NEMZETI KÖZSZOLGÁLATI EGYETEM
Katonai Műszaki Doktori Iskola

Koczka Ferenc

Felsőoktatási rendszerek védelmi kérdései

Doktori (PhD) Értekezés

Tézisfüzet

Témavezető:

Dr. Krasznay Csaba

BUDAPEST, 2023

Tartalom

1. Összefoglaló

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

Amellett, hogy a magyar jogszabályok nem rendelkeznek közvetlenül a felsőoktatás informatikai védelmi környezetéről, az egyetemek működése és a dolgozók attitűdjei is eltérnek a gazdasági szférában megszokottól. Az egyetemi környezetet az oktatói és kutatói szabadság mellett a nyitottság jellemzi, mely konfliktushelyzetet teremt 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 [1]. A FireEye fehér könyve [2] 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, az üzemeltetés célja pedig a minél szigorúbb védelmi eljárások bevezetése és érvényesítése, mely a felsőoktatásban nehezen kezelhető helyzetet teremt. Ezt a jelenséget Adams már 2003-ban megfogalmazza, és a kultúrák összecsapásának *(clash of cultures)* nevezte [1].

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 komoly 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, melyet az informatikai rendszereiknek is követniük kell. Személyes tapasztalatom, hogy ezek a változások a Covid19 helyzet által kikényszerített gyors változásokhoz hasonlóan általános negatív hatást fejt ki az általános informatikai biztonságra.

Kutatásom elsődleges célja a felsőoktatás informatikai állapotának tudományos vizsgálata, adatvagyonának feltárása, valamint annak bizonyítása, hogy informatikai rendszereik védelmi besorolásait heterogén módon végzik el. Különböző adatbázisok alapján kimutattam, hogy nem

csak belső informatikai incidenseket szenvednek el, hanem kibertámadók célpontjai is, a rendelkezésre álló adatok alapján elemeztem ezek motivációit és módszereit. Sérülékenységvizsgálattal adatbázist építettem egy magyar egyetem informatikai rendszerének sebezhetőségeiről, és annak elemzésével kimutattam néhány jellegzetességét. A mérési eredményekből kiindulva kidolgoztam egy, az alkalmazott rendszerek és köztük fennálló adatkapcsolatokon alapuló metodikát, amely alkalmazásával a felsőoktatási intézmények védelme megerősíthető és a környezeti változásokra azonnali válasz adható.

2. A vizsgált probléma

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. 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 jogi szabályzás megengedő jellege mellett ezek az intézmények nagy mennyiségű érzékeny adatot kezelnek, mely arányos és költséghatékony védelmének nélkülözhetetlen feltétele az informatikai rendszerekben tárolt értékek azonosítása, melyeket a szektor intézményei részben azonos szoftverek eltérő környezetben tárolnak és működtetik alkalmazói rendszereiket. Magyar viszonylatban ezeket ismeretlen számban érik támadások, továbbá változásaik tendenciáira sem ismertek mérések vagy kutatási adatok.

A hatékony védelem meghatározó eleme a rendszerek sérülékenységeinek ismerete, ugyanakkor nem áll rendelkezése az oktatási intézmények állapotát leíró adat, melynek ismeretében az adott rendszerekre vonatkozó arányos védelmi intézkedések a már azonosított adatvagyon ismeretében pontosan meghatározhatók és alkalmazhatók lennének. A problémát egyetemi informatikai rendszereken végzett, azok felépítésére adaptált sérülékenységvizsgálat igazolhatja.

A bemutatott problémákra adott válaszok alapján a felsőoktatási intézmények védelmi hatékonyságának javítására ideális megoldást adhat egy metodika kidolgozása, mely a szféra

sajátosságainak figyelembe vétele mellett lehet képes az egymáshoz kapcsolódó rendszerek tranzitív védelmi feladatainak meghatározásában.

A téma aktualitását az alábbi tényezők adják:

- Jogszabályi háttér várható változása. Az Európai Unió NIS2 ajánlása számos új, az informatikai biztonság javítására szolgáló követelmény mellett korábbiak szigorítását javasolja, miközben jelentősen bővíti az érintett intézmények körét is. Míg a korábbi ajánlások a kritikus infrastruktúrákat és digitális szolgáltatókat célozták, a NIS2 hatálya lényegesen szélesebb körre terjed ki úgy, hogy az adott ágazat érvényben levő jogszabályaival koherens módon alkalmazható maradjon. Ezek a változások minden bizonnyal a felsőoktatási intézmények számára is komoly, jogszabályi szinten megjelenő változást hoznak.
- A felsőoktatás adatvagyonának csak részleges ismerete. Jelenleg nem áll rendelkezése olyan tudományos kutatás, mely a szektor adatvagyonának felmérését célozta volna.
- Az informatikai biztonságra az elmúlt időszakban nem csak a Covid19 és a szerkezeti átalakítások, hanem a háborús helyzet, és megváltozott gazdasági és munkaerőpiaci körülmények is negatív hatással voltak.
- A megfelelő vizsgálatok hiányában nem áll rendelkezésre adat a felsőoktatási rendszerek sérülékenységeinek mértékéről, azok kihasználhatóságáról, koráról.

