Doktori (PhD) értekezés

Tervezet

Koczka Ferenc

2023.XX.XX

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. A fejlesztések főként a felsőoktatási intézményekben indultak el, különféle alkalmazásokba integrálva a meglevő szakmai és kutatási tapasztalatokat. Közben az iskolák a működési feladataik támogatására is megkezdték az informatikai eszközök alkalmazását, 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 indukálta 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, ez meggyőződésem szerint azonban dolgozatom célterületére, a felsőoktatási rendszerekre is érvényes.

A magyar felsőoktatási intézmények informatikai védelmi területen meglehetősen heterogén képet mutatnak, működésük nem egységes, nem összehangolt, védelmi rendszereik egyediek és eltérők, szabályzataik azonos elemeket 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 fő 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 rendszert 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. Dolgozatom írásakor még öt budapesti és egy vidéki egyetem állami fenntartású, többségük az elmúlt időszak összevonásai és átszervezései után vagyonkezelői alapítványként, kisebb részük pedig egyházi fenntartásban működik tovább. Az átalakítási folyamatokban az egyetemi informatikai rendszereket egyesítették, átadandó adataikat a fogadó fél adatbázisaiba másolták, közben a régi rendszerek archívumait is fenntartják. A fúziók eredményeként hazai viszonylatban korábban nem látott méretű intézmények jöttek létre, hatalmas mennyiségű adatot kezelve úgy, hogy rendszereikben olyan személyes adatok is megjelennek, amelyek tulajdonosai soha nem álltak kapcsolatban velük. Az intézmények gyors átalakítására szabott szoros határidők az informatikai védelem szempontjából bizonytalan helyzeteket hoztak, amit a jogszabályi környezet engedékenysége sem tett könnyebbé.

Nem csak az átalakulási 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 mindig is egyéni utak mentén valósultak meg. Az informatikai rendszerek megtervezését és kialakítását az üzemeltetésért felelős szervezeti egységek végzik, a megvalósítás anyagi hátterének biztosítása pedig azon múlik, hogy képesek-e meggyőzni az intézményi vezetőket vagy a fenntartót azok szükségességéről. A bizonytalan anyagi háttér, a főként a saját erős beruházások helyett a pályázati forrásoktól várt fejlesztések nem teszik lehetővé egy többéves fejlesztési terv alapján működő, garantált és tervezhető finanszírozású rendszer koncepciójának kidolgozását. Ugyanakkor az egyetemi informatikai rendszerekben tárolt adatvagyon mennyisége, azok jellege, incidenseik száma, a technikai és humán oldalon is kimutatható 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.

Az elmúlt évtizedekben 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. Folyamatosan dolgozom állandó vagy külsős

oktatóként a felsőoktatásban 1990 óta. Több szervezetnél voltam informatikai vezető, tudományos munkám alapkérdéseit azonban főleg azok a problémák inspirálták, melyeket kilenc éven át az Eszterházy Károly Egyetem informatikai osztályvezetőjeként/igazgatójaként kellett menedzselnem. Ezekben az években tapasztaltam meg azokat a különbségeket, melyek a feladatkörből, finanszírozásból és nem utolsósorban az intézményi kultúrából adódóan egy komplex egyetemi informatikai vezetési feladatkört a gazdasági ágazatban megszokottól markánsan eltérővé tesznek.

Amellett, hogy lehetőségem volt megismerni egy egyetem mindennapi életének informatikai aspektusait, átszerveztem az azt fenntartó csoport feladatait és működését. Tudományos konferenciákon és egyéb szakmai rendezvényeken betekintést nyertem más magyar és külföldi egyetemek informatikai rendszereibe és üzemeltetési kérdéseibe és azt tapasztaltam, hogy annak ellenére, hogy a feladatkörük általánosságban azonos, köztük számos markáns eltérés áll fenn.

Kutatásom számára kivételes lehetőséget nyújtott a tény, hogy informatikai vezetőként a kutatásetikai követelmények betartása mellett 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 biztosítana. Több éven át erős felsővezetői támogatást kaptam az üzemeltetésben, így tudomásom szerint a magyar felsőoktatásban egyedüliként végezhettem olyan méréseket, mely során a teljes munkavállalói kör adathalászatra adott válaszreakcióit, vagy pl. hamisított weboldalon tanúsított viselkedését tanulmányozhattam. Ezért ezúton is szeretnék köszönetet mondani egykori és munkatársaimnak, akik számos segítséget nyújtottak a vizsgálataimhoz szükséges informatikai környezet kialakításában és a konkrét műszaki megvalósításban.

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. Az informatikai

[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.

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 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 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 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 legnagyobb adatkört a nagy létszámú hallgatói, oktatói és kutatói körök személyes adatai jelentik, ideértve azokat is, akiknek a jogviszonya már nem áll fenn az adott intézménnyel. Az informatikai rendszerek különleges adatokat leginkább a különféle munkajogi kedvezmények igazolásaként, vagy hallgatók számonkérésekor különféle előnyöket biztosító egészségügyi igazolások dokumentálása céljából tartalmaznak. Más, a GDPR által meghatározott különleges adatok tapasztalatom szerint meglehetősen ritkán kerülnek az informatikai rendszerekbe, leginkább olyan levelezési vagy egyéb feliratkozást igénylő csoportlisták fordulnak elő, melyek szervezeti tagságra, vagy valamilyen személyes irányultságra engednek következtetni. A személyes adatok védelme az egyetemek nagy mérete, szerteágazó, és 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 kaptak munkavállalói azonosító számokat is [2].

A második terület az intézmények sajátosságaiból adódóan a kutatási és fejlesztési adatok köre, melynek az intézmények közti megoszlása feltételezhetően nem homogén, de a mennyiségük az Európai Unió pályázatai támogatásainak felhasználása következtében 2020-ig erősen emelkedő tendenciát mutatott. A folyamat során az egyetemek önálló kutatócsoportokat, kutatóintézeteket hoztak létre, a kutatási projektekben már megjelenhettek közérdekű, valamint más területek stratégiai fontosságú adatai is. Ezek kezelését az egyetemi dolgozók és kutatók az általános jogszabályok keretein túl saját döntésük alapján végezték és ezen a területen is vannak személyes tapasztalataim a szabálytalan kezelésükről. A szigorú adatkezelési stratégiával ellentétes irányú erőt jelent az egyetemek tradicionálisan nyílt működése, mely egyaránt jellemző a felsőoktatásban az oktatási területre és a kutatóintézetekre is. Amellett, hogy az új eredmények publikálása a kutatómunka szerves részét képezi, a kutatók minőségértékelésének alapjául is szolgál, 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 adatok védelmét, tekintettel arra, hogy ez az adatkör kiemelt értéket jelenthet a gazdasági szereplők és a kiberkémkedésben érdekeltek számára. Megítélésem szerint a felsőoktatási intézményekben ezen az adatok védelme nem értékarányos.

Az egyetemi önállóság, az oktatók és kutatók szabadságának, az útkeresésüknek támogatása a köz- és gazdasági szférától eltérő módszereket igényel az egyetemi informatikai üzemeltetőktől, ezért esetükben a védelmi kérdéseket is más szemszögből kell megközelíteni. A témára irányuló nemzetközi gyakorlat áttekintésekor nem találtam kifejezetten a felsőoktatás védelmi rendszereinek működését szabályzó törvényi előírásokat.

Néhány felsőoktatási intézményre, vagy azok kiemelt jelentőségű szervezeti egységeire viszont szigorúbb szabályzás vonatkozik. Jelenleg a Budapesti Műszaki és Gazdaságtudományi Egyetem, a Debreceni Egyetem, a Dunaújvárosi Egyetem, a Pécsi Tudományegyetem és a Szegedi Tudományegyetem egyes kutatócsoportjai, a kutatóintézetek és a Nemzeti Közszolgálati Egyetem főként kutatási feladataik okán nemzetbiztonsági védelem alatt állnak [3].

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 informatikusok szerepe kimerül a munkaállomások és a védett kapcsolatok biztosításában. Hasonló a helyzet a felelősségi körökben is: nem találtam olyan intézményt, amely rendelkezne a központi szolgáltatásban tárolt adatainak mentésével, vagy kivonási stratégiája lenne. Emellett kijelenthető, hogy a felsőoktatásban az infrastruktúra nagyságát, 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 hangsúlyos csomópontok mellett olyan elemek is működhetnek, melyek védelmi szintje az elvárható minimum alatt van. Az egyetemi autonómia ellenére a rendszereiket az akadémiai szféra és a fenntartói érdekek mentén saját hatáskörben tervezik meg és alakítják ki. Az adminisztratív védelmi dokumentumok kialakítása szintén így történik, és kötelező érvényű jogszabályi keretek nélkül a védelmi intézkedések kikényszerítése csak erős anyagi támogatás és vezetői felelősségvállalás mellett lehetséges, az ehhez szükséges eszköz- és szaktudás megszerzését és szinten tartását az elmúlt évek gazdasági és munkaerőpiaci folyamatainak változásai pedig rendszerint negatívan befolyásoltak.

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 segítséget nyújtottak. Jelenleg a KIFÜ a felsőoktatás számára a hálózati védelmet csak általános elvek mentén látja el, üzemeltetési szempontú szigorú törvényi kötelezettségei ennek a szervezetnek sincsenek. A Nemzetbiztonsági Szakszolgálat feladatkörébe nem tartozik bele az egyetemek informatikai védelme, ugyanakkor a gyakorlatban elvárja a nyomozati tevékenységek támogatásához, vagy forenzikus vizsgálatok lefolytatásához szükséges, az egyetem informatikai rendszereiben rögzített adatok rendelkezésre állását, ugyanakkor annak hiányát jogszabályi előírás hiányában nem szankcionálja. A Kibervédelmi Intézet szerepvállalása is hasonló: csak abban az esetben van kapcsolata 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. Hipotéziseimet olyan feltételezések alapján választottam meg, melyek érvényességéről az eddigi munkaköreim során szerzett gyakorlati tapasztalatok alapján győződtem meg, célom azok tudományos igényességű bizonyítása.

1.2.Kutatási célkitűzések

Kutatásom elsődleges célja, hogy bebizonyítsam, hogy a felsőoktatási informatikai rendszereinek üzemeltetésére jogi szempontból alulszabályozott, hogy megvilágítsam az egyes részterületek kritikus pontjait, módszertani útmutatást és javaslatot adjak az informatikai rendszerek besorolására, valamint sérülékenységeinek állandó monitorozására. Vizsgálataim dokumentálása során egyaránt törekszem a 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 veszélyeztetettség kimutatása és ajánlás kidolgozása az informatikai rendszerek besorolására. Jelenleg nem áll rendelkezésre a felsőoktatási intézmények adatvagyonát leíró részletes és hiteles információforrás. Ennek felmérésére az intézmények informatikai- és informatikai biztonsági szabályzatai nyújthatnak információt, ezek többsége listázza az egyes informatikai rendszerek biztonsági osztályba sorolását. Ezek elemzése lehetőséget ad a védendő rendszerek számbavételére és az osztályba sorolásuk összehasonlításra. Célom az ezekben tárolt adatok jellegének és érzékenységének, és amennyiben lehetséges, mennyiségének meghatározása, valamint annak bizonyítása, hogy a helyi üzemeltetésű rendszereik változatos adatforrásokban nagy mennyiségű érzékeny adatot tartalmaznak. Dokumentumelemzéssel felkutatom az egyes egyetemek informatikai rendszereit és összevetem azok besorolásait, és kimutatom azok indokolatlan különbözőségeit. Hazai és nemzetközi adatok elemzésével képet alakítok ki az oktatási rendszereket ért incidensekről, megállapítom azok trendjeit, motivációit és eszközeit. Indukció módszerével bizonyítom, hogy a felsőoktatási rendszerek informatikai védelme csak részleges. Az így feltárt helyzetkép alapján ajánlást adok a felsőoktatási intézmények leggyakoribb informatikai rendszereinek egységes besorolására.

2. Az informatikai környezet védelmi állapotának felmérése és különféle, a felsőoktatási rendszerekben jelenlevő sérülékenység kimutatása és elemzése. Mérésekre alapozva kimutatom, hogy a felsőoktatási informatika elemei számos sérülékenységet tartalmaznak, így egyaránt magas kitettségűek belső és külső támadók számára. Mérés útján bizonyítom, hogy a rendszereket érik kibertámadások és léteznek azok a motivációk, amelyek az ezek feletti kontroll megszerzését, működésük befolyásolását és adattartalmuk bizalmasságának, sértetlenségének és rendelkezésre állásának megsértését célozzák. Áttekintem a támadások eszközrendszerét és létrejöttük korai jelzésének lehetőségeit. Azonosítok két, a szakirodalomban már ismertetett, de a felsőoktatásban korábban nem mért problémát, és

megmutatom, hogy a felsőoktatási intézmények nyílt forrású felderítéssel szemben kialakított védelme nem kielégítő.

3. Az informatikai rendszerek kvantitatív eljárással történő sérülékenységi mérésének a felsőoktatásban alkalmazható módszerének bemutatása és eredményeinek elemzése. Az informatikai rendszerek sérülékenységeinek számszerűsítésére szolgáló CVSS pontrendszer csak általános mérési módszert nyújt, önmagában nem ad lehetőséget a különféle biztonsági osztályokba sorolt rendszerek azonos műszaki tartalmú sérülékenységeinek eltérő súlyozására. Célom a CVSS, és a kapcsolódó eljárások bemutatása, valamint Eszterházy Károly Egyetemen végzett többlépéses mérési eredményeim elemzése és következtetések levonása.

4. Egy felsőoktatási rendszer jelszó adatbázisának feltörhetőségének vizsgálata, eredményeinek elemzése és összevetése egy adathalász támadás hatékonyságával. Célom az Eszterházy Károly Egyetem központi címtárszolgáltatásában tárolt SHA1 és NTLM titkosítású jelszavak előképeinek megszerzésére alkalmas módszertan mérés alapú vizsgálata, azok nyilvános adatbázisban történő elérhetőségének és mennyiségének megállapítása, valamint egy egyetemmel és egy kutatóintézettel történő összevetése. Végül meg kívánom állapítani, hogy várhatóan a jelszavak tömeges feltörési kísérlete, vagy a social engineering alkalmazása biztosíthat nagyobb mennyiségű értékes adatot egy támadó számára.

1.3.Kutatási hipotézisek

H1. A felsőoktatási rendszerek adminisztratív szabályzása heterogén tartalmú, emellett azonos súlyú védelmi kérdéseket eltérő prioritásként kezelnek annak ellenére, hogy adatvagyonukban gazdasági és stratégiai szempontból jelentős mennyiségű adat áll rendelkezésre, melynek védelme nemzeti érdek.

H2. A felsőoktatási rendszerek sérülékenységeinek kvantitatív mérésére adaptálható egy számszerű mérésen alapuló metodika, valamint megadható az informatikai rendszerek biztonsági osztályokba sorolására szolgáló ajánlás.

H3. A felsőoktatási informatikai rendszerek központi és kihelyezett telephelyein működő elemeinek a publikus internet irányából mért sérülékenységi szintje a perifériális telephelyek esetében magasabb, és jelentős mennyiségű, 2020 előtt ismertté vált sebezhetőséget tartalmaznak.

H4. A felsőoktatási információs rendszerek jelentős mennyiségű, hibás konfigurációs beállításból eredő technikai információ elemzését teszik lehetővé, melyek egy potenciális

támadó számára segítséget nyújthatnak egy támadás megtervezéséhez és sikeres végrehajtásához.

H5. A felsőoktatás saját rendszereiben működő e-mail címek jelszavai egy brute force előkép-meghatározási eljárással szemben csak részlegesen védettek, melynek eredményességét elsősorban a támadó előkép meghatározási stratégiája határozza meg. A felsőoktatási rendszerek e-mail címeinek védelme során kockázatot jelent a különböző internetes jelszógyűjteményekben hozzájuk társított jelszavak mennyisége (H.5-2), egyetemi környezetben pedig egy OSINT információk alapján felépített, phishing támadással kicsalható legfeljebb 9 karakteres jelszavak mennyisége alacsonyabb, mint a jelszó adatbázis általam javasolt stratégiára optimalizált brute force technikával megszerezhetőké (H.5-3).

1.4.Kutatási módszerek

Kutatásom során empirikus és teoretikus kutatási módszert alkalmaztam. A szakirodalom feldolgozása során jogszabályokat, szabványokat, ajánlásokat, jógyakorlatokat kutattam fel, melyeket a saját vezetői, üzemeltetői, fejlesztői, valamint oktatói tapasztalataimmal vetettem össze, ezekből indukció útján általánosításokat tettem. A jelentősebb informatikai incidensekről esettanulmányokat készítettem. A szabályzatok feldolgozása során dokumentumelemzést, összehasonlító kritikai elemzést alkalmaztam. Statisztikai módszerek alkalmazására törekedtem minden olyan esetben, amikor számszerű mérési eredményeket kaptam. Különféle mérőeszközökön alapuló méréseket végeztem, az információbiztonság mérésének módszere a kísérlet volt. A 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.

Kutatási adatok megszerzésére közérdekű adatigénylést, valamint interneten elérhető statisztikák felkutatását alkalmaztam. A Hackmageddon adatfájljainak feldolgozását mySql adatbázisba konvertálás után dolgoztam fel. Az adatok kiértékelésére több Python nyelvű programot készítettem.

A kitűzött célok elérése érdekében tudományos és szakmai konferenciákon részt vettem, melyeken információt gyűjtöttem a felsőoktatás azonos területein dolgozó kollégáktól és szakemberektől, feldolgoztam, elemeztem és értékeltem a megszerzett tapasztalatokat és ismereteket. Folyamatosan gyűjtöttem a felsőoktatási rendszereket érintő 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. A magyar felsőoktatási informatikai rendszerekben tárolt adatvagyon meghatározása

Az arányos és költséghatékony védelem kialakításának első lépése az informatika rendszerekben tárolt védendő értékek azonosítása. Magyarországon 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 [4]. 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, közülük is csak hat volt publikusan is elérhető. A hivatkozott források közt egyetlen magyar sem volt, és utalás sem szerepelt a hazai egyetemekre [5]. Bár a hazai és nemzetközi összehasonlításban számos azonosság jelenik meg, melyet a linzi székhelyű Johannes Kepler Universität-en végzett tanulmányutam is megerősített, a hazai felsőoktatás védelmi kérdéseinek vizsgálatakor számos különbség is feltételezhető. Ezek azonosításához fel kell térképezni a felsőoktatás értékeit, az szférát érő informatikai incidenseket, sebezhető pontjaikat és 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 [6] és a Nemzeti Kiberbiztonsági Stratégia [1] adja. Ezt a 2013-as kormányrendeletet az informatika gyors fejlődése, és az EU hálózati és információs rendszerek biztonságáról szóló irányelvével való összhangért, és a 2022-ben megváltozott háborús helyzet által jelentett magasabb kockázat következtében célszerű lenne rövidebb időközönként aktualizálni.

Magyarország Nemzetbiztonsági Stratégiája kiemelten foglalkozik a magyar kibertér védelmével, a kibertérből érkező támadásokkal, azok negatív hatásainak elkerülésével. Katonai szempontú megközelítése összhangban van a nemzetközi gyakorlattal, mely a kiberteret az ötödik műveleti térként határozza meg, az ebben jelentős anyagi károk okozására képes képességeket fegyverként definiálja. Feladataként határozza meg a magyar honvédség

kiberképességeinek fejlesztését és a nemzetközi együttműködést. Kiemelten védendő szektorként az e-közigazgatást, közműszolgáltatást, stratégiai vállalatokat, a létfontosságú rendszerelemeket definiálja. A kibertámadások leggyakoribb elkövetői körét a szervezett bűnözői körökben, nemzetközi terrorszervezetekben, kiberbűnözői csoportokban, szélsőséges vallási közösségekben, magán biztonsági cégekben és egyéb transznacionális hálózatokban határozza meg. Kiemeli kibertámadások intenzitásának erősödését, az erre irányuló kutatások fontosságát, és kitér a felhasználói információbiztonság jelentőségére is [6].

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) [7] ajánlásaihoz, a NATO 2010-es stratégiai koncepciójához [8], a 2011-es kibervédelmi politikájához és a Szövetség kibervédelmi elveihez és céljaihoz [9]. Sem a Nemzetbiztonsági Stratégia, sem a Nemzeti Kiberbiztonsági Stratégia nem említ felsőoktatási intézményeket.

A magyar kibervédelem szervezeti hierarchiájának csúcsán a Belügyminisztérium (BM) áll, ami eltér az általános nemzetközi gyakorlattól. Az állami és önkormányzati szervezetek felügyeletét a Nemzetbiztonsági Szakszolgálat (NBSZ) keretében működő Nemzeti Kibervédelmi Intézet (NKI) látja el, mely három szakmai területet fed le. A kibertérből érkező fenyegetettségek, illetve támadásokra specializált szervezet a Kormányzati Eseménykezelő Központ (GovCERT). A Nemzeti Elektronikus Információbiztonsági Hatóság feladata a jogszabályok érvényesítése, illetve a betartásuk ellenőrzése. A Biztonságirányítási és Sérülékenységvizsgálati Osztály az Ibtv. hatálya alá tartozó szervezetek üzemeltetését támogatja ideértve a védelmi képességeik fejlesztését is. A NISZ Zrt. a törvény hatálya alá tartozó szervezetek számára központosított infrastruktúrát és ahhoz kapcsolódó szolgáltatásokat biztosít.

A fenti szervezetek nem nyújtanak szolgáltatásokat az akadémiai szféra számára. A HM CERT 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 tevékenységük az eseménynaplók ellenőrzésekor egyértelműen nyomon követhetők. A felsőoktatás nem tartozik ezen szervezetek hatókörébe sem, így néhány kivételtől eltekintve csak az onnan kiinduló spam tevékenység jelzése történik meg számukra. 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. De ezek a szervezetek jogi szempontból is korlátozottak, 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, melyben lényegesen több sérülékenységi probléma jelentkezik, mint a felsőoktatásban, ezért a rendelkezésükre álló erőforrásokat inkább ezekre az intézményekre fordítják. 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.

Külföldi gyakorlatban sem találtam példát kifejezetten oktatási intézményekre szabott szabályzásra, de 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, mely 82. paragrafusában előírja, hogy „a mások számára számítógépes adatokat kezelő vállalkozásoknak értesíteniük kell az adatok tulajdonosait, ha azok jogosulatlan felhasználó birtokába jutnak” [10]. 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 Királyság, 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.
Egy tervezet, melyet Ausztrália Belügyminisztériumának Kritikus Infrastruktúra Központja adott közre 2020-ban, a felsőoktatási intézményeket ért támadások megnövekedett száma miatt [11, p. 3] egyenesen a kritikus infrastruktúrák körébe sorolná azokat [11, p. 4], vállalva a velejáró műszaki fejlesztések finanszírozását is.

