek opcionális kapcsolata is lehetséges.

Bér- és munkaügyi rendszer

Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 3. Biztonsági osztály: 5

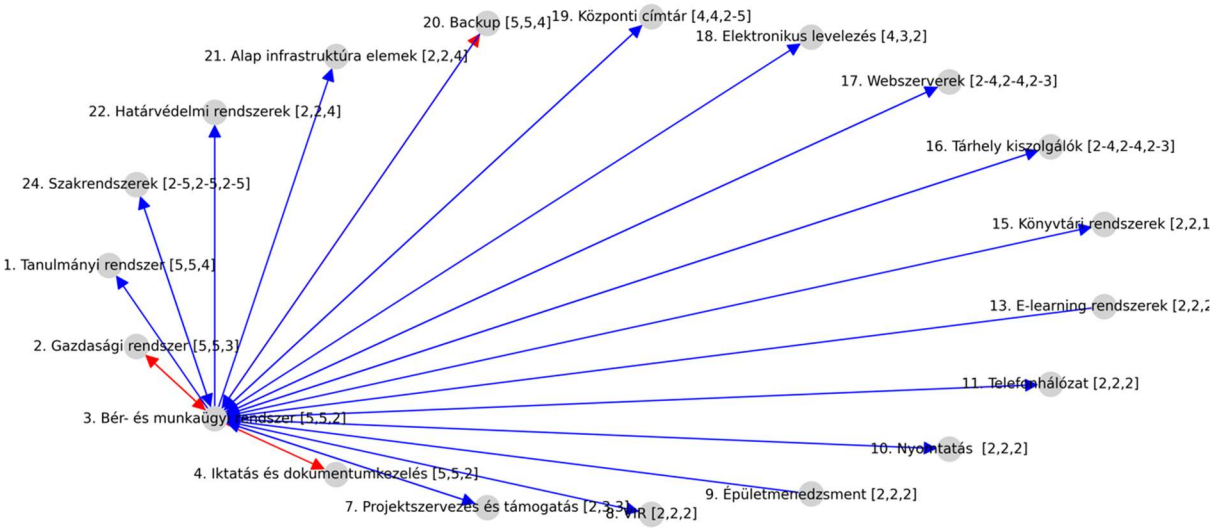
Bár a bér- és munkaügyi rendszerek funkciói jelentős összefonódást mutatnak, azok nem feltétlenül működnek egyetlen integrált rendszerként, és mivel eltérő jogszabályi feltételek vonatkoznak az állami és az egyházi fenntartású intézményekre, számos példát találunk arra, hogy az egyes intézményekben eltérő szoftver környezet felelős ezen területek támogatásáért. Mivel a bérrendszerek funkcióinak alapját a munka- és személyügyi adatok adják, ezért vizsgálatuk és biztonsági besorolásuk egy rendszerként javasolt.

A bér- és munkaügyi rendszerek fő feladata a munkatársak személyes- és a munkavégzéssel kapcsolatos egyéb adatainak nyilvántartása mellett az illetmények és kapcsolódó adatok, pl. jelenléti ívek, szabadságok, gyed stb. rögzítése. Tipikus a munkavállalóhoz kapcsolódó egyéb dokumentumok rögzítésének lehetősége is (nyelvvizsgák, végzettségek dokumentumai). Különleges adatot csak a munkavégzéssel összefüggésben tárolnak, melynek előfordulása e rendszerre nézve legfeljebb eseti jellegű. Ennek adatbázisa alapján történik meg a bérek számfejtése, a nyugdíj és társadalombiztosítási adatok jelentése. Kiegészítő funkcióik révén támogatást nyújtanak a teljesítményértékelésben, új munkatársak toborzásában, de a projektmunkák során támogatást nyújthatnak az ideális személyek kiválasztásában is.

Bizalmasság. A bér- és munkaügyi rendszerek esetében is kiemelt fontosságú a bizalmasság fenntartása. Egy esetleges adatszivárgás esetén nagymennyiségű személyes adat kerülhet nyilvánosságra, így a rendszer védelmére különösen nagy hangsúlyt kell helyezni.

Sértetlenség. A rendszer adatainak sérülése vagy illetéktelen megváltoztatása gazdasági előnyt nyújthat egy támadó számára, egy esetleges belső támadó képes lehet akár a fizetési adatok módosítására is. A közvetlen haszonszerzés lehetősége a bér- és munkaügyi rendszer számára magas szintű védelmet követel meg.

Rendelkezésre állás: a rendelkezésre állás sérülésének hatása a tanulmányi rendszerhez hasonlóan időszakonként eltérő. Az egyetemek személy- és munkaügyi szervezeti egységeinek folyamatos feladatvégzésének ellehetetlenülése viszonylag rövid ideig tolerálható, a bérek utalásának időben történő elvégzése pedig a legtöbb intézményben szigorú határidőhöz kötött,.



18. ábra. A bér- és munkaügyi rendszer lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. Ezek a rendszerek szoros kapcsolatban állnak a gazdasági rendszerekkel, projektfeladatok elszámolásához a projektszervezési és támogatási rendszerrel. Opcionális kapcsolataik létezhetnek az épületmenedzsmenttel (pl. oktatók, dolgozók munkahelységeinek nyilvántartásáért), automatizált kapcsolataik működhetnek az e-learning rendszerekkel a különféle rendszeres és kötelező, tipikusan tűzvédelmi vagy munkavédelmi oktatások lefolytatása és nyilvántartása érdekében. Általános kapcsolataik lehetnek a tárhely kiszolgálókkal és webszerverekkel. Azonosítási szolgáltatásokat ezek a rendszerek is a központi címtártól vehetnek igénybe, a rendszer mentését a backup rendszerek végzik.
Kimenő adatok és hozzáférések. A rendszerből számos más rendszer vesz át adatokat vagy alkalmaz automatizált kapcsolatokat. A gazdasági rendszer, az iktatás, a projektszervezési rendszer kapcsolatai a legjellemzőbbek, de az oktatók és dolgozók adatait a Neptun személyügyi modulja számára is átadhatják. A munkaügy munkatársai láthatják el a címtár karbantartását a munkaköri változások, be- és kilépések esetén, de erre a munkaügyi rendszer automatizált kapcsolatot is fenntarthat. A személyi változások adminisztrálása során bekövetkező változások más rendszerekre is hatással lehetnek, a különféle hálózati hozzáférések, VPN kapcsolatok, vezetéknélküli hálózatok terén. A VIR-ben számos, a bér- és munkaügyi rendszeren alapuló döntéstámogatást segítő statisztika jeleníthető meg.

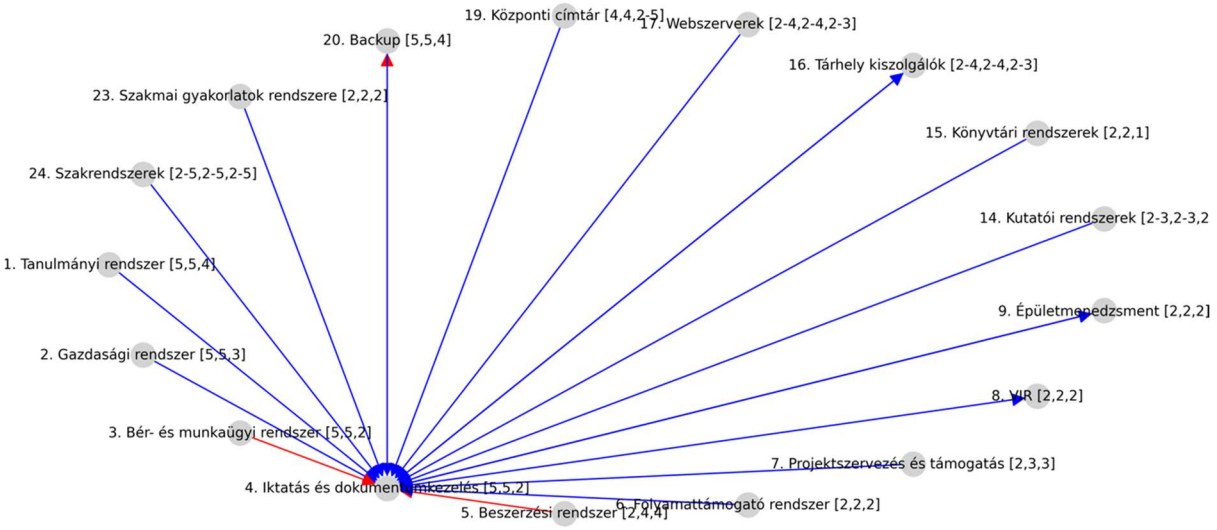
Iktatás és dokumentumkezelés

Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 2. Biztonsági osztály: 5

A vizsgált szabályzatok az iktatást és a dokumentumkezelést elkülönült feladatként írták le, ugyanakkor, mivel funkcióik megközelítőleg azonosak és a kezelt adatok alapján besorolásuk sem különbözik, gyakran Enterprise Content Management (ECM) néven említik. Adatbázisukban az iktatási szabályzatban foglaltaknak megfelelően tárolásra kerül az intézmény papír alapú hivatalos levelezésének egy része, az ügyintézési folyamatok, munka- és megbízási szerződések és számos más dokumentum, mely az intézményben zajló folyamatok kezelésében és nyomon követésében elengedhetetlen.

Bizalmasság. A rögzített dokumentumok számos személyes adatot tartalmaznak, a jelentős részben belső vagy bizalmas információkat, titoktartási szerződéssel védett dokumentumokat tartalmazó rendszer szivárgása vagy nyilvánosságra kerülése az intézmény reputációját jelentősen rontaná. Ez feltehetően peres eljárások alapjául szolgálhatna, és az intézmény számos területen szenvedhetne el versenyhátrányt egy így kialakult helyzetben.

Sértetlenség. A rendszer sértetlenségének szintje az abban tárolt adatok fontosságából, adatvesztés esetén pedig a pótlásuk alapjául szolgáló alternatív források, pl. fizikai irattárak rendelkezésre állásából kerül meghatározásra. E rendszer esetében is elmondható, hogy a kisebb egyetemek, illetve az iktatási feladatokat a hagyományos manuális iratkezeléssel párosító szervezetek esetében ez a szint alacsonyabban határozandó meg.
Rendelkezésre állás. Sérülése esetén a feltorlódó dokumentumok manuális kezelése és utólagos bevitele rövidebb ideig feltehetően kezelhető az intézmények számára; ez indokolja az alacsony besorolási értéket.



19. ábra. Az iktatás és dokumentumkezelési rendszer lehetséges adatkapcsolatai.
Forrás: saját szerkesztés.

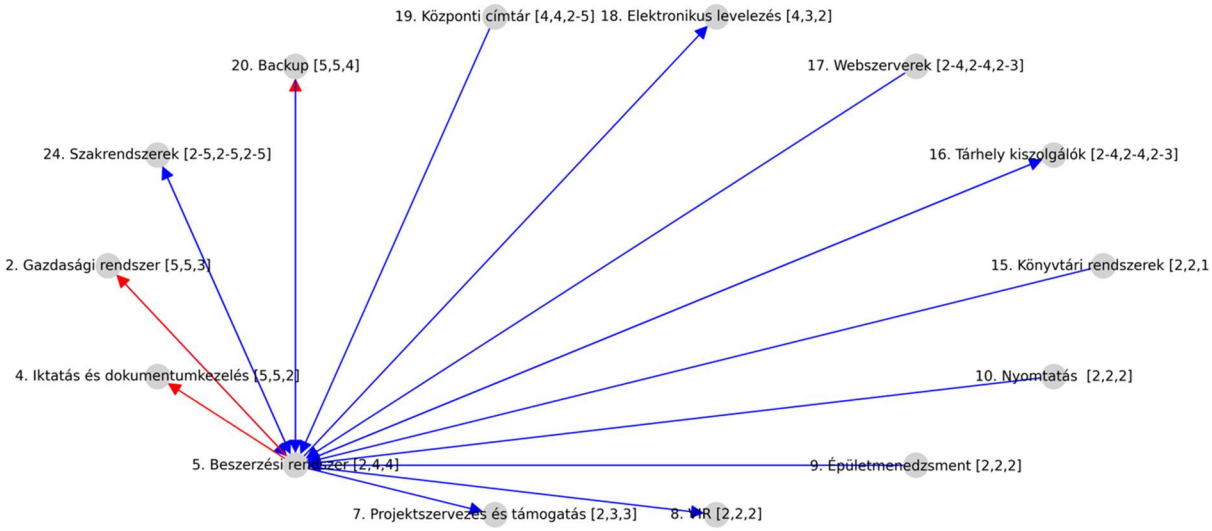
Bejövő adatok és hozzáférések. Az iktatási rendszer számos más, magas védelmi szintű rendszerből fogad adatokat. A tanulmányi rendszerben előállított elektronikus dokumentumok, döntések jegyzőkönyvei mellett számos folyamat generálhat az iktatási rendszerben rögzítendő tételeket. A gazdasági rendszerrel hasonló kapcsolat állhat fenn: az abban keletkező dokumentumok automatikus iktatásától és a szerződésektől a fizetési felszólításokon át az eszközök átadás-átvételi dokumentumáig számtalan irat kerülhet az automatizált folyamatok eredményeként az iktatási rendszerbe. A bér- és munkaügyi rendszer szintén nagymennyiségű hivatalos iratot állít elő, melyek az iktatási folyamat egyszerűsítése érdekében szintén automatizálhatók. A hallgatók szakmai gyakorlatának rendszere, a könyvtár, a kutatói rendszerek, épületmenedzsment, projektszervezés és támogatási rendszer, a folyamattámogatási rendszerekhez szintén kapcsolódhatnak automatizált iktatási feladatok. Amennyiben a rendszerhez web alapú kezelőfelület

is rendelkezésre áll, a webszerverekkel is adatkapcsolatban van, a központi címtár szabályozza rendszerbe történő bejelentkezéseket. Lehetséges bejövő kapcsolatot jelenthetnek a különböző szakrendszerek, pl. más, bevételes tevékenységek kiszolgáló rendszerei, melyek szintén adatokat adhatnak át a beszerzési rendszer számára.
Kimenő adatok és hozzáférések. A rendszer sokkal kisebb számú kimenő adatkapcsolattal rendelkezik. A tárhely kiszolgálókat a rendszer által generált vagy más forrásban keletkezett fájlok tárolására alkalmazhatják. A VIR valószínűsíthetően az iktatási folyamatra, az ügyek számára és jellegére, esetleg a nyitott ügyekre vonatkozó összesített statisztikákat kap vagy állít elő. A rendszer adatait a mentési rendszerek tartalmazzák.

Beszerzési rendszer

IBTV szerinti javasolt besorolás: *Bizalmasság: 2, sértetlenség: 4, rendelkezésre állás: 4. Biztonsági osztály: 4*

Az egyetemek a nagy számú beszerzési feladat, és a közbeszerzési kötelezettség összetett eljárási folyamatainak kezelését gyakran beszerzési rendszerrel támogatják. A rendszerek adattartalma elsősorban a beszerzendő eszközökre, beszállítókra, és a beszerzések összegére terjed ki.
Bizalmasság. A felsőoktatási intézmények közbeszerzésre kötelezettek, beszerzéseik nyilvánosak, a beszállítóik cégek, így a támogató rendszer alig tartalmaz személyes adatot. Tartalmuk nyilvánosságra kerülésével bekövetkező kockázat minimális, legálisan közérdekű adatigénylés útján részben megszerezhető. A beszerzések tartalmának illetéktelenek számára történő megismerése ugyanakkor számos esetben nem kívánatos: a beszerzendő termékek, azok fajtáinak és árának ismeretében a beszállítók kartell, vagy a piacitól eltérő árakat alakíthatnak ki, a beszerzett informatikai eszközök és alkatrészek, azok javítási története, a karbantartási szerződésekben foglalt eszközlista OSINT megismerhetősége az intézményeknek nem érdeke.
Sértetlenség. A rendszer adatainak sértetlensége a rendszer működésének alapfeltétele, illetéktelen módosításának és kiesésének következménye a különböző revíziók, pályázati ellenőrzések során többletmunka, akár pályázati források visszafizetési kötelezettsége is lehet.
Rendelkezésre állás. A rendszer működésképtelenségének következményei az üzletfolytonossági tervben foglaltak függvényében változhatnak.