Összességében a felsőoktatás helyzete több szempontból is egyedinek tekinthető, melyek vizsgálata eddig hazai viszonylatban nem történt meg, és nemzetközi viszonylatban sem áll rendelkezésre róluk jelentős számú kutatás vagy adat.

A cél elérésére dolgozatom az alábbi logika mentén épül fel:

1. A téma aktualitása, témaválasztás, és környezet. A fejezetben bemutatom a felsőoktatási intézmények informatikai rendszereivel kapcsolatos jogszabályi hátteret és kapcsolódó intézményeket, valamint a vonatkozó szakirodalmi források alapján meghatározom adatvagyonuk fő területeit. A fejezet részletezi a kutatási kérdéseket, a hipotéziseket és a kutatási módszereket.
2. A szabályzatok elemzéséhez meghatározom a magyar felsőoktatási intézmények reprezentatív mintáját a hallgatói- és oktatói létszám, fenntartó és nemzetbiztonsági felügyelet alapján. Ezen alapulva elvégzem szabályzataik elemzését, feltárom

alkalmazott informatikai rendszereiket és bizonyítom biztonsági besorolásaik különbözőségét. Több adatforrás felkutatásával, rendszerezésével és elemzésével kimutatom a felsőoktatási rendszereket ért támadások és incidensek mennyiségét, jellegét, időbeni változásaik mértékét és más szektorokhoz viszonyított arányukat. Közérdekű adatigényléssel gyűjtött adatok alapján bizonyítom a magyar felsőoktatási intézmények informatikai incidenseinek alacsony jelentési hajlandóságát.

3. Az egyetemi informatikai rendszerek védelmét befolyásoló humán szempontok feltárását követően bemutatom a sérülékenységek méréséhez kapcsolódó ismert módszereket, a működésüket megalapozó adatbázisokat és mérőeszközöket. Az általános, több egyetemre kiterjedő sérülékenységvizsgálatot megelőzően megvizsgálom annak jogszerűségi szempontjait, és egy egyetem elemzését lehetővé tevő esettanulmány alapján ellenőrzöm hipotéziseim bizonyíthatóságát. Az esettanulmány igazolhatósága esetén további mérésekkel bizonyítom azok általános jellegét, így hipotéziseim bizonyítását.
4. A vizsgálatok eredménye igazolja egy, a szektor egészére alkalmazható ajánlás szükségességét, melynek felépítésével bizonyítom, hogy az ibtv. szerinti besorolás kibővítésével létrehozható egy olyan metodika, mely az általános besorolási szabályok mellett figyelembe veszi a speciális intézményi tevékenységeiket, az alkalmazott szoftverek adottságait, adattartalmukat és a köztük fennálló adatcserével járó folyamatokat. A metodika alapvető eleme az egyes rendszerek állandó vagy rendszeres adatkapcsolatait leíró mátrix, változásait egy rendszeres sérülékenységvizsgálaton alapuló felülvizsgálat során feltárt sérülékenységek vagy konfigurációs hibák mutatják. A metodika alkalmazásával a meghatározott biztonsági besorolások pontosabbá válnak, az ideális védelmi eljárások meghatározása a rendszerrel szemben támasztott módosított bizalmassági, sértetlenségi és rendelkezésre állási besorolás változása alapján rövid időn belül módosítható.

3. Kutatási kérdések és módszerek

Kutatásomat a magyar felsőoktatási intézmények informatikai rendszereinek vizsgálata körében végeztem, kutatási kérdéseimet és hipotéziseimet ehhez kapcsolva, az alábbiak szerint határoztam meg:

1. Problémafelvetés: a felsőoktatási intézmények informatikai biztonsági szabályzatai nem egységesek, és hibás biztonsági besorolásokat alkalmaznak.

    a. KK1: milyen informatikai rendszerek működnek a magyar felsőoktatásban?

    b. KK2: milyen adatkört tárolnak ezek a rendszerek?

    c. KK3: milyen biztonsági besorolást alkalmaznak az intézmények az egyes rendszereik esetében?

    Hipotézis: a magyarországi felsőoktatási rendszerek adminisztratív szabályzásai heterogén tartalmúak és azonos feladatkört ellátó rendszereket eltérő besorolással kezelnek.