A magyar jogszabályi környezet tehát nem rendelkezik közvetlenül a felsőoktatásról. 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 [12]. 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 [13].
Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) 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 [14].
A nemzetközi gyakorlat nem sok területen különbözik a magyartól, de egyes országokban felismerték a szféra adatvédelmének fontosságát. Számos ország esetében fogalmaznak meg ajánlásokat a kritikus infrastruktúrák számára, amelyet más szervezetek is alkalmazhatnak a saját működésük biztonságossá tételére, ez érhető el és ajánlott az akadémiai szféra számára is. Az egyik 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 jógyakorlatok biztosítása. Az ajánlás három részből épül fel: a keretrendszerből, a végrehajtási szintekből és a keretprofilokból. 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 [15].
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 [16]. 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 újraalkotását 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 regisztrációs 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 nem csak helyi, hanem Európai Uniós reakció adható. Ugyanakkor a jogalkotó a jelentéktelen incidensek bejelentési kötelezettségeinek újragondolásával 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.
Ki kell emelni az irányelv megvalósításának a szervezetek költségvetésére gyakorolt hatását is: 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. 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 ismert és nyilvánosan elérhető metodika áll rendelkezésre, az egyes rendszereket az egyetemek eltérően minősítik. 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 a gyakorlat eszköz- és funkcióközpontú meghatározást eredményez, amely rendszerszintű információ hiányában csak részlegesen veszi figyelembe az intézmény valódi céljait, így attól jelentősen eltérhet. A technikai szemléletű informatikai munkatársak és az intézményi vezetők pedig valószínűleg teljesen máshová helyezik a súlyponti kérdéseket.
Az értékek azonosítása az intézmények eltérő szervezeti felépítése következtében különböző területi vezetők felelőssége, amelynek során meghatározzák az intézmény értékeit, azok előállítását szolgáló célokat és az elérésükhöz szükséges fő követelményeket. Szinte minden egyetem esetében ilyen a hallgatói létszám növelése, a tudományos publikációk mennyiségi

vagy minőségi javítása, vagy az intézmény által kiadott diplomák értéke szakmai körökben, vagy a közvéleményben. Ezek eléréséhez számos feltétel, szolgáltatás és egyéb körülmény szükséges, amelyek számszerűsítésére a kulcsfontosságú teljesítménymutató (*Key Performance Indicator,* KPI) alkalmazható. A KPI-k azonosítása a célok eléréséhez szükséges elemeket mérhetővé, így leírhatóvá és összehasonlíthatóvá teszik. A KPI-k azonosítása nem csak informatikai szempontból lényeges. Valójában számos olyan létezik, amelynek nincs informatikai vonatkozása, de meghatározásuk az intézményi informatikai folyamatok súlyának azonosításában jelentős szerepet játszik. A felsőoktatási KPI-k képzésére Ballard doktori disszertációja nyújt példát, amelyben az Amerikai Egyesült Államok 34 felsőoktatási intézményének 2139 különböző kulcsfontosságú teljesítménymutatóját vizsgálta, amit 24 kategóriába sorolt be, és azonosítja azon adatok és folyamatok körét, amelyek az intézményi célok eléréséhez szükségesek [16]. A felsőoktatási rendszerek általános értékei néhány fő területre koncentrálódnak, ezek a személyes, oktatási, kutatási és működési adatok.

2.3.Személyes adatok

Az egyetemek egyik legértékesebb adatköre személyes adatokból áll. A McDonald Hopkins fehér könyve az amerikai egyetemek esetében nemcsak egyetemi hallgatók, oktatók és kutatók személyes adatait említi, hanem adományozók, kurátorok, igazgatósági tagok, öregdiákok, diákok, szülők, jelentkezők, személyzet, betegek mellett fogyasztók és eladók adatait is [17]. Ezek egy része a magyar egyetemek esetében a kulturális, működési és finanszírozási különbségek miatt nem is értelmezhető, például hazánkban a végzett hallgatók támogató szerepének is 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 [18]. 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 tanulmányi történetüket, ösztöndíj és tandíj adatokat, és olyan, rendszerint valamilyen csökkent képességet leíró egészségügyi adatokat is, amelyeknek a tanulmányok során szerepe lehet[3].

[2] A magyar felsőoktatás kizárólag a Neptunt alkalmazza, melyet 1997-ben elsőként az akkori BME-n vezettek be.

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

Az oktatók és kutatók adatai magyar és nemzetközi viszonylatban is érzékeny adathalmazt jelentenek. Egy olyan incidens, amely a tanulmányi rendszer adatainak sérülését vagy nyilvánosságra kerülését eredményezné, az adott egyetem reputációját is jelentős mértékben ronthatná. Egy jelentős mértékű adatsértés következménye a GDPR-ban meghatározott jelentős büntetési tétel kiszabása lehetne, mely a legtöbb magyar egyetem esetében komoly veszteséget eredményezne. Ilyenre Magyarországon eddig nem volt példa, bár dolgozatom írásakor az alsóbb szintű oktatási intézmények tanulmányi rendszerével (Kréta) kapcsolatos, nagy mennyiségű adat szivárgásával járó incidens vizsgálata még nem zárult le. A tanulmányi rendszer adatainak elvesztése a legsúlyosabb következményekkel járna egy felsőoktatási intézmény számára. A tanulmányaikat folytató hallgatók tantárgy- és vizsgaeredményeinek elvesztése lehetetlenné tenné a követelmények teljesítésének ellenőrzését, körülményesen lennének kiadhatók a korábbi diplomák, és kétségessé válna az államilag támogatott félévek elszámolása is. Bár az adatok egy része más forrásból pótolható lenne (például a befizetett tandíjak esetében) a tanulmányi rendszert ért végzetes incidens komoly reputációs kárt okozna. A rendelkezésre állást érintő incidensek elsősorban a tárgyfelvételi- és vizsgaidőszakban okoznának komolyabb működési problémákat.

A nagy mennyiségű adat megfelelő kezelése különleges felelősséget ró az akadémiai szférára is. Több jogellenes adatkezeléssel kapcsolatos eljárás ismert, melyet a Nemzeti Adatvédelmi és Információs Hatóság (NAIH) indított az egyetemek hibás adatkezelési gyakorlata miatt [19] [20]. Az informatikai incidensekkel kapcsolatos valós kép megismerését nagyban nehezíti, hogy bár azok bejelentése a NAIH felé kötelező, a gyakorlatban az ritkán történik meg.

2.4.Oktatási rendszerek

A jelenléti oktatás fellazítására egyre több egyetem törekszik. A Covid19 következtében, 2020-ban bevezetett kényszerintézkedések egyértelművé tették, hogy az egyetemi kurzusok bizonyos 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 [21].

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. A korábban jellemző szóbeli vizsgák helyét egyre inkább a gépi számonkérések vették át, amelyek 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. Egy potenciális LMS-rendszer-sérülékenység ugyanakkor lehetőséget ad a vizsgaeredmények módosítására, így azok motivációt jelenthetnek belső és külső támadók számára egyaránt [22].

2.5.Kutatási adatok

A tudományos kutatás az akadémiai szféra intézményeinek egyik elsődleges tevékenysége. A kutatási adatok körébe a nyers és feldolgozott kutatási adatok, tudományos ismeretek, elemzések eredményei és a tudományos publikációk tartoznak [23]. A FireEye tanulmányában a vállalati, kutatási és harmadik féltől származó adatokat, például az ipari együttműködések során az intézmények számára átadott adatokat minősíti kulcsfontosságúaknak [24]. Giszczak kutatásában olyan projektekre is kitér, amelyekben egyetemi kutatások kormányzati együttműködésből származó adatokat használnak fel [17].

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 kritikus kutatási feladatokban vállalt szerepük miatt a kritikus infrastruktúra-elemek közé sorolja, és kötelezi őket a besorolásnak megfelelő informatikai védelem kialakítására [11].

2.6.Működési adatok

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

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 személyügyi-, bér- és gazdasági folyamatokat kezelő szoftverek ma jórészt 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 legtöbb esetben nem létezik kivonási stratégia, 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.Kiberfenyegetettségek a felsőoktatásban

Számos egyetem szenvedett már el különböző típusú informatikai incidenseket. A média kibervédelemmel foglalkozó híreiben szinte alig található oktatási intézmény ellen irányuló támadásról szóló híradás, de az egyetemi informatikai üzemeltetők több ilyenről is beszámolnak. Ezek mennyiségi és súlyossági besorolásához, valamint statisztikai módszerekkel történő elemzésükhöz konkrét adatokra van szükség.

Nemzetközi viszonylatban több, elsősorban amerikai adatforrásokra támaszkodhatunk. Az ottani tendenciákból vonhatunk le következtetéseket a várható hazai változásokra is, de azok nem lesznek alkalmazhatók a különbségek figyelembevétele nélkül. Sajnos a különböző forrásokból származó adatok eléggé eltérő képet rajzolnák ki. Az Open Security Foundation szerint az összes biztonsági incidens 35%-a a felsőoktatásban történik, ezt személy szerint túlzónak tartom [24]. Giszczak kutatása szerint 2016 első felében 50%-kal nőtt a felsőoktatási adatokkal kapcsolatos jogsértések száma. Munkájában bemutatja, hogy a reputációs veszteség megjelenik a kutatási támogatások és az adományok megszerzésekor, amelynek mértékét kiszivárgott rekordonként körülbelül 300 dolláros kárként határozza meg [17].

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 több forrásból is megerősítettek. A rendszerekbe történő belépés, alapvető webes alkalmazások támadása és egyéb hibák a jogsértések 80%-át teszik ki. A betörések 25%-át belső szereplők, 75%-ukat külső támadó kezdeményezi, melyek célja 95%-ban anyagi haszonszerzés, és csak 5%-ban valamilyen kémkedési szándék. Az incidensek 63%-a személyes, 41%-a hitelesítő, 23%-a egyéb, 10%-a pedig belső adatok megszerzésére irányul. A jelentés az összegzésében kiemeli: „Az oktatási szolgáltatások kísértetiesen hasonló tendenciát követnek, mint a többi iparág többsége; drámaian megnövekedett a ransomware-támadások száma, mely a jogsértések több mint 30%-a. Ezen túlmenően ennek az iparágnak meg kell védenie magát az ellopott hitelesítő adatokkal és az adathalász támadásokkal szemben, amelyek potenciálisan felfedhetik az alkalmazottak és diákok személyes adatait” [25].

A hackmageddon.com[5] 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[6]. 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[7] (PRC) adatbázisa nem tesz különbséget az oktatási intézmény egyes típusai közt, így az ez alapján levont következtetések nem felsőoktatás-specifikusak, hanem a teljes oktatási szférát jellemzik.
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

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

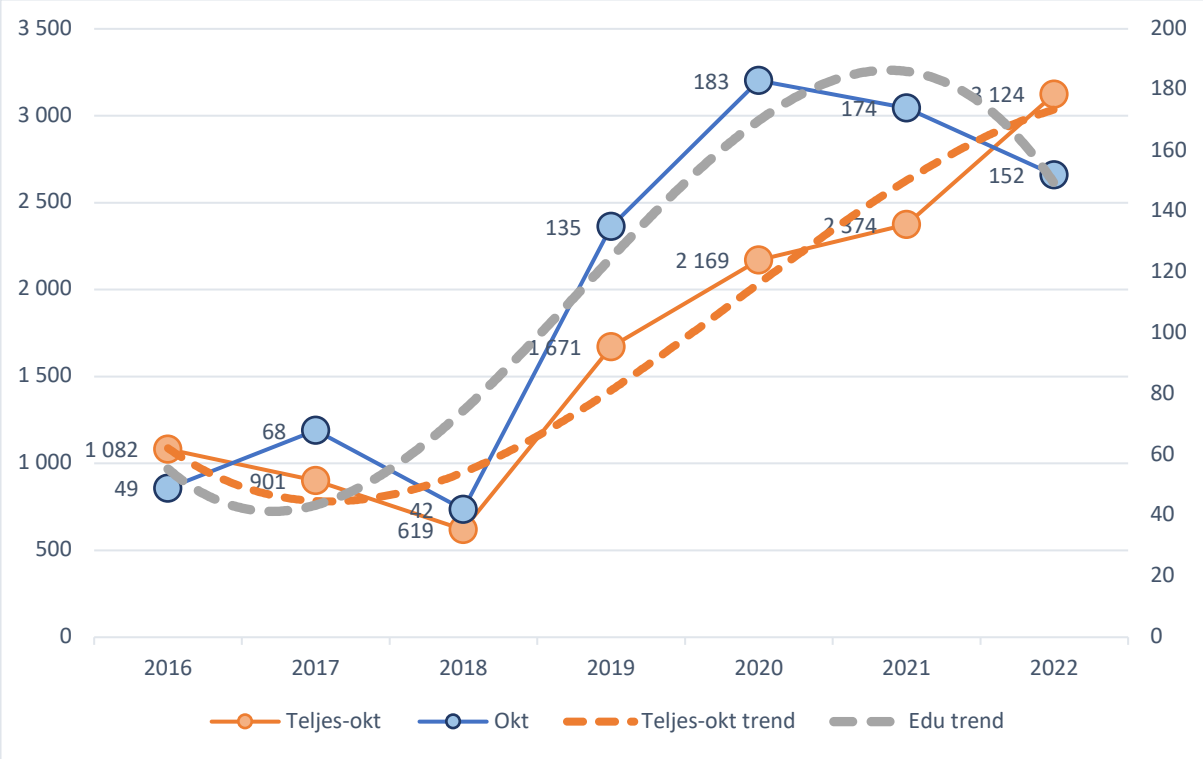
érintő incidensek száma követ (Okt). A két adat százalékos aránya évről évre mutatja az oktatási intézmények az oktatási szférára irányuló támadások részarányát. Az *Éves részarány* a vizsgált évek összes adatsértésének az adott évre eső arányát írja le, mely az adott évben az adott területre jutó adatsértések számának és az összes támadásnak (11.940, illetve 803) százalékos értékben kifejezett hányadosa.

Év	NemOkt	Okt	%	Éves részarány	
2016	1.082	49	**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: saját szerkesztés a Hackmageddon adatai alapján.

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

A trend igazolására mindkét adatsort egy diagramban ábrázoltam, melynek pontjait az kizárólag a jobb áttekinthetőség érdekében összekötöttem (a két pont közötti értékek alakulásáról az ábra nem ad információt). A diagram az összehasonlíthatóság érdekében az y tengelyen kettős skálázást alkalmaz. Az ábra szaggatott vonalai az adott értéksor harmadfokú regresszióval kifejezett trendjét ábrázolják. Ezek egyértelműen rámutatnak arra, hogy míg a narancsszínnel jelölt, összes támadást leíró trend 2018 óta egyértelmű emelkedő tendenciát követ, az oktatási szektor esetében ez a trend 2021-ben megfordult. Megjegyzendő, hogy bár harmadfokú regresszió természeténél fogva nem alkalmazható hosszútávú előrejelzésre, a diagramon szereplő trendvonal a szférát ért támadások csökkenő tendenciáját prognosztizálja.



1. ábra. A támadások teljes és az oktatási szektorra irányuló adatai és változásainak trendje. Forrás: saját szerkesztés.

Ez a tendencia ellentmond a külföldi szakirodalomban széles körben elemzett, a Covid19 által megkövetelt rapid informatikai változtatások következményeként megvalósított, a távolléti oktatás támogatását szolgáló informatikai fejlesztések biztonságcsökkentő hatásának. Zalat és szerzőtársai tanulmányukban arra a következtetésre jutottak, hogy az online tanulásra való átállás a tanulás támogatásához szükséges informatikai szolgáltatásokban működési zavarokat eredményezett, melyek jellemzően szolgáltatáskiesések vagy szolgáltatás megtagadásos támadások következtében alakultak ki [26]. A 2022-es évben mért csökkenés valószínűsíthető oka pedig az orosz-ukrán háború következményeként a kiberműveletek célpontjainak áthelyezése.

A Hackmageddon adatbázisában a támadások motiváció szerinti besorolását is elvégezték, melyek a Cybercrime (CC), Cyber Espionage (CE), a Cyber Warfare (CW) és a Hacktivism (H) kategóriákba esnek[8]. Ezeket az oktatási intézmények vonatkozásában szintén év szerinti bontásban vizsgáltam annak érdekében, hogy változásuk trendje mellett a támadók motivációinak változásokra is következtetni lehessen. Az adatok elemzése alapján elmondható, hogy az oktatási szférát ért támadásokat túlnyomórészt a kiberbűnözés, főként az anyagi

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

előnyök megszerzése hajtja. 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 egyetlen Cyber Warfare eset 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 nem a Cyber Warfare-be, hanem a Hacktivizmusba sorolja. Összességében azonban elmondható, hogy ezek szerepe az oktatási szektorban csupán 4%.

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

2. táblázat. Az oktatási szektort ért incidensek motivációinak évek szerinti megoszlása. Forrás: Hackmageddon adatai alapján saját szerkesztés.

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

	2016	2017	2018	2019	2020	2021	2022	Összesen	%
CC	762	681	500	1380	1840	1971	2310	9444	81,2%
CE	48	143	81	205	236	267	396	1376	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	1667	2152	2312	3050	11637	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: Hackmageddon adatai alapján saját szerkesztés.

A motivációk ismerete nagyban befolyásolhatja a védekezés módszertanának kidolgozását, a védendő rendszerek azonosítását és a védelmükre szolgáló eszközök kiválasztását is. Ez alapján az oktatási intézményeknek elsősorban azokra a rendszerekre kell koncentrálniuk, melyek a támadóik számára anyagi haszonszerzés lehetőségét kínálják, tehát általánosságban érzékeny adatok megszerzésére vagy 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 marad a támadási technikák közel negyede, és ennek trendje is erősödött az elmúlt években, ráadásul a támadások egyre nagyobb részét ez a típus teszi ki. Az account hijacking során ellopják vagy átirányítják egy személy valamilyen hozzáférését 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 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 a 2020 és 2021-es évek Zoom bombing technikájában, mely során amellett, hogy a meetingek képzési algoritmusának nyilvánosságra

kerülésével kiszámítható volt a belépéshez szükséges csatlakozási link, a belépési eljárás gyengeségének következtében idegenek lehetetlenítették el 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 aránya az előzetes feltételezéseimet messze alulmúlták. A sérülékenységek általános kihasználását az adatok alig támasztják alá, és kis számban detektáltak a szektorral szemben kezdeményezett túlterheléses támadás is. Az SQL injection elenyésző kihasználása is meglepő egy olyan szektorban, ahol a feladatok egy részét komoly szakmai tapasztalattal nem rendelkező munkatárs végzi el, vagy hallgatói munka keretében kerül megvalósításra: a komolyabb szoftverfejlesztési gyakorlat nélkül készített web-alapú rendszerek rendszerint nem elsődleges szempontként kezelik a biztonsági kérdéseket. Az említett támadási forma valószínűsíthetően a szoftverfejlesztési technikáknak és biztonságosabb keretrendszereknek köszönhetően ma már aligha használható ki hatékonyan. A lista utolsó helyén megjelenő jelszófeltörési eljárást alkalmazását összesen három esetben regisztrálták.

Megjegyzendő, hogy ezek az értékek hirtelen megváltozhatnak, amennyiben a szektorban tömegesen alkalmazott szoftver (esetleg hardver) biztonsága sérül. Magyar viszonylatban ilyen incidens volt az eKréta rendszer elleni támadás, mely során egy megtévesztő levél alkalmazásával, rendszerben jelen levő a többszörös konfigurációs hibák kihasználásával végül magyar tanulók adatai nagy mennyiségben szivárogtak ki. Az eset példa nélküli volt, az 1. sz. mellékletben szereplő közérdekű adatigénylés tanúsága szerint a Nemzeti Adatvédelmi Hatóság felé 2018. február és 2023. március között jelentett 124 esetből 62 az eKréta rendszer feltörésével kapcsolatos adatsértés, 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: Hackmageddon adatai alapján saját szerkesztés.

Ahhoz, hogy a Hackmageddon adatbázisát hazai viszonylatban is érvényesnek tekinthessem, megvizsgáltam az adatok forrásának ország szerinti eloszlását. Megállapítottam, hogy annak 90%-a összesen hat országból származik, magyar adatok pedig egyáltalán nem szerepelnek benne. Ennek következtében a magyar oktatási szféra kitettségének mértékéről ezek nem adnak információt, ezért ebben a helyzetben az indukció módszerének alkalmazása lászik célszerűnek: az eddig tett megállapítások érvényességének kiterjesztése magyar viszonylatra is. Ugyanakkor az egyes országok eltérő sajátosságai, a rendszereikben tárolt adatok mennyisége és érzékenysége következtében ez kritika nélkül nem tehető meg, és remélhetően a magyar 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: Hackmageddon 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 mértékre tehető, mely kismértékű

ingadozás mellett 2016 óta jelentős mértékben nem változott. A támadók előszeretettel alkalmaznak malware-ekre alapozott támadási módszereket, de lehetőség szerint igyekeznek megszerezni és felhasználni a felhasználók különböző hozzáféréseit. A 2022-ben folyó háború ellenére ezeknek az intézményeknek a kiberhadviselésben nem látszik szerepük. A támadók tevékenysége elsősorban a kibertérre vagy ott elkövetett bűncselekményekre alapozott, így feltehetően az anyagi haszon megszerzésére irányul.

Az oktatási intézmények érintettségének vizsgálatának érvényességét egy másik, a PrivacyRights.org (PRC) által működtetett adatbázis alapján végeztem el, mely 2021 októberében 9.015 incidens adatait tartalmazta[9]. Adatbázisuk kategóriákba sorolja az incidenseket elszenvedő szervezeteket és az incidensek típusát is. 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 adataival: míg az utóbbi esetében az adatbázis kifejezetten a támadási célú eseményeket, addig a PRC az egyes szervezetek saját munkatársai által elkövetett hibák következtében megvalósuló incidenseket is rögzítik – ezt a különbséget a két adatbázis összehasonlítása során figyelembe kell venni. 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.)

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

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 összehasonlíthatók más szektorokkal. Az összehasonlíthatóság érdekében elkészítettem a szektorok és incidens típusok mátrixát, amit a 2. 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, a kormányzatot és a hadsereget is. Bár ez az érték határozottan nagyobb a Hackmageddon 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 adhatnak 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.

2.8.Hazai incidensek

Az amerikai egyetemek a jogszabályi különbségekből adódóan a hazaitól eltérő adatkezelést valósítanak meg. A könnyen értékesíthető adatok körébe főleg a bankkártyák engedély nélküli felhasználásához kapcsolódó adatok és az SSN *(Social Security Number)* tartoznak[10]. A

[10] Az Amerikai Egyesült Államokban az SSN-t egy csaló számos módon használhatja fel. Alkalmazható a személyazonosság ellopására hitelszámla megnyitásakor, kölcsönigényléskor, de ismeretében állami szolgáltatások is igénybe vehetők, akár adóbevallás is benyújtható. Az SSN birtokában munkaviszony létesíthető,

magyar egyetemek általánosan alkalmazott rendszereiben 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 reputációs veszteségekről. Informatikai vezetői gyakorlatom alatt több alkalommal kellett az egyetemet érintő célzott megtévesztéses incidenst részben kezelnem, ezek teljes kárértéke meghaladta a 100M Ft-ot. jellegzetes incidens volt az a célzott támadás, mely egy olyan megtévesztő levél helytelen kezelésével indult, mely hatására a gazdasági szervezeti egység egy munkatárs módosította egy közismert egyetemi szolgáltató bankszámlaszámát a gazdasági rendszerben. A kampányban több egyetem is érintett volt, mely következtében több magyar egyetem milliós nagyságrendű havi számláit hónapokon át ismeretlen csalók számlaszámain egyenlítették ki.
Az általam ismert legnagyobb anyagi kárértékű incidens forrása egy ügyintézői bűncselekmény volt, aki a tanulmányi rendszer manipulálásával közel tíz éven át volt képes hallgatói tandíjak sikkasztására. 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 [27]. A Pázmány Péter Katolikus Egyetem (PPK) tanulmányi rendszerét 2020-ban egy zsarolóvírus tette átmenetileg elérhetetlenné [28].
Sem a Hackmageddon, sem a PRC adatbázisa nem tartalmaz hazai adatokat, így azokból elsősorban a fejlett országok csoportjának nemzetközi helyzetére lehet következtetéseket levonni. A magyar felsőoktatást ért incidensek számára nem találtam KSH adatokat, de a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) archívumában fellelhető egy NAIH/2018/7420/2/Z számú adatigénylésre adott válasz, mely a 2018 május 25. és december 18. között történt adatsértések listáját tartalmazza [29]. A dokumentum 239 bejelentett esetet sorol fel, melyben mindösszesen öt felsőoktatási intézmény érintett.