20. ábra. A beszerzési rendszer lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Kimenő adatok és hozzáférések. A rendszer lehetséges kimenő adatkapcsolatai a beszerzések során végrehajtandó további folyamatok elvégzésére irányulnak. A gazdasági rendszerbe főként a beszerzési folyamatok lezárását követő számlázási és fizetési adatok, az anyaggazdálkodási alrendszer felé a leltár, a garanciális kötelezettségek nyilvántartásához szükséges, valamint a fenntartási időszakra vonatkozó adatok kerülhetnek. A projekttervezés és támogatási rendszer részére a pályázati- és projekt finanszírozású beszerzések elszámolásához épülhet fel adatkapcsolat. A tárhely kiszolgálókat a beszerzési folyamat során keletkező fájlok projektmappákban történő összegyűjtésére alkalmazhatják, melyek változatos, a beszerzésekhez kapcsolódó adatokat tartalmazhatnak. A rendszer manuális vagy automatizált értesítéseket küldhet az elektronikus levelezési rendszeren keresztül. A különféle szakrendszerekkel fennálló esetleges adatkapcsolatot az intézményen belül működő egyéb szakrendszerek függvényében kell felkutatni.

Folyamattámogató rendszer

IBTV szerinti javasolt besorolás: *Bizalmasság: 2, sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2*

A felsőoktatási intézmények egy része folyamataik kezelésére valamilyen általános célú folyamattámogató-rendszert alkalmaz[45]. Ezekben egy megfelelően képzett informatikai szakember képes a folyamatok definiálásra, az abban résztvevők szerepköreinek meghatározására, az alá-

[45] Több egyetem esetében ez a Modulo.

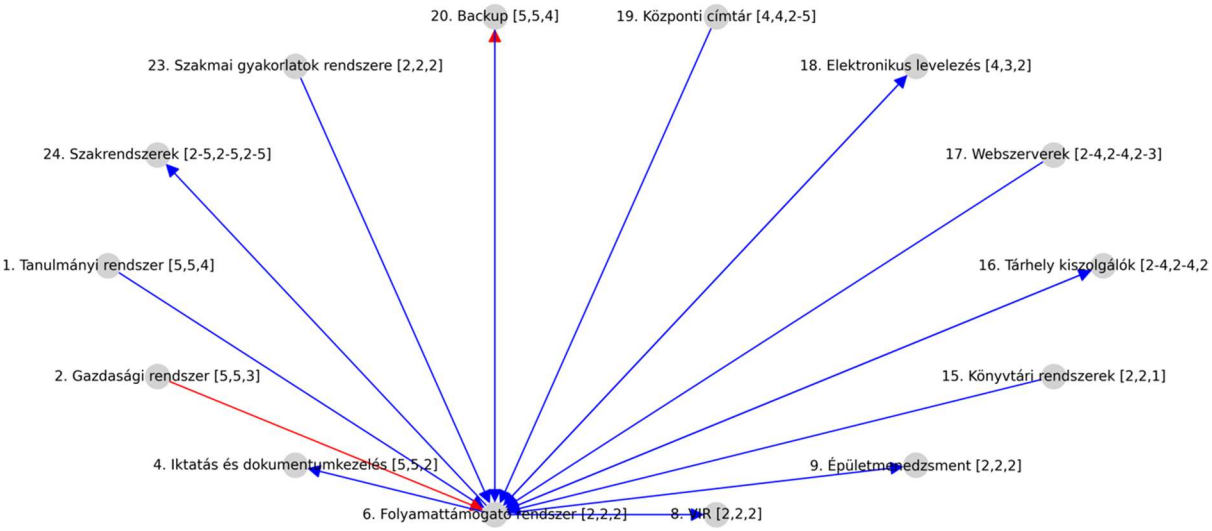
írási sor kialakítására; alkalmazásával a belső ügyviteli folyamatok egységesíthetők és automatizálhatók a domain igényléstől a kiutazási igények lebonyolításáig. Azonosítási szolgáltatása a jellemzően központi címtárra alapozva történik, a tárolt személyes adatok mennyisége pedig a kezelt folyamatok függvénye. Besorolását nagyban befolyásolja az abban megvalósított funkciók bizalmassági, sértetlenségi és rendelkezésre állási követelménye, így konkrét javaslat csak a leggyakoribb, általános esetre adható meg.

Bizalmasság. A folyamatkezelés bizalmassági besorolását az abban tárolt adatok mennyiségének és érzékenységének maximuma határozza meg. Újabb folyamatok bevezetésekor a bizalmasság besorolását felül kell vizsgálni.

Sértetlenség. Az érvényben levő jogszabályok alapján a folyamatkezelési eljárás lezárásakor a keletkező dokumentumokat adott ügytípus esetén mindenképp nyomtatni, majd az érintettek aláírása után azokat iktatni kell. Bár az elektronikus aláírást támogató rendszerek esetén ez részben elhagyható, az ügyiratkezelés során a rendszer adatai más forrásban is gyakran rendelkezésre állnak. A rendszer sértetlenségének ibtv. szerinti besorolása a fentiek mellett az abban tárolt kis mennyiségű személyes adat és az ügymenet személyes ellenőrzése okán is alacsony, de ebben a kezelt folyamatok és adataik függvényében eltérések állhatnak fenn.

Rendelkezésre állás. Általános tapasztalat, hogy a folyamatok automatizálásnak alapját azok korábbi, papíralapú eljárásai alkotják, ezért az ügykezelés azok hagyományos útján is elvégezhetők, a kezelt ügyek pedig az intézmény szempontjából jellemzően nem kritikus fontosságúak. Így a rendszer rendelkezésre állásának kisebb tartamú sérülése nem kritikus az intézmények számára.

Bejövő adatok és hozzáférések. A folyamattámogató rendszer számos más rendszerrel építhet ki adatkapcsolatot. Tipikusak lehetnek a tanulmányi rendszerből indított folyamatok, a gazdasági és beszerzési rendszerek, könyvtári rendszerek egyes folyamatai. A tárhely kiszolgálók, webszerverek, az elektronikus levelezés és mentési rendszerek általános kapcsolatai mellett a központi címtár e rendszer esetében is elláthat azonosítási szolgáltatásokat.



21. ábra. A folyamattámogató rendszer lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

A kimenő adatok és hozzáférések elsősorban az iktatási rendszer felé irányulnak, a különféle hibák bejelentő űrlapjai az épületmenedzsment rendszerbe küldhetnek automatikusan adatokat. A rendszer adatainak mentése szintén a backup rendszerbe történik. A VIR, a tárhely kiszolgálók, az elektronikus levelezés és a szakrendszerek kapcsolata opcionális.

Projektszervezés és támogatás

IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 3, rendelkezésre állás: 3. Biztonsági osztály: 3*

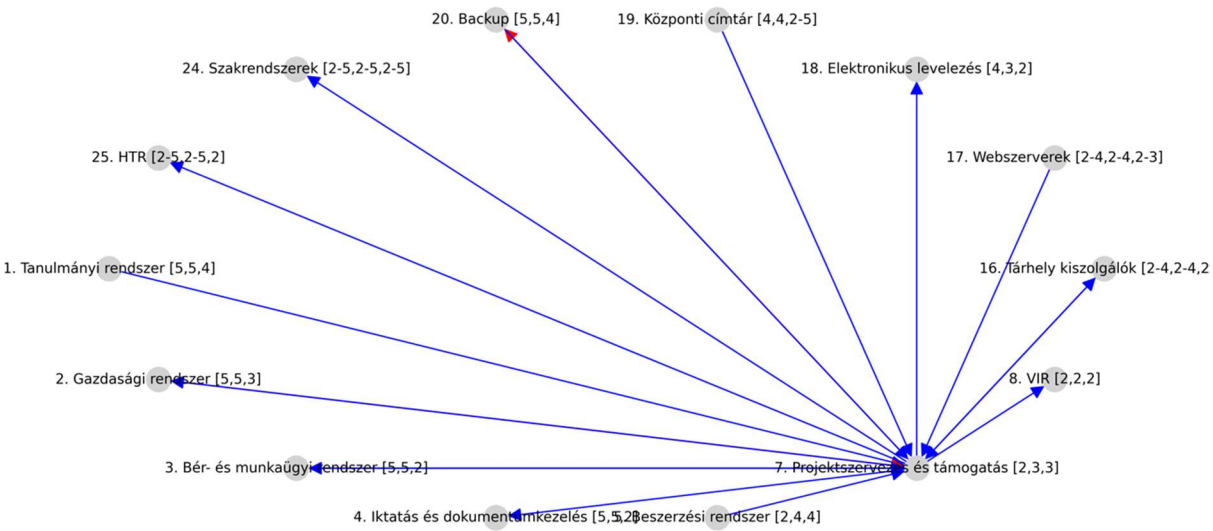
Az egyetemek számára létfontosságú a különféle pályázati erőforrások megszerzése, a sikeres pályázati anyagok előállítása és benyújtása, a pályázati indikátorok teljesítésének nyilvántartása, azok gazdasági vonatkozásai, utóéletével és lezárásával kapcsolatos teendők ellátása. A pályázatokkal kapcsolatos információk ugyanakkor jórészt nyilvánosak, ez az adattartalom nem indokol magas bizalmassági besorolást. A pályázati források értéke a korábbi években egyes egyetemek esetében a teljes költségvetés jelentős részét képezte, így a projektszervezést támogató rendszerek sérülése vagy a rendelkezésre állásának kritikus időpontban történő elvesztése nem csak a pályázatok előkészítési időszakában, hanem a megvalósítási és az elszámolási szakaszban is súlyos anyagi következményekkel járhat.

Bizalmasság. A rendszer adatai pályázatok változatos szakmai tartalma miatt intézményenként eltérőek lehetnek. A pályázatok pénzügyi elszámolásai, az abban dolgozók kifizetései, a teljesítési igazolások mellett más, ezekhez kapcsolódó egyéb adatok érzékeny, részben személyes

adatok, melynek védelme minden intézmény elemi érdeke. Ugyanakkor az állami finanszírozású intézmények működési adatai nyilvánosak, közérdekű adatigényléssel részben megismerhetők, így a rendszerben tárolt teljes adatkör bizalmassági szintje alacsony marad.

Sértetlenség. A rendszerben tárolt adatok célja a projektek működésének biztosítása, az anyagi erőforrások menedzsmentje és az elszámolások határidőre történő lebonyolítása mellett a pályázatban résztvevő személyekkel kapcsolatos előírások teljesítésének támogatása. A feladatok ellátásának alapfeltétele a rendszer sértetlensége, és bár manuális úton a legtöbb funkció kiesése pótolható, azok jelentős idő-, munkaerő- és anyagi erőforrástöbblet igénnyel járhatnak.

Rendelkezésre állás. A rendszerrel szemben támasztott elvárások alapján határozható meg a rendelkezésre állás mértéke is, melyet a futó és fenntartási időben levő pályázatok száma és jellege is befolyásol. A rendszer kisebb időtartamú kiesése általában tolerálható az intézmények többsége számára.



22. ábra. A projektszervezés és támogatási rendszer lehetséges adatkapcsolatai.
Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A projektszervezési és támogatási rendszer elsősorban a tanulmányi, gazdasági, bér és munkaügyi, valamint a beszerzési rendszerrel állhat adatkapcsolatban főként a projektek személyi- és elszámolási feladatainak ellátásának céljából.

Kimenő adatok és hozzáférések. A rendszer adatokkapcsolattal rendelkezhet a gazdasági rendszerrel és az iktatással. Az elektronikus levelezés alkalmazása tipikus a projektfeladatok ellátása során, a VIR pedig elsősorban a projektfinanszírozás és előrehaladás jelentéseivel támogatja a vezetői döntéseket. A rendszer adatokat küldhet az egyes szakrendszerek számára, a

HTR felé pedig a hallgatók számára nyújthat tájékoztatást az őket érintő projektekkel kapcsolatban.
A rendszer és adatainak mentését és helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek.

Épületmenedzsment

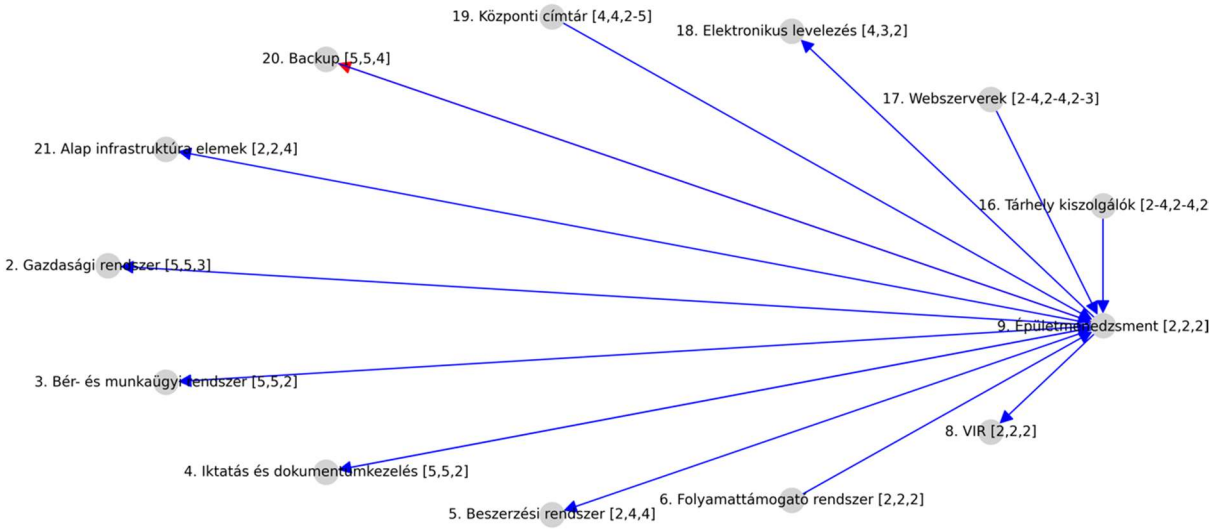
IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2*

Az épületmenedzsment rendszerek a műszaki üzemeltetés rendkívül összetett feladatkörének ellátását támogatják, főbb funkcióik a teljesség igénye nélkül: épületek nyilvántartása, berendezések időszakos és rendszeres karbantartásának nyilvántartása és figyelmeztetés a kötelező karbantartások elvégzésére, helpdesk szolgáltatás a hibák bejelentésére, riasztó-, beléptető- és kamerarendszerek menedzsmentje, kulcskezelés, hivatali gépkocsik üzemeltetése, gazdasági döntések háttértámogatása stb. Tekintettel arra, hogy a magyar egyetemek egy része különböző településeken számos ingatlannal rendelkezik, informatikai háttértámogatás hiányában az épületmenedzsment feladatokat csak manuális úton, kézi nyilvántartásokkal is képes lenne ellátni. Egy ilyen rendszer általában csak minimális mennyiségű személyes adatot tartalmaz, ugyanakkor kiesése egyes elemek hibás működését, karbantartási feladatok elmaradását, esetleg hatósági eljárást és pénzbüntetést vonhat maga után.

Bizalmasság. Az épületmenedzsment rendszerek bizalmassági követelményeit a gyakorlatban elsősorban nem a személyes adatok, hanem a különféle támadások alapjául szolgáló információk nagy mennyisége határozza meg. A rendszerek szivárgása esetén nyilvánosságra kerülhet az intézményben működő különböző műszaki berendezések típusa, helye, továbbá lehetséges hálózati kapcsolatainak ismeretében azok támadási pontjai is.

Sértetlenség. A rendszer több más rendszer számára szolgáltat adatokat, a különféle gazdasági elszámolások támogatása és a javítási feladatok automatizálása mellett akár épületgépészeti berendezések vezérlését, működésének szabályzását is kezdeményezheti. A sértetlenség besorolását ezen kapcsolatok ismeretében szükséges meghatározni.