2. Problémafelvetés: magasabb számú sérülékenység mérhető a magyar felsőoktatási intézmények perifériális telephelyein üzemelő eszközein, mint a központban üzemelők esetében?

    a. KK1: milyen mennyiségű és jellegű sérülékenységek mutathatók ki az egyes telephelyeken üzemelő informatikai eszközökben?

    b. KK2: milyen arányban tér el ezek száma?

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

3. Problémafelvetés: jellemzően az egyes informatikai eszközöket működtető szoftverek, vagy az üzemeltetés által okozott konfigurációs hibák okozzák az informatikai rendszerek sérülékenységeit?

    a. KK1: milyen arányban mutathatók ki a CVSS ötfokozatú besorolása szerinti sérülékenységek a magyar felsőoktatási intézményekben?

    b. KK2: magasabb a hibás konfigurációs beállítások következményeként kimutatható hibák száma?

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

4. Problémafelvetés: javítható az informatikai rendszerek besorolási és védelmi eljárásrendje folyamatos sérülékenységvizsgálat elemzésével, valamint az egyes rendszerek kapcsolatai alapján az érintett rendszerekre történő kiterjesztésével?
    a. KK1: milyen ibtv. szerinti biztonsági besorolást célszerű alkalmazni az egyes rendszerekre?
    b. KK2: milyen tényezők befolyásolhatják a besorolás eltérését az egyes rendszerek esetén?
    c. KK3: Milyen kapcsolati mátrix írja le az egyes rendszerek közti lehetséges adatkapcsolatokat és milyen természetűek ezek?

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

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 eltérések 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 [3, 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 [3, pp. 83-128].

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.

4. A kutatás tapasztalatainak összefoglalása

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 e 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 üzemelteltető személyzet által javítható több éve fennálló beállítási hibák, melyek korrekciója a rendszerkonfigurációkra vonatkozó szigorúbb szabályzás mellett az elavult szoftver-, egyes esetekben 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.

5. 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. Hipotézisek levezetése

Vizsgálataimat négy hipotézis mentén rendszereztem, melyek az adatvagyon felmérése – jogi szabályozás megengedő jellege – informatikai incidensek és támadások előfordulása – sérülékenységek és hibás konfigurációs jelenléte az informatikai rendszerben – védelmi metodika kidolgozása gondolatmeneten alapultak.

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

A felsőoktatási intézmények adatvagyonának, informatikai rendszereinek feltárásának és ibtv. szerinti besorolásának egyik lehetséges módszere az informatikai szabályzatok dokumentumelemzése. A vizsgálandó egyetemek reprezentatív mintájának meghatározása után összegyűjtöttem szabályzataikat, a nem nyilvánosak esetében kértem azok kutatási célú rendelkezésre bocsájtását. Az egyes szabályzatok közti strukturális eltéréseket az általánosan alkalmazotthoz igazítottam, azok által alkalmazott skálákat harmonizáltam, végül listáztam rendszereiket és azok besorolását.

H1. hipotézist igazoltam: bár a kulcsrendszerek esetében kis mértékű eltérés volt tapasztalható, összességében számos rendszer besorolása eltérő, melyek közt kétpontos különbség is kimutatható volt.

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

A hipotézis bizonyításához az IT biztonság elemzésének elterjedt módszereinek vizsgálatát követően sérülékenységvizsgálattal gyűjtött adatok alapján végeztem. 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 értékeléséhez részben 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 adatokat elemeztem.
H2. hipotézis nem igazolható. Az esettanulmányban szereplő egyetem esetében nem volt szignifikáns különbség a központi infrastruktúra és a perifériális területeken mérhető sérülékenységek aránya tekintetében.

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

A mérések kiterjesztéseként kialakítottam a belső rendszer vizsgálatához szükséges műszaki követelményeket, a részletes elemezhetőség érdekében kialakítottam az egyetemeket jellemző szakterületi felosztást annak érdekében, hogy különbözőségeik megállapíthatók legyenek, és bemutattam azt a 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 rendszerek 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.
H3. hipotézist igazoltam: a vizsgált rendszerekben jelentős számban fordultak elő konfigurációs hibák és azok kora többségében meghaladta az egy évet.

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

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 soroltak, így azok védelmi eljárásai is valószínűleg eltérnek. A hipotézis igazolására kidolgozott metodika 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 testre szabtam az ibtv. besorolási kritériumait, 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 el. 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.

H4. hipotézist igazoltam: meghatároztam egy felsőoktatási informatikai rendszerekre alkalmazható kockázaton alapuló besorolási metodikát.