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 feladat, és nyilvánosságra kerülése esetenként komolyabb károkat is okozhat tulajdonosának.

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: NAIH/2018/7420/2/Z ügyirata.

Mivel ez az időszak kevesebb, mint hét hónapot ölel fel, ezért a kutatásom szempontjából releváns adatokat a NAIH egy közérdekű adatigénylés formájában küldte meg számomra, 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 2018 február és 2023 márciusa közötti időszakra gyűjtötték ki[11] és adták át.

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 a NAIH adatszolgáltatása alapján.

Az öt évre kimutatott harmincas esetszám irreális, mely arra enged következtetni, hogy a magyar felsőoktatási intézmények nem jelentik a bekövetkezett adatsértéseket. A közölt esetek túlnyomórészt következmények nélkülinek tűnnek, súlyosságuk elenyésző, a téves címre kiküldött levelek, vagy az online oktatás anyagának közzététele nyilvános videomegosztó portálon minden valószínűség szerint nem okoztak az érintett intézmény reputációjában

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

komolyabb kárt. A három sikeres ransomware támadás személyes ismereteim alapján biztosan kevés, én magam többről tudok a vizsgált időszakban. Az adathalász tevékenységek rendkívül magas száma miatt egyáltalán nem tartom valószínűnek, hogy csak négy alkalommal fordult volna elő, különös tekintettel a külföldi oktatókra, akik a helyi szokások gyenge ismerete és a hiányos magyar nyelvtudás miatt nehezen tudják felismerni egy magyar nyelvű levél adathalász természetét.

A jelentés alapján megállapítható, hogy a felsőoktatási intézmények valószínűsíthetően elmulasztják az adatsértések jelentését a NAIH felé, ennek valószínűsíthetően csak a már nyilvánosságra került, vagy jelentéktelen incidensek esetében tesznek eleget. Ezért a továbbiakban a magyar felsőoktatási intézményeket ért támadások számát ismeretlenként kezelem, így a nemzetközi tendenciák alapján kimutatott adatokat és trendeket veszem alapul.

2.9.A felsőoktatási rendszerek adatvagyona

Kutatásom első részében bemutattam, hogy a felsőoktatási intézményeket érik támadások, és elsősorban külföldi adatok alapján meghatároztam ezek nagyságát. H.1. második részének igazolására ebben a fejezetben bemutatom, hogy a magyar felsőoktatási intézmények jelentős mennyiségű értékes adatvagyonnal rendelkeznek, így bizonyítom azok védelmének szükségességét.

H.1. és H.2. vizsgálatához nem sok elérhető forrást találtam. A személyes adatok mennyiségének és érzékenységének meghatározását az Oktatás Hivatal (OH) által üzemeltetett Felsőoktatási Információs Rendszerre (FIR) alapoztam. A felsőoktatási intézmények az aktuális hallgatói és oktatói létszámaikat havi rendszerességgel jelenik az OH felé, ezek forrása az intézményben működő tanulmányi rendszer, technikailag a folyamatot ennek egy modulja végzi el. A FIR adatait az OH nyilvánosan is elérhetővé teszi[12], a hallgatókra és oktatókra vonatkozó adatokat az egyetem Tanulmányi Osztálya bocsájtotta rendelkezésemre. 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

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

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

Az adatok értelmezése során figyelembe kell venni, hogy a FIR adatrekordjainak száma a felsőoktatási intézmények rendszereiben tárolt rekordok összessége, így ott 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 megállapítom, hogy az intézmények tanulmányi rendszereiben tárolt adatok személyes- és különleges adatok mennyisége országos viszonylatban is jelentős, az Eszterházy Károly Katolikus Egyetem esetében több mint 120.000 fő, tehát kiemelkedően védendő adatkört jelent. A teljesség kedvéért meg kell említeni az adatok többszörözésének egy másik okát, ennek forrása felsőoktatási intézmények átszervezéséből adódó adatmigráció. A jogutódlásból adódó jogszabályi kötelezettség okán egy intézmény beolvadása, áthelyezése vagy önállóvá válása során elfogadott gyakorlat a fogadó intézmény tanulmányi rendszerébe történő teljes migráció. A rendszeres átszervezések eredményeképp így olyan hallgatói adatok is jelen lehetnek egy intézmény tanulmányi rendszerében, amellyel egy hallgató soha nem állt kapcsolatban[13].

A kutatásaim során a FIR adatbázisán kívül más, országos, az felsőoktatás adatvagyonára vonatkozó statisztikai adatot nem leltem fel, így H.1. és H.2. bizonyítását 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 kívántam meghatározni 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.

[13] 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. https://karolyrobertcampus.uni-mate.hu/a-károly-róbert-campus-története1

törvény ajánlásait, és elvégezték a rendszereik biztonsági osztályba sorolását, az tükrözi adatainak fontosságát, értékét és valószínűsíthetően az érzékenységét is.

A kutatást dokumentumelemzés módszerével végeztem [30]. Bár alkalmazása számos előnyt kínál, alkalmazása előtt a potenciális hibák elkerülése érdekében felmértem annak hátrányait is. Yin összefoglaló táblázata alapján a dokumentumelemzés potenciális gyengeségei esetemben az alábbiak lehetnek [31]:

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. 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 tesz közzé releváns adatokat, vagy egy egyetem nem közli azokat, másikat választok helyette[14].
- Tekintettel arra, hogy 2013 februárjában a FIR nyilvántartásában 236 felsőoktatási intézmény szerepelt, és nem állt rendelkezésemre erőforrás, hogy a kutatásomat mindegyikre kiterjesszem, ezért az intézmények körét úgy szűkítettem, hogy a vizsgáltak reprezentálják a teljes egyetemi kört. A szabályzatokat így a reprezentatív mintavételezés szabályainak megtartásával választom ki, ennek érdekében meghatározom azokat a szempontokat, melyekkel a magyar egyetemek teljes spektruma lefedhető.

[14] 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.

- Nem minden egyetem teszi közzé a szabályzatait, ezért ezekben az esetekben személyes megkeresés útján szerzem be azokat. Ez a BGME és a PKE esetében állt fenn, ugyanakkor a kis egyetemek többsége nem helyez hangsúlyt a minőségi szabályzatok készítésére. Helyettük más egyetemet kerestem, de az alacsony hallgatói létszámmal rendelkezők osztályában alig találtam olyat, mely elfogadható ilyennel rendelkezik.

A fentiek alapján tehát a törvényi kötelezettség mellett a reprezentatív mintán elvégzett dokumentumelemzés ad információt az adatvagyon számottevő elemeiről, emellett azok biztonsági besorolásai is összehasonlíthatók, mely igazolhatja a H.2. helyességét.
Első lépésként definiáltam azokat a szempontokat, amelyek alapján kiválasztható az egyetemeknek az a legszűkebb halmaza, mely vizsgálata után az indukció módszerével megalapozott általánosítás végezhető. A kiválasztás 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 méretet kizárólag a hallgatói és az oktatói létszám együttese alapján definiáltam, amihez nem az intézmény eddigi teljes életciklusa alatt mért összesített, hanem a jelenlegi hallgatói létszámot vettem figyelembe. Ez pontosabban írja le az egyetem jelenlegi helyzetét, így nem érvényesül valamilyen múltbéli tényező befolyásoló hatása. A pontossága ugyanakkor megkérdőjelezhető, mert a már említett, az egyetemek átszervezése során létrejött új intézmények adatai újak, így annak ellenére, hogy jelen pillanatban nagy számú hallgatót képeznek, az életciklusukra vonatkozó adat a fiatal koruk következtében alacsony lesz.
Az egyetem mérete nem csak a hallgatói, hanem a dolgozói létszám alapján is mérhető, ezért megvizsgáltam, hogy ezen a téren mekkora eltérések tapasztalhatók. A dolgozói létszám figyelembevételének érdekében kiszámítottam az egy hallgatóra jutó számot (a FIR nem különbözteti meg a kinevezéses munkaviszonyú oktatókat az óraadóktól) és azt tapasztaltam, hogy arányuk jelentős eltérést mutat az intézmények profiljának függvényében. Mértéke számos művészeti és a kifejezetten hittudományokhoz kötődő egyetemek esetében magas, míg az általános intézmények esetében többségében inkább alacsony érték. 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 tehát 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 használtam[15]. Az egyetemek típusait és hallgatói létszámát az alábbi táblázatban foglaltam össze.

Fenntartó típus	Darab	Összes hallgató
Alapítvány (ALAP)	4	788
Magyar állam (ALLM) [16]	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- vagy közalapítványok által fenntartottakat. Az intézmények számát így 61-re redukáltam úgy, hogy közben a vizsgált hallgatók létszáma száma csak 851-gyel csökkent. Az így kapott adatkört továbbra is reprezentatívnak tekintem.

A gazdasági társaságok által üzemeltetett egyetemek informatikai védelmi szempontú súlyát a Budapesti Metropolitan Egyetem kivételével nem ítéltem jelentősnek, ezért ebből a fenntartói körből ezt az egy egyetemet vontam be a vizsgálati körbe. A külföldi szervezetek esetében

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

[16] 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.

kizártam azokat, melyek nem működnek, hasonlóképp jártam el a nulla hallgatói létszámúakkal 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[17].

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, esetleg egy informatikától távolabb eső, vallási vagy művészeti profilú intézmény kisebb hangsúlyt 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 szinten is jelentős Virológiai Nemzeti Laboratórium), érdemesnek tartottam nekik helyt adó egyetemeket a vizsgálati körbe bevonni.

A kiválasztási szempontok alapján az alábbi táblázatban szereplő egyetemek informatikai szabályzatait és informatikai biztonsági szabályzatait választottam ki és töltöttem le a weblapjukról. Egy esetben, a DUE szabályzatai közt leltem fel egy katasztrófaelhárítási tervet, melyet szintén bevontam a vizsgálatomba. Érdemes megjegyezni, hogy ezeket nem minden intézmény, főleg a kis egyetemek és főiskolák nem tették közzé, nem készítették el vagy azok nem válnak el más szabályzatoktól. Esetükben az adott felsőoktatási intézmény helyett másikat választottam, de a reprezentativitás megtartása érdekében a Tokaj-Hegyalja Egyetemet másik alkalmas egyetem hiányában megtartottam[18].

[17] 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.

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

Az elemzett intézményeket az alábbi táblázat sorolja fel, az ebben alkalmazott rövidítések azonosak az előző táblázatban is használt, az OH fenntartói adatszolgáltatásban alkalmazottal.

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.

2.10. A szabályzatok elemzése

A szabályzatok elemzésének első lépése a kódolás megtervezése és paramétereinek meghatározása volt. A kódolási folyamat során meg kell keresni a szövegben a kiválasztott szempontokat leíró tartalmakat, és rögzíteni kell azok értékeit az a megfelelő kategóriákban. A folyamat szakszerű elvégzése informatikai szabályzatok esetben lényegesen egyszerűbb, mint humán területeken történő alkalmazásakor, 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. A szövegek elemzését három területre terjesztettem ki.

A szabályzatkészítési gyakorlat alapján feltételeztem, hogy bár az egyetemek számára nem kötelező érvényű az 2013/L. tv. szerinti besorolások elvégzése, azt ennek ellenére igyekeznek alkalmazni. Ezért elsődleges szempontként a szabályzatokban megjelenő informatikai rendszerek felsorolását és az besorolásuk rögzítését határoztam meg. A dokumentumok elemzése során feljegyeztem a kiválasztott egyetemek szabályzataiban felsorolt rendszereket és a törvény szerinti biztonsági besorolásukat.

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. Az önállóságát megtartó ELTE szabályzata 2007 óta van érvényben, és a BGME 2014-es szabályzata is minden bizonnyal tartalmaz aktualizálandó részeket.

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 találtam). A képet valamelyest javítja, hogy a vizsgált egyetemek közül a Budapesti Műszaki és Gazdaságtudományi Egyetem és a Pázmány Péter Katolikus Egyetem szabályzatai publikusan nem érhetők el, azokat az egyetem informatikai munkatársai bocsájtották rendelkezésemre, így a szakrendszerek megismeréséhez egy potenciális OSINT felderítőnek eggyel több lépést kell megtennie. Csak két esetben nem tartalmaz 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 felsorolást adnak olyan magas besorolású rendszerekről, amelyek egészségügyi adatokat tartalmazhatnak. Bár a vizsgált körben csak a Pécsi Tudományegyetem szerepelt, a kontrollként áttekintett SOTE 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 PTE megnevezte az alkalmazott orvosi rendszereket is[19]. Az informatikai szabályzatok több esetben tartalmazták az alkalmazott rendszerek megnevezését. A védett kutatólaborokról ugyanakkor semmilyen használható információ nem volt elérhető – Pécsi Egyetem Virológiai Nemzeti Laboratóriuma önálló szervezeti egység, mely az egyetem informatikai egységeitől teljesen elkülönítve működik. A Dunaújvárosi Egyetem informatikai munkatársai viszont nem tudtak információt adni arról, hogy mely szervezeti egységük tartozik nemzetbiztonsági felügyelet alá.

Nem volt megállapítható szignifikáns különbség a fenntartó alapján sem. 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.

A H.1. igazolásához összehasonlítottam az egyes rendszerelemek besorolásait azokban az esetekben, ahol rendelkezésre álltak az ehhez szükséges adatok. 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 funkció szerint említették. Azokról, melyek minden bizonnyal léteznek, de a besorolásuk nem történt meg, 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 kovertáltam. Mivel az intézmények túlnyomórészt a négyfokozatú skálát alkalmazták (A-D osztályokat neveztek meg), 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 végezték el az egyetemek.

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

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

Rendszerelem	Említés	Max	Min	Diff
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 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 már csak 88%-ban kerültek említésre, 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 utóbbinak már az értelmezése sem egységes a szabályzatokban, feltehetően ez okozza a besorolások nagy eltérését. A middleware-nek számos különböző formája létezik a leginkább közismertek a Java engine, domain name system vagy a webes API szolgáltatások [32]. Céljuk a legtöbb esetben olyan háttérszolgáltatások nyújtása, amelyek lehetővé teszik az alkalmazások kommunikációját, integrációját vagy koordinációját. Az E-Learning rendszerek nagy eltérése feltehetően a szoftverek eltérő személyes adat tartalmából adódik, az NKE és a DUE ezt 1-es szintre, míg a PTE a 3-asba sorolta. Ezeket a rendszereket csak hárman, a könyvtári rendszereket pedig csak ketten tartották besorolásra érdemesnek.

Az elemzés alapján kimondható, hogy 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 felsőoktatási rendszerek adminisztratív szabályzása heterogén tartalmú, emellett azonos súlyú védelmi kérdéseket eltérő prioritásként kezelnek annak ellenére, hogy adatvagyonukban gazdasági és stratégiai szempontból jelentős mennyiségű adat áll rendelkezésre, melynek védelme nemzeti érdek.**

2.11. Ajánlás a felsőoktatási rendszerek besorolására

A dokumentum elemzésével bizonyítottam, hogy a felsőoktatási informatikai rendszerek biztonsági besorolásának gyakorlata nem egységes, és a szabályzatok készítése során azonos rendszerelemekre eltérő besorolást adnak. Figyelembe véve, hogy a felsőoktatási rendszerek profilja megközelítőleg azonos, ajánlást adok a szektor egészére alkalmazható besorolási keretre, ettől javaslatom szerint csak abban az esetben indokolt eltérni, amennyiben azt valamilyen intézményi tevékenység, az alkalmazott szoftver természete vagy adattartalma azt indokolja. Javaslom, hogy az informatikai szabályzatok felépítésekor az intézmények végezzék el az ajánlásban szereplő összes rendszerelem besorolását, alapvetően az abban szereplő értékelést vegyék alapul, valamint szükség esetén egészítsék ki azokkal a rendszerekkel, melyek az intézményükre nézve specifikusak. Az ajánlás kidolgozása során annak érdekében, hogy az érintett rendszerek minél szélesebb körét feltérképezhessem, nem csak a korábbi vizsgálatban kiválasztott 11 intézményt vettem alapul, hanem további szabályzatok releváns részeit is áttekintettem és felhasználtam.

Az informatikai szabályzások nyilvános közzététele számos információt nyújthat egy esetleges támadás előkészítése során. Ezért javaslatom szerint a szabályzatok nyilvános, valamint az intézmény munkatársai által széles körben elérhető részeiben kerülni kell nem csak a rendszerek felsorolását és besorolásaik közlését, hanem minden olyan, az informatikai rendszereket érintő információ közzétételét, amelyet jogszabály nem ír elő. Minden olyan részletet, mely egy lehetséges támadót segíthet célja elérésében, a szabályzatok elkülönített mellékleteiben, vagy attól elkülönítve javaslok rögzíteni, melyek hozzáférési köre az érintettek számára korlátozott kell, hogy legyen.

A felsőoktatási rendszerek besorolását az állami és önkormányzati szervekre már kidolgozott 41/2015 BM rendelet 1-es melléklete szerint, az egyetemek szakterületi besorolása alapján célszerű elvégezni. Bár az egyetemek többségükben csak egy A-D közötti négyfokozatú skálát alkalmaznak, javaslatom a rendeletben is alkalmazott öt biztonsági osztályt alkalmazza. Mivel a felsőoktatás néhány területen eltérő sajátosságokkal rendelkezik, ezért a rendelet besorolási szempontjaiból a nem releváns részeket elhagytam, másokat pedig a szektorhoz alakítottam. Így besorolások elvégzése során az alábbi szempontrendszer alkalmazását javaslom:

1. 5-ös biztonsági osztályba sorolandók azok a rendszerek, amelyek az intézmény működésében létfontosságúak, vagy azok, melyek sérülése, kiesése esetén az alapvető funkciók ellátása lehetetlenné válik, 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 olyan nagy mennyiségű információt tartalmaznak, melyek bizalmasságának és sértetlenségének megőrzése kiemelt fontosságú az intézmény menedzsmentje számára. Hasonlóan ide sorolandók be a jelentős mennyiségű személyes vagy más érzékeny adatokat tartalmazó rendszerek, kiemelten az orvosképzést végző intézmények különleges, pl. egészségügyi adatokat tartalmazó szakrendszerei. Végül ide sorolandók a jelentős értékű, vagy kiemelt kutatások folyamatát és tudományos vagy üzleti eredményeit támogató rendszerek, és amennyiben létezik ilyen, a kritikus infrastruktúrák működéséhez kapcsolódó alrendszerek.

2. A 4-es biztonsági osztályba sorolt rendszerelemek azok, melyek esetében az intézmény működésében jelentős zavar áll be, egyes funkciók működése leáll vagy jelentős funkcióvesztést szenved el. A rendszerek kiesésében elszenvedett kár jelentős, és annak következményei a nyilvánosság számára ismertté válnak. A működés vagy az ügymenet során keletkezett bizalmas adat, valamint nagymennyiségű személyes vagy különleges adat nyilvánosságra kerül vagy elvész.
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 sérülése következhet be. Anyagi kár keletkezése esetén az az adatokért felelős nagyobb szervezeti egység (pl. igazgatóság) saját költségvetésében kezelhető, viszont az intézmény külső reputációjában nem keletkezik kár és az incidens saját hatáskörben kezelhető.
4. A 2-es osztályba sorolandó minden olyan rendszer, mely nem tárol bizalmas, az intézmény működésében jelentősnek mondható információt, minimális mennyiségű személyes adatot tartalmaz, vagy az azokban tárolt információk jogszerű felhasználás mellett más, publikus forrásól is elérhetők. A rendszerrel kapcsolatos problémák kezelése az intézményen belül elvégezhetők, azoknak nincs semmilyen negatív hatása az intézmény reputációjára. Az esetleges anyagi kár az adatokért felelős szervezeti egység saját költségvetésében kezelhető.
5. Az 1-es osztály rendszerei nem tartalmaznak semmilyen érzékeny adatot, a bekövetkező káresemény jelentéktelen, és az intézmény működésében nem okoznak érzékelhető kiesést.

Az egyes részterületeket három csoportba, oktatási és kutatási, a működést támogató szakrendszerek, és az IT infrastruktúra területeibe javaslom besorolni. Az egyes rendszerelemek és javasolt biztonsági osztályok ajánlásainak kidolgozása során alapjában véve az OVI táblákban alkalmazott metodikát használtam fel adaptálva azt a felsőoktatási intézményekre.

2.11.1. Működést támogató rendszerek

Tanulmányi rendszer

Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 4. Biztonsági osztály: 5

A tanulmányi rendszer ma minden felsőoktatási intézmény esetében az SDA által fejlesztett és supportált Neptun, melynek adattartalmának ismertetésére a fejezet első szakaszában került sor. Ez minden egyetem számára nélkülözhetetlen rendszerelem, hiányában a jogszabályi megfelelés nem teljesíthető. Hiányában nem továbbíthatók a FIR jelentések, melyek az állami támogatás elszámolásában alapvető szereppel bírnak, továbbá az alkalmazott modulok függvényében meghiúsulhat a tandíjak befizetése, számlák kiállítása és küldése. Kiesése esetén az intézmény csak az üzletfolytonossági tervében foglaltak szerint, manuális helyettesítő eljárásokkal képes ellátni fő profilja, az oktatás adminisztrációját, mely a szorgalmi időszakban kisebb, tantárgyfelvételi és a vizsgaidőszakban viszont komolyabb fennakadást okoz. A tanulmányi rendszer hiányában nem adhatók ki igazolások a korábbi tanulmányokról és az intézmény részéről problémát jelent a kiadott diplomák igazolása is[20]. A tanulmányi rendszer az államilag támogatott félévek számának pontos meghatározásában is szereppel bír.