Rendelkezésre állás. A rendszer részleges kiesésének következményeit a kieső funkcionalitás következményei határozzák meg. Az alapfunkciók részleges vagy időleges elérhetetlensége a legtöbb esetben nem kritikus.



23. ábra. Az épületmenedzsment lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A rendszer adatkapcsolatban állhat a folyamattámogató (vagy hibabejelentő) rendszerrel, melyen keresztül karbantartási vagy javítási igények kezdeményezhetők.

Kimenő adatok és hozzáférések. Az épületek fenntartásának feladatai jelentős részben a gazdasági és beszerzési rendszerhez kötődnek, melynek automatizálását egy jól megtervezett rendszer folyamatos adatkapcsolatai révén képes elvégezni. Az elvégzett feladatok iktatása, az érvényben levő szerződések adatai az iktatási rendszerből származhatnak. A szobák kiosztását, a szabad és foglalt helységek adatait megoszthatja a munkaügyi rendszerrel. A vezetői döntések támogatására változatos statisztikákat adhat át a vezetői információs rendszernek. Amennyiben működnek épületautomatizálási funkciók, az alap infrastruktúra elemeivel kiépített adatkapcsolatok is működhetnek.

A rendszer és adatainak mentését és helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók, valamint a webes felületen működő rendszerek esetében webszerverek is közreműködhetnek.

Nyomtatás

IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2*

A nyomtatási rendszerek az esetek túlnyomó többségében nem kezelnek személyes adatokat, azonosítási funkcióikat a címtárszolgáltatáson keresztül valósítják meg. Ezért biztonsági besorolásuk alacsony. Kivételt azok a valószínűleg ritka részterületek jelenthetnek, melyek esetén a nyomtatás rendelkezésre állásának kiesése súlyos következményekkel jár, vagy a nyomtatási alrendszer központi spool-jában tárolt érzékeny dokumentumok kiszivárgása esetén adatsértés valósul meg.

Bizalmasság. A nyomtatási alrendszeren áthaladó dokumentumok jellege határozza meg. Egy központi nyomtatáskezelő rendszer sérülékenysége esetén fennáll az elvi lehetősége a nyomtatásra küldött dokumentumok szivárgásának, mely érzékeny adatokat tartalmazhat. Személyes vagy más adatok tömeges sérülésének valószínűsége a nyomtatási rendszer esetén alacsony. Amennyiben a nyomtatók szkennelési feladatok ellátására is képesek, a besorolást ennek figyelembevételével kell megtenni. A központi nyomtatáskezelők által kezelt személyes adatok mennyiségét megvalósításonként érdemes vizsgálni, a gyakorlatban a gyártók az azonosítási és jogosultságkezelési feladatok megvalósításakor a címtárszolgáltatás alkalmazására törekszenek.

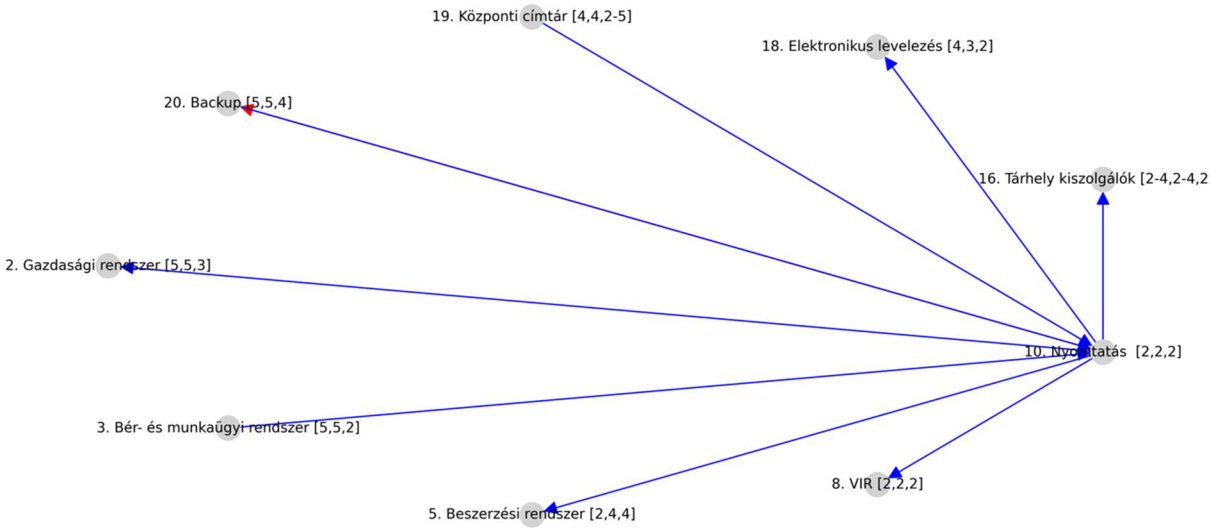
Sértetlenség. Nem találtam a nyomtatási rendszerekben tárolt adatok megváltoztatására irányuló incidenst, ezért ennek biztonsági besorolásának javasolt szintje 2.

Rendelkezésre állás. Az egyetemek nyomtatási igénye rendszerint magas, így a rendszer részleges kiesése is problémát jelent számukra, melynek kockázata helyi, vagy tartalék berendezések üzemben tartásával csökkenthető.

Bejövő adatok és hozzáférések. A rendszer nem rendelkezik számottevő bejövő kapcsolatokkal.

Kimenő adatok és hozzáférések. A rendszer adatkapcsolattal rendelkezhet a gazdasági rendszerrel, melynek költségelszámolási adatokat adhat át. A beszerzési rendszer számára automatikusan adhat le kellékanyag és papír beszerzési igényeket, jelezheti a karbantartások megrendelésének igényét. A VIR felé elsősorban gazdaságossági és kihasználtsági információk küldésére szolgáló adatkapcsolatok állhatnak rendelkezésre. A fájlszerverek és levelező rendszerek a beszkennelt dokumentumok tárolásában és továbbításában vesznek részt.

A rendszer és adatainak mentését és helyreállítását a mentési alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek.



24. ábra. A nyomtatási rendszerek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Telefonhálózat

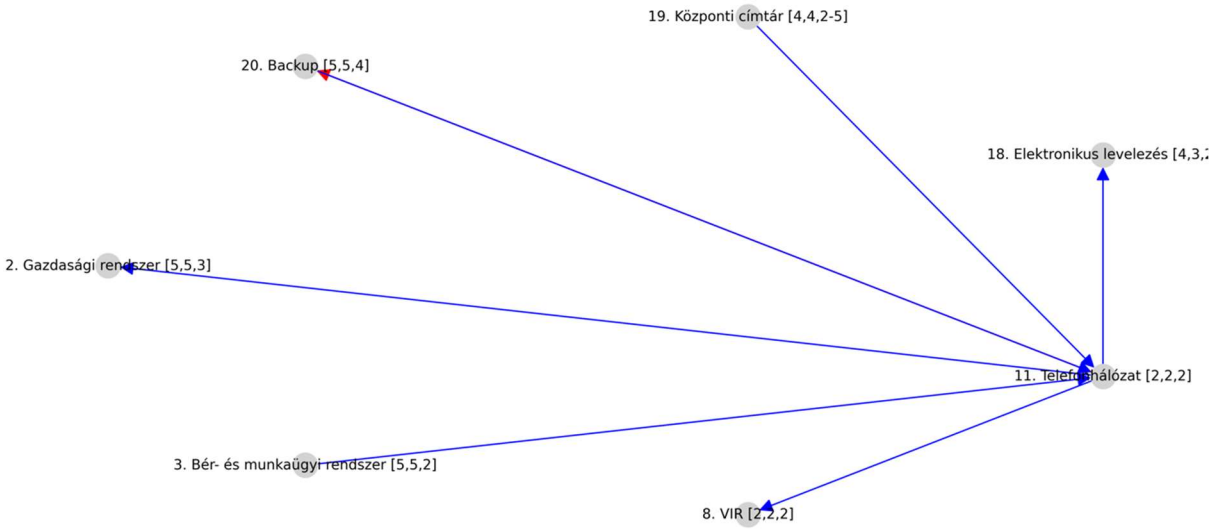
IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2*

A digitális telefonhálózatok tartalmazhatnak belső telefonkönyvet, így a készülékek megjeleníthetik hívó fél nevét, és az elszámolási adatok is személyre bonthatók. Amennyiben az alkalmazott központ tartalmaz ilyet, azt a 2-es szintbe, a hagyományos, vagy személyes adatokat nem tartalmazó telefonhálózatok esetén az ibtv. szerinti besorolás 1.

Bizalmasság. Bár a telefonhálózat rendszerében tárolt híváslista kezelése céghez kötött, a hívó vagy a hívott fél azonosíthatósága esetén az személyes adatkezelésnek minősül, így bizalmasságát legalább 3-as szintre kell sorolni. A listák felhasználhatósága gazdasági vagy más haszonszerzésre nem jellemző.

Sértetlenség: a telefonhálózat adatainak sérülése jellemzően nem okoz működésképtelenséget, legfeljebb a költségelszámolási rendszerben jelenhetnek meg téves adatok. Az intézmény működésében ez nem okoz érzékelhető problémát.

Rendelkezésre állás: a mobiltelefonok széles körű elterjedése miatt a rendszer rövidebb idejű kiesése legfeljebb minimális működési zavart okoz, mely könnyen áthidalható.



25. ábra. A telefonhálózat lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A bér- és munkaügyi rendszer címtárkapcsolatán keresztül a telefonrendszerek adatai is feltöltésre kerülhetnek.
Kimenő adatok és hozzáférések. A gazdasági rendszer elszámolási adatokat vehet át a költségelszámolási alrendszertől. A VIR tartalmazhat a telefonrendszerrel összefüggő adatokat. Az elektronikus levelezés üzeneteket, faxokat vagy hangüzenetek hangfájlokba konvertált másolatait juttathatják el a munkatársak számára.
A rendszer és adatainak mentését és helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek.

5.1.1. Oktatás- és kutatástámogató rendszerek

A szabályzatokban szereplő biztonsági besorolások alapján az oktatást és kutatást támogató rendszerek is eltérő képet mutatnak.

Hallgatói laborok

IBTV szerinti javasolt besorolás: *Bizalmasság: 1 sértetlenség: 1, rendelkezésre állás: 1. Biztonsági osztály: 1*

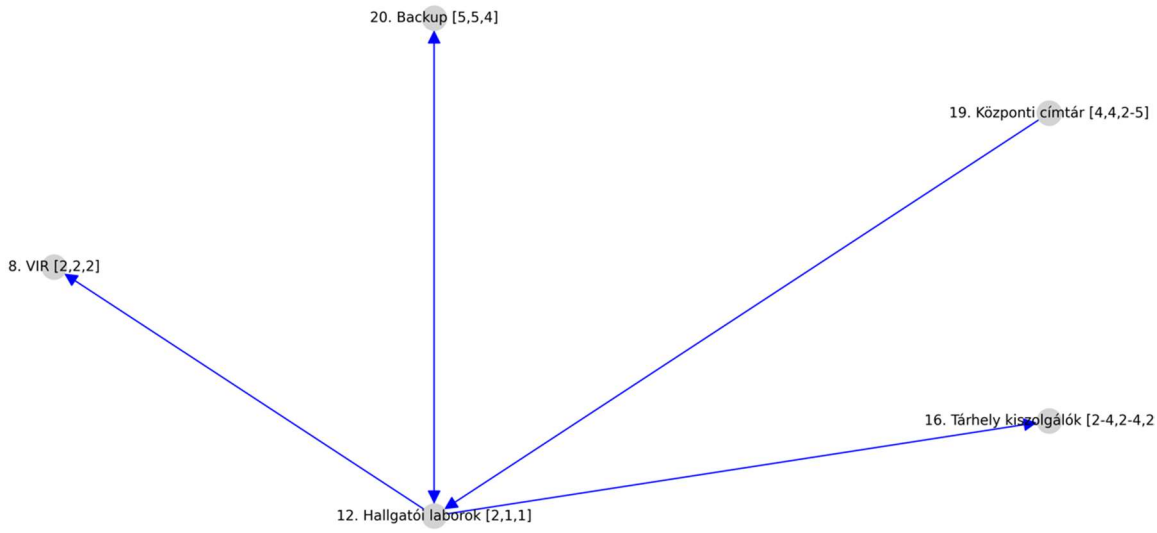
A hallgatói számítógépes laborok nem tartalmaznak személyes adatokat, rendszerint az intézmény hálózatában egy elkülönített VLAN-ban működnek, ugyanakkor a hallgatói jogosultságainak beállítására vonatkozó stratégiában eltérések tapasztalhatók. A laborok rendelkezésre

állását eredményező incidensek lehetséges következményei elhanyagolhatók, így ibtv. szerinti besorolásuk 1-es.

Bizalmasság. A hallgatói laborokban nem jelenik meg az intézmény szempontjából számottevő adat.

Sértetlenség. Adatok hiányában nem értelmezett.

Rendelkezésre állás. Adatok hiányában nem értelmezett.



26. ábra. A hallgatói laborok lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések: a központi címtár szabályozhatja a belépési jogosultságokat.

Kimenő adatok és hozzáférések: opcionális hozzáférés lehetséges a VIR, tárhely kiszolgálók és a mentési rendszerekhez.

E-learning rendszerek

IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2 rendelkezésre állás: 2. Biztonsági osztály: 2*

Számos egyetem biztosít a hallgatók számára e-learning rendszereket, melyben az egyes kurzusokhoz elektronikus tananyagok elérését teszi lehetővé. A népszerű rendszerek számos egyéb funkciót is biztosítanak a számonkérési lehetőségtől az online beszélgetésekig. Azok az E-learning rendszerek, melyek funkcionalitása pusztán a tananyagok közzétételében merül ki, tehát nem, vagy csak minimális mértékben kezelnek személyes (hallgatói) adatokat, nem jelentenek különösebb kockázatot, ezért biztonsági besorolásuk alacsony. Amennyiben az adott

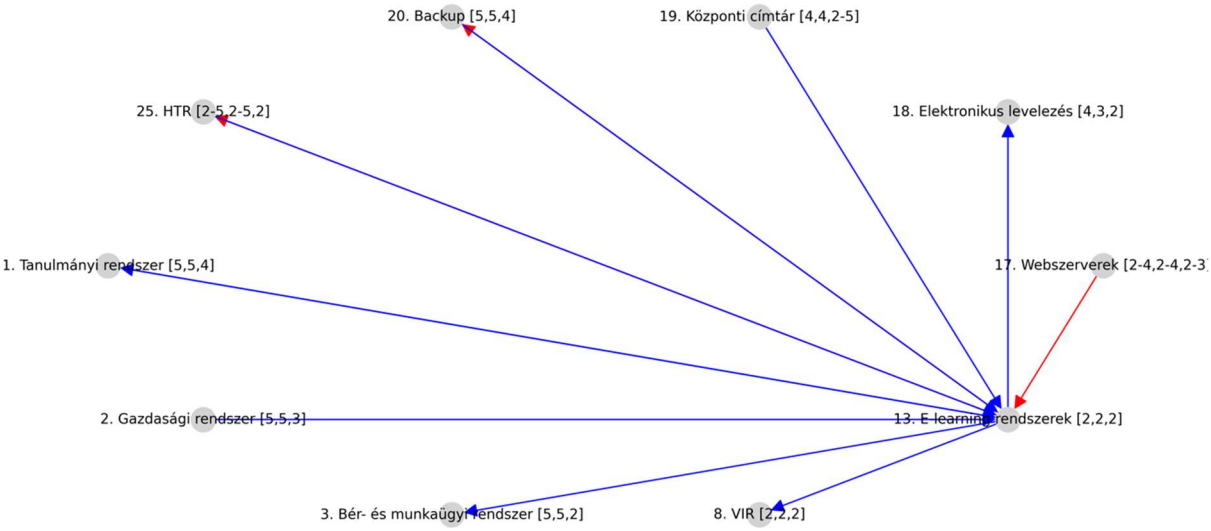
rendszer személyes adatokat, például bejelentkezési azonosítókat, valamint az egyes kurzusokon elért eredményeket esetleg több szemeszterre visszamenőleg is tárol, automatizált adatkapcsolatot tart fenn más rendszerekkel, magasabb biztonsági szintbe kell sorolni.