7. A kutatási eredmények gyakorlati hasznosíthatósága és 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.

8. Jövőbeli kutatási irányok

Dolgozatom elkészítése során nagy mennyiségű adatot gyűjtöttem. A Hackmageddon oktatási szektorra vonatkozó adatainak elemzésével folyamatosan követhetővé tehető a szektort ért kibertámadások mennyisége, más szektorokhoz viszonyított aránya és változásának iránya. További adatbázisok elemzésével naprakész információk állíthatók elő az oktatási intézményeket nem támadás jellegű informatikai incidenseiről. A sérülékenységvizsgálati adatok további elemzésével új összefüggések tárhatók fel, további intézmények elemzésével általános jellegük igazolható lehet.

A H4. bizonyításával kidolgozott védelmi metodika gyakorlati alkalmazásával annak működőképessége javítható, esetleges hibái módosíthatók. A megfelelő szoftveres háttér kidolgozásával alkalmazása automatizálható, az egyetemek saját sérülékenységvizsgálatával pedig kidolgozható lehet egy olyan közös felsőoktatási védelmi rendszer, mely alkalmazásával a bemutatott metodika hatóköre további egyetemekre is kiterjeszthető lehet.

9. Irodalomjegyzék

[1] 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.

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

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

10. A disszertáció témájához kapcsolódó publikációk jegyzéke

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. KNBSZ. (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://www.koczka.com.

11. Szakmai önéletrajz

Koczka Ferenc a Nemzeti Közszolgálati Egyetem (NKE) Katonai Műszaki Doktori Iskolájának 2022. július 8-án abszolutóriumot szerzett hallgatója. Jelenleg az Eszterházy Károly Katolikus Egyetem Számítástudományi Tanszékének, valamint a Nemzeti Közszolgálati Egyetem Kiberbiztonsági Tanszékének tanársegédje.

A doktorjelölt az egri 1. sz. Általános iskola zenei tagozatának befejezése után a Gárdonyi Géza Gimnáziumban érettségizett. Ezt követően éves sorkatonai szolgálatot töltött a bajai 1. sz. lövésszázadnál, majd az egri Ho Si Minh tanárképtő főiskolán matematika—fizika szakos tanári diplomát szerzett. Már a sorkatonai szolgálata során a figyelme a számítástechnika felé fordult, és főiskolai tanulmányai során is főként erre koncentrált. Több számítástechnikai versenyen ért el 1-3 helyezést, szakdolgozata egy számítógépes nyelvi oktatóprogram volt, mellyel az OTDK-n is helyezést ért el. A MTS Pro Scientiis aranyérmének birtokosa.

A főiskolai diploma megszerzését követően, 1990-ben lehetőséget kapott a főiskola tanársegédi munkakörének betöltésére, melynek során általános informatikát tanított. Közben elvégezte az Eötvös Loránd Tudományegyetem számítástechnika tanári szakát, majd ezt követően a Debreceni Egyetem pedagógia szakos tanári diplomáját is megszerezte. Tanulmányai közben folyamatosan fejlesztette tudását, figyelme 1994-ben a Unix rendszerek felé fordult, mely szakmai pályafutását mindvégig meghatározta. Több, az informatikai rendszerek üzemeltetését tárgyaló szaktanfolyamon vett részt.

1999-től 9 hónapon át az Állami Nyugdíjpénztár Felügyelet informatikai főosztályvezető-helyetteseként dolgozott, melyet egy internetszolgáltató, majd hálózatfejlesztő cégnél folytatott. 2004-től saját vállalkozásának fejlesztésébe kezdett, elsősorban informatikai rendszerek tervezésére és fejlesztésére koncentrált.

A felsőoktatással nem szakadt meg a kapcsolata, óraadóként folyamatosan tanított az egri egyetemen, fő tárgyai a számítógépes hálózatok és operációs rendszerek voltak. 2013-ban elnyerte az egyetem informatikai osztályvezetői pályázatát, melyet 2022 augusztusáig töltött be. Ez alatt átszervezte az egyetem informatikai szervezeti egységét, centralizált informatikát és szerver- és hálózat működtetésére specializált csoportot hozott létre. Ezen időszak alatt több RedHat szakvizsgát tett, majd elvégezte az NKE Információbiztonsági Vezető szakképzését. Ekkor határozta el, hogy az informatikai biztonság területén kívánja továbbképezni magát és jelentkezett a Katonai Műszaki Doktori Iskolába. A képzés során szerezte meg felsőfokú angol nyelvvizsgáját, melyet mindkét egyetem oktatójaként hasznosít, heti 2-6 órában tart angol nyelvű órákat. A doktori képzés során számos publikációja, egy elektronikus tankönyve, több

könyvfejezete jelent meg, tudományos- és a felsőoktatási informatikai rendszerek üzemeltetői számára releváns konferenciákon tart elsősorban a felsőoktatási rendszerek üzemeltetésével kapcsolatos előadásokat.