Bár a Neptun üzemeltetése igénybe vehető a szolgáltató infrastruktúráján is, számos egyetem saját telehelyén működteti azért, mert így biztosított a rendszert működtető adatbázis és a hozzá tartozó Application Programming Interface-re (API) alapozott további szolgáltatások kialakítása és üzemeltetése. Bár ezek jellemzően azonosítási szolgáltatásokat kínálnak, de számos más rendszer számára adatforrásként működhetnek. Számos egyetem hozott létre valamilyen, a hallgatói lemorzsolódás megelőzését célul kitűző rendszert, különféle támogató rendszereket, a vezetői döntéseket megalapozó, bár tapasztalataim alapján kevés intézményben működő vezetői információs rendszert (VIR), de a Neptun működésképtelensége több intézmény esetében megbénítaná az EduRoam és az EduID azonosítási funkcióinak működését a hallgatók számára. A távolléti oktatás menedzsmentjének támogatásához pedig több egyetem

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

fejlesztett ki kommunikációs- és adatcsere interfészeket különféle LMS-ekkel (pl. az ELTE esetében a Teams és Moodle adminisztrációjának részleges automatizálására).
A tanulmányi rendszer elvesztése, vagy adatainak nyilvánosságra kerülése komoly reputációs problémát okozhat az intézmények számára, ahogyan azt 2022-ben a szintén az SDA fejlesztésében levő Kréta rendszer feltörése esete már megmutatta. A rendszer támadására már több alkalommal volt példa – a nyilvánosságra került esetek többnyire a rendszerbe épített üzenetküldési szolgáltatást támadásáról szólnak [33]. 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.

Gazdasági rendszer

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

A gazdasági rendszereket a szabályzatok eltérően értelmezték, melynek csak egyik oka az integrált szoftverek alkalmazása. Jelen ajánlásban gazdasági rendszer alatt elsősorban a pénzügyi rendszert értem. A gazdasági szervezeti egységek működését számos alrendszer segíti, melyek közül a leggyakoribbak: beszerzési rendszer, szerződésnyilvántartó rendszer és a folyamattámogató rendszer, ezeket a már említett személy- és bérügyi rendszerek kivételével ebbe az osztályba soroltam. Jelenlegi működésük és központosításuk az intézmény fenntartójától függően eltérő. A vagyonkezelő alapítványokba sorolt egyetemek legtöbbje külső szolgáltatótól veszi igénybe, egy központosított, SAP alapú integrált rendszert alkalmaznak. Kivonási terv vagy stratégia, lokális adatmentés vagy archív helyi rendszer ismereteim szerint egyikük esetében sem áll rendelkezésére, 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. A gazdasági rendszer működési zavara esetén az intézmény nem tudja ellátni a bejövő és kimenő számláinak kezelését, nem tud eleget tenni a NAV felé irányuló kötelezettségeinek, és az állam felé irányuló kötelező adatközléseknek sem függetlenül attól, hogy az saját infrastruktúrán vagy szolgáltatásként kerül megvalósításra.
A gazdasági rendszer szerepe a felsőoktatási intézményekben kiemelt, kiesése minimális ideig tolerálható, adatainak elvesztése komoly anyagi és reputációs veszteséget okoz.

Bér- és munkaügyi rendszer

Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 2. 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 intézmények eltérő szoftver környezetben valósítják meg a területek támogatását. Mivel a bérrendszerek funkciói a személyügyi adatokra alapozottak, működésük önállóan nem képzelhetők el, ezért besorolásukat egy rendszerként javaslom megtenni.
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 képessége is (nyelvvizsgák, végzettségek dokumentumai). Különleges adatot csak a munkavégzéssel összefüggésben tárolnak, melynek előfordulása e rendszerre nézve eseti. Ennek adatbázisa alapján történik meg a bérek számfejtése, a társadalombiztosítási adatok jelentése. Kiegészítő funkcióik révén támogatást nyújtanak a teljesítményértékelésben, az új munkatársak toborzásában, de a projektmunkák során segíthetik az ideális személyek kiválasztását is.
A bér- és munkaügyi rendszerek szerepe is kiemelt a felsőoktatási intézményekben, adatszivárgás esetén nagymennyiségű személyes adat kerülhet nyilvánosságra, rendelkezésre állásának elvesztése pedig egyrészt zavart okozna a bérek idejében történő átutalásában, ami az intézmény vezetésének reputációjában okozna kárt, adatvesztéssel járó sérülésének következményei pedig nem lennének a szervezeten belül tarthatók.

Iktatás és dokumentumkezelés (ECM)

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

A szabályzatok az iktatást és a dokumentumkezelést elkülönült feladatként írták le, ugyanakkor, mivel funkcióik megközelítőleg azonosak, és a kezelt adatok alapján besorolásuk sem különbözik, Enterprise Content Management (ECM) néven együttes kezelésüket javaslom.
Ezek a rendszerek az intézmények iratkezelését látják el. Adatbázisukban tárolásra kerül a hivatalos levelezés, az ügyintézési folyamatok, munka- és megbízási szerződések és számos más dokumentum, mely az intézményben zajló folyamatok kezelésében és nyomon követésében elengedhetetlen. Az iktatási rendszerek dokumentumai számos személyes adatot tartalmaznak, és az intézmények olyan belső dokumentumait is, melyeket titoktartási szerződés véd, vagy melynek nyilvánosságra kerülése az intézmény reputációját jelentősen rontaná.

Ugyanakkor a rendelkezésre állásának rövid idejű elvesztése feltehetően kezelhető az intézmények számára, ez indokolja a rendelkezésre állás alacsony besorolását.

Beszerzési rendszer

Bizalmasság: 2, sértetlenség: 4, rendelkezésre állás: 4. Biztonsági osztály: 4

A beszerzési rendszerek kiemelt szerepe a felsőoktatási intézmények közbeszerzési kötelezettségének következményeként jelenik meg. A beszerzési eljárások rendkívül magas komplexitásúak, hosszú ideig tartanak és – főleg pályázati finanszírozás esetén – szigorú mérföldkövek jelentette határidőket tartalmaznak. A beszerzések szabályszerű lebonyolításának végrehajtása, valamint a beszerzési folyamatok szabályosságának bizonyítása mind a pályázati ellenőrzések, mind pedig az Állami Számvevőszék vizsgálatai során komoly feladatot ró a beszerzési szervezeti egységekre, így a beszerzési rendszer rendelkezésre állásának problémái esetén üzletfolytonossági terv hiányában a feladataikat nem tudják ellátni, ami a beszerzési folyamatok zavarához, és az elszámolási feladatok háttérdokumentumainak elérhetetlenségéhez vezethet.

A közfeladatot ellátó szervezetként működő egyetemek gazdálkodása és beszerzései is nyilvánosak, így azokban a nem publikus információ mennyisége viszonylag alacsony, ez indokolja a bizalmasság alacsony besorolását.

Folyamattámogató rendszer

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

A felsőoktatási intézmények egy része folyamataik kezelésére valamilyen általános célú folyamattámogató-rendszert alkalmaz[21]. Ezekben egy megfelelően képzett informatikai szakember képes a folyamatok definiálásra, az abban résztvevők szerepköreinek meghatározására, az aláírási sor kialakítására; alkalmazásával a belső ügyviteli folyamatok egyszerűen egységesíthetők és automatizálhatók a domain igényléstől a kiutazások folyamatának lebonyolításáig. Mivel ezek a folyamatok a korábban meglevő, papíralapú eljárások elektronikus megvalósításai, továbbá az ügykezelés azok hagyományos módján is elvégezhetők, ezért többségük szempontjából a sértetlenségük és rendelkezésre állásuk nem kritikus. Azonosítási szolgáltatásait a legtöbb esetben nem önállóan, hanem központi címtárra alapozva végzik, a tárolt személyes adatok mennyisége pedig a kezelt folyamatok függvénye. Besorolását nagyban befolyásolja az abban megvalósított funkciók bizalmassági, sértetlenségi

[21] Több egyetem esetében ez a Modulo.

és rendelkezésre állási követelménye, így konkrét javaslatomat csak a leggyakoribb, általános esetre adtam meg, melyet a konkrét folyamatban résztvevő adatok jellege alapján kell módosítani.

Projektszervezés és támogatás

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 indokolja a bizalmasság alacsony besorolását. A pályázati források értéke ugyanakkor a legtöbb egyetem esetében eléri a teljes költségvetés 5%-át, így sérülése vagy a rendelkezésre állásának kritikus időpontban történő elvesztése nem csak a pályázat benyújtási időszakában, hanem az elszámolási szakaszban is súlyos anyagi következményekkel járhat.

VIR

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

A Vezetői Információs Rendszer (VIR) adatkezelése során feltételeztem, hogy annak tartalma más szakrendszerek kumulált adatokat tartalmazó jelentései alapján épül fel, és az rendszeres időközönként aktualizálásra kerül. Ebben a működési modellben a VIR rendszerek nem tartalmazzák konkrét személyek adatait, ugyanakkor adatkapcsolataik révén hozzáférésük lehet más szakrendszerekhez. Ezért a VIR adatkapcsolatainak természete nagyban meghatározza az esetleges sérülése során fellépő kockázatot.

Az egyetemek jórésze közintézmény, melynek adatai az állampolgárok számára pl. egy közérdekű adatigénylés formájában megismerhetők, így abban 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. A VIR az elmondottakkal szemben viszont lényegesen magasabb kockázati elem, amennyiben adatkapcsolatai révén képes más szakrendszerek (tipikusan a legmagasabb érzékenységű tanulmányi, személyügyi és gazdasági rendszerek) adatainak közvetlen hozzáférésére.

Épületmenedzsment

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, gazdasági döntések háttértámogatása stb. Tekintettel arra, hogy a magyar egyetemek egy része különböző településeken számos inagtlannal rendelkezik, informatikai háttértámogatás hiányában az épületmenedzsment feladatokat csak manuális úton, kézi nyilvántartások alapján lenne képes ellátni. Ezek a rendszerek csak minimális mennyiségű személyes adatot tartalmaznak, ugyanakkor kiesésük esetén az el nem végzett feladatok hatósági eljárást, és pénzbüntetést vonhatnak maguk után, így szerepük nem hanyagolható el.

Nyomtatás

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

A nyomtatási alrendszerek az esetek túlnyomó többségében nem kezelnek személyes adatokat, azonosítási funkcióikat a címtárszolgáltatáson keresztül valósítják meg. Ezért ezeket a rendszereket a legalacsonyabb biztonsági besorolásba kell helyezni. 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 esetlegesen érzékeny dokumentumok kiszivárgása esetén adatsértés valósul meg.

Telefonhálózat

Bizalmasság: 1-2 sértetlenség: 1-2, rendelkezésre állás: 1-2. Biztonsági osztály: 1-2

A digitális telefonhálózatok rendelkeznek belső telefonkönyvvel, és egy munkatárs hívószámának megkereshetősége mellett erre alapozva megjeleníthetik hívó fél nevét. Amennyiben az alkalmazott központ tartalmaz ilyet, azt a 2-es szintbe, a hagyományos, vagy személyes adatokat nem tartalmazó telefonhálózatok esetén 1-esbe javaslom sorolni.

2.11.2. Oktatás- és kutatástámogató rendszerek

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

Hallgatói laborok

Bizalmasság: 1 sértetlenség: 1, rendelkezésre állás: 1. Biztonsági osztály: 1

A hallgatói számítógépes laborok nem tartalmaznak személyes adatokat, rendszerint az intézmény hálózatában egy elszeparált VLAN-ban működnek, ugyanakkor a hallgatói jogosultságainak beállítására vonatkozó stratégiában eltérések tapasztalhatók. A laborok rendelkezésre állását eredményező incidensek lehetséges következményei elhanyagolhatók, így besorolásukat a legalacsonyabb szintbe javaslom.

E-learning rendszerek

Bizalmasság: 1-2 sértetlenség: 1-2, rendelkezésre állás: 1. Biztonsági osztály: 1-2

Számos egyetem rendelkezik elektronikus tananyagokkal, melyek az egyes kurzusok során elsajátítandó ismeretanyagot részben vagy egészben fedik le. Azok az E-learning rendszerek, melyek funkcionalitása pusztán a tananyagok átadásában merül ki, és adatkezelést nem valósítanak meg, pusztán a rendelkezésre állás területén jelenthetnek nem biztonsági jellegű kockázatot. Ezért ezek a rendszerek javaslatom szerint szintén a legalacsonyabb biztonsági osztályba sorolandók.

Amennyiben az adott rendszer személyes adatokat, például bejelentkezési azonosítókat, valamint az egyes kurzusokon elért eredményeket tárol, a bizalmasság és a sértetlenség kritériumain keresztül biztonsági osztály javasolt értéke 2.

Kutatói rendszerek

Bizalmasság: 2-3 sértetlenség: 2-3, rendelkezésre állás: 1. Biztonsági osztály: 2-3

A kutatói rendszerek besorolásakor nem vettem figyelembe azokat a kiemelt kutatócsoportokat, melyek a kutatási eredmények, a kutatás jellege vagy körülményei következtében nemzetbiztonsági felügyelet alá tartoznak, ezek működése önálló, az egyetemekétől eltérő jogszabályok mentén történik. Az ettől eltérő kutatási projektek során, mely magában foglalja a több tudományegyetem által is 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 a 3-as besorolást javaslom.

Könyvtári rendszerek

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 több-kevesebb személyes adatot tartalmaz. 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.

2.11.3. 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.

Tárhely kiszolgálók

Bizalmasság: 1-4 sértetlenség: 1-4, rendelkezésre állás: 1-3. Biztonsági osztály: 4

A tárhely kiszolgálók tipikus elemei a fájlszerverek illetve a különféle, az intézményi infrastruktúrán kialakított felhőszolgáltatásként működő szoftverek. Ezek biztonsági besorolása adattartalmuk ismerete és besorolása nélkül nem határozható meg. Azon kiszolgálók esetében, melyek nem tartalmaznak az intézmény szempontjából releváns vagy személyes adatokat (ilyenek a számítógépes laborok fájlszerverei) a legalacsonyabb biztonsági osztályba sorolandók. Egyéb esetekben a bizalmasság és a rendelkezésre állás besorolását az adattartalom érzékenysége alapján kell meghatározni.

Mindkét esetben célszerű a szerverek tartalom szerinti többszörözése és ez alapján a besorolásuk egyedi elvégzése, valamint – amennyiben szükséges – az informatikai hálózat különböző védettségű pontjain történő elhelyezése.

Webszerverek

Bizalmasság: 1-4 sértetlenség: 1-4, rendelkezésre állás: 1-3. Biztonsági osztály: 4

A webszerverek virtuális tárhelyszolgáltatásuk révén számos website kiszolgálását képesek ellátni, ezért besorolásuk az egyes site-ok adattartalmának ismerete nélkül nem határozható meg. Ezért besorolási alapelvei a tárhelyszolgáltatásokéval egyezik meg: amelyek nem

tartalmaznak az intézmény szempontjából releváns, vagy személyes adatokat, a legalacsonyabb biztonsági osztályba sorolandók, más esetben a bizalmasság és a rendelkezésre állás besorolását az adattartalom érzékenysége alapján kell meghatározni, és esetükben is javalom az adattartalom érzékenysége alapján történő szeparációt.

Elektronikus levelezés

Bizalmasság: 4 sértetlenség: 3, rendelkezésre állás: 2. Biztonsági osztály: 4

Az elektronikus levelezés biztonsági besorolása annak adattartalma függvényében lenne pontosan meghatározható. Tekintettel arra, hogy az elektronikus levelek mellékleteiben bármely szakrendszerekből származó riport, vagy egyéb bizalmas adat szerepelhet, valamint az intézményi e-mail címek önmagukban is személyes adatok, az elektronikus levelezés bizalmasságának javasolt besorolása 4. Adatbiztonság szempontból a sértetlenség és a rendelkezésre állás ezeknél a rendszereknél néhány szélsőséges esettől eltekintve nem kritikus.

Központi címtár

Bizalmasság: 4 sértetlenség: 4, rendelkezésre állás: 2-5. Biztonsági osztály: 4

A központi címtár besorolása az azt igénybe vevő rendszereken keresztül végezhető el. A címtárszolgáltatás integrálásában az informatikai üzemeltetők mellett a minden más terület érdekelt, mivel az egy ponton történő azonosítás megkíméli a munkatársakat a különböző rendszerekhez tartotó jelszavak memorizálásának kényszerétől, ugyanakkor kockázatot is jelent a hozzáférés kiszivárgása esetén – ekkor ugyanis az azonosítási szolgáltatást igénybe vevő összes rendszerelem kompromittálhatóvá válik. A nagymennyiségű személyes adat tárolása következtében a címtárat érintő adatszivárgás komoly problémát okozhat a szervezet számára, a rendelkezésre állás elvesztésének következményei a kapcsolódó rendszerek rendelkezésre állásának függvényében változnak. Ezért besorolásának értékét ezért az arra alapozó rendszerek rendelkezésre állási követelményének maximuma adja.

A szolgáltatáson alapul az intézményi telefonkönyv vagy tudakozó is, melyet több szabályzat külön említ, és működése ideális esetben a címtáron alapul.

Backup

Bizalmasság: 5, sértetlenség: 5, rendelkezésre állás: 4. Biztonsági osztály: 5

A mentési rendszerek a szakrendszerek és egyéb egyetemi adatforrások adatait több verzióban is tartalmazzák. Egy mentési rendszerben történt adatszivárgás következményei azonosak a forrásrendszer adatainak nyilvánosságra kerülésével, ezért bizalmasságának besorolási értéke

az abba mentett szakrendszer mértékével azonos. Bár sértetlensége és rendelkezésre állása a normál üzemben nem kiemelkedő, egy informatikai incidens során kiemelt fontosságúvá válik, ezért az adatmentési rendszerek besorolását minden esetben az abba mentett szakrendszerekhez rendelt legmagasabb értékkel megegyezőnek javaslom.

Alap infrastruktúra elemek

Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 4. Biztonsági osztály: 4

Számos szabályzat végzett besorolást az alap informatikai infrastruktúra egyes részkomponensein, melyeket inkább adattartalmuk alapján célszerű csoportosítani. A leggyakoribb elemek a számítógép hálózat alap infrastruktúrája, a middleware rendszerek, tanúsítvány szolgáltatások, DNS, infrastruktúra felügyeleti rendszerek (Nagios, Icinga stb.). Bár ezek a részelemek az informatikai üzemeltetés számára rendkívül fontosak, ennél fogva gyakran indokolatlanul felülértékeltek, személyes vagy intézményi adatokat nem tárolnak, sérülésük során adatvesztés nem történik. Kritikus viszont a rendelkezésre állásuk: ennek mértékét a kiszolgált rendszerek rendelkezésre állási besorolásának maximuma határozza meg.

Határvédelmi rendszerek

Bizalmasság: 2 sértetlenség: 2, rendelkezésre állás: 4. Biztonsági osztály: 4

A határvédelmi eszközök közé elsősorban a tűzfalakat, kisebb számban routereket, esetleg korlátozásokkal konfigurált switcheket értenek. Bár ezek az eszközök lényeges szerepet játszanak az informatikai hálózat elemeinek kiszolgálásában, maguk az eszközök nem tartalmaznak személyes adatot, így a bizalmasság és a sértetlenség besorolása alacsony. Hangsúlyozandó, hogy ezen eszközök sikeres kompromittálása súlyos biztonsági hibák kiinduló állomása lehet, így védelmüket magas prioritással kell ellátni. A rendelkezésre állás sérülésének következményei a kiszolgált rendszerek rendelkezésre állásának függvényében változnak. Mértékét ezért a védett rendszerek rendelkezésre állási besorolásának legmagasabb értéke adja.

2.11.4. Szakrendszerek

Főként az orvosképzés profilú egyetemek tértek ki szabályzataikban olyan szakrendszerek besorolására, melyek csak az adott szakképzésben relevánsak. Számos más egyetem is rendelkezhet ilyen, speciális szakrendszerrel, melyek besorolására azok adattartalma, kiszivárgásuk, sértetlenségük és rendelkezésre állásuk sérülésének ismerete nélkül nem adható

javaslat. Ugyanakkor javaslom a nyílt hozzáférésű szabályzatokban e speciális szakrendszerek megnevezésének mellőzését, és kizárólag általános funkcióinak leírását.

2.12. Összegzés

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

A tág értelemben vett informatikai védelem terén az egyetemek nemzetközi és magyar viszonylatban több hasonlóságot mutatnak, így a nemzetközi tendenciák változását valószínűleg a hazaiak is követik majd. Ugyanakkor több ponton eltérések érzékelhetők, amelyekre vonatkozó megállapításaimat magyar szakirodalmi források hiányában személyes tapasztalataimra alapozva tettem meg. A magyar egyetemek esetében nem látszik jelentős különbség a kezelt adatok széles körében, a jogszabályi háttér viszonylagos megengedő jellegében és az egyetemekre szabott jogszabályok hiányában. Komolyabb különbség merül fel a károkozásra közvetlenül alkalmas adatelemek terén: az 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 a gazdasági és a tanulmányi rendszert.

Az oktatói és kutatói terület által generált védelmi problémák viszont közel azonosnak tűnnek, amelyekre a szakirodalmi hivatkozások is fellehetők.

A kiberfenyegetések azonosítására nem állt rendelkezésre olyan mennyiségű magyar adat, amely lehetővé tenné a nemzetközi összehasonlítást. Ezért főként amerikai adatok alapján mutattam ki, hogy az oktatási szektor az informatikai incidensek 6-9%-ban érintett terület, és megállapításokat tettem az egyes incidenstípusok jelenlétének gyakoriságára is. A fejlett országokban a szféra fő problémái az egyetem nyitott kultúrája, az informatikai veszélyhelyzetek felismerésének hiánya, a vezetői támogatás problémái, a saját használatú eszközök és a finanszírozási kérdések köré csoportosulnak. A fejlődő országok egyetemei esetében ezek a problémák fokozottan jelentkeznek.

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 és javaslatot tettem azok elemeinek besorolására. Javaslatom és az elemzett dokumentumok besorolásai jelentős különbséget mutattak, így megállapítható, hogy a szabályzatok kialakítását nem megfelelően végzik el.

“If you can not measure it, you can not improve it.”

Lord Kelvin

3. Felsőoktatási intézmények sérülékenységelemzésen alapuló vizsgálata

3.1.A felsőoktatási rendszerek különbözősége

A felsőoktatási rendszerekkel szemben támasztott védelmi követelmények szoros szabályozása nemzetközi viszonylatban sem jellemző, a szakirodalom csak néhány törekvést említ ennek megváltoztatására. Az Amerikai Egyesült Államokban sem létezik átfogó, a felsőoktatásra szabott jogi környezet, az informatikai rendszerekkel kapcsolatos szabályzást több, különböző területet lefedő jogszabály valósítja meg úgy, hogy azok államonként is eltérhetnek. A tanulói adatok védelme az európai gyakorlatnál sokkal régebbre nyúlik vissza: az USA Oktatási Minisztériuma a Family Educational Rights and Privacy Act-ben (Családi oktatási jogok és adatvédelmi törvény, FERPA) szabályozza a tanulói adatkezeléssel kapcsolatos előírásokat. Ennek hatálya kiterjed minden olyan általános, középiskolai vagy felsőoktatási intézményre, valamint minden olyan állami vagy helyi oktatási intézményre, amely az Egyesült Államok Oktatási Minisztériumának valamely vonatkozó programja keretében pénzeszközöket kap. Azok az iskolák, amelyek nem tartják be a FERPA szabályait, a szövetségi finanszírozás elvesztését kockáztatják [34].

Magyarországon sincs kifejezetten felsőoktatásra szabott szektorspecifikus jogszabályi keret, így az informatikai működést pusztán az általános szabályzók mentén kell biztosítani. A személyes adatok védelméről szóló általános GDPR mellett a legfontosabbak a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, de a szektorra nézve relevánsak a Btk. vonatkozó részei is [35] [13].