Bizalmasság. Az e-learning rendszerek által kezelt személyes adatok mennyisége intézményenként vagy rendszerenként eltérő lehet. Egy alaprendszer működése is bejelentkezési adatokat követel meg, melyet vagy saját, vagy központi címtárszolgáltatásra alapozhat, utóbbi esetben a kezelt személyes adatok mennyisége elenyésző. Más megvalósításban az oktatók és hallgatók személyes adatai nagy mennyiségben kerülhetnek rögzítésre, kiegészítve a számonkérés módját befolyásoló egészségügyi adatokat tartalmazó igazolásokkal. A megadott bizalmasság ibtv. szerinti besorolása az alaprendszerre érvényes, amennyiben a szóban forgó rendszer további adatokat tartalmaz, vagy képes adatok átvételére a tanulmányi rendszerből, vagy pl. vizsgajegyek automatizált bevitelére, a bizalmassági szintjét a kezelt adatok mennyiségétől és érzékenységétől függően akár a legmagasabb, 5-ös szintig is fel kell emelni.

Sértetlenség. Az e-learning rendszereket ért támadások egy csoportja az érdemjegyek és a különféle számonkérések eredményeinek meghamisítására, és a különféle tesztkérdések megszerzésére irányul. Bár nemzetközi viszonylatban ismertek ilyen támadások [31], azok bekövetkezésének valószínűsége, így az ibtv. szerinti besorolása is alacsony. A rendszerben tárolt személyes adatok módosításának szintén alacsony motivációs bázisa van, a vizsga- és évközi jegyek megváltoztatásának csak egy rövid idő intervallumban van értelme, azok hosszú távú nyilvántartása a tanulmányi rendszer feladata.

Rendelkezésre állás. Az e-learning rendszerek rendelkezésre állásának követelménye a tanulmányi rendszerhez hasonlóan időszakonként eltérő. Szorgalmi időszakban kisebb sérülése tolerálható, és bár a számonkérések közbeni kiesése is kezelhető, annak előfordulásai nagyban rontják a rendszer reputációját, végső soron akadályozzák az intézményt az alapfeladatai elvégzésében. Ugyanakkor tartós kiesése esetén a hagyományos számonkérési eljárásokkal a működés minden esetben biztosítható.

Bejövő adatok és hozzáférések. Az e-learning rendszerek működésének automatizálása leginkább a tanulmányi rendszerrel kiépített adatkapcsolatok alapján lehetséges, így számos egyetem fejlesztett ki ilyen megoldást. Ezek elsősorban a tárgyfelvétellel, tantárgyleírásokkal, valamint a különféle számonkérések eredményeinek rögzítésével kapcsolatosak, de előfordulnak online konferencia vagy webináriumi foglaltságkezelő integrációk is. A bevételes tevékenységek vagy önköltséges képzések támogatásában előfordulhat adatkapcsolat a gazdasági rendszerrel, valamint érkezhetnek adatok a HTR-től is.



27. ábra. Az e-learning rendszerek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

A kimenő adatok és hozzáférések elsődleges célpontja a már említett feladatok ellátása érdekében szintén a tanulmányi rendszer. A HTR és a VIR számára is természetes adatforrás lehet az e-learning rendszer. Bevételes oktatási tevékenységek támogatására szintén létrehozhatók automatizált folyamatok a bér- és munkaügyi rendszer felé, az elektronikus levelezés pedig a rendszerből érkező üzenetek továbbítását láthatja el.

A rendszer és adatainak mentését és helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek.

Kutatói rendszerek

IBTV szerinti javasolt besorolás: *Bizalmasság: 2-3 sértetlenség: 2-3, rendelkezésre állás: 1. Biztonsági osztály: 2-3*

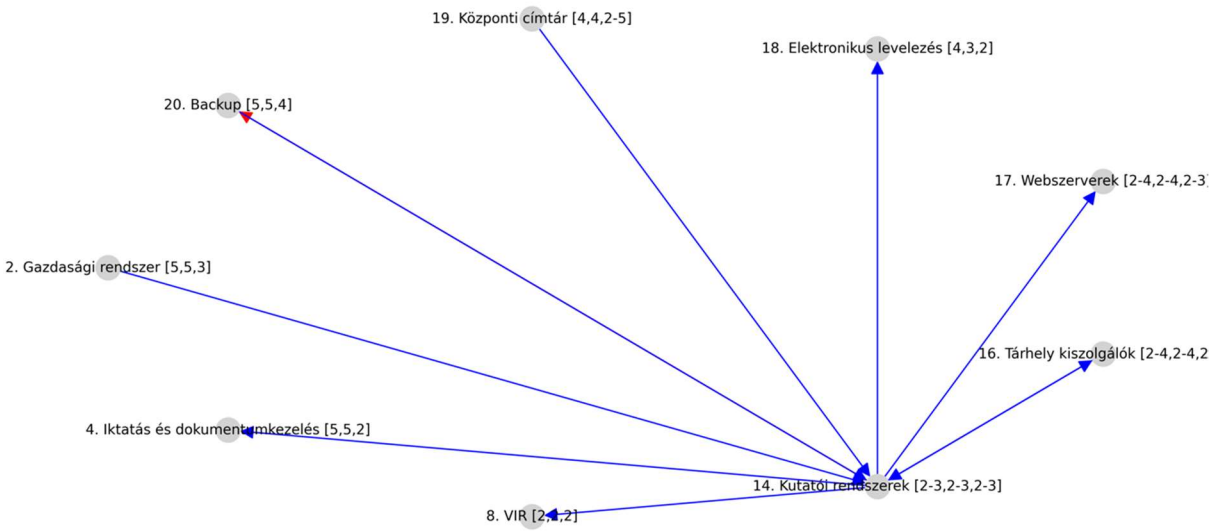
A kutatói rendszerek általános besorolása nem terjed ki azokra az önálló működésű, kiemelt kutatócsoportokra, melyek kutatási eredmények, kutatásuk jellege, tárgya vagy körülményei következtében nemzetbiztonsági felügyelet alá tartoznak. Ezek az elkülönült szervezeti egységek az egyetemekétől eltérő jogszabályi környezetben működnek. Az általános kutatási folyamatokban, mely magában foglalja a több tudományegyetem által említett HPC-t is, amennyiben személyes adatok feldolgozása történik, azokat az érintettek hozzájárulása mellett, egyedi adatkezelési szabályzással és a GDPR követelményeinek betartásával kell kezelni. A személyes adatokat nem kezelő kutatások esetében az anyagi ráfordítások lehetséges elvesztése, valamint a pályázati forrásból finanszírozott kutatások esetleges meghiúsulása és a pályázati támogatás

visszafizetésének kényszere okán a 2-es, a nagy mennyiségű személyes adatok feldolgozását igénylő kutatási adatok esetében magasabb szintű besorolás célszerű.

Bizalmasság. Besorolását az adattartalom és kapcsolatok ismeretében az ibtv. szerinti besorolási szempontok szerint kell elvégezni.

Sértetlenség. Besorolását az adattartalom és kapcsolatok ismeretében az ibtv. szerinti besorolási szempontok szerint kell elvégezni.

Rendelkezésre állás. Besorolását az adott rendszerrel szemben támasztott követelmények alapján, általában alacsony szinten, egyedileg kell meghatározni.



28. ábra. A kutatói rendszerek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. Tekintettel arra, hogy a kutatói rendszerek általában adott tudományos feladat ellátására létrehozott célszoftverek, leginkább csak más szoftverekkel történő kapcsolattartásuk valószínű, emellett elképzelhető a gazdasági rendszerrel kiépített automatizált kapcsolat.

Kimenő adatok és hozzáférések. Amennyiben a rendszer működése során iktatás köteles dokumentumok keletkeznek, azok az iktatási rendszer felé automatizált adatkapcsolattal is küldhetők.

A rendszer és adatainak mentését és helyreállítását a mentési alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek, a VIR felé vezetői döntéstámogatáshoz szükséges adatokat adhat át. Az alkalmazott szoftverek esetenként központi azonosítási szolgáltatásokat is igénybe vehetnek.

Könyvtári rendszerek

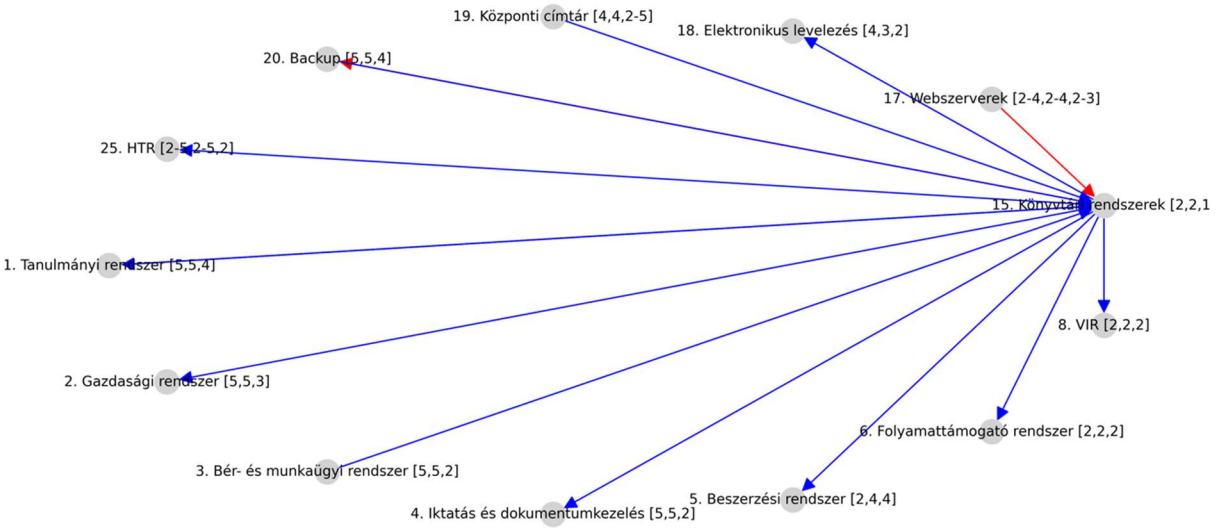
IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 1. Biztonsági osztály: 2*

Számos egyetemi szabályzat nem tér ki az egyetemi könyvtárak besorolására, miközben a legtöbb könyvtári rendszer önálló olvasói adatbázisa révén számottevő mennyiségű személyes adatot tartalmazhat. Ezek köre nem túl széles, a bejelentkezési adatok mellett a személyazonosság igazolására és az értesítési folyamat során használható egyéb adatok, valamint a kölcsönzési események rögzítése jellemző. A könyvtári adatok bizalmasságának és sértetlenségének besorolását a rendszerben tárolt nagyobb mennyiségű személyes adat indokolja, a rendelkezésre állás sérülésének kezelése legfeljebb a könyvtári személyzet számára jelent többletfeladatot.

Bizalmasság. Mértéke a könyvtári rendszerekben tárolt személyes adatok mennyiségétől függ. Amennyiben az adott rendszer működése nagy mennyiségű hallgatói adat importálásán alapul, vagy ezek átvételére a tanulmányi rendszerrel adatkapcsolatot működtet, a besorolás mértékét magasabb szinten kell meghatározni.

Sértetlenség. A könyvtári rendszer sérülésének hatásai a könyv- és folyóirat állomány, valamint a kölcsönzési adatok mellett a rendszerben tárolt személyes adatokra is kiterjedhet, mely az alapfunkciók ellehetetlenülését eredményezi.

Rendelkezésre állás. Sérülése esetén a könyvtári kölcsönzési szolgáltatás kiesésével kell számolni, mely más könyvtárakkal, elektronikus forma igénybevételével vagy az olvasótermi szolgáltatások igénybevételével időlegesen kezelhető.



29. ábra. A könyvtári rendszerek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A kölcsönzési rendszer a hallgatói adatokat a tanulmányi rendszerből, dolgozók esetén a munkaügyi rendszerből veheti át. A késedelmi díjak kivetéséhez és beszedéséhez, a tagsági díjakhoz kapcsolódó pénzügyi műveletek elvégzéséhez a gazdasági rendszerrel állhat fenn adatkapcsolat.
Kimenő adatok és hozzáférések. Adatkapcsolat működhet a tanulmányi rendszerrel, és a gazdasági rendszerrel. A könyvtári rendszerben keletkező dokumentumok automatizált eljárás során az iktatórendszerbe kerülhetnek. A könyvek, folyóiratok és egyéb eszközök beszerzési igényei a beszerzési rendszerbe szintén automatizált folyamat során, esetleg a folyamattámogató rendszeren keresztül juthatnak el. A könyvtári rendszer emellett adatokat adhat át a HTR számára is, melyeket az elsősorban kényelmi szolgáltatások nyújtására használ fel.
A rendszer és adatainak mentését és szükség esetén helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek, a VIR felé vezetői döntéstámogatáshoz szükséges adatokat adhat át.

5.1.2. IT rendszerek

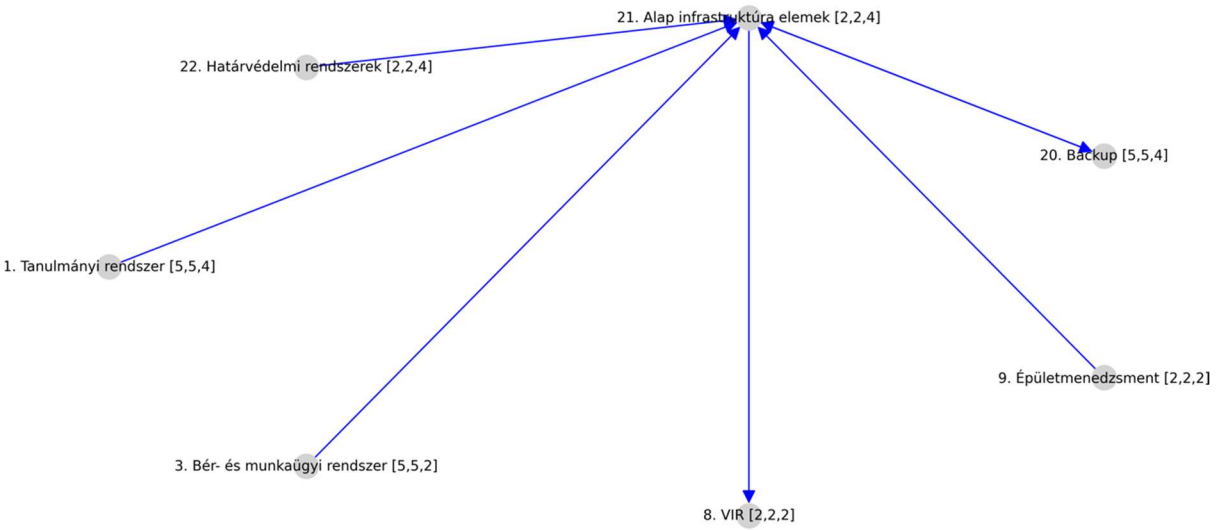
Az IT rendszerek csoportját azok a rendszerkomponensek képezik, melyek az intézmény folyamatainak szempontjából nincs önálló funkciójuk, szerepük a rájuk épülő szakrendszerek műszaki háttértámogatásában merül ki. Besorolásukat az informatikai szakemberek végzik, és gyakran magasabb értékre állítják be, mint amelyet az értékelési szempontok alapján hozzájuk kellene rendelni.

Alap infrastruktúra elemek

IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 4. Biztonsági osztály: 4*

Egy alap informatikai infrastruktúra elem olyan szerver, és hálózati elem, mely feladata a rendszerek működtetését szolgáló hardver- és szoftver komponensek biztosítása. A leggyakoribbak a számítógép hálózat alap infrastruktúrája, a middleware rendszerek, tanúsítvány szolgáltatások, DNS, infrastruktúra felügyeleti rendszerek (Nagios, Icinga stb.). Egyes részelemeik (pl. diszk alrendszerek) adattartalmának meghatározásakor tekinthetők egyszerű, kapcsolatrendszer nélküli alkatrészeknek, de meghatározhatók úgy is, mint olyan rendszer működési alapot, mely minden rendszer működtetésében, adatai tárolásában, adatkapcsolatai felépítésében és lebonyolításában nélkülözhetetlen szerepet játszik. Személyes vagy intézményi adattartalom közvetlen hiányában ibtv. szerinti besorolásban ezek a rendszerek alacsony besorolásúak, ugyanakkor működésük az informatikai rendszer legtöbb elemére nézve elengedhetetlen.

Bizalmasság. A legtöbb informatikai alapstruktúra elem nem tartalmaz személyes adatot, ugyanakkor számos olyan, a szolgáltatáshoz kapcsolódó adatot vagy konfigurációs beállítást tartalmazhatnak, melynek szivárgása esetén az informatikai rendszer védelme sérül. Tipikus példák erre a névszerverekben tárolt adatok, diszk alrendszerek közvetlen elérését lehetővé tevő hozzáférési kódok, vagy tanúsítványokhoz kapcsolódó privát kulcsok, vagy biztonsági algoritmusok tervezési hibájának következtében támadhatóvá vált hálózati eszközök [101].
Sértetlenség. Az alap infrastruktúra elemek többségén a sértetlenség nem értelmezett, a szoftver elemek esetében ez azonban akár a teljes informatikai infrastruktúra hibás működését eredményezheti. Az alap infrastruktúra elemei kibertámadások célpontjai is lehetnek: a DNS bejegyzések rosszindulatú módosításával indított támadások nehezen észlelhetők és gyakran komoly kárt okozhatnak.
Rendelkezésre állás. A legtöbb elem esetén kritikus követelmény melynek mértékét a kiszolgált rendszerek rendelkezésre állási igényének maximuma határozza meg.



30. ábra. Az alap infrastruktúra elemek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. Az alap infrastruktúra elemek esetében a bejövő kapcsolati gráf elemei inkább elméleti adatkapcsolatokat ír le. A tanulmányi és a munkaügyi rendszerben végzett személyügyi módosítások során végrehajtott mechanizmus eredményeként történhetnek automatikus konfigurációs módosítások valamely alap infrastruktúra elemben. A határvédelmi rendszerek módosításai során szintén végbe mehetnek az alap struktúrát érintő változtatások. Az épületmenedzsment rendszerekbe integrált vezérlési funkciók által generált kapcsolatok szintén inkább elvi megfontolás tárgyát jelentik.

Kimenő adatok és hozzáférések. A VIR és mentési rendszerek adatkapcsolatai szintén lehetséges, de a gyakorlatban kevéssé valószínű kommunikációt jelentenek.

Határvédelmi rendszerek

IBTV szerinti javasolt besorolás: *Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 4. Biztonsági osztály: 4*

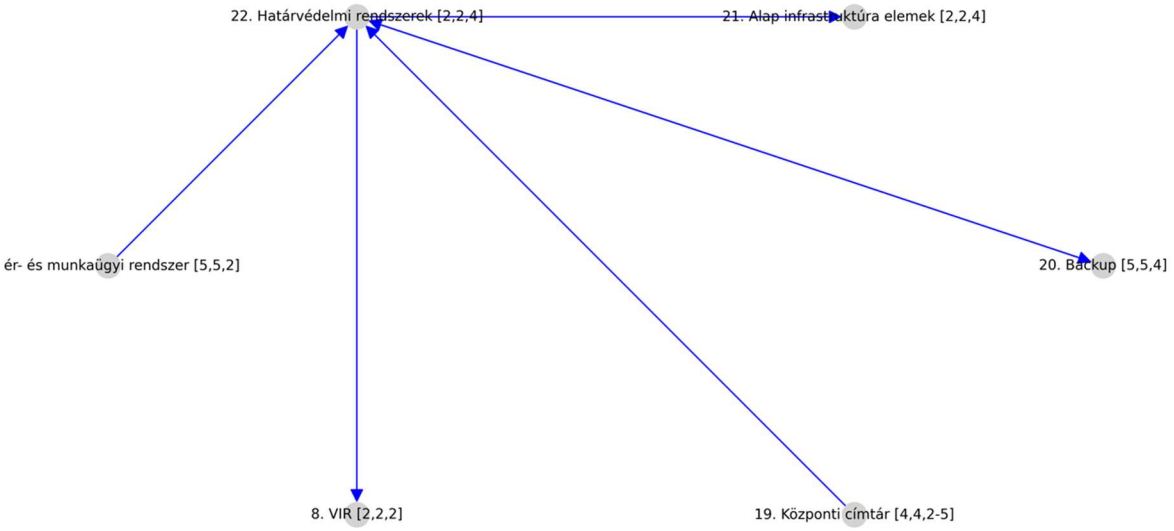
A határvédelmi eszközök közé elsősorban a tűzfalak, VPN szerverek, útválasztók, esetleg VLAN korlátozásokat tartalmazó kapcsolók tartoznak. Bár ezek az eszközök lényeges szerepet játszanak az informatikai hálózat elemeinek kiszolgálásában, maguk az eszközök néhány kivétellel nem tartalmaznak személyes adatot, így a bizalmassági és a sértetlenségi besorolásuk alacsony. Hangsúlyozandó, hogy sikeres kompromittálásuk súlyos biztonsági hibák kiinduló állomása lehet, így védelmüket magas prioritással kell ellátni. A rendelkezésre állás sérülésének következményei a kiszolgált rendszerek rendelkezésre állásának függvényében változnak.

Bizalmasság. Az eszközök jellemzően nem tárolnak személyes adatot, ugyanakkor forgalmi adatok rögzítését és riportok generálását végezhetik, melyek elemzésekor a forrás, vagy célszemély adatai felismerhetők. Működésük megismerése azonban lehetővé teheti egy támadó számára az abban levő konfigurációs hibák feltárását és lehetőség szerinti kihasználását.

Sértetlenség. Személyes adatok hiányában az ibtv. szerint nem indokolt ezen rendszerek magas sértetlenségi besorolása. Ugyanakkor a határvédelmi eszközök módosításával a védett rendszerek egy vagy több védelmi vonal szolgáltatásait elvesztik, ezért azok sértetlenségének elvesztése számos más rendszerre nézve jelenthet súlyos kockázatot.

Rendelkezésre állás. Besorolási értékét a fentiek alapján a védett rendszerek rendelkezésre állási besorolásának legmagasabb értéke adja.

Bejövő adatok és hozzáférések. A határvédelmi rendszerek beállítási feladatait rendszerint a rendszermérnökök látják el. A dolgozói be- és kilépések, munkakör változások következtében szükséges változtatások a munkaügyi rendszerből indítva automatizált módon is megtörténhetnek, mely során a határvédelmi rendszerek működési paraméterei módosulhatnak (ez inkább elméleti lehetőség). A legtöbb rendszer saját azonosítási szolgáltatással rendelkezik, így a címtár szolgáltatások alkalmazása leginkább VPN szolgáltatásokat kínáló rendszerek esetében fordul elő.



31. ábra. A határvédelmi rendszerek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Kimenő adatok és hozzáférések. A határvédelem ritkán rendelkezik más rendszerekbe irányuló adatkapcsolattal. A berendezések elméletben nyújthatnak adatszolgáltatást a VIR számára, vagy végezhetnek további automatizált konfigurációs beállításokat egyes alap infrastruktúra elemeken, de a gyakorlatban ez alig fordul elő.

A rendszer adatainak mentését és helyreállítását backup alrendszer végezheti, de ezen eszközcsalád esetében egy másik, kifejezetten erre a célra szolgáló célrendszert szokás alkalmazni.

A határvédelmi rendszerek sérülékenysége esetén, amennyiben az a védett rendszerek biztonságának csökkenésével jár, a sérülékenységet a lehető leghamarabb meg kell szüntetni, meg kell vizsgálni a külső kapcsolatok leállításának szükségességét, a javítást követően pedig a rendszer konfigurációját felül kell vizsgálni.

Szakmai gyakorlatok rendszere

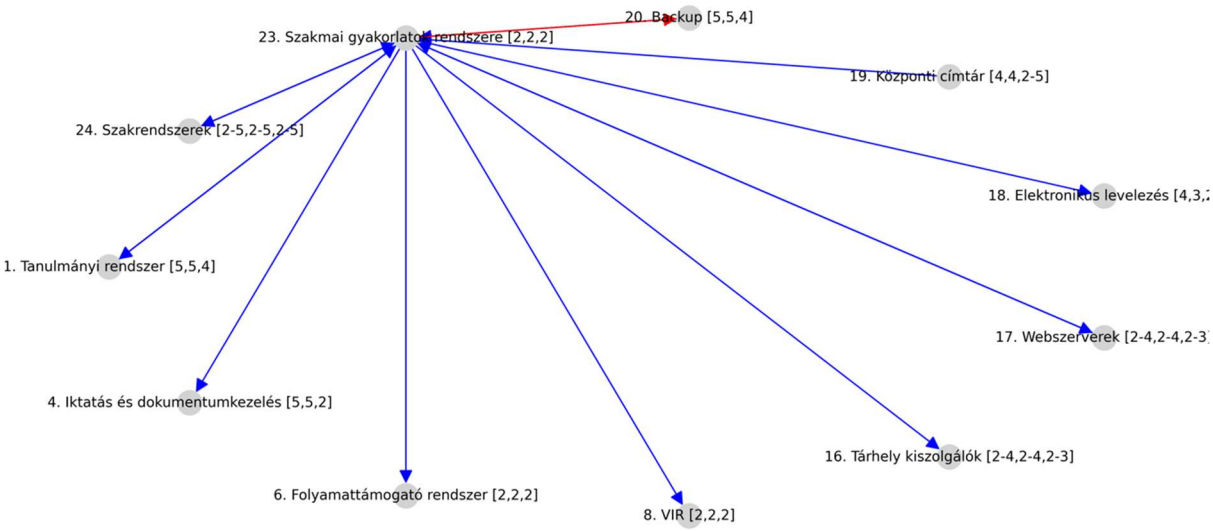
Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2

Az egyetemek képzéseinek jellemző követelménye valamilyen szakmai gyakorlat teljesítése, melyek jellemzően az egyetemtől független cégeknél vagy szervezeteknél végezhetők. A rendszerben nyilvántartásra kerülnek a gyakorlati helyek és a hallgatók adatai, valamint a gyakorlat teljesítés értékelési dokumentumai.

Bizalmasság: a rendszer a gyakorlati helyek helyekről rendszerint csak általános, más, publikus forrásból is elérhető adatot tartalmaz, és a lista a legtöbb esteben nyilvános is. A hallgatói adatok mennyisége minimális, talán az értékelési dokumentumok tartalmazhatnak máshol nem elérhető személyes adatokat.

Sértetlenség. A rendszer sértetlensége az intézmény szempontjából sem kritikus. Az ebben tárolt adatok kis ráfordítással pótolhatók, a jegyzőkönyvek a kiállító szervezettől vagy a hallgatótól beszerezhetők.

Rendelkezésre állás. A rendszer kiesése esetén meghiúsuló folyamatok manuális eljárással helyettesíthetők, így a tanulmányi előrehaladást nem akadályozza.



32. ábra. A szakmai gyakorlatok rendszerének lehetséges adatkapcsolatai.
Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. A szakmai gyakorlatok rendszere a hallgatói információkat elsősorban a tanulmányi rendszerből szerzi meg, lehetséges további adatforrásai a szakrendszerek közül kerülhetnek ki.

Kimenő adatok és hozzáférések. A szakmai gyakorlatok sikeres vagy sikertelen lebonyolításának adatait a rendszer elsősorban a tanulmányi rendszer felé továbbítja, de adatkapcsolatot tarthat fenn egyes szakrendszerekkel, az iktatási rendszerrel, vagy a folyamattámogatási rendszerrel.

A rendszer és adatainak mentését és helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek.

Tekintettel a rendszer alacsony ibtv. szerinti besorolására, sérülékenysége esetén szinte minden kapcsolódó rendszer érintett lehet, bekövetkezésekor a tanulmányi rendszer és az iktatás mellett a magasabb besorolású szakrendszerek kapcsolódási pontjainak védelmi felülvizsgálata javasolt.

Szakrendszerek

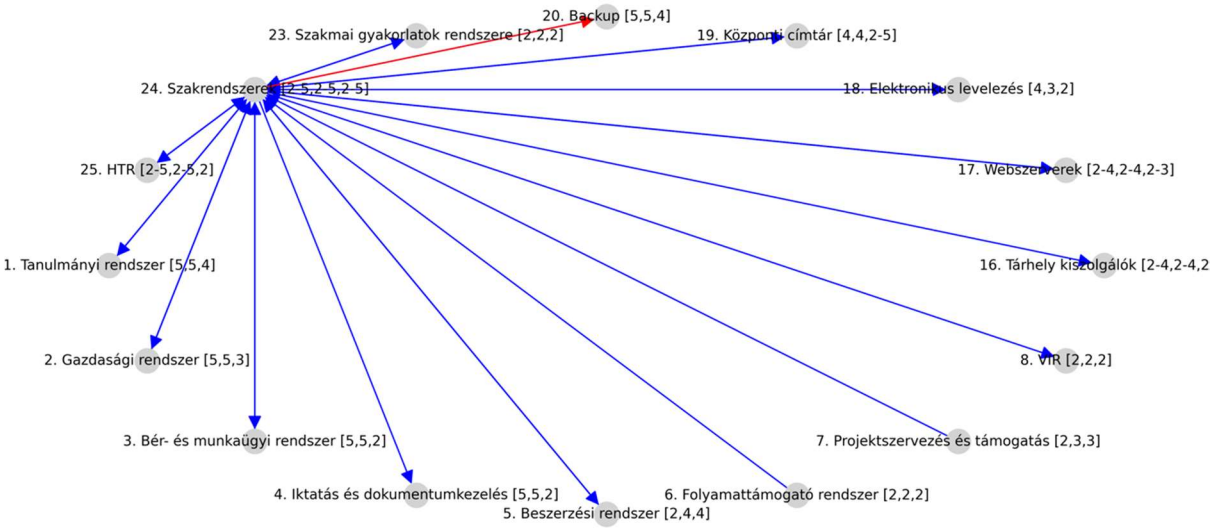
IBTV szerinti javasolt besorolás: *Bizalmasság: 2-5 sértetlenség: 2-5, rendelkezésre állás: 2-5. Biztonsági osztály: 2-5*

Főként az orvosképzést végző egyetemek tértek ki szabályzataikban olyan szakrendszerek besorolására, melyek csak az ebben a szakképzésben jelennek meg. Számos más egyetem is rendelkezhet hasonló, speciális szakrendszerrel, melyek besorolása azok adattartalma, kiszivárgásuk, sértetlenségük és rendelkezésre állásuk sérülésének ismerete nélkül nem adható meg. Ugyanakkor az OSINT megakadályozása érdekében a nyílt hozzáférésű szabályzatokban célszerű ezen speciális szakrendszerek megnevezésének mellőzését.

Bizalmasság. Besorolását az adattartalom és kapcsolatok ismeretében az ibtv. szerinti besorolási szempontok szerint kell elvégezni.

Sértetlenség. Besorolását az adattartalom és kapcsolatok ismeretében az ibtv. szerinti besorolási szempontok szerint kell elvégezni.

Rendelkezésre állás. Besorolását az adott rendszerrel szemben támasztott követelmények alapján, egyedileg kell meghatározni.