A 2011. évi CXII. törvény adja meg a személyes adat fogalmát is, 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". [14]

A felsőoktatás általánosságban, néhány kutatási terület kivételével nem tartozik a 2013. évi L. törvény és annak végrehajtási rendeletének hatálya alá, a kezelt adatok mennyisége alapján így

nehezen indokolható kontraszt érzékelhető egy vidéki önkormányzat és egy egyetem működési keretei között.

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

3.2.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 a szerző személyes tapasztalatai is egybeesnek ezzel [36]. A FireEye fehér könyve [24] a biztonsági eszközök korlátozó hatását emeli ki, amely akadályozza az információhoz való hozzáférést. Az oktatók és kutatók nyomást gyakorolnak az egyetemi vezetésre a biztonsági intézkedések fellazítása érdekében, ugyanakkor egy esetleges incidens esetén az üzemeltetést okolhatják. Ezt a jelenséget Adams már 2003-ban megfogalmazza, és a kultúrák összeütközésének *(clash of cultures)* nevezi [36].

Az informatikai védelem gyengítését célzó törekvések számos ponton jelennek meg, amelyek hosszasan sorolhatók. A jelszóképzési szabályokkal történő szembefordulás, a körülményes *secure printing* kötelezettsége alóli kibújás személyes tapasztalataim szerint olyan belső szervezeti egységeknél is megjelenik, amelyek bizalmas dokumentumok tömegét kezelik, éppen azok egy részénél, amelyek védelme érdekében a biztonságos rendszereket bevezették. A távoli munka biztosítása érdekében bevezetett bonyolultabb VPN-kliensek alkalmazási kényszere is számos kritikát kap. Tipikus a kutatási feladatok ellátására pályázati forrásból beszerzett szerverek fizikai birtoklási vágya, amelyeket egyszerű irodákban, megfelelő fizikai védelem nélkül, helyi, 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 különösen jellemző, és ezek a legfeljebb részlegesen felügyelt, a családtagokkal közös használatú gépek különösen nagy kockázatot jelentenek.

Az informatikai üzemeltetés szervezeti felépítésben elfoglalt helye is meghatározó. Azok az egyetemek, amelyekben ezt a szervezeti egységet túl alacsony szintre helyezik, lehetővé teszik más egységek számára, hogy a hierarchia okán magukra nézve ne tekintsék szigorúan kötelezőnek az informatikai szakemberek előírásait. Az egységes informatikai koncepció és üzemeltetés nehezen tartható fenn azokon az egyetemeken, amelyek lehetővé teszik a

különböző szervezeti egységek számára önálló informatikus foglalkoztatását, mivel ők csak egy laza kapcsolat mentén működnek együtt a többi üzemeltetővel. Amennyiben a szeparáció elengedhetetlen, inkább a hierarchikus modell kialakítására érdemes törekedni.

A nyilvánosság igénye nem csak az egyetemi kultúra következménye. A közintézmények esetében megkövetelt átláthatóság a nyílt forráskódú felderítés (*Open Source Intelligence,* OSINT) aranybányája, amely nagyban növeli egy célzott támadás megtervezését és sikerét. A nyílt adatok közt gyakran szerepelnek szabályzatok, szerződések, beszállítók és számos más olyan információ, amelyet egy potenciális támadó az intézmény belső működésének, eszközparkjának felderítésére használhat fel.[22] Amennyiben egy ilyen személy számára ismert a célintézmény eszközparkja, a már említett CVE-adatbázis alapján képes azonosítani azok sérülékenységeit, ami egy támadás sikerét sokkal valószínűbbé teszi.

3.3.Információbiztonsági tudatosság

Egy hagyományos szervezettel szemben a felsőoktatási intézmények hallgatósága évről évre változik. A végzett hallgatók elhagyják az intézményt, és helyüket egy új évfolyam váltja fel. Az új hallgatók számára szolgáltatások tömegét kell biztosítani úgy, hogy azok nyilvános hozzáférhetősége biztonsági kockázatot jelent. Al-Janabi és Al Shourbaji kutatásában a közel-keleti oktatási intézmények hallgatói körében meglevő információbiztonsági hiányosságokra mutatnak rá [37]. Fő okként a biztonsági követelmények betartásának elmulasztását, az általános ismeretek hiányát, a felhasználók kockázatos viselkedését és meggyőződéseit, valamint a technológia nem megfelelő használatát jelölték meg.

A social engineering (SE) támadások az egyetemi környezetben is sikeresnek bizonyultak [38]. 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 [38]. Eltérő metodikával magyar egyetemi környezetben végeztem SE felmérést melynek eredményeit a H.6-3 bizonyításakor ismertetem. Az alacsony információbiztonság-tudatossági szint oka az informatikai eszközökhöz való viszonyulás, következményei pedig a folyamatosan visszatérő jelszósértések és alapvető adatbiztonsági tevékenységek elmulasztása voltak.

3.4.Erőforrások és vezetői támogatás

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

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 [24]. 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.

Az informatikai eszközpark mellett az üzemeltetést végző személyzet rendelkezésre állása és szaktudása is komoly problémát jelent az egyetemek számára. A gazdasági szféra elszívó ereje, az alacsony bérek, a távolléti munkavégzés lehetősége nem teszi vonzóvá az akadémiai szférát. 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 viszonylag könnyebb feladat, a szerver- és hálózatüzemeltetést, a speciális szakrendszerekben jártas kollégák a piaci elszívó hatással szembeni hosszú idejű megtartása már minden felsőoktatási intézmény számára megerőltető feladatot jelent. Az jelenlegi dolgozók pedig rendszerint a másodlagos gazdaságban egészítik ki jövedelmüket, így 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 nem dokumentált úton 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 a támogatás is megszűnik. Tapasztalataim szerint nem elhanyagolható az amatőr programozók szerepvállalása, akik nem feltétlenül ismerik a sem a lehetséges támadásvektorokat, sem az elvárt védelmi metodikákat, így az általuk fejlesztett megoldások alapvető biztonsági követelményeket hagynak figyelmen kívül. A távoli hozzáférést is biztosító 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 a nem tervezett és felügyelt 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 H.1. bizonyításából következően a legnagyobb számú hallgatót képző 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, melyre több olyan, részben a potenciális támadók által is alkalmazható módszer létezik, mely képet ad egy rendszer aktuális állapotáról.

Ilyen elemzések módszereire a szakirodalom az alábbiakat említi:

1. *Sebezhetőségi felmérés.* Ebben az eljárásban a rendszer ismert sebezhetőségeit kutatják fel, mely magában foglalja az egyes sérülékenységek azonosítását és értékelését is. A vizsgálat elvégezhető rendszeresen vagy alkalomszerűen, automatizáltan vagy manuális úton is, de az esetek túlnyomó többségében azt erre a célra kifejlesztett szoftverre alapozzák.
2. A *Behatolásvizsgálat (penetrációs teszt)* egy olyan tesztelési eljárás, melynek során a rendszer tulajdonosa által megbízott szakemberek csoportja olyan támadást hajt végre, amelyet potenciális támadók is megtehetnek. A teszt elsődleges célja a már említett

sebezhetőségi felmérés, azaz azoknak pontoknak a meghatározása, amelyek lehetőséget nyújtanak a rendszer kompromittálására, vagy az adataihoz történő hozzáférésre. A teszt végrehajtását követően hozott intézkedéseknek az ismertté vált eljárások alkalmazásának lehetőségét ki kell zárniuk. Különböző változatai ismertek, melyek elsősorban a vizsgált rendszerre vonatkozó előzetes ismerthalmazban különböznek, eszközkészletük pedig gyakran a publikusan, vagy zárt csoportokban elérhető, már rendelkezésre álló támadó szoftver eszközökkel[23] történik.

3. *Kockázatértékelés:* az eljárás magában foglalja a rendszert érintő kockázatok azonosítását, azok értékelését, azok prioritási rendjét, valamint meghatározza azok kezelését.
4. *Biztonsági ellenőrzés:* A biztonsági ellenőrzés az informatikai rendszerben alkalmazott biztonsági intézkedések átfogó felülvizsgálata. Ez magában foglalhatja a biztonsági irányelvek, eljárások és konfigurációk felülvizsgálatát annak biztosítása érdekében, hogy azok hatékonyak legyenek és megfeleljenek az iparági szabványoknak.
5. A *kódelemzés* célja sérülékenységek azonosítása egy szoftver forráskódjának felülvizsgálatával.
6. *A fenyegetés modellezésének* első eleme a kódelemzéshez hasonlóan, egy rendszer konfigurációjának elemzésével történik, amit a lehetséges fenyegetések és azok következményeinek meghatározása követ. A kockázatok elemzése után a rendszer konfigurációjának módosításával, további, például határvédelmi eszközök telepítésével vagy szabályzati úton meghozott védelmi intézkedések bevezetésével csökkentik a lehetséges kockázatokat.
7. A *hálózatbiztonsági elemzés* a hálózati infrastruktúra biztonságának elemzésére irányul, beleértve a fizikai eszközöket, azok konfigurációit és az alkalmazott hálózati protokollokat.
8. Az *adatbiztonsági elemzés* feladata a rendszeren belüli adatok biztonságának értékelése, beleértve az adatok tárolásának, továbbításának és hozzáférésének módjait is.

[23] A támadó eszközök egyik legismertebb gyűjteménye a Kali Linux, mely az általános eszközkészlet (pl. portszkennerek) mellett támadásra alkalmas szoftverek valamilyen módon korlátozott változatait tartalmazza. Több alternatívája létezik, pl. a Blackbox, a BlackArch vagy a Parrot Security.

Az üzemeltetéséret felelős szervezeti egység számára a belső folyamatok ismerete, a rendelkezésre álló dokumentációs háttér és a szállítói támogatás hatékonyabb védelmi eljárások kidolgozást teszi lehetővé, ugyanakkor egy támadó különböző technikákkal (pl. OSINT) kombinálva ezek számottevő részét megismerheti. Egyetemi környezetben és más, közbeszerzésre kötelezett intézmények esetén a nyilvánosság érdekében közzétett beszerzési eljárások, szállítók, a beszerzett eszközök, valamint a jogszabályban előírt szoftverek megismerésével[24] 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. Hipotézisem bizonyításának eszköze a sebezhetőségi felmérés, melynek eredményéből vonom le a következtetéseimet.

3.5.A sérülékenységek felderítése és mérési metodikája

Egy szervezet informatikai rendszerében jelenlevő sérülékenységek azonosítása elengedhetetlen a jól működő védelmi stratégia kidolgozásához. Az intézkedések ideális sorrendjének meghatározásához és hogy az annak érdekében alkalmazott eszközök vagy módszerek működőképességének ellenőrzéséhez elengedhetetlen egy metrika kialakítása és az az alapján végzett folyamatos mérés. Nagyobb szervezetekben 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.

A sérülékenységek kezelése során a nagyobb kár okozására alkalmas veszélyhelyzet előidézésére vagy kár 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 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

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

generált riportok kimutathatják az egyes rendszerelemek forgalmi alapon megállapított érintettségét, 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, de a mélytanulásban elért tudományos eredmények alkalmazhatóságát számos kutatás vizsgálja [39, p. 2]. Az IDS-ek fő hátrányának a támadó minták hálózati detektálása és az azokat tartalmazó csomagok célpontjai közti kapcsolat hiányát tartom. Egy ilyen rendszer beüzemelése után során az Eszterházy Károly Egyetem forgalmának analízise legnagyobb számban a Log4J sérülékenység kihasználására irányuló forgalomról számolt be, miközben az egyetemi informatikai rendszer nem tartalmazott olyan komponenst, amely erre érzékeny lett volna.

Az IPS (Intrusion Prevention System) az IDS kiterjesztéseként működik úgy, hogy egy támadó minta azonosítása esetén képes megszakítani a kommunikációban részvevő számítógépek forgalmát. Az IPS alkalmas lehet a forenzikus vizsgálatok elvégzésének támogatására is. Egy IPS esetén bekövetkező téves riasztások viszont már komolyabb következményekkel járhatnak, mivel a kapcsolatok indokolatlan blokkolása a rendszer rendelkezésre állását nagyban leronthatja [40].

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 [41, 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.

3.6.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 [42]. 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 kommentek rögzítésére alkalmas mezővel látták el. Lényeges, hogy az adatbázis nem tartalmaz a 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[25] (NVD), vagy a CERT/CC Vulnerability Notes-ban találhatók meg. Emellett más, nyilvános közzétételi források is léteznek, többek közt a szoftver gyártók saját megoldásaikban, 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, szinkronizálva van a CVE-listával, 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).” [43]

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)[26]. 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 folyamatában 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

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

exploit adatbázisok[27] 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 a támadások száma azok kibocsájtásakor jelentősen megnő. Eredményük azt is sugallja, hogy a közzétett és a javított sebezhetőségeket is valószínűleg jobban kihasználják, mint azokat, amelyeket még nem publikáltak [44].

3.7.A sérülékenységek számszerű meghatározása

A kockázatelemzés során alkalmazható módszertanok, az azt támogató szabványok és jógyakorlatok gyakran nem adnak lehetőséget az egyes sérülékenységek kvantitatív eszközöket a kockázat becsléséhez. Egyes szervezetek különböző sebezhetőségi pontozási keretrendszereket definiáltak a kockázat minőségi[28] vagy mennyiségi értékelésére[29]. 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[30], de több más, hasonló célú rendszer is ismert. 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 [45]. Ennek első változata 2005-ben jelent meg, melyet azóta többször is továbbfejlesztettek, és jelenleg is több különböző verziója van használatban. 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

[27] Ilyen forrás érhető el pl. a https://www.exploit-db.com/ oldalon.
[28] A Microsoft a kockázatokat kritikus, fontos, közepes és alacsony súlyossági skála alapján sorolja be.
[29] 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.
[30] https://www.first.org/cvss/

emellett számos különféle határvédelmi rendszerbe és sebezhetőségi vizsgálatokat végző szoftverbe is beépítésre került, mely 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:

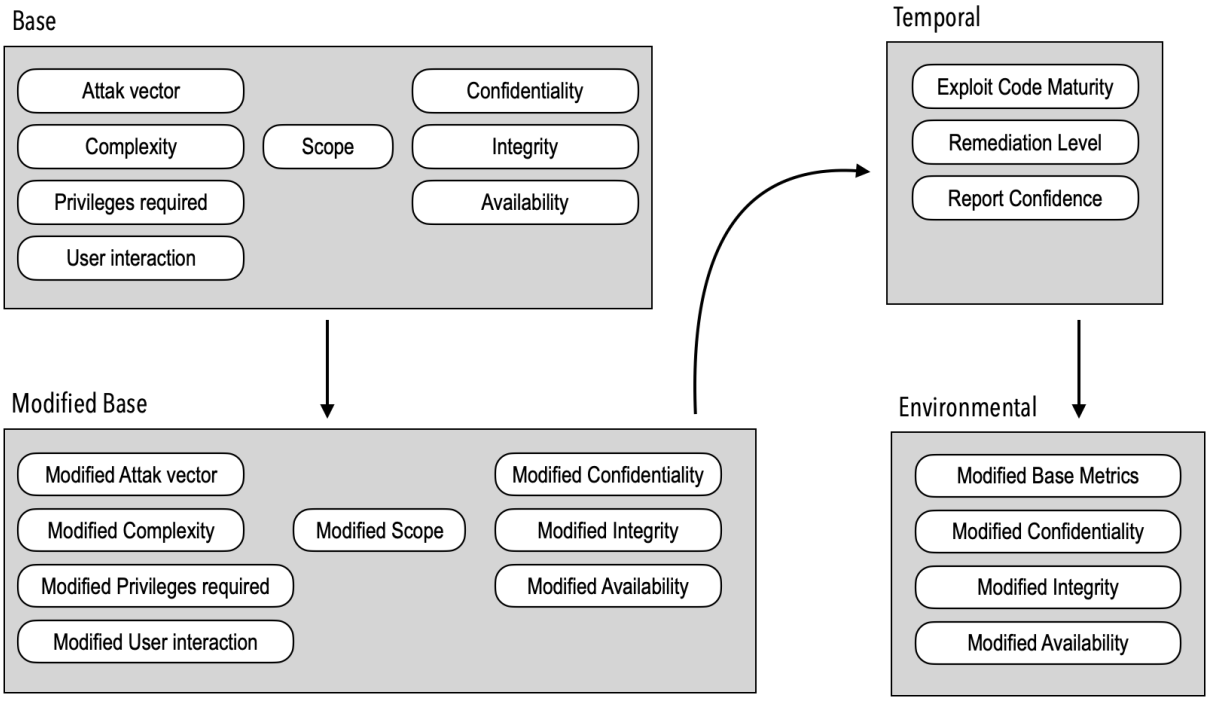
- Az új sérülékenységekre az NVD adatbázisban 2019. szeptember 10-én kezdték meg a 3.1-es változat szerinti értékelést, ekkor indult a korábbi rekordok visszamenőleges újraértékelése is.
- Murray 2020-as vizsgálatában kimutatta, hogy 2019-ben az NVD adatbázisának csak 18%-a tartalmazott CVSS 3.1-es értékelést, 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 [46].

A CVSS elsődleges célja a sérülékenység által jelentett potenciális veszély számszerű[31] kifejezése. 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.
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,

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

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.



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

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.

A base metrikacsoportot négy, időben állandó komponensegyütteséből alkotott érték határozza meg. Kiszámításukkor és az általuk jelentett kockázat kiértékelésekor a metodika elvárja annak feltételezését, hogy a támadó ismeri a megtámadni kívánt rendszer belső felépítését, és annak működéséről a számára szükséges adatokkal rendelkezik. Ennek értelmében a kihasználhatóságot lehetővé tevő körülmények meghatározása során fel kell tételezni, 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 [47]. 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 pontozás minősége javítható.

3.7.1. A CVSS pontszám meghatározása

Az *attack vector (AV)* mérőszáma a támadó és a sérülékeny rendszer között megkövetelt távolságot írja le. A magasabb mérőszám egyúttal feltételezi a támadók nagyobb számát is. Ennek alapján az AV értékei az alábbiak lehetnek:

N(etwork): amennyiben a sérülékenység kihasználása a célpont nagy kiterjedésű hálózati kapcsolatán, tipikusan egy meglevő internetkapcsolaton keresztül hajtható végre. Az ilyen besorolású sérülékenységek okozta fenyegetettségek magas értékét a *Zerodium*[32] *Bounty* programjának értékelése is alátámasztja: a legnagyobb értékű kifizetéseket a cég az ún. zero click sérülékenységekért kínálja [48].

A(djacent): ha a sérülékenység kihasználása továbbra is valamilyen hálózati kapcsolaton keresztül valósítható meg, ugyanakkor annak területi kiterjedése korlátozott. Tipikus példái a Bluetooth vagy WiFi

[32] 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.

kapcsolatokat megkövetelő sebezhetőségek, esetükben a személyes jelenlét nélkül a támadás nem kivitelezhető.

L(ocal): amennyiben a sebezhetőség vagy helyi jelenlétet, vagy valamilyen más felhasználó hozzáférésének megszerzése után elért sikeres helyi bejelentkezést igényel. Ezt kell alkalmazni minden olyan sérülékenység esetén, amelyek egy informatikai berendezés konzoljához való személyes hozzáférést, távoli bejelentkezést, vagy az adathalász levelek malware mellékletein alapuló kártékony kód indítását igénylik.

P(hysical): amennyiben a támadónak a sérülékenységhez fizikai hozzáférésre van szüksége. Jellemző példái egy rendszert tartalmazó háttértár kiszerelése és egy más rendszerben, a védelmi rendszer 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[33]. Tereshkin tanulmányában rámutatott, hogy a fizikai hozzáférés abban az esetben is lehet eredményes, ha egy számítógép merevlemeze teljes egészében erős titkosítással van ellátva, így az ilyen típusú támadások a megfelelő környezeti feltételek mellett sikeresek lehetnek [49].

Az *attack vector* meghatározása nem minden esetben egyértelmű, és esetenként 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 [46].

Az *Attack Complexity (AC)* mérőszáma a sérülékenység kihasználásának gyakorlati lehetőségét írja le. Értéke high vagy low lehet és a korábbiak szellemében meghatározásakor feltételezni kell, hogy a megtámadni kívánt rendszer konfigurációja lehetővé teszi a támadás lebonyolítását.

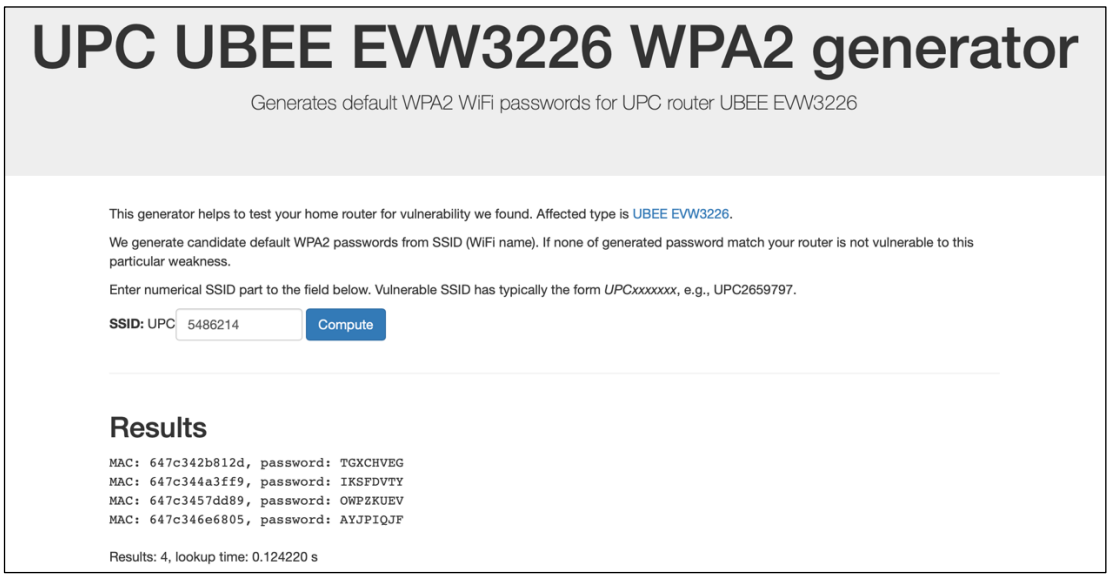
[33] Ez a támadás a hotelszobákban felügyelet nélkül hagyott számítógépek manipulálásával, fizikai elemeinek kompromittált változatra történő cseréjével megvalósított metodikák. A szakszolgálatok az ilyen típusú támadások elkerülésére javasolják a kisméretű, állandóan személyes felügyelet alatt tartható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

H(igh): ha a sérülékenység kihasználásához a környezeti feltételek eleve rendelkezésre állnak, vagy azt nem befolyásolják megkövetelt feltételek vagy körülmények, így az újra és újra sikeresen végrehajtható.

L(ow): amennyiben a sikeres támadás a célrendszer környezeti feltételeinek függvénye, melyet a támadás előtt ki kell alakítani. Tipikus példák a *man in the middle* típusú támadások, melyeknek környezeti előkészítő szerepük van a támadás következő lépcsőjének lebonyolításában [50].