33. ábra. A szakrendszerek lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

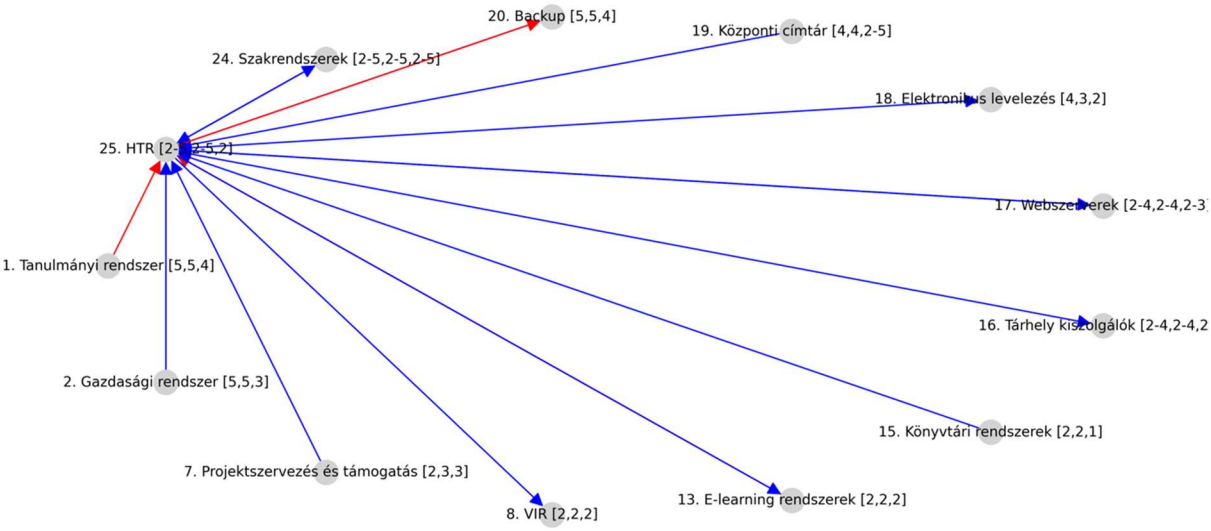
Bejövő adatok és hozzáférések. A szakrendszerek feladatuktól függően számos további rendszerből vehetnek át adatokat, illetve rendelkezhetnek adatkapcsolattal. A fenti ábra a rendszer lehetséges kapcsolati gráfját írja le, melyet az adott szakrendszer esetében egyedileg kell meghatározni.
Kimenő adatok és hozzáférések. Egy szakrendszer számos más rendszer számára adhat át adatokat, a lehetséges kapcsolatokat szintén a fenti kapcsolati gráf tartalmazza.
Egy szakrendszer és adatainak mentését és helyreállítását is a backup rendszer végezheti, azonosítási feladatait a címtárszolgáltatás láthatja el, működésükben a tárhely kiszolgálók és webszerverek is közreműködhetnek.

Hallgatói támogatói rendszer (HTR)

IBTV szerinti javasolt besorolás: *Bizalmasság: 2-5 sértetlenség: 2, rendelkezésre állás: 2. Biztonsági osztály: 2*

A hallgatói támogatói rendszerek elsődleges feladata a hallgatók tanulmányainak elősegítése, lemorzsolódási arányának csökkentése. Működésük a tanulmányi tevékenység nyomon követésén alapul, melyhez megvalósítástól függően a tanulmányi rendszer adatait használják fel. A rendszer képes figyelmeztetést adni a határidők közeledtekor, jelzést ad, amennyiben a hallgató hiányzásainak száma indokolatlanul magas, valamint, ha a tanulmányi előmenetele, zárthelyi dolgozatai, beadandó feladatai alapján valamely kurzust nem tudja majd teljesíteni. A rendszerbe további tájékoztatási és kényelmi funkciók kerülhetnek beépítésre az órarendtől a tantermek megkeresését támogató navigációs szolgáltatáson át a különféle programajánlókig.
Bizalmasság. Egy adatbiztonság szempontjából helyesen megtervezett HTR rendszer minimális mennyiségű személyes adatot tartalmaz, funkcióit tanulmányi rendszer különféle rendszerhívásain keresztül implementálja. Egy ily módon megtervezett rendszerben a személyes adatok szivárgásának valószínűsége alacsony. Amennyiben a HTR a tanulmányi rendszer adataihoz nem kontrollált módon fér hozzá, és fennáll a nagy mennyiségű adat szivárgásának lehetősége, bizalmassági besorolását a kapcsolat hozzáférésének függvényében magasan, akár a tanulmányi rendszerrel azonos szinten kell meghatározni.
Sértetlenség. Tekintettel arra, hogy a HTR nem alapszolgáltatás, valamint működése túlnyomórészt más rendszerekből származó adatokon alapul, sértetlensége önmagában nem kritikus. Az egyes támogatói rendszerek változatos funkcionalitása következtében a sértetlenség besorolási szintje eltérhet ettől.

Rendelkezésre állás. A lemorzsolódás elkerülésére érdekében kifejlesztett funkciók időleges kiesése tolerálható a felhasználók számára, inkább a rendszer egyéb, kényelmi szolgáltatásainak elérhetetlensége okozhat problémát. Ezek többségükben más rendszerekben elérhetők vagy nélkülözhetők, így a rendelkezésre állás ibtv. szerinti besorolása alacsony.



34. ábra. A HTR lehetséges adatkapcsolatai. Forrás: saját szerkesztés.

Bejövő adatok és hozzáférések. a HTR elsődleges, és leginkább érzékeny adatai a tanulmányi, gazdasági, és projektszervezés rendszerből érkezhetnek. Az előrehaladás és a tanulmányi előmenetel monitorozása az e-learning rendszerek adatai alapján is történhet. Kényelmi szolgáltatásai többek közt a könyvtári rendszerek, valamint a webszerverek szolgáltatásain alapulhatnak.
Kimenő adatok és hozzáférések. A HTR adatkapcsolattal rendelkezhet az e-learning rendszerek, esetleg a tárhely kiszolgálók felé.
A rendszer és adatainak mentését és helyreállítását a backup alrendszer végezheti, működésében a tárhely kiszolgálók és webszerverek is közreműködhetnek.
A HTR sérülékenysége esetén azonnal felül kell vizsgálni minden magas besorolású rendszerrel kiépített automatizált kapcsolatát, és amennyiben fennáll annak kockázata, hogy azok adatai a HTR-en keresztül szivároghatnak ki, azokat le kell zárni.

5.2. Összegzés

Az informatikai szabályzatok eltérései bizonyították, hogy a magyar egyetemek az informatikai rendszereik biztonsági besorolási során csak felületesen alkalmazzák az ibtv. által megfogalmazott alapelveket. Ennek következtében azonos feladatkörű rendszereket különböző szintekbe sorolnak, így azok védelmi eljárásai is valószínűleg eltérők. A fejezetben ezért kidolgoztam egy metodikát, mely alkalmazásával a besorolás pontossága jelentősen javítható, a felsőoktatási rendszerekre szabott, és képes azonnali válaszokat adni az egyes rendszerekben megjelenő sérülékenységek másodlagos hatásaira.

A metodika első szintje a felsőoktatásban alkalmazott informatikai rendszerek feltérképezése, funkcióinak meghatározása, valamint a kezelt adattartalmuk hozzávetőleges meghatározása. A felsőoktatás sajátosságai és az alkalmazott rendszerek jellege alapján elvégeztem az ibtv. besorolási kritériumainak testreszabását, majd erre alapozva meghatároztam az egyes rendszerek bizalmassági, sértetlenségi és rendelkezésre állási besorolásait vagy azok intervallumát.

A második szint kialakítása során feltérképeztem egy egyetem informatikai rendszerei közt fennálló adatkapcsolatokat, majd annak általánosításával meghatároztam a lehetséges továbbiakat, melyet egy kapcsolati mátrixban rögzítettem. A mátrix validálását az egyes rendszerek részletes leírása során több lépésben végeztem.

A harmadik szintet az egyes rendszerek részletes leírása, a lehetséges bejövő és kimenő adatkapcsolatok részletes feltárása adja, mely kitér az egyes rendszerek eltérő működési módjainak következő eltérésekre is. A szint kidolgozása során bizonyítottam, hogy az ajánlott és az szabályzatok elemzésben vizsgált besorolások közt esetenként jelentős eltérések tapasztalhatók.

Egy kockázatelemzésen alapuló besorolási eljárás a környezeti változások következtében rendszeres felülvizsgálatot igényel, ezek általános gyakorlata nem alkalmaz az egyes rendszerelemek sérülékenységein alapuló dinamikus, azonnali válaszlépéseket definiáló elemet. A metodika alkalmazásával a kapcsolati mátrix vagy azt leíró irányított gráf alapján egy sérülékenység esetén nem csak az érintett rendszer, hanem további iterációk során minden további rendszer érintettsége azonnal meghatározható, annak besorolása felülvizsgálható és az aktuális sebezhetőségi állapot ismeretében a szükséges védelmi intézkedések meghozhatók.

A metodika alkalmazásával a magyar felsőoktatási intézmények egységesíthetik az informatikai szabályzataik felépítését, és rendszereik besorolását, elvégezhetik a rendszereik által kezdeményezett adatkapcsolatok feltárását, és erre alapozva kialakíthatják intézményre szabott

kapcsolati mátrixukat. Folyamatos sérülékenységvizsgálati elemzések alapján meghatározhatják kapcsolódó rendszereik érintettségét és azonnali védelmi megoldásokat érvényesíthetnek.

6. Összegzett következtetések

Értekezésem hipotézisei a felsőoktatási informatikai rendszerek védelmi kérdéseihez kapcsolódnak. Kutatási eredményeim alapján az alábbi összegzett következtetéseket teszem:
Szabályzatok elemzésével kimutattam, hogy a magyar felsőoktatási intézmények jelentős adatvagyonnal rendelkeznek, feltérképeztem az azokat kezelő rendszerek jellegét és kezelt személyes adataik hozzávetőleges mennyiségét. Főként nemzetközi adatok elemzésével bizonyítottam, hogy az informatikai rendszerek incidensei, vagy az ellenük indított támadások számának hozzávetőleg 6–9%-a irányul oktatási intézmény ellen. Kimutattam, hogy hazai viszonylatban nem állnak rendelkezésre a szférát ért informatikai incidenseket leíró releváns adatbázisok vagy nyilvántartások, valamint a felsőoktatási intézmények jelentési hajlandósága alacsony. A magyar jogszabályi környezett elemzésével bizonyítottam, hogy az oktatási szektor nem rendelkezik a specifikus szabályzással szemben más, állami tulajdonban vagy fenntartásban levő szervezettel, melyek lényegesen kisebb mennyiségű érzékeny adatot kezelnek úgy, hogy informatikai rendszereik kialakításában és üzemeltetésében szigorú jogszabályi kereteknek kell megfelelniük. Az egyetemek informatikai rendszereinek biztonsági besorolására és szabályzataik homogenitásának bizonyítására dokumentumelemzésen alapuló kutatással elemeztem szabályzataik reprezentatív mintáját, és megállapítottam, hogy azok védelmi szintje az OSINT adatgyűjtés ellen alacsony szintű, köztük jelentős eltérések tapasztalhatók, részben elavultak, a kis létszámú egyetemek esetében pedig alacsony kidolgozottsági szintűek, esetenként nem is léteznek.
Miután bizonyítottam, hogy az egyetemi informatikai rendszerek nagy mennyiségű érzékeny adatot tartalmaznak, védelmük módszerei kizárólag az intézmény informatikai vezetésének saját hatáskörben hozott döntései alapján kerülnek meghatározásra, megvizsgáltam ezen rendszerek védettségi állapotát belső és külső támadásokkal szemben. Ennek eredményeként bizonyítottam, hogy az informatikai rendszerelemek sérülékenységi szintje nem különbözik a központi és perifériális campusok közt, miközben azokban számos, sok éve ismert sérülékenység mutatható ki. Bizonyítottam továbbá, hogy a feltárt sebezhetőségeik jelentős arányban az üzemeltető személyzet által javítható több éve fennálló beállítási hibák, melyek korrekciója a rendszerkonfigurációkra vonatkozó szigorúbb szabályzás mellett az elavult szoftver-, és esetenként a hardver eszközpark cseréjével küszöbölhető ki.
Miután kimutattam, hogy a felsőoktatási informatikai rendszerek megközelítőleg azonos környezetben, megközelítőleg azonos természetű adatokat tartalmaznak, miközben biztonsági besorolásuk, így feltehetően a védelmükre alkalmazott eljárások is eltérők, valamint rendszereik

nagy mennyiségű ismert sérülékenységet tartalmaznak, és érik is őket informatikai incidensek és kibertámadások, ajánlást dolgoztam ki azok egységes besorolására. Ezt a 2013 évi L. törvény és a 41/2015 BM. rendeletre alapoztam, de azt a rendszerek közti általános és lehetséges adatkapcsolatok térképére alapozott hatáslánc követésének kiterjesztésével bővítettem ki. A rendszerenként kimutatott kapcsolatok alapján, folyamatos sérülékenységvizsgálati eljárások eredményeinek elemzésével az egyes rendszereket érő kockázatok változására adott gyors válaszként felülvizsgálhatók biztonsági besorolást meghatározó komponensek, következésképp az alkalmazott védelmi eljárások is. A kapcsolati mátrix alapján így az érintett rendszerek egyértelműen azonosíthatók és a védelmi intézkedések rájuk is kiterjeszthetők.

6.1. Új tudományos eredmények

Hipotéziseim bizonyításával az alábbi új, tudományos eredményeket értem el:

E1. Bizonyítottam a magyar felsőoktatás informatikai rendszereinek biztonsági besorolásában fennálló inhomogenitást, melyet nemzetközi adatbázisok adatainak elemzésével támasztottam alá, továbbá ehhez kapcsolódóan listáztam a felsőoktatási intézmények informatikai rendszereit, részben elavult állapotát és OSINT információk gyűjtésének lehetővé tételét.

E2. Megcáfoltam, hogy a magyarországi felsőoktatási intézmények perifériális informatikai rendszerei kisebb számú, az internet irányából elérhető sérülékenységet tartalmaznak.

E3. Reprezentatív minta segítségével bizonyítottam a fennálló sérülékenységek magas számát és életkorát a magyar felsőoktatási információs rendszerekben, valamint kimutattam, hogy a sebezhetőségek túlnyomórészt konfigurációs hibák eredményei.

E4. Kidolgoztam egy rendszerek közötti adatkapcsolatokon, valamint folyamatos sérülékenységvizsgálati elemzésen alapuló metodikát, mely alapján a magyarországi egyetemi informatikai rendszerek besorolása dinamikus kockázatelemzés segítségével megvalósítható.

6.2. Ajánlások

PhD értekezésemben megfogalmazott eredményeimet elsősorban oktatási és kutatási intézmények, főleg egyetemi informatikai vezetők és az informatikai biztonságért felelős munkatársai figyelmébe ajánlom. A dolgozat elkészítése során elvégzett kutatások eredményei, a mérések módszertana és összegyűjtött adatainak feldolgozási módszerei segítséget nyújthatnak más intézményekben történő adaptáláshoz, és továbbfejlesztéséhez. A dolgozatban alkalmazott szoftverek és metodikák alkalmazásának megfontolását mindazon szakemberek számára is javaslom, akik más szektorban szeretnék az informatikai biztonság mérésén, és a sérülékenységek állapotának folyamatos mérésén alapuló védelmi rendszer kidolgozását és fenntartását megvalósítani. Áttekintését javaslom továbbá azon kutatóknak, akik elsősorban magyar felsőoktatási intézményekben a témához kapcsolódó további tudományos vizsgálatok elvégzését és eredményeik hasznosítását célul tűzik ki célul. Eredményeim és megállapításaim alapul szolgálhatnak a küszöbön álló jogszabálymódosítások során.

További kutatásra ajánlom a rendszerek sérülékenységei adatait, melyekből megítélésem szerint a grounded theory alkalmazásával további tudományos értékű megállapítások tehetők.

Emellett ajánlásom kiterjed a felsőoktatási vezetők közös fórumának kialakítására és közöttük egy „forró vonal” létrehozására a szektort érintő informatikai incidensek gyors kezelhetősége érdekében. A korábbi időszak számos eseménye bizonyítja, hogy ennek hiányában egy, a teljes szektort érintő támadás esetén a felsőoktatási intézmények nem képesek azonnali védelmi intézkedések megtételére. A törvényhozók számára pedig ajánlást teszek a felsőoktatási informatikai rendszerek üzemeltetésével kapcsolatos szabályzás szigorítására, és a 2013 évi L. törvény hatálya alá helyezésére.

Végül javasom a dolgozatomban kidolgozott besorolási rendszer alkalmazását a felsőoktatási intézmények szabályzatainak kidolgozásakor és rendszereik biztonsági besorolásainak meghatározása során.

6.3. Témakörből készült publikációk

Lektorált folyóiratban megjelent cikkek

[M1] Koczka Ferenc, Négyesi Imre: Az információbiztonság fejlesztésének lehetőségei az akadémiai szférában. Hadtudományi Szemle, Ludovika Egyetemi Kiadó, Budapest, 13. évf. (2020) 1. sz. 113–130. oldal. DOI: 10.32563/hsz.2020.1.9

[M2] Koczka Ferenc: A felsőoktatási intézmények informatikai védelmének szektorspecifikus kérdései. Hadmérnök, Ludovika Egyetemi Kiadó, Budapest

[M3] Koczka Ferenc: Egy egyetemi informatikai rendszeren végzett sérülékenységvizsgálat módszere és néhány tapasztalata. Felderítő Szemle, megjelenés alatt.

[M4] Koczka Ferenc: Szemelvények egy felsőoktatási rendszer informatikai védelmének tapasztalataiból. Networkshop 2023 konferenciakötet, megjelenés alatt.

Idegen nyelvű kiadványban megjelent cikkek

[K1] Koczka, F. (2020) "Opportunities of Darknet Operations in Cyber Warfare: Examining its Functions and Presence in the University Environment", AARMS – Academic and Applied Research in Military and Public Management Science. Budapest, 19(1), pp. 65–81. doi: 10.32565/aarms.2020.1.6.

[K2] Koczka, F. (2021) "Security of Encryption Procedures and Practical Implications of Building a Quantum Computer", AARMS – Academic and Applied Research in Military and Public Management Science. Budapest, 19(3), pp. 5–22. doi: 10.32565/aarms.2020.3.1.

Konferencia kiadványban megjelent előadás

[O1] Koczka Ferenc: Információbiztonsági teszt az Eszterházy Károly Egyetemen. Networkshop 2018, Hungarnet, 2018.04.04-06. Doi: 10.31915/NWS.2018.1

[O2] Koczka Ferenc: Issues of Legal Regulation of Hungarian Higher Education IT Systems, Austrian Computer Society (OCG), Budapest, 2021.05.10-11. DOI: 10.24989/ocg.v341.22

[O3] Koczka Ferenc: OSINT technológiák és alkalmazási lehetőségeik a felsőoktatási rendszerek ellen, Online térben az online térért: Networkshop 30 országos online konferencia, 2021. április 6-9. Doi: 10.31915/NWS.2021.21

Könyvfejezetek:

[F1] Krasznay Csaba, Koczka Ferenc: A távolléti oktatás jelentette kiberbiztonsági és adatvédelmi kihívások, Járvány sújtotta társadalom: A koronavírus a társadalomtudományok szemüvegén keresztül (tanulmánykötet), Budapest, 2021.

[F2] Koczka Ferenc: Az ellátási láncok támadása, azaz mi történik, ha már a nyomtatott áramkör sem megbízható? Taktikák és stratégiák a kiberhadviselésben, NKE, Budapest, 2021.

Konferenciák

[N1] Koczka Ferenc: Hiding illegal contents on the net: is it possible or even necessary? In Service of The Nation Conference, Budapest, 2019.11.22.

[N2] Koczka Ferenc: Felsőoktatási rendszerek védelmi problémái. XXIII. Tavaszi Szél Konferencia, Budapest, NKE, 2020.

[N3] Koczka Ferenc: Kinek a felelőssége? Networkshop 2020 online konferencia, 2020. 09.03.

[N4] Protection Issues in Higher Education Systems, CASPA Seminar and Workshop in Tallinn, 2021.10.04-08.

[N5] Egy új kockázat az informatikai védelemben: a kvantumszámítógép. Információvédelem menedzselése XCIX. Szakmai fórum, Budapest, 2022.01.19.

[N6] IDS bevezetésének tapasztalatai az Eszterházy Károly Egyetemen. Networkshop 2022 Konferencia, Debrecen, 2022.04.21.

[N8] IDS bevezetésének tapasztalatai az Eszterházy Károly Egyetemen. Networkshop 2022 Konferencia, Debrecen, 2022.04.21.

[N9] Koczka Ferenc – Prantner Csilla – Biró Csaba: A posztkvantum kriptográfia aktuális kérdései. Networkshop 2023 konferencia.

Egyetemi jegyzet

[E1] Koczka Ferenc: A Unix operációs rendszer. https://oprendszer.koczka.com.

Publikációk és hipotézisek kapcsolata

Tudományos eredmény	Publikáció
H1.	M1, M3
H2.	F1, F2
H3.	O1
H4.	M2, K1, O2

7. Irodalom

[1] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 2013.

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 2022.

[3] 41/2015. (VII. 15.) BM Rendelet, Magyar Közlöny, 103. szám.

[4] Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete, 27. 04. 2016. [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. Hozzáférés dátuma: 2022.01.

[5] A. I. P. Sudrastawa, Sariyasa, K. Y. E. Ayanto, Sensitive Personal Data Publication on Higher Education Information System Websites in Indonesia, in 2nd International Conference of Computer and Informatics Engineering (IC2IE), Indonesia, 2019.

[6] 2009/2015. (XII. 29.) Kormány határozata nemzetbiztonsági védelem alá eső szervek és létesítmények köréről, 2015.

[7] Horváth D., A. Mitev: Alternatív Kvalitatív Kutatási Kézikönyv, Budapest, Alinea Kiadó, 2015.

[8] L. Cohen, M. Lawrence, M. Keith: Research Methods in Education, London, Routledge, 2017.

[9] G. Wangen, J. B. Ulven: A Systematic Review of Cybersecurity Risks in Higher Education, Future Internet, 13. kötet, 1-40 o., 2021.

[10] N. Rahima, Z. Othmanb, F. Z. Hamidc: Cyber Security and the Higher Education Literature: A Bibliometric Analysis, International Journal of Innovation, Creativity and Change, 12. kötet, 12. szám, 2020.

[11] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 2020.

[12] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin és N. B. Hamdullah, Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, 62. kötet, 1. szám, 82-97 o., 2022.

[13] A. Alruwaili: A Review of The Impact of Training on Cybersecurity Awareness, International Journal of Advanced Research in Computer Science, 10. kötet, 5. szám, 1-3 o., 2019.

[14] Cyber security and defence European Parliament resolution of 22 November 2012 on Cyber Security and Defence (2012/2096(INI)), 2012.

[15] Stratégiai Koncepció az Észak-atlanti Szerződés Szervezete tagállamainak védelméért és biztonságáért. Lisszabon, Elérhető: https://2010-2014.kormany.hu/download/b/52/20000/nato_strategiai_koncepcio.pdf Hozzáférés dátuma: 2022.03.

[16] NATO, Defending the networks - The NATO Policy on Cyber Defence, 2011. Elérhető: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf Hozzáférés dátuma: 2022.03.

[17] D. Appelman: California Requires Disclosure of Database Security Breaches, Usenix, Usenix, 2004.

[18] Australian Government Department of Home Affairs, 11 2020. [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: 2022.04.

[19] 2011. évi CCIV. törvény a nemzeti felsőoktatásról, 2011.

[20] 2012. évi C. törvény a Büntető Törvénykönyvről, 2012.

[21] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Gaithersburg, NIST, 2018. https://doi.org/10.6028/NIST.CSWP.04162018

[22] NIST Roadmap for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2019.

[23] Az Európai Parlament és a Tanács (EU) 2022/2555 Irányelve, 2022.

[24] P. J. Ballard: Measuring Performance Excellence: Key Performance Indicators for Institutions Accepted into the Academic Quality Improvement Program (AQIP), 2013.

[25] J. J. Giszczak, D. A. Paluzzi: Pass or Fail? Data Privacy and Cybersecurity Risks in Higher Education, McDonald Hopkins, 2016.

[26] E. K. Kwaa-Aidoo, M. Agbeko: An Analysis of Information System Security of a Ghanaian University, International Journal of Information Security Science, 7. kötet, 2. szám, 90-99. o., 2017.

[27] Rendszeres szociális ösztöndíjakkal kapcsolatos adatkezelés a Budapesti Műszaki és Gazdaságtudományi Egyetemen, NAIH/2020/54.

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

[29] I. G. Butnaru, V. Nita, A. Anichiti: 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.

[30] B. Sebastian, L. V. Ulrike: ChatGPT Participates in a Computer Science Exam, 2023.03.23. [Online]. Elérhető: https://arxiv.org/pdf/2303.09461.pdf. Hozzáférés dátuma: 2023.08.

[31] L. W. Loo: Student Hacking into University's Learning Management System to Save His Grades: A Cautionary Tale, Singapore Management University, Singapore, 2016.

[32] Unit-Department for ICT and Joint Services in Higher Education and Research, Direktoratet for IKT og fellestjenester i høyere tdanning og forskning, Norway, 2019.

[33] FireEye Inc.: Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about It. White paper, Fireeye Inc., 2015.

[34] G. Kapitány: Hekkerek támadták meg a PTE informatikai rendszereit: a Lázlap is leállt!, Pécs Aktuál, 2023.04.24.

[35] I. Bongiovanni: The least secure places in the universe? A systematic literature review on information security management in higher education, Computers & Technology, 86. kötet, 350-357 o., 2019. https://doi.org/10.1016/j.cose.2019.07.003

[36] J. Chapman: Higher Education Policy Institute, 2019. [Online]. Elérhető: https://www.hepi.ac.uk/wp-content/uploads/2019/03/Policy-Note-12-Paper-April-2019-How-safe-is-your-data.pdf. Hozzáférés dátuma: 2023.08.

[37] Verizon: Educational Services, 2022. [Online]. Elérhető: https://www.verizon.com/business/resources/reports/dbir/2022/data-breaches-in-education/. Hozzáférés dátuma: 2022.04.03.

[38] 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, 3. szám3, 1-12. o.

[39] N. Dragoni, A. L. Lafuente, F. Massacci, A. Schlichtkrull: Are we preparing students to build security in? A survey of European cybersecurity in higher education programs [Education], IEEE Security & Privacy, 19. kötet, 1. szám, 81-88. o., 2021.

[40] G. Vámosi: Ezerhétszáz 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.

[41] 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. Hozzáférés dátuma: 2022.01.10.

[42] Nemzeti Adatvédelmi és Információszabadság Hatóság, Közérdekű adatigénylés, 2018.12.08. [Online]. Elérhető: https://kimittud.hu/request/12018/response/17739/attach/3/NAIH%202019%20741.pdf. Hozzáférés dátuma: 2022.12.10.

[43] M. Schreier: Qualitative Content Analysis in Practice, London, SAGE Publications Ltd, 2012.

[44] K. R. Yin: Case study research and applications: Design and methods (Sixth Edition), Sage publications, 2017.

[45] S. Vinovski: Where is Middleware?, IEEE Internet Computing, 6. kötet, 2. szám, 83-85. o., 2002.

[46] U.S. Department of Education: 34 CFR Part 99—Family Educational Rights And Privacy, U.S. Department of Education, 2011.

[47] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, 2020.04.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2011-112-00-00.29. Hozzáférés dátuma: 2023.04.10.

[48] A. Adams, A. Blandford: Security and Online Learning: to Protect or Prohibit, in Usability Evaluation of Online Learning Programs, UK, Information Science Publishing, 2003, pp. 331-359.

[49] S. Al-Janabi, I. Al-Shourbaji: A Study of Cyber Security Awareness in Educational Environment in the Middle East, Journal of Information & Knowledge Management, 1. kötet, 2016.

[50] A. Bochner, J. Abbott, J. L. Camp: Potential Reuse of University Credentials, in USENIX Symposium on Usable Privacy and Security (SOUPS), Vancouver, 2021.

[51] C. Herley, V. P. Oorschot és A. S. Patrick: Passwords: If We're So Smart, Why Are We Still Using Them?, Financial Cryptography and Data Security, 5628. kötet, 2009.

[52] A. Adams, A. M. Sasse: Users Are Not The Enemy, Communications of the ACM, 1999. kötet, 42/12. szám, 40-46. o.

[53] S. Chiasson, A. Forget, R. Biddle, P. v. Oorschot: Influencing Users Towards Better Passwords: Persuasive Cued Click-Points, People and Computers XXII Culture, Creativity, Interaction (HCI), Ottawa, 2008.

[54] W. Meng, L. Zhu, W. Li, J. Han, Y. Li: Enhancing the security of FinTech applications with map-based graphical password authentication, Future Generation Computer Systems, 101. kötet, 1018-1027. o., 2019.

[55] J. Kävrestad, J. Zaxmy, M. Nohlberg: Analyzing the usage of character groups and keyboard patterns in password creation, Information & Computer Security, 28. kötet, 3. szám, 347-358. o., 2020.

[56] J. Bonneau: The science of guessing: analyzing an anonymized corpus of 70 million password, in IEEE Symposium on Security and Privacy, 2012.

[57] G. Wangen: Unrecorded Security Incidents at NTNU. Bachelor's Thesis., Trondheim, Sweden, NTNU Open Gjøvik., Sweden, 2019.

[58] F. Koczka: Információbiztonsági teszt az Eszterházy Károly Egyetemen, Hungarnet Egyesület, Budapest, 2018.

[59] R. Morris, K. Thompson. Password Security: a Case History, 1979. Elérhető: https://rist.tech.cornell.edu/6431papers/MorrisThompson1979.pdf.

[60] Mitre: Mitre | Att&ck, [Online]. Elérhető: https://attack.mitre.org. Hozzáférés dátuma: 2023.08.10.

[61] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, J. Li: Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity, Energies, 2509. kötet, DOI: 10.3390/en13102509, 2020.

[62] E. Aminanto, K. Kwangjo: Deep learning in intrusion detection system: An overview., in International Research Conference on Engineering and Technology, Bali, 2016.

[63] A. Patel, M. Taghavi, K. Bakhtiyari, J. J. Celestino: An intrusion detection and prevention system in cloud computing: A systematic review, Journal of Network and Computer Applications, 36. kötet, 1. szám, 25-41. o., 2013.

[64] F. Zhang, S. Zhou, Z. Qin, J. Liu: Honeypot: a supplemented active defense system for network security, in Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, Chengdu, China, 2003.

[65] E. D. Mann, M. S. Christey: Towards a Common Enumeration of Vulnerabilities, in The MITRE Corporation, Bedford, 1999.

[66] Mitre: Common Vulnerabilities and Exposures, Elérhető: https://www.cve.org/About/History.

[67] A. Arora, N. Anand, R. Telang: Does information security attack frequency increase with vulnerability disclosure? An empirical analysis., Information Systems Frontiers, 8. kötet, 350-362. o., 2006.

[68] First Inc: CVSS, [Online]. Elérhető: https://www.first.org/cvss/v3.1/specification-document. Hozzáférés dátuma: 2023.06.11.

[69] P. Johnson, R. Lagerström, M. Ekstedt, U. Franke: Can the common vulnerability scoring system be trusted? A Bayesian analysis, IEEE Transactions on Dependable and Secure Computing, 16. kötet, 6. szám, 2018.

[70] A. Murray: What Is CVSS v3.1? Understanding The New CVSS. Mend Report, Mend, Mend.io, 2020.

[71] P. Karger, R. Schell: Multics Security Evaluation: Vulnerability Analysis, Information Systems Technology Applications Office Deputy for Command and Managements Systems Electronic Division, 1974.

[72] A. M. N. F. Shaker, A. M. Mohamed, Zero Click Attack, in The International Undergraduate Research Conference, 2021.

[73] A. Tereshkin, A. Tereshkin, Evil maid goes after PGP whole disk encryption, in Proceedings of the 3rd International Conference on Security of Information and Networks, SIN'10, 2010.