A sérülékenységeknek csak kisebb csoportja képes kifejteni a hatását úgy, hogy a célrendszerben semmilyen előzetes jogosultsággal nem rendelkezik. A többlépcsős támadások első lépését a már ismertetett környezeti előkészítés során megszerzett különféle szintű jogosultságok jelentik. Egy sebezhetőség besorolásakor a *Privileges Required (PR)* az adott sérülékenységen alapuló támadás működőképességéhez szükséges jogosultságot írja le. Képzése a korábbiakkal ellentétesen történik, a magas értéket az alacsony hozzáférési igényű sérülékenységekhez kell rendelni.

H(igh): ha a sebezhetőség kihasználásának nem előfeltétele a rendszer elemeihez vagy konfigurációjához való hozzáférés. Magyar példaként a UPC internetszolgáltató egyes végberendezéseinek nevezetes sérülékenysége szolgálhat, mely során a hozzáférési jelszavakat az altaluk használt SSID-iből generálták, így egy meghatározott eszközhöz tartozó jelszó legfeljebb egy 16 lépéses eljárással képezhető.



3. ábra. Egy UPC router alapértelmezett jelszavának feltörése.
Forrás: https://ubee.deadcode.me.

L(ow): amennyiben a sérülékenység kihasználásának feltétele legalább egy korlátozott hozzáférés birtoklása. Gyakori példa erre egy adatbázis teljeskörű hozzáférését nyújtó hiba kihasználása, melyet csak a rendszerbe bejelentkezni képes felhasználó tud kihasználni.

N(one): ha a sérülékenység kihasználásának előfeltétele a rendszer teljeskörű hozzáférési jogosultságának birtoklása. Egy adott számítógép rendszergazdai szintű kompromittálásának következménye lehet például egy jelszó ismerete nélküli bejelentkezési képesség egy olyan másik gépre, mely a már feltört gépet megbízható kapcsolati forrásnak tekinti. Hasonlóképpen, egy rendszer teljeskörű hozzáférése az első lépcső lehet az abban tárolt titkosított, vagy más, másodlagos úton védett adatforrások megszerzéséhez[34].

A *User Interaction (UI)* azt mutatja meg, hogy egy sérülékenység kihasználásához szükséges-e egy másik személy közreműködésére. Értékei:

R(equired): ha a sérülékenység sikeres kihasználásának elengedhetetlen előfeltétele egy, a rendszerhez valamilyen szintű hozzáféréssel rendelkező felhasználó művelete. Az adathalász levelek, azok a malware-t tartalmazó mellékletei tipikusan megkívánják egy a megtévesztett felhasználó együttműködését, valamint ez a követelmény áll fen minden *social engineering* támadás esetében.

N(one): abban az esetben, ha a sérülékenység alkalmazhatósága nem kíván meg személyes közreműködést.

A *scope* metrika azt mutatja meg, hogy egy adott sérülékenység hatása kiterjedhet-e olyan területre is, mely eredetileg nem tartozott annak hatókörébe. Egyetlen logikai értéket vehet fel, melynek meghatározásában szerepet játszik a sérülékenység műszaki háttere is. A CVSS dokumentációjában nem találtam kapcsolatot a hatókör értékének módosító hatására a környezeti metrikák kiszámításakor, de szerepét adott körülmények közt egyértelműnek tartom. Lehetséges értékei:

[34] Az adatbázis-kiszolgálók rendszerint saját jogosultsági rendszerrel rendelkeznek, mely az operációs rendszer teljes kontrollja mellett hozzáférhető egy támadó számára.

C(hanged): amennyiben a sérülékenység következtében az érintett komponens hatókörén túlnyúló erőforrás is érintetté válik. Ilyen eset lehet pl. egy alkalmazás sérülékenysége következtében megszerzett adminisztrátori jogkör, mely az eredeti, szűkebb körön túllépve, a rendszer teljes egésze felett biztosít kontrollt a behatoló számára.

U(nchanged): amennyiben a sérülékenység sikeres kihasználása sem teszi lehetővé, hogy a támadó a sebezhető komponens hatóköréből kilépjen.

A hatás mérőszámait az adott sérülékenység kihasználásakor elszenvedett lehetséges következmények alapján képezik.

Confidentiality (C): a bizalmasság sérülése következtében fellépő hatás nagysága, amennyiben a sérülékenység hatással lehet az érintett rendszerben tárolt adatok megismerhetőségére. Értékei:

H(igh): amennyiben a tárolt adatok bizalmassága teljes mértékben sérül, például egy adatbázisrendszer tetszőleges részén tárolt adatok a támadó számára kiolvashatók.

L(ow): amennyiben az adatok bizalmassága csak részlegesen sérül, például lehetőség nyílik ugyan a rendszerben tárolt adatok közvetlen lekérdezésére, de azok egyébként más forrásból is elérhető nyilvános adatok.

N(one): amennyiben az érintett rendszerben tárolt adatok bizalmassága nem sérül.

Integrity: a rendszer egészére, vagy az abban tárolt adatok sértetlenségére gyakorolt hatás. Míg a bizalmasság sérülése esetén csak az adatokhoz való illetéktelen hozzáférés jelenti az incidens kritikus pontját, a sértetlenségi kritérium meggyengülésének következménye annak megbízhatatlansága lesz. Értékei:

H(igh): amennyiben a sérülékenység kihasználása során a támadó képes az érintett adattartalmat meghatározó elemek, így fájlok, adatstruktúrák, programok tartalmának módosítására, például egy korlátlan hozzáférést biztosító felhasználói account megszerzésével.

L(ow): amennyiben az adatok integritása csak részlegesen sérül, például csak egy másik, hasonlóan korlátozott jogosultsági körrel rendelkező biztosító felhasználói fiók megszerzése válik lehetővé.

N(one): amennyiben az érintett rendszerben tárolt adatok integritása a sérülékenység kihasználás során sem sérül.

Az *Availability (A):* a rendszer rendelkezésre állására kifejtett hatás, melynek eredménye a rendszer funkcióinak vagy szolgáltatásainak részleges vagy teljes leállása. Értékkészlete azonos a bizalmasság és a sértetlenség esetében már megismerttel:

H(igh): amennyiben a sérülékenységet kihasználó támadás vagy azok ismételt sorozata következtében, akár azt követően is fennáll a szolgáltatási képesség kiesése. Közismert példái a DDOS támadások.

L(ow): amennyiben a támadás vagy azok sorozata nem képes a szolgáltatás teljeskörű vagy tartós megszakítására, de annak rövidebb kiesését vagy lassulását okozhatja.

N(one): amennyiben az érintett rendszer rendelkezésre állása nem, vagy nem érzékelhető mértékben sérül.

Mivel a base metrikacsoport értékét nyolc, egymástól független érték határozza meg, ezért annak tömör leírására a napi gyakorlatban a már említett vectorstringet alkalmazzák, mely 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 vectorstring egyes elemcsoportjait a / karakter választja el. Az első pozíción a CVSS verziószáma helyezkedik el, amit a base metrikacsoport egyes elemeinek rövidített neve, majd egy kettőspont elválasztó karakter után az adott metrika értéke követ. Az általános formában az egyes metrikák értékkészletének elemeit a | karakterrel választottam el.

A base score kiszámításához a metrika besorolásonként egy-egy számértéket definiál, melyet az alábbi táblázat ír le[35]:

Metrika	Elem	Pont
Attack Vector (AV)	Network	0,85
	Adjacent	0,62
	Local	0,55
	Physical	0,2
Complexity (AC)	Low	0,77
	High	0,44

[35] Common Vulnerability Scoring System version 3.1: Specification Document. CVSS Version 3.1 Release. FIRST, 2019. https://www.first.org/cvss/specification-document. Letöltve: 2023.01.10.

Metrika	Elem	Pont
Privilege required (PR)	None	0,85
	Low	0,62 / 0,68 (S)
	High	0,17 / 0,5 (S)
User interaction (UI)	None	0,85
	Required	0,62
Confidentiality impact, (CI) Integrity impact (II), Availability impact (AI)	High	0,56
	Low	0,22
	None	0

13. táblázat. A CVSS egyes metrikaelemeihez tartozó pontértékek.
Forrás: Common Vulnerability Scoring System version 3.1: Specification Document.

3.7.2. Módosított alapmetrikák

Nem állítható, hogy a base metrika pontozása 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. A módosított metrika képzésekor a módosított megnevezések egy „M” (modified) előtagot kapnak, és a kiszámításhoz használt értékek az új besorolás szerintiek szerint alkalmazandók.

3.7.3. A környezeti hatás mérőszámai

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 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 által jelentett gyengeség 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.

Amennyiben rendelkezésre állnak környezeti mérőszámok, úgy a base csoport értékei helyett azokat lehet alkalmazni. Értékei:

Not defined: ha nem áll rendelkezésre információ az érték meghatározásához.

H(igh): amennyiben a rendszerben tárolt adatok bizalmassága, sértetlensége vagy rendelkezésre állása teljes mértékben sérül, és annak katasztrofális hatása van a szervezet működésére nézve.

L(ow): ha a rendszerben tárolt adatok bizalmassága, sértetlensége vagy rendelkezésre állása nagy mértékben sérül, és annak súlyos hatása van a szervezet működésére nézve.

N(one): amennyiben a rendszerben tárolt adatok bizalmassága, sértetlensége vagy rendelkezésre állása csak kis mértékben sérül, és annak nincs jelentős hatása a szervezet működésére.

Egy sebezhetőség végső pontértékének kiszámításához elsőként az *Impact Base Score* értékét kell meghatározni, melyet az alábbi kifejezés ír le:

$$ISC_{Base} = 1 - ((1 - Impact_{Conf})) \cdot (1 - Impact_{Integ}) \cdot (1 - Impact_{Avail}))$$

Az *ImpactSubscore* értéke az alábbi algoritmus alapján számítandó ki:

$$ISS = (\ Scope\ Changed\ )\ ?$$
$$7{,}52 \cdot (ISC_{Base} - 0{,}029) - 3{,}25 \cdot (ISC_{Base} - 0{,}02)^{15}\ :$$
$$6{,}42 \cdot ISC_{Base}$$

E két érték alapján az alábbi algoritmus alapján határozható meg a *Base Score* értéke:

```
Base Score =
  if ImpactSubScore <= 0:
     0
  else:
     if Scope changed:
        RoundUp (Minimum (1.08 × (Impact + Exploitability), 10))
     else:
        RoundUp (Minimum ((Impact + Exploitability), 10))
```

melyben a *RoundUp()* kiszámítása az alábbi formula alapján történik:

$$RoundUp(x) = (\ x\ \cdot 10 == int\ (\ x\ \cdot\ 10\ )\ ?\ x : int(x + 0{,}1)$$

A fentiek alapján az **AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H** vectorstring által leírt sérülékenység Base Score értéke egy tizedesjegyre kerekítve 9,8:

$$Exploitability\ = 8.22 \cdot 0{,}85 \cdot 0{,}77 \cdot 0{,}85 \cdot 0{,}85 = 3{,}88$$
$$Impact = (1 - (1 - 0{,}56) \cdot (1 - 0{,}56) \cdot (1 - 0{,}56)) \cdot 6{,}42 = 5{,}87$$
$$Base\ Score = 3{,}88 + 5{,}87 = 9{,}75$$

Végül, a CVSS összesített pontszáma alapján az adott sérülékenységet az alábbi táblázat alapján sorolja be az öt lehetséges szint egyikébe:

Súlyosság	CVSS pontszám
Nincs (None)	0
Alacsony (Low)	[0,1-3,9]
Közepes (Medium)	[4,0-6,9]
Magas (High)	[7,0-8,9]
Kritikus (Critical)	[9,0 - 10,00]

14. táblázat. A CVSS pontértékek besorolása.
Forrás: Common Vulnerability Scoring System version 3.1: Specification Document.

3.8.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, vagy hogy a sérülékenység milyen régóta áll fenn, vagy hogy az adott környezetben egyáltalán kihasználható-e.

A CVSS-szel szembeni másik kritika az alkalmazott formulákon alapul. Bozorgi és társai [51, 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."[36] 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 [52]. 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 [53]. Tipikus típusai a már említett IDS vagy a felismert minták alapján a hálózati forgalom szabályozására is képes IPS rendszerek [54]. A kockázat mértékét a gyakorlatban ezt a sérülékenységvizsgálati szoftverekbe épített Exploit Prediction Scoring System (EPSS) algoritmus teszi lehetővé [55], 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[37]. 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.

[36] 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.

[37] A kiszámítás módját a FIRST a https://www.first.org/epss/model oldalon publikálta.

- Biztonsági szkennerszoftverek riportjait,[38] 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[39] származó, az egyes sérülékenységek kihasználáshoz szükséges kész kódok alkalmazhatóságát.
- Biztonsági cégek napi jelentéseit a sérülékenységek megjelenéséről, valamint aktivitásuk változásáról.

Bár konkrét szakirodalmi hivatkozást még nem találtam, a mesterséges intelligencia elmúlt időszakban történt ugrásszerű fejlődése eredményeképp az minden bizonnyal az EPSS rendszerek komponensei közt is megjelenik.

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 várhatóan 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.

3.9. Egy egyetemi rendszer sérülékenységvizsgálatának elemzése

[38] Ilyen szoftver pl. a Sn1per vagy a Nuclei.
[39] A legismertebb változatok a Metasploit vagy az ExploitDB.

Személyes szakmai tapasztalataim alapján feltételezem, hogy az egyetemi informatikai rendszerek üzemeltetői a nagy informatikai központok elemeit magasabb prioritással kezelik, így azok menedzsment feladatait magasabb időkeretben és prioritással végzik el. Ebből következően a perifériális elemek védelmének fenntartására tett lépések alacsonyabb intenzitásúak, így az ott tárolt adatokkal kapcsolatos közvetett kockázat magasabb, mint a központi infrastruktúra esetén. Ennek tudományos értékű bizonyítását a H.3-ban fogalmaztam meg: **a felsőoktatási informatikai rendszerek központi és kihelyezett telephelyein működő elemeinek a publikus internet irányából mért sérülékenységi szintje a perifériális telephelyek esetében magasabb és jelentős mennyiségű, jelentős mennyiségű, 2020 előtt ismertté vált sebezhetőséget tartalmaznak**. H.4-et szintén üzemeltetési tapasztalataim alapján állítottam fel, melynek lényegét a számos esetben tapasztalt hibás konfigurációs beállítások következtében sérülékennyé vált rendszerek támadhatósága, vagy annak elősegítése jelenti. Eszerint **a felsőoktatási információs rendszerek jelentős mennyiségű, hibás konfigurációs beállításból eredő technikai információ elemzését teszik lehetővé, melyek egy potenciális támadó számára segítséget nyújthatnak egy támadás megtervezéséhez és sikeres végrehajtásához.**

Mindkét hipotézis igazolását valós körülmények közt működő egyetemi informatikai rendszer elemzésével kívánom bizonyítani, melynek alapfeltétele releváns adatok tervszerű gyűjtése, valamint a hipotézisek igazolásához szükséges csoportosítás kialakítása. H.3. első részének alapjául az egyes campusok publikus internet irányából mérhető sérülékenységeinek felderítése és azonosítása szolgál, míg a belső hálózati elemek sérülékenységeinek feltérképezése olyan mérési eljárás kidolgozását igényli, mely lehetőség szerint minél több interfész elérését teszi lehetővé. H.4. bizonyítását ezért a belső hálózat adatai alapján végeztem el, míg H.3. esetében a belső és külső mérőberendezéssel gyűjtött adatokra külön-külön végzek vizsgálatot.

A szükséges adatok megszerzését vulnerability scanner szoftverre alapozva terveztem, s mivel ezeknek számos különböző megvalósítása létezik, végül a Nessus, a Nexpose és az OpenVas alkalmazások valamelyikének alkalmazását mérlegeltem.

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 fenntartott és fejlesztett adatbázisok következtében a szoftver ára meglehetősen magas. Kipróbálható változata teljes funkcionalitással csak 7 napon át, maximum 16 IP címre működik.

A Nexpose a Nessushoz nagyon hasonló termék, hasonló funkciókkal, Metasploit és Jira mellett hozzávetőleg 50 további szoftver integrációjának lehetőségével[40]. Bár fő funkcióiban, a mérési adatok összegyűjtésében alig különbözik a Nessustól, néhány különbség felfedezhető, melyek közül az egyik legfontosabb a CVSS kihasználhatósági pontszámok közlése. Ez a virtuális gépként is letölthető szkenner is több adatforrás alapján működik: a kipróbálható változat egy hónapon át nyújt teljes szolgáltatási kört 500 IP címre.

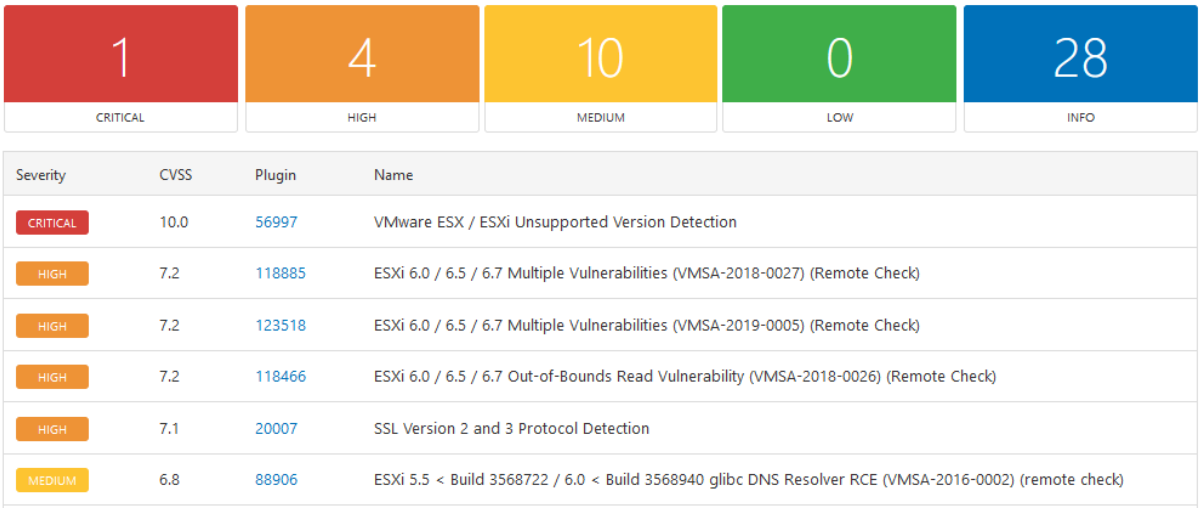
Az Open Vulnerability Assessment System (OpenVAS) egy nyílt forrású szoftver, melyet 2002 óta fejlesztenek. Elsősorban rendszerüzemeltetőknek szánják, így beállítása és működtetése, felügyelete nagyobb szakértelmet kíván. Ez a keretrendszer is elsősorban a sebezhetőségek felderítését célozza, és bár szintén nagy sérülékenységi adatbázissal rendelkezik, de annak mérete elmarad a Nessusétól [56, pp. 52-58]. Mivel ingyenes szoftver, hosszú távon is működtethető szemben a kereskedelmi szoftverekkel, melyek alapára is meglehetősen magas, s a kiegészítő modulok licenszeivel az többszörösére is emelkedhet.

A sebezhetőségi vizsgálatok első szakaszát a KIFÜ által üzemeltetett és 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 a KIFÜ szervere számára csak a határvédelmi rendszerek által engedélyezett forgalmi kapcsolatok voltak hozzáférhetők, az abban szereplő eredmények csak a publikus internet irányából érkező támadások elemzése során tekinthetők relevánsnak, melyek kielégítik a H.3. első részének bizonyításához szükséges adathalmaz követelményeit. A Nessus alkalmazásával adataim egy legális licensszel rendelkező, korlátozás nélküli, frissítések rendszeres letöltésére képes szkennerből származtak.

A Nessus riportjai előre meghatározott IP tartományok elemeinek egyszeri vizsgálata alapján készültek, mely során a szkenner IP cím szerint listázta a vizsgált hostokat. A szoftver elvégzte

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

a megtalált sérülékenységek Critical, High, Medium, Low és Info osztályokba történő besorolását, és minden egyedi IP 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 vizsgált egyetem több campus-on működik, ezek mindegyikében található informatikai eszközpark. 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. Az egyetem működését biztosító fő infrastruktúra itt helyezkedik el, tehát az intézmény adatvagyonának jelentős része itt található. Kutatásomban a „C” campus alkotja a központi informatikai helyszínt. 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 összeköttetéssel érik el. Ezeken a helyszíneken egy-egy informatikus látja el helyi támogatási feladatokat. E két campus szerepe a kiszolgáló informatikai infrastruktúra értelmében perifériális.

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 csak 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 14. táblázat szerinti, a First által ajánlott értékhatárokat. 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 [57].
- 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 helytelennek tartom. 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.

A mért adatok alapján készítettem el azt a táblázatot, mely campusokra és a módosított besorolás szerinti osztályokra bontva tartalmazza a sérülékenységek számát, valamint a CVSS 3.0 pontszámaikat:

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	6
High	118,8	16	155,7	21	0	0	29,4	4
Medium	875,2	163	1249,5	231	0	0	110,7	20

Low	83,2	32	148,2	57	0	0	0	0
Info	0	2327	0	2819	0	63	0	171

15. 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 túlnyomórészt 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 közel 30%-kal magasabb volt a tesztelhető gépek száma, ennek megfelelően a hibák száma minden kategóriában határozottan növekedett: kettővel a magas kockázatú hibák mennyisége, mely mellett a magas, közepes és alacsony kockázatúakon túl 21%-kal magasabb számú, Info besorolású hiba volt kimutatható. Ez azonban alig utal a sérülékenységi szint általános növekedésére: a pontszámok és darabszámok hányadosával képzett arányszámok a két campus esetében elhanyagolható eltérést mutattak.

H.3. 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 a felsőoktatási intézmények átszervezése során új, önálló egyetemként folytatja a működését. Tekintettel arra, hogy a „C" campus 8 hónappal később, kontrollként indított második mérése nem mutatott releváns különbséget, ez 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 magasabb. 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

16. 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 nem kellő mennyiségű adat hiányában nem adható.

Az R értékét vizsgálva 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 megállapítható, hogy a **H.3. első részhipotézise nem igazolható. A központi és kihelyezett telephelyen működő elemek a publikus internet irányából mért sérülékenységi szintje megközelítőleg azonos, azok közt releváns különbség nem mutatható ki.**

3.10. Belső rendszervizsgálat

A kutatás első fázisában a sérülékenységek vizsgálata külső forrásból történt, mely számára csak azok a szolgáltatási területek voltak láthatók, melyeket a határvédelmi rendszerek lehetővé tettek. Mivel a Verizon jelentésében 25%-ra teszi az oktatási intézmények belső támadóinak arányát [25], a hatékony védelem szempontjából lényeges a rendszer belső kitettségének vizsgálata is. Egy ilyen mérés lebonyolítása egy már működő infrastruktúra esetén bonyolult műszaki problémát jelent, mivel biztosítani kell a szkenner hozzáférést a hálózat minden vizsgálandó eleméhez, így annak kommunikációját nem akadályozhatják tűzfalak vagy VLAN szeparációk. Ezen adatsor alapján végeztem el H.3. második részhipotézisének (a továbbiakban H.3-2.) igazolását, mely állítása szerint az intézmény belső számítógépei **jelentős mennyiségű, 2020 előtt ismertté vált sebezhetőséget tartalmaznak.** A hipotézis felállításakor figyelembe vettem a nagy számú, hálózatba kötött számítástechnikai eszközt, menedzsmentjüket ellátó kislétszámú személyzetet, valamint a rendelkezésre álló anyagi erőforrások szűkösségét. A hipotézis igazolása során részletesebb kép alakítható ki az egyes szakterületek állapotáról és további összefüggések feltárására is sor kerül.

A mérési adatok elemzését szakterületi felbontásban kívántam elvégezni, ezért nem csak a publikus internet irányába nyitott rendszerelemeket kezeltem külön, hanem a belső, szegmentált hálózatok elemeit is. Ehhez a korábbi mérési eszközrendszer csak abban az esetben lett volna alkalmazható, ha a határvédelmi eszközök konfigurációinak módosításával az első fázisban alkalmazott szkenner képes lenne belső hálózati elemekkel történő kommunikációra. Az elérésükhöz szükséges útvonalak kialakításához módosítani kellett volna az egyetemi tűzfalak konfigurációit, mely a gyakorlati megvalósítás során szinte biztosan hálózati üzemzavarokat okozott volna. Ezt nem kívántam felvállalni, mint ahogyan egy harmadik fél számára egy esetleges hozzáférést biztosító, az intézmény belső hálózati sérülékenységeinek detektálására képes eszköz elhelyezését sem. Így egy új, a belső tűzfalrendszer mögött már létező alkalmas pontra egy új szkenner gépet telepítettem. A konfiguráció így teljes egészében az intézmény saját felügyelete alatt állt, megfelelt a vizsgálat kritériumainak, és a már említett Nexpose limitációkat 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 a kutatásom jelen fázisában szerepük nem releváns. Az eredeti VLAN-okhoz a felosztás alapján hozzárendeltem a szakterületeket melyeket a Nexpose adatbázisának bővítésével, a lekérdezések végrehajtásának érdekében 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 működése során keletkező adatok tárolása és közzététele. Ez a terület más magyar tudományegyetemekkel összevetve a vizsgált adatkörben kifejezetten kevés 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 működnek olyan eszközök, amellyel a kollégiumok hálózati kijárata mögötti infrastruktúra látható lett volna. Tekintettel arra, hogy a kollégiumok munkaállomásai nem egyetemi tulajdonúak és azok konfigurációira az egyetemi IT üzemeltetésnek minimális hatása van, ezen hálózatok elemeivel kapcsolatban semmiféle bizalmi szabályt nem érvényesítünk. Az egyetem számára jelenleg nem áll rendelkezésre olyan hálózati infrastruktúra, mellyel a kollégiumok gépei is vizsgálhatók lettek volna, így a kollégiumok 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[41].

H.3. bizonyításához Nexpose egy hónapig 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 tartották bekapcsolva, így az említett korlát a számítógépek más-más halmazára érvényesült. Munkaidőben a dolgozók gépei 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.

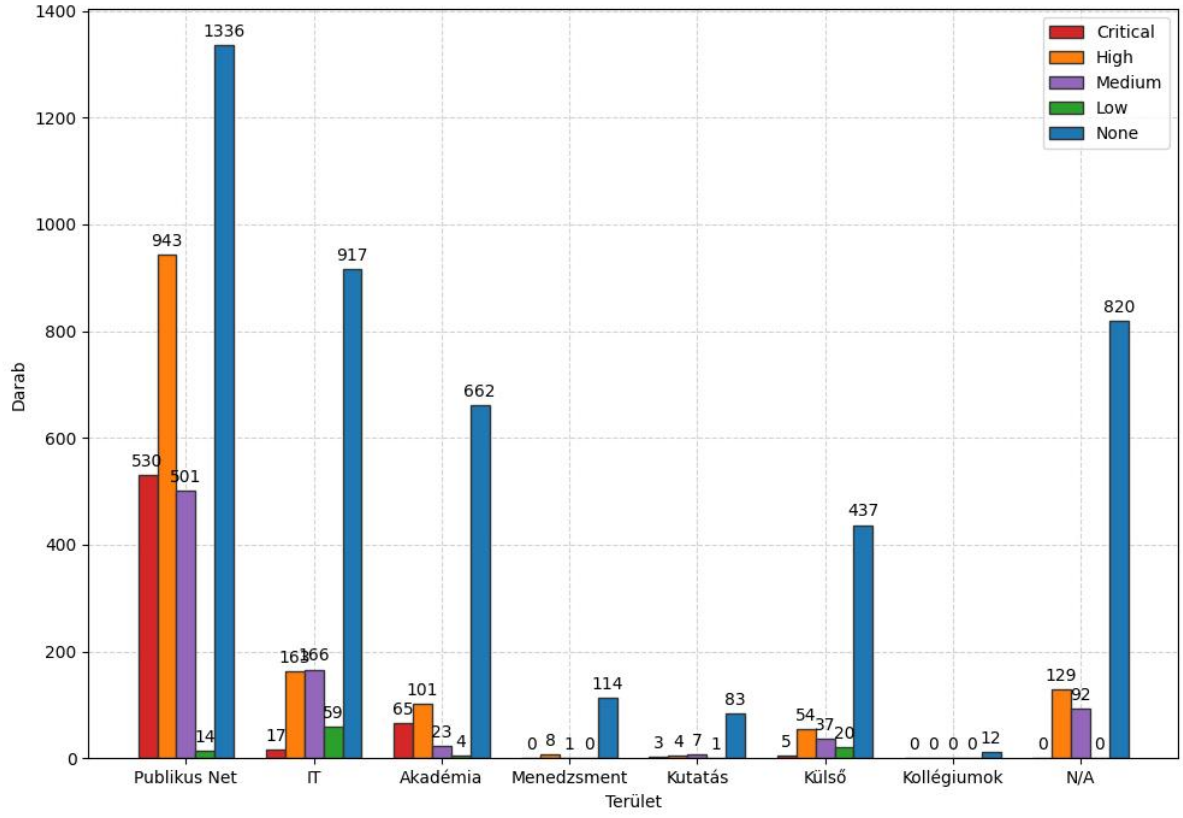
A Nexpose az adatait két különböző adatbázisban is képes rögzíteni. Egy viszonylag egyszerű felépítésű MySQL adatbázist alkalmaz az áttekintő adatok tárolására, és egy PostgreSQL alatt

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

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 hálózatan 745 hoston 38,2%-kal több, 7.382 volt detektálható. Bár a két szoftver eltérő adatbázissal rendelkezik, kétségtelen, 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%-os érték.

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 emelkedtek. Az alacsony kockázatú sebezhetőségek számát viszont kevéssel alacsonyabbnak mértem, melynek oka a belső és külső mérés közt eltelt idő lehetett. A legmagasabb értéket mutató None (melyet a Nessus Infoként azonosít) viszont 2.327-ról 1.336-ra csökkent.



5. ábra. A sebezhetőségek száma és súlyossága szakterületi felosztásban.

Forrás: saját szerkesztés

A diagram alapján elvégezhető H.4. hipotézis igazolása. Az Info 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 vagy 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).

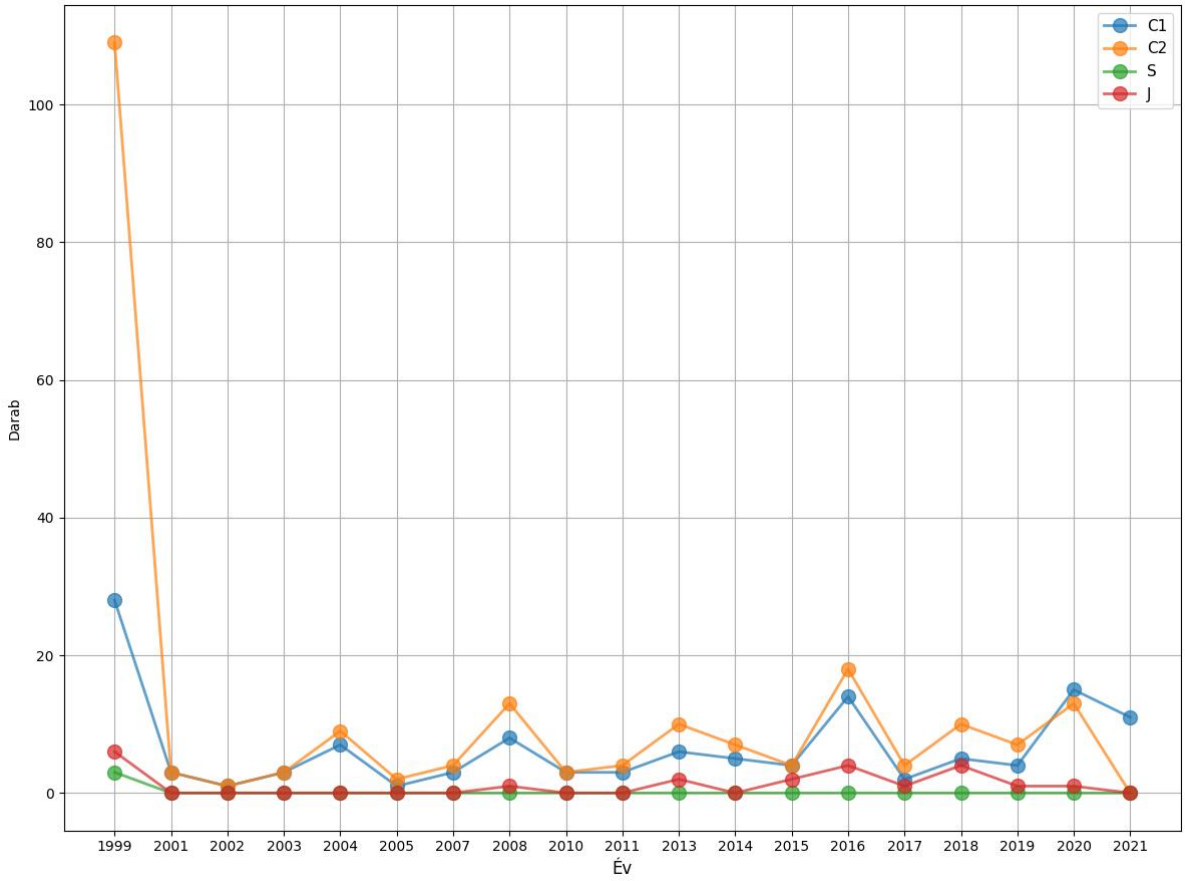
	Hostok száma	**Rekordok száma**	**Info típus darabszáma**	**Info típus aránya**	**Kh/n**
„C” campus a publikus internet felől	102	2559	2327	0,91	22,81
„C” campus belső hálózatból	745	7382	4381	0,59	5,88
„J” Campus a publikus internet felől	13	203	171	0,84	12,15
„S” Campus a publikus internet felől	7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

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

A mért adatok alapján megállapítható, hogy a konfigurációs hibák aránya a rendszer elemeinek számával növekszik, és ezek jelentős részét a helyesen konfigurált határvédelmi eszközök a publikus internet irányából eltakarják. A konfigurációs hibák mennyisége nagy számú szolgáltatás esetén meghaladják a kisebb központok, tipikusan a perifériális campusokban mért értéket. Figyelemre méltó ugyanakkor a 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 **H.4. a vizsgált felsőoktatási intézmény esetében bizonyításra került, tehát a felsőoktatási információs rendszerek jelentős mennyiségű, hibás konfigurációs beállításból eredő technikai információ elemzését teszik lehetővé, melyek egy potenciális támadó számára segítséget nyújthatnak egy támadás megtervezéséhez és sikeres végrehajtásához.** Tekintettel arra, hogy ezek az intézmények közel azonos feladatkört közel azonos feltételek mellett látnak el, H.4. indukció alkalmazásával történő kiterjesztése további felsőoktatási intézményekre is elvégezhető, konkrét vizsgálatokat viszont célszerű az intézmények saját informatikai szervezeti egységeinek kidolgozni és végrehajtani.

A belső hálózatot leíró adatok ismeretében igazolható H.3. második állítása, melyre a sérülékenységek korának ismeretében adható válasz. Ennek alapjául a CVE adatbázis nevezéktana szolgált, az egyes sérülékenységek azonosítói tartalmazzák regisztrációjuk évszámát, melynek ismeretében a már felépített adatbázisból könnyen kinyerhető az adott sérülékenység korának meghatározásához szükséges évszám. Természetesen a konfigurációs hibák CVE azonosító hiányában nem köthetők évhez, így a hipotézis vizsgálatában ezek nem vesznek részt. Az alábbi diagram az internet irányából elérhető sérülékenységeket csoportosítja regisztrációjuk éve szerint. 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.



6. ábra. A publikus forrásból elérhető sérülékenységek kor szerinti eloszlása a CVE nevezéktana alapján. Forrás: saját szerkesztés.

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 típust írt le. A képet tovább árnyalja, hogy 130 esetben (34,6%) fordult elő az 1999-es évben 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 [58, 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 azonosítanám, beállításával egy támadó képes lehet egy SNMP szerver által menedzselt

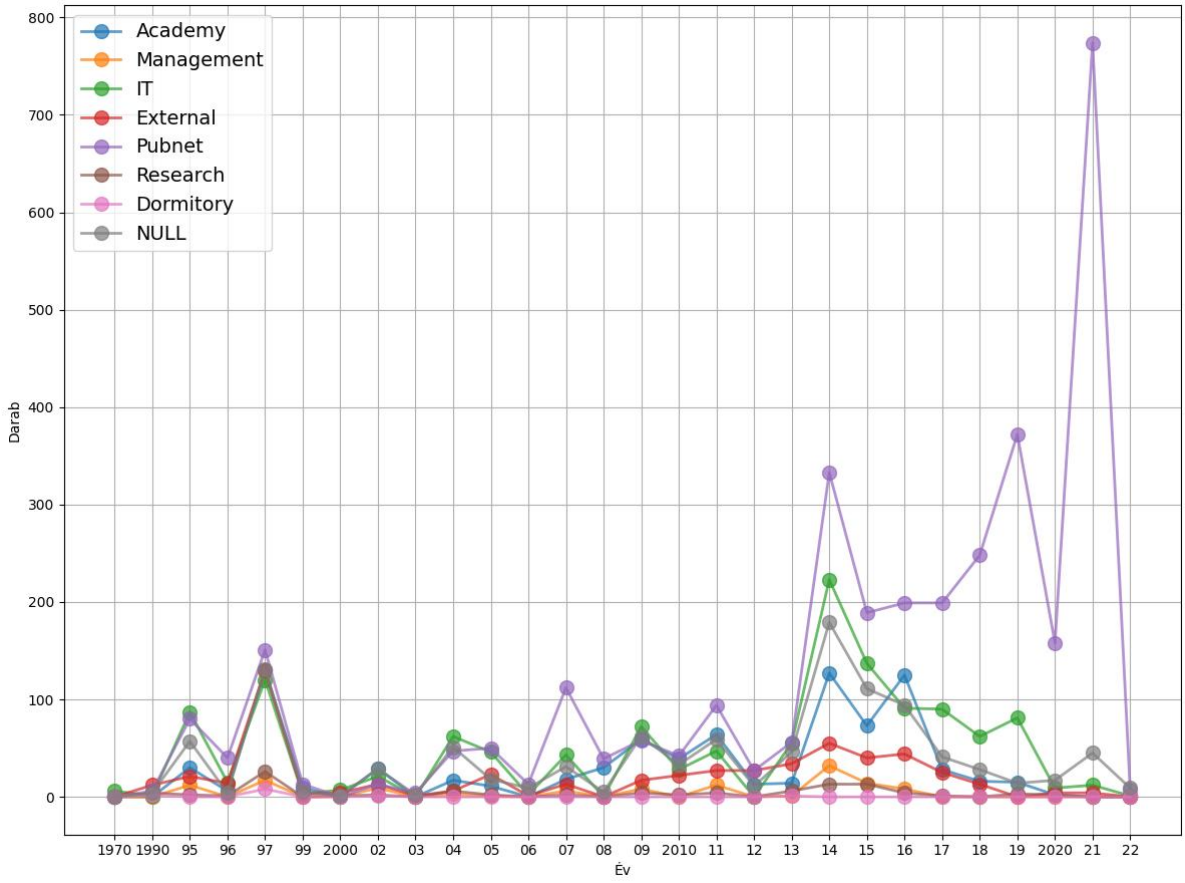
eszközbe bejelentkezni, annak konfigurációjához hozzáférni, adott körülmények közt akár módosítani is. A további, rendkívül régi hibák elavult webszervereket, titkosítási protokollokat vagy azok gyenge algoritmusait, különféle szerver szolgáltatások SSL hibáit írják le, de már ezekben az években ismert 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 jelzések 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. Az érintett egyértelműen ismét a publikus internetszolgáltatások és az IT, valamint a szolgáltatásokat igénybe vevő akadémiai szféra berendezései voltak. Az érintett rendszerek ekkor is Linux (512), MS Windows (115), VMWare ESXi (85) és a már említett Canon nyomtatók (68) mellett a Cisco operációs rendszerei (35).

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



7. ábra. A belső hálózatban detektálható sérülékenységek szakterület kor szerinti eloszlása a CVE nevezéktana alapján. Forrás: saját szerkesztés.

A legmagasabb pontszámot elért gép egymaga 463 különböző sérülékenységet tartalmazott, melyből 123-hoz exploit is elérhető, 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, és a feltöréséhez rendelkezésre álló 59 exploittal foglalta el a legsérülékenyebb informatikai eszközök listájának második helyét.

H.3-2. igazolása az alábbi összefoglaló táblázat alapján végezhető el. Ez tartalmazza a „C1” campus mérésének összesítését a 2020-as évet megelőző és az azt követő bontásban. A hipotézis igazolására az évszámok összevethetősége érdekében a belső hálózati mérés

konfigurációs hibák nélküli részhalmazát használtam azért, mert a külső mérésben csak ezek esetében volt évszám hozzárendelhető.

	Mérés					
	Belső, teljes	%	Belső, nem Info	%	Külső, nem Info	%
2020 előtt	6.338	83,5%	1.962	47,0%	335	88,1%
2020-től	1.044	16,5%	1.039	53,0%	40	11,9%
Összesen	7.382	100,0%	3.001	100,0%	375	100,0%

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

A táblázat adatai alapján H.3-2. mindkét mérési sorozat alapján igazolható. Az első, publikus internet irányából mért nem Info típusú sérülékenységek száma 375 volt. Ebből 11 darab 2021-ben, és 29 darab 2020-ban regisztrált sebezhetőség volt. A fennmaradó 335 sérülékenység CVE azonosítója 2020 előtti regisztrációról tanúskodik, melyek aránya így 88,1%.

Ugyanezt az értékelést a belső hálózatból indított mérési adatokra is elvégeztem, itt a nem Info típusú sebezhetőségek száma, 3.001, melyből 1.039 regisztrációs dátuma 2020 vagy későbbi. A fennmaradó 1.962 sérülékenység 2020-at megelőző évben került be a CVE adatbázisába, eszerint a hibák 47%-a 2020 előtti, mellyel **igazoltam H.3-2-t, mely szerint (az egyetemi hálózatok) jelentős mennyiségű, 2020 előtt ismertté vált sebezhetőséget tartalmaznak.**

Amennyiben a mérést a teljes belső hálózatra, és évszámként a szkenner adatbázisába való bekerülés évét tekintem alapul, H.3-2. szintén igazolható, ekkor a 2020 év előtti sérülékenységek, és nyilvántartásba vett konfigurációs hibák aránya 83,5%.

3.11. 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 sebezhetőségeit leírására képes metrika alkalmazása jelentős támogatást nyújt az informatikai üzemeltetés szereplői számára. Megfelelő 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 mérés 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 EKE IDS-sel kapcsolatos mérési eredményeit, hasznosíthatósági korlátait és tapasztalatait, majd H.3. és H.4. 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 az egri Eszterházy Egyetem sérülékenységvizsgálatának 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 H.3-1 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 egyetemet jellemző szakterületi beosztást annak érdekében, hogy különbözőségeik megállapíthatók legyenek, és bemutattam azt a műszaki hátteret, mely alapján 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* két évvel, 2020 előtt is ismertek voltak. Kimutattam, hogy az informatikai rendszer egyes elemei 2021-ben még mindig tartalmaznak olyan hibákat, melyek már 2009-ben is ismertek voltak. Végül szakterületenként megvizsgáltam a sérülékenységek számának kiugrásait, és a konkrét sérülékenységek megvizsgálásával magyarázatot adtam ezekre.

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 egy lépés tehető a shadow informatika felszámolása felé.

4. Jelszóhash-ek védelmi képességének tesztelése és nyilvánosságra került jelszavak mennyiségi vizsgálata publikus adatforrásban

A jelszavak napjainkban is a legelterjedtebb hitelesítési módszernek számítanak, annak ellenére, hogy a tudományos kutatás, és az ipari szereplők is azt jósolták, hogy a jelszavas hitelesítést felváltják és elavulttá teszik. [59] [60] A jelszavakhoz kapcsolódó biztonsági problémakör minden szervezet esetében kiemelt területet jelent, melyek jelentős részét a szakirodalom a felhasználói információbiztonság-tudatosság szintjéhez köti. A jelszavak használhatóságával kapcsolatban számos tanulmány fogalmazott meg kritikákat, és személyes tapasztalataim is alátámasztják a jelszavakkal kapcsolatos policy kijátszásának jelenlétét az informatikai rendszerekben, ugyanakkor más azonosítási módszerek alkalmazása nehézkes, a személyazonosság biometrikus[42] igazolása pedig csak indokolt esetben alkalmazható [61]. A felsőoktatás speciális működési környezete, mely a foganatosítható védelmi tevékenységekre is kihatással van, több területen is megjelenik:

- Az oktatói- és kutatói kör ellenáll az informatikai eszközök korlátozásainak, mely esetenként valóban korlátozza kutatói és oktatói szabadságukat.
- Az oktatók és kutatók érdekellentétben állnak a működtetésért felelős személyzettel.
- A felsővezetői támogatás inkább az akadémiai munkavállalói kör felé tolódik, és a konfliktusok elkerülésének érdekében inkább a gyengébb de kényelmes megoldásokat preferálják.
- A közvetlen jogszabályi követelmények hiánya.

Ezek egyenként is komoly gyengítő hatást jelentenek az informatikai védelemben, de együttes hatásuk ellen az IT osztályok gyakran úgy védekeznek, hogy az akadémiai szféra számítógépeit alig különböztetik meg a publikus elérésű gépektől. Bár a jelszavakhoz kötődő támadási metodikák sikeres kivitelezésének lehetősége leginkább az azt birtokló felhasználók magatartásához kötődik, az üzemeltetést végzők is számos ponton javíthatják a kapcsolódó biztonsági eljárásokat.

[42] 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”

E hipotézisem megfogalmazásakor is elsősorban a saját munka- és vezetői tapasztalatom során szerzett feltételezésekből indultam ki. Eszerint a felsőoktatásban dolgozók jelszókezelésével kapcsolatos problémák, a komplex jelszavak alkalmazásával szembeni ellenállás, az összetettséget biztosító feltételek megkerülésének kísérletei különféle súlyosságú incidensekhez vezethetnek, amelyek egy része az informatikai üzemeltetés számára is érzékelhető, így elindítják az incidenskezelési folyamatot. Bár a felhasználók nemkívánatos cselekményei csak részlegesen előzhetők meg (elég a ransomware mellékletre kattintó munkatársakra gondolni), a jelszókezelés folyamatába beépített technikai kontrollok jelentősen csökkentik az ehhez kötődő kockázatokat. A szabályok betartásának műszaki úton történő kikényszerítése viszonylag egyszerű feladat, így a jelszavak komplexitásának betartatása vagy a rendszeres időközökre előírt jelszócsere viszonylag könnyen kikényszeríthető[43]. Technikai úton viszont nem akadályozható meg az e-mail címek vagy jelszavak újbóli, akár magáncélra történő felhasználása sem, így összességében az informatikai üzemeltetés nem rendelkezik teljes kontrollal a jelszavak védelmének területén.

A nem kellően védett jelszavak kiszivárgásáról szóló események a híradásokból is közismertek; az adatsértésekkel kapcsolatos számszerű adatokat többek közt a *Have I Been Pwned* (HIBP) [62] site biztosít. Ez az adatforrás a legnagyobb adatsértések során nyilvánossá vált adatok leírása mellett 2023. januárjában egy közel 12,5 milliárd rekordot tartalmazó adatforrásra alapozva nyújtja szolgáltatásait, és a rekordok száma viszonylag rövid idő alatt is szignifikáns növekedést mutat.

A fentiek alapján egyrészt feltételezhető, hogy a felsőoktatási rendszerekben dolgozók e-mail címeihez tartozó jelszavak komplexitása nem kielégítő, azok kiszivárgása esetén a megfelelő technikai megoldásokra alapozva egy részük „feltörhető". Feltételeztem továbbá, hogy az egyetem hozzáférésekhez tartozó jelszavak kisebb-nagyobb arányban publikus adatforrásban, pl. a már említett HIPB-on is fellelhetők. Bár a felsőoktatásban dolgozókkal kapcsolatban feltételezhető, hogy a napi szintű számítógép használatból, valamint a saját szakterületen szerzett magas szakmai képzettségből egyúttal egy magasabb szintű információbiztonsági-tudatosság is következik, sajnos ez a gyakorlati tapasztalataim alapján ez nem általános. Ezért a jelszavakkal kapcsolatosan kettős hipotézist fogalmaztam meg, melyet ezért két lépésben bizonyítok.

[43] A felhasználók leleményességével érdemes számolni, előfordult, hogy egy olyan rendszerben, amely nem tette lehetővé az utolsó 10 jelszó használatát, a követelményt egy felhasználó egymást követő 11 jelszócserével játszotta ki.

H6. A felsőoktatás saját rendszereiben működő e-mail címek jelszavai egy brute force előkép-meghatározási eljárással szemben csak részlegesen védettek, melynek eredményességét az alkalmazott hashképzési eljárás erősségével szemben a támadó előkép meghatározási stratégiája határozza meg. A felsőoktatási rendszerek e-mail címeinek védelme során kockázatot jelent a különböző internetes jelszógyűjteményekben hozzájuk társított jelszavak mennyisége.

A hipotézis vizsgálatát két részben végzem el. Egyrészt igazolom, hogy mind az SHA-1, mind az NTLM algoritmusok alkalmazása esetén az előképek ismeretében a jelszóvédelem megkerülhető, és bizonyítom, hogy erős algoritmusokkal titkosított jelszavak feltörése a megfelelő szoftver eszközök birtokában egyszerű módszerekkel is lehetséges. A vizsgált jelszó lenyomatok az Eszterházy Károly Egyetem központi címtárában található, működő környezetben használt jelszavakból képzettek, így kutatásomban valós környezetben alkalmazott jelszavak elemzését végzem el. Kifejezetten nem célzom a felhasználói információbiztonság-tudatosság mérését vagy vizsgálatát, mivel ezzel kapcsolatban már bőséges szakirodalom és tudományos mű született, ehelyett kifejezetten a felsőoktatást vizsgáló, az abban fennálló jelenlegi helyzet adatokkal alátámasztott leírására, a különböző formában tárolt jelszavak visszafejtésének sikerességére, valamint intézményi e-mail címek és valamely rendszerben hozzájuk rendelt jelszavak publikus adatbázisban történő feltalálhatóságának vizsgálatára törekszem.

4.1.Titkosítási eljárások

A titkosítási eljárásoknak számos csoportja létezik, a jelszavakkal kapcsolatban azonban három alapvető típust érdemes vizsgálni [63]. Titkosított üzenetek továbbításának ideális módszere a nyilvános kulcsú titkosítással végzett kulcscsere után alkalmazott szimmetrikus kódolás, a sértetlenség ellenőrzésére (de nem kizárólag arra) a lenyomatképzési algoritmusok általánosak. A szimmetrikus kulcsú titkosítás alkalmazása esetén a titkosításra és a visszafejtésre használt kulcs azonos, mely egyaránt üzenetek kódolására és dekódolására. Több nagyszerű ilyen algoritmus ismert, tipikus példái a rendkívül összetett 3DES vagy az AES. Ezek különféle algoritmusok útján előállított kulcsok matematikai képletekben történő alkalmazásával, több iteráció során képzett helyettesítésekkel végzik el az elküldeni kívánt üzenet titkosított formájának kialakítását úgy, hogy ismereteink szerint annak dekódolására a kulcs ismerete nélkül a mai informatikai eszközökre alapozva nincs realitása. A szimmetrikus titkosítási eljárások nagy előnye a sebesség, a legtöbb algoritmus teljesítménye elegendő ahhoz, hogy

nagymennyiségű adat titkosítását rövid idő alatt lehessen elvégezni. A folyamat leginkább kockázatos elemét a kulcs továbbítása jelenti, mivel ez a szimmetrikus titkosítás önálló alkalmazása mellett bizalmi alapon, nyílt adatként kerül továbbításra a kommunikációban résztvevő felek közt. Ez a pont jelentett végzetes hibát a Második Világháborúban az Enigma haditengerészet által használt M3-as típus védelmében, az U-110-es tengeralattjáró elfogása során megszerzett titkosító gép és a beállításait előíró dokumentumok közel 9 hónapon át tették lehetővé a német haditengerészet üzeneteinek visszafejtését [64].

A nyilvános kulcsú titkosítási algoritmusok (PKC – Public Key Cryptography) eltérő módon működnek. Jelenleg a Rivest-Shamir-Adleman (RSA) a legnépszerűbb, mely titkosításra és digitális aláírásra egyaránt alkalmazható. Az Elliptic Curve Digital Signature Algorithm (ECDSA) népszerűségét többek közt annak köszönheti, hogy kisebb kulcshossz mellett éri el az RSA algoritmusának teljesítményét. A kifejezetten digitális aláírásra alkalmazható Digital Signature Algorithm (DSA) a NIST DSS aláírási szabványát valósítja meg.

A PKC kriptográfiai eljárásainak alapját egy kulcspár képezi, amelyet nyílt eljárással, rendszerint nagy prímszámok felhasználásával lehet generálni. A kulcspár egyik elemét a generálója nyilvánossá teszi (ez a public key), a másikat pedig titkos kulcsként (private key) definiálja, és törekszik arra, hogy megakadályozza harmadik fél általi megismerését. A kulcspár működésének lényege, hogy a kulcspár tetszőleges felével titkosított üzenet csak annak párjával dekódolható, így magával a kódolást végző eredetivel sem. A gyakorlatban ezért egy üzenetet kódolását ezért a vevő nyilvános kulcsával végzik, kihasználva, hogy annak dekódolását kizárólag a címzett által birtokolt másik, titkos fél ismeretében lehet elvégezni. Az eljárás fordított alkalmazása során a digitális aláírás valósul meg. Ekkor egy aláíró saját privát kulcsával titkosítja üzenetét, melyet a publikusan elérhető nyilvános kulcsa ismeretében bárki képes visszafejteni. A sikeres dekódolás egyúttal a dokumentum eredetiségét bizonyítja.

Ezek az algoritmusok nem érintettek a kulcstovábbítás problémájában, mert az eljárás soha nem kívánja meg a privát kulcs másik fél számára történő átadását. Ezért ezek az kriptográfiai eljárások azokban az esetekben is képesek a bizalmasság és a sértetlenség biztosítására, mely során egy harmadik fél a kommunikációban részvevők teljes forgalmát lehallgatja. A gyakorlati alkalmazásuk során azonban két ponton hátrányt szenvednek. Az RSA alkalmazása során, két fél első kommunikációjakor képzendő ujjlenyomat előállításakor elvi lehetőség van egy *man in the middle* típusú támadás eredményes megvalósítására, ezért a kapcsolat kezdeményezőjének meg kell győződnie arról, hogy valóban a célrendszerrel kommunikál. Technikai támogatás hiányában ennek felelősségét az algoritmus a felhasználóra hárítja, ami végfelhasználók esetében nem várható el. A gyakorlati alkalmazás másik korlátozó tényezője

a magas számítási teljesítmény igényük, ennek következtében hosszú kommunikációs folyamatok, vagy nagy mennyiségű adathalmazok titkosítására nem szokás ezeket az algoritmusokat önállóan alkalmazni.

A sebesség problémájára a nyilvános kulcsú és a szimmetrikus titkosítás együttes alkalmazása ad választ. Számos esetben, többek közt az SSH[44] működésében is PKC-t alkalmaznak a kapcsolat felépítésére, melyet csak a szimmetrikus kulcs biztonságos cseréjére alkalmaznak. Ez biztonságosan megoldja a kulcs továbbításának problémáját, így a kapcsolatot a továbbiakban a gyors, és kis erőforrást igénylő szimmetrikus kulcsú titkosítással folytatják [65]. A kulcscserére irányuló kutatások számos kriptográfiai algoritmust elemeznek, és hasonlítanak össze, valamint újabb és újabb eljárások alkalmazására tesznek javaslatot. [66]

4.2.Lenyomatképzési eljárások

A titkosítási eljárások mellett a kutatásom szempontjából kiemelt algoritmusokat az ún. lenyomat (hash) képző eljárások jelentik. Algoritmusaik nem reverzibilis függvényeket valósítanak meg, működésük során csupán egy tetszőleges hosszúságú adatsorból, az ún. előképből, egy egyirányú folyamat végrehajtásával egy, az eljárásra jellemző hosszúságú kimenetet, az ún. lenyomatot állítanak elő [67]. Az egyirányúság garantálja, hogy a kimenetként kapott lenyomatból az eredeti előkép matematikai úton nem állítható elő. Az algoritmusokkal előállított lenyomat nem az eredeti adatsor titkosított formája, abból az eredeti adat nem állítható vissza, csupán sértetlenségének ellenőrzését teszi lehetővé. Az, hogy a hashképzés tradicionális értelemben nem tekinthető titkosítási eljárásnak, a dekódolhatóság hiányából következik.

Gyakorlati alkalmazásuk során azt használják ki, hogy egy lenyomatképző algoritmus azonos előképből mindig azonos hash-t generál, így ideális különféle adatsorok sértetlenségének megállapítására vagy jelszavak olvasható formában történő tárolásának elkerülésére. A sértetlenség megállapításakor alkalmazott eljárásban az előkép lenyomatát egy alternatív kapcsolaton keresztül juttatják el a fogadó fél számára, aki azt újra kiszámítva összehasonlítja a feladó által küldött értékkel. Amennyiben a lenyomatképzést egy jelszó helyességének meghatározására alkalmazzák, a felhasználó által megadott jelszóból újra generálják a lenyomatot, és azt összehasonlítják a korábban már megadott és tárolttal. Mivel egy ideális hash algoritmus esetén erősen érvényesül az ún. lavinahatás, mely fennállása esetén a forrás

[44] Az SSH jelentése Secure Shell, amely egy számítógépes protokoll és az azt használó program neve is. Erős titkosítást használva számos funkciót valósít meg: lehetővé teszi távoli számítógépekbe történő bejelentkezést, fájlok másolását, és titkosított alagutak kialakítását is.

egyetlen bitjének megváltozása a lenyomat gyökeres megváltozásával jár, így a sértetlenség egyszerűen könnyen megállapítható.

A módszert a legtöbb informatikai rendszer kettős céllal alkalmazza. Egyrészt lehetőséget nyújtanak arra, hogy a jelszavak ne legyenek hozzáférhetők az informatikai rendszerek üzemeltetői számára. Másrészt számos adatszivárgás ismert, mely során érzékeny adatok kerültek nyilvánosságra, ezek közt több olyan is előfordult, melyben különféle formában tárolt jelszavak kerültek ismeretlenek birtokába. Ezért az informatikai rendszerekben szigorú biztonsági követelmény, hogy jelszóállományai csak lenyomatokat tároljanak, és semmiképp ne tárolják azokat olvasható (cleartext) formában. A jelszavak ilyen formájú titkosításának szükségességét az is bizonyítja, hogy a világ legnagyobb informatikai cégeinek rendszereit is érték már olyan kibertámadások, mely során nagy tömegű személyes adat szivárgott ki tőlük [68] [69] [70] [71]. Egyes esetekben ezek titkosítatlan, így olvasható jelszavakat tartalmaztak, másokban csak lenyomatok kerültek illetéktelen kezekbe, melyeket támadóik spamküldő szolgáltatóknak kínáltak fel, vagy a darkneten értékesítettek[45].

Gyakran alkalmazott hashképzési eljárások az 1993-ban publikált Secure Hash Algorithm (SHA) különböző erősségűre hangolt változatai, melynek első változatát 1993-ban publikálták, és több családban (SHA-1, SHA-2, SHA-3) fejlesztették tovább. Az algoritmus ereje paraméterezésével szabályozható, tipikusak az SHA-224, SHA-256, SHA-384 és SHA-512 variánsok, melyekben a számok az eljárás során használt kulcsok hosszára utalnak. [72, p. 38] Kriptográfiai szempontból a hash algoritmusoknak komoly szerepük van, a jelszóellenőrzés mellett gyakran alkalmazzák fájlok sértetlenségének ellenőrzésére. Több kriptovaluta, pl. a Bitcoin működése is a hashképzésen alapul, utóbbi esetében a bányászat folyamata adott tulajdonságú, pl. 8 darab 0-val kezdődő SHA-256-os hash-ek megtalálását célozza [73, p. 42]. Mivel azok a metodikák, melyek egy hash ismeretében képesek lehetnek egy előkép előállítására, komoly gazdasági hasznot jelenthetnek, ezért a támadásban érdekelt felek jelentős erőfeszítéseket tesznek azok megtalálására.

4.3.A jelszótárolás műszaki háttere

Az első Unix rendszerek a felhasználói jelszavakat titkosítás nélkül, közvetlenül olvasható formában tárolták, és a védelmet a jelszófájl olvashatóságának megakadályozásában látták.

[45] A haveibeenpwned.com oldalon megvizsgálható, hogy egy adott e-mail cím érintett volt-e valamilyen incidensben, amit a rendszer jelenleg 10.1 Mrd. hozzáférést tartalmazó adatbázisa alapján vizsgál. Az oldal az adatszivárgásokról is közöl információkat, ezekben olyan, kifejezetten népszerű, nagy cégek is szerepelnek, mint az Adobe vagy a Dropbox.

Annak ellenére, hogy a jelszavak ilyen rögzítési formájában rejlő kockázatokra Robert Morris és Ken Thompson már 1979-es cikkükben felhívták a figyelmet arra, hogy számos olyan incidenst ismerünk, melyeket a jelszavak olvasható formájú hozzáférése tett súlyossá, mivel annak nyilvánosságra kerülése tömeges hozzáférési eljárást biztosít egy esetleges támadó számára. [74] A hozzáférések megszerzése nem feltétlenül egy működő rendszer kompromittálása során valósulhat meg, az abból készített adatmentések nem kielégítő védelme, riportok helytelen kezelése, vagy kapcsolódó rendszerek sérülékenységei is eredményezhetik azt. Ennek elkerülésére az eredeti jelszavak helyett gyakran azok valamelyik hash eljárással képzett formáját rögzítik, biztosítva, hogy az általuk előállított lenyomatokból matematikai úton az eljárás algoritmusának ismeretében sem legyen képezhető az eredeti bemeneti adat. A hash eljárások azért különösen alkalmasak jelszóvédelmi eljárások alkalmazására, mert a titkosítási eljárásban alkalmazott kulcs maga a jelszó, így nincs szükség egyéb kulcsok előállítására és védelmére, emellett az eljárás garantálja a jelszavak alkalmazhatóságát egy másik gépre történő átvitel után is.

Az alkalmazott hash algoritmusok azonban nem örökéletűek, a számítógépes hardver fejlesztések jelentette teljesítménynövekedés következtében a valamikor jól teljesítők is elavulnak és könnyedén feltörhetővé válnak, de tervezési vagy implementációs hibák következtében is cserélendővé válhatnak. Morris és Thompson a Unix jelszavainak védelméről szóló cikkükben a 60-as éveket említik a probléma kiindulópontjaként, és több, ma is alkalmazott megoldást javasoltak:

- A Unix harmadik kiadása vezette be a crypt() függvényt, melyet jelszavakból képzett hash-ek előállítására használtak. így a belépés engedélyezése a megadott jelszó és a rendszerben korábban, a felhasználóhoz rögzített hash egyezőségének feltétele. A kezdetben használt egyszerű algoritmusokat először a DES, majd annak többszöri alkalmazása váltotta fel. 1994-ben vezették be az MD5-öt, amit az SHA-1 követett. A mai, *de facto* szabvány az SHA-2 család, amely többek között konfigurálható lassúsági tényezővel rendelkezik és akár a futtató hardver teljesítményéhez is hangolható.
- Az ún. salt bevezetése, mely a szivárványtáblák alkalmazását lehetetleníti el. Utóbbi lényege a gyakran használt, vagy szisztematikusan képzett jelszavak és hash-einek felsorolásával felépített táblázat, mely az eredeti jelszó előállítását egy lineáris keresésre vezeti vissza. A salt mechanizmus lényege a jelszó kiegészítése egy véletlenszerű karaktersorozattal, mely így a szivárványtáblák működéséhez szükséges elemek számát kezelhetetlen méretűre növeli. [75]

- A kódolt jelszavak olvashatóságának megakadályozása a SUN nevéhez kötődik, a Unix rendszereken az 1980-as évek közepén vezették be a kódolt jelszavakhoz történő hozzáférését megakadályozó shadow fájt. Az ún. Shadow Suite csomagot a Linux rendszerek a 90-es évek óta alkalmazzák.

A kibertámadások egyik legfontosabb motivációja személyes és gazdasági, valamint hozzáférési adatok megszerzése. Ezek védelmének egyik módszere a titkosított tárolás, különös tekintettel a hozzáférési jelszavakra, melyek a már említett lenyomat helyett olvasható formában történő rögzítése a ma már durva szakmai hibát jelent. A GDPR – bár konkrét előírásokat nem foganatosít a jelszavakkal kapcsolatban – komoly szankciókat helyez kilátásba személyes adatok tömeges kiszivárgása esetén, ezért a legtöbb szervezet elemi érdeke, hogy a rendszereiben ne legyenek jelen olvasható jelszavak. Konkrét titkosítási eljárást egyik jogszabály sem fogalmaz meg, így a fejlesztőn múlik az alkalmazott módszer kiválasztása és implementálása.

4.4.A titkosítási eljárások gyengeségei

A számítástechnikai eszközök fejlődése során számos, korábban széleskörben használt kriptográfiai algoritmus bizonyult gyengének. Az eljárások cseréjére alapjában véve két, egymástól eltérő okból lehet szükség, egyrészt a használt algoritmusok elvi hibája, vagy valamilyen implementációs hiba miatt. Az utóbbi oka a legtöbb esteben valamilyen programozási hiba, amely az egyébként tökéletes matematikai alapokon működő algoritmust is sebezhetővé teszi. Tipikus forrásai voltak a hibás véletlenszám-generátorok, amelyek valójában nem véletlenszámokat generáltak, ezért a helyes működést garantáló megjósolhatatlan bemeneti adatok helyett reprodukálható vagy ismétlődő bemenetet nyújtottak. Ilyen implementációs hibát produkálhat kulcsfontosságú adatok memóriában hagyása az programkód lefutása után, vagy annak elérhetősége más alkalmazások számára. Az Enigma esetében implementációs hibának tekinthető a kiválasztott rotorok típusára, azok sorrendjére és azok kezdeti beállításaira vonatkozó megkötés, amely drasztikusan lecsökkentette a kulcstér méretét. Az implementációs hibák jellemzője, hogy azok csak egy-egy operációs rendszer, vagy eszköz esetén állnak fenn, míg más, azonos kriptográfiai eljárást alkalmazókban nem.

Egyes titkosítási eljárások feltörésére számos ismert eljárás létezik, melyek egy része csak elméletben működőképes, míg mások a gyakorlati alkalmazásuk során bizonyították működőképességüket.

A Side-channel Attack során nem magát a kriptográfiai eljárást támadják, hanem azt előállító rendszer fizikai vagy működési jellemzőin keresztül elérhető másodlagos információkat elemzik. Ennek során a támadók figyelik a rendszer energiafogyasztását, elektromágneses sugárzását vagy különféle időzítési információkat, és az ebből levont következtetések alapján szűkítik a kulcstér méretét. Yarom és Berger 2014-es kutatásukban bizonyították, hogy eljárásuk egyetlen aláírási folyamat kifürkészése után egy asztali számítógépen 1 másodpercnél rövidebb idő alatt volt képes feltörni az ECDSA titkosítást, mely során az X86 architektúrájú számítógépek sérülékenységét használtak ki, mely „lehetővé teszi a folyamatok számára, hogy monitorozzák más folyamatok olvasási és végrehajtási hozzáférését a megosztott memória lapjainak hozzáféréshez.” [76, p. 2].

A Side-channel Attack-hoz hasonló az idő alapú támadás módszere, mely során a támadó azt használja ki, hogy a kriptográfiai műveletek végrehajtási ideje az abban résztvevő kriptográfiai kulcstól függ, így az idő ismeretében következtetni lehet magára a kulcsra is. Endrődi és Csorba már 2014-ben demonstrálta a módszert, mely során egy 512 bites RSA kulcsot 300 ezer megfigyelés után percek alatt, míg egy 128 bites RSA kulcsot 10 ezer megfigyelés után másodpercek alatt fejtettek meg [77].

Egy nehezen kivitelezhető, de több algoritmus kivezetését eredményező eljárás a collision attack (ütközéskeresés). Ez abból az egyszerű tényből indul ki, hogy az egyes hashképzési eljárások kimenetének hossza az alkalmazott algoritmus függvényében azonos, melyből következően egy érvényes lenyomathoz elméletben nem egy, hanem végtelen sok előkép tartozik. Ez a tény minden lenyomatképző algoritmust nagyban gyengít, mert végtelen sok helyes előképből kell megtalálni egyet, így a szükséges kereséséi iterációk száma nagyban csökkenthető. Így, amennyiben kidolgozható egy olyan gyakorlati eljárás, amely elfogadható időn belül képes az eredetitől eltérő, alternatív előkép előállítására