[74] A. Mallik: Man-In-The-Middle_Attack: Understanding in Simple Words, Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2. kötet, 2. szám, 109-134. o., 2018.

[75] M. Bozorgi, L. Saul, S. Savage, M. G. Voelker: Beyond Heuristics: Learning to Classify Vulnerabilities and Predict Exploits, in In Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Washington, 2010.

[76] L. Allodi, F. Massacci: Comparing vulnerability severity and exploits using case-control studies, ACM Transactions on Information and System Security, 17. kötet, 1. szám, 1-20. o., 2014.

[77] L. Allodi, F. Massacci: Security Events and Vulnerability Data for Cybersecurity Risk Estimation, Risk Analysis - Special Issue: Advances in Risk Analysis with Big Data, 37. kötet, 8. szám, 2017.

[78] F. Valeur, G. Vigna, C. Kruegel, R. A. Kemmerer: A Comprehensive Approach to Intrusion Detection Alert Correlation, IEEE Transactions on Dependable and Secure Computing, 1. kötet, 3. szám, 146-169. o., 2004.

[79] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, M. Roytman: Exploit Prediction Scoring System (EPSS), Digital Threats: Research and Practice, 2. kötet, 3. szám, 1-17. o., 2021.

[80] O. Negoita, M. Carabas: Enhanced Security Using Elasticsearch and Machine Learning, in Science and Information Conference, 2020.

[81] L. Demetrio, B. Biggio, G. Lagorio, F. Roli, A. Armando: Explaining Vulnerabilities of Deep Learning to Adversarial Malware Binaries, arXiv:1901.03583, 2019.

[82] Tihanyi N., Vargha G., Frész F.: Biztonsági tesztelés a gyakorlatban, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[83] Törőcsik M., Kozlovszky M.: IT sérülékenység vizsgáló szoftverek összehasonlító elemzése, in Networkshop 2013 Konferencia, Sopron, 2013.

[84] I. Chalvatzis, C. P. Rallis, A. D. Karras: Evaluation of Security Vulnerability Scanners for Evaluation of Security Vulnerability Scanners for Resilience towards Risk Assessment, in 2019 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), China, 2019.

[85] S. Stanković, S. Gajin, R. Petrović: A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis, in Proceedings, Ix International Conference Icetran, Novi Pazar, 2022.

[86] Google Inc.: Google Security Blog, Google Inc., 2015.12.15. [Online]. Elérhető: https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html. Hozzáférés dátuma: 2022.10.10.

[87] M. A. Dissanayaka, S. Mengel, L. Gittner, H. Khan: Vulnerability Prioritization, Root Cause Analysis, and Mitigation of Secure Data Analytic Framework Implemented with MongoDB on Singularity Linux Containers, in Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis, 2020.

[88] D. Rountree: Cryptography. Security for Microsoft Windows System Administrators, ISBN 9781597495943, 2011.

[89] C. Herley: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, Microsoft Research, 2010.

[90] P. A. Henry: Authentication Tokens, in Information Security management Handbook, 2. kötet, 146. o. ISBN 1-4200-6708-7.

[91] D. Ferbrache: Passwords are broken – the future shape of biometrics, Biometric Technology Today, 2016. kötet, 3. szám, 5-7. o., 2016.

[92] Adobe Inc.: Customer security alert, Adobe Inc., 2013.10.28. [Online]. Elérhető: https://helpx.adobe.com/x-productkb/policy-pricing/customer-alert.html. Hozzáférés dátuma: 2023.03.12.

[93] A. Agarwal: Security update and new features, Dropbox Inc., 2012.07.31. [Online]. Elérhető: https://blog.dropbox.com/topics/company/security-update-new-features. Hozzáférés dátuma: 12 03 2023.03.12.

[94] N. Raymond: Sony to pay up to $8 million in 'Interview' hacking lawsuit, Reuters, 2015.10.20. [Online]. Elérhető: https://www.reuters.com/article/us-sony-cyberattack-lawsuit-idUSKCN0SE2JI20151020. Hozzáférés dátuma: 2023.03.12.

[95] K. Toubba: Notice of Recent Security Incident, LastPass Inc., 2022.12.22. [Online]. Elérhető: https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/. Hozzáférés dátuma: 2023.03.12.

[96] T. Hunt: The 773 Million Record "Collection #1" Data Breach, 07 01 2019. [Online]. Elérhető: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/. Hozzáférés dátuma: 2020.06.19.

[97] C. Endrődi, K. Csorba: Kriptográfiai algoritmus implementációjának időalapú támadása, in Networkshop konferencia, Budapest, 2004.

[98] P. P. Pittalia: A Comparative Study of Hash Algorithms in Cryptography, International Journal of Computer Science and Mobile Computing, 8. kötet, 6. szám, 147-152. o., 2019.

[99] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, Report on Post-Quantum Cryptography, National Institute of Standards and Technology, Gaithersburg, 2016.

[100] A. Papp: Feltörték több hazai egyetem Neptun rendszerét, 2023.04.27. [Online]. Elérhető: https://24.hu/belfold/2023/04/27/kozlemeny-elte-corvinus-neptun-uzenetek-informatikai-rendszer-tamadas/. Hozzáférés dátuma: 2023.04.27.

[101] V. Mathy, F. Piessens: Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, Conference on Computer and Communications Security, Dallas, 2017.

Ábrák jegyzéke

Táblázatok jegyzéke

Mellékletek

1. sz. melléklet. A NAIH adatszolgáltatása a magyar oktatási intézményeket ért, a nyilvántartásukban szereplő incidensekről. (A NAIH-3731-2/2023. számú irat melléklete.)

Dátum	**Szervezet neve**	**Adatvédelmi incidens jellege**
2019.02.19	Százhalombattai 1. számú Általános Iskola	az iskola szerverét feltörték, adatokat titkosítottak rajta
2018.05.31	Pécs Tudományegyetem	adathalász e-mail alapján egy felhasználó kiadta az e-mail fiókjának adatait
2018.06.22	Budapesti Metropolitan Egyetem	egy egyetemi hallgató visszaélt oktatójának Neptun belépési azonosítóival
2018.08.30	Pécsi Tudományegyetem	hírlevélhez téves csatolmány
2018.12.20	Eötvös Loránd Tudományegyetem	a szerver számítógépen nagy mennyiségű adatállomány elérhetetlenné vált
2019.02.04	Pécsi Tudományegyetem	egy e-mail címzettjei láthatták egymás e-mail címeit
2019.03.08	Eötvös József Általános Iskola és Óvoda	zsarolóvírus
2019.04.12	Budapesti Műszaki és Gazdaságtudományi Egyetem	postai küldemény téves címre küldése
2019.04.15	Pécsi Tudományegyetem	egy e-mail címzettjei láthatták egymás e-mail címeit
2019.06.21	Debreceni SZC Bethlen Gábor Közgazdasági Szakgimnáziuma	érettségin tanulói személyes adatok nem bizalmas kezelése
2019.06.28	Liszt Ferenc Zeneművészeti Egyetem	Neptunban egy üzenet megküldése véletlenül több címzettnek
2019.08.02	Veszprém Megyei Gyermekvédelmi Központ, Általános Iskola, Szakiskola, Készségfejlesztő Iskola és Területi Gyermekvédelmi Szakszolgálat	adat illetéktelen továbbítása
2019.11.29	Pázmány Péter Katolikus Egyetem	személyes adatokat tartalmazó dokumentumok véletlenül nyilvános hulladéktárolóba lettek dobva
2020.02.03	Szent István Egyetem	belső levelezőrendszerből ismeretlen módon kikerült információk nyilvánosságra kerülése
2020.03.03	Eötvös Loránd Tudományegyetem	zsarolóvírus
2020.03.20	Makói Katolikus Általános Iskola és Óvoda	zsarolóvírus
2020.04.17	Soproni Egyetem	zsarolóvírus
2020.05.02	Pécsi Tudományegyetem	zárt bizottsági ülést egy illetéktelen személy is online végighallgathatott
2020.05.15	Közép-európai Egyetem	egy e-mail címzettjei láthatták egymás e-mail címeit
2020.06.08	Eötvös Loránd Tudományegyetem	egy e-mail címzettjei láthatták egymás e-mail címeit

2020.07.24	Közép-európai Egyetem	zsarolóvírus
2020.08.19	Shetland U.K. Nyelviskola Oktató és Szolgáltató Kft.	hackertámadás
2020.09.25	Szent István Egyetem	felvételi honlap megrongálása (deface)
2020.09.28	Pécsi Tudományegyetem	online oktatás anyagának engedély nélküli feltöltése videómegosztó portálra
2020.11.18	Karolina Katolikus Általános Iskola, Székesegyházi Kórusiskola és Alapfokú Művészeti Iskola	levelezőlistán téves adatok megosztása
2020.11.26	Budapesti Corvinus Egyetem	adathalászat egy régi adatbázisból
2020.11.27	Pécsi Árpád Fejedelem Gimnázium és Általános Iskola	digitális óra megosztása
2020.12.18	Debreceni Egyetem	e-mail téves címre kiküldése
2021.02.22	Bogyiszlói Általános Iskola	e-naplóba nem odavaló jegyek kerültek beírásra illetéktelen személy által
2021.03.12	Pécsi Tudományegyetem	Neptunba téves személyes adatok feltöltése
2021.03.31	Pécsi Tudományegyetem	egy e-mail címzettjei láthatták egymás e-mail címeit
2021.04.23	Budapesti Osztrák Iskola	MS Team hozzáférés kompromittálódása
2021.04.29	Sztehlo Gábor Evangélikus Óvoda, Általános Iskola és Gimnázium	egy e-mail véletlenül több email címre is ki lett küldve
2021.04.29	Sztehlo Gábor Evangélikus Óvoda, Általános Iskola és Gimnázium	adat kiküldése tévedésből több e-mail címre is
2021.06.23	Veszprém Megyei Gyermekvédelmi Központ, Általános Iskola, Szakiskola, Készségfejlesztő Iskola és Területi Gyermekvédelmi Szakszolgálat	számítógépen tárolt adatokhoz való hozzáférés lehetséges volt
2021.06.24	Veszprém Megyei Gyermekvédelmi Központ, Általános Iskola, Szakiskola, Készségfejlesztő Iskola és Területi Gyermekvédelmi Szakszolgálat	személyes adatokat is tartalmazó pendrive elvesztése
2021.08.13	Pécsi Tudományegyetem	egy e-mail címzettjei láthatták egymás e-mail címeit
2021.08.26	Balatonfüredi Református Általános Iskola és Óvoda	külső merevlemez eltűnése
2021.09.10	Dunakeszi Tankerületi Központ	álláspályázó személyes iratanyagának rossz címre küldése
2021.11.29	Kocha Valéria Gimnázium, Általános Iskola, Óvoda, Kollégium és Pedagógiai Intézet	levél véletlenül több címzettnek ment ki
2022.01.16	Nemzeti Közszolgálati Egyetem	adathalászat
2022.01.19	Eszterházy Károly Katolikus Egyetem	adathalászat

2022.01.24	Monori Tankerületi Központ	egy általános iskolába besurranó személy az osztályteremből eltulajdonította a tanári laptopot
2022.03.21	Monori Tankerületi Központ	a tankerületi igazgató hivatalos, nyilvánosan elérhető e-mail fiókját feltörték, és spam küldésre használták.
2022.06.16	Kocha Valéria Gimnázium, Általános Iskola, Óvoda, Kollégium és Pedagógiai Intézet	téves melléklet csatolása ez üzenethez
2022.06.30	Vas Megyei SzC Hefele Menyhért Szakképző Iskola	hackertámadás
2022.07.09	Pécsi Tudományegyetem	Neptun üzenet címzettjei láthatták egymás nevét és Neptun kódját
2022.08.16	Európa 200 Gimnázium	zsarolóvírus
2022.08.25	Óbudai Egyetem	egyetem egy oldala hozzáférhetővé vált illetéktelen személyek részére
2022.09.15	Várkerti Általános Iskola Vásárhelyi András Tagiskolája	pedagógus fiókjainak feltörése, nevében üzenetek küldése
2022.09.22	Közép-Pesti Tankerületi Központ	munkavállalói személyi anyag téves címre postázása
2022.11.07	Kísérleti Orvostudományi Kutatóintézet	illetéktelenek hozzáfértek a levelezőrendszerhez
2022.11.09	Bajai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Kecskeméti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Szigetszentmiklósi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Székesfehérvári Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Kisvárdai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Békéscsabai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Jászberényi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Külső-pesti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Szegedi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Észak-budapesti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Nyíregyházi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Zalaegerszegi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens

2022.11.09	Salgótarjáni Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Szombathelyi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Soproni Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Szigetvári Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Miskolci Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Berettyóújfalui Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Kiskőrösi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Dél-Pesti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Egri Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Balassagyarmati Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Mohácsi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Kaposvári Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Dunaújvárosi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Karcagi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Sárospataki Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Esztergomi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.09	Érdi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Szolnoki Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Sárvári Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Közép-budai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Észak-Pesti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Pápai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Tamási Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens

2022.11.10	Szekszárdi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Belső-Pesti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	eKréta Informatikai Zrt.	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Hajdúböszörményi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Pécsi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Kazincbarcikai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Debreceni Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Szerencsi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Monori Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Dunakeszi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Balatonfüredi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.10	Váci Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Mezőkövesdi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Nagykanizsai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Mátészalkai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Tatabányai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Klebelsberg Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Győri Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Gyulai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Ceglédi Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Dél-budai Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Tolna Megyei Szakképzési Centrum	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens

2022.11.11	Kelet-Pesti Tankerületi Központ	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Veszprémi Szakképzési Centrum	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Érdi Szakképzési Centrum	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.11	Dunaújvárosi Szakképzési Centrum	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.15	Kratochvil Károly Honvéd Középiskola és Kollégium	eKRÉTA rendszerhez kapcsolódó adatvédelmi incidens
2022.11.18	Szigetszentmiklósi Bíró Lajos Általános Iskola	kamera előzetes engedély nélküli felhelyezése
2022.12.16	Károli Gáspár Református Egyetem	illetéktelen személy spam üzenetteket küldött egy egyetemi fiókból
2023.01.16	Dunakeszi Tankerületi Központ	egy szakgimnázium a neten közzétette a felvételiző tanulók személyes adatait is tartalmazó táblázatot
2023.01.27	Károli Gáspár Református Egyetem	egy hallgató fiókját feltörték, nevében spam emaileket küldtek ki
2023.02.01	Károli Gáspár Református Egyetem	egy dolgozó fiókját feltörték, nevében spam emaileket küldtek ki
2023.02.09	Pécsi Tudományegyetem	személyes adatok kiadása illetéktelen személynek
2023.02.17	Déli ASzC Móricz Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium	e-naplóba nem oda való jegyek kerültek beírásra illetéktelen személy által
2023.02.24	Károli Gáspár Református Egyetem	egy dolgozó fiókját feltörték, nevében spam emaileket küldtek ki
2023.03.06	Károli Gáspár Református Egyetem	hallgatói fiók feltörése
2023.03.11	Nemzeti Közszolgálati Egyetem	egy felhasználói fiók kompromittálódott, spamek kiküldésére használták

2. sz. melléklet. Az egyes sérülékenységek száma éves bontásban. Forrás: saját szerkesztés.

Év	Mérés		
	Belső hálózatból	Belső hálózatból Info típus nélkül	Külső hálózatból Info nélkül
1970	6	0	0
1990	29	0	0
1995	289	0	0
1996	80	0	0
1997	713	0	0
1999	33	0	146
2000	13	0	0
2001	0	0	6
2002	117	0	2
2003	7	0	6
2004	192	0	16
2005	151	0	3
2006	25	0	0
2007	225	11	7
2008	74	0	22
2009	280	0	0
2010	166	0	6
2011	307	0	7
2012	78	0	0
2013	213	42	18
2014	962	77	12
2015	577	84	10
2016	565	565	36
2017	384	331	7
2018	367	367	19
2019	485	485	12
2020	192	188	29
2021	835	835	11
2022	17	16	0
Összesen	**7382**	**3001**	**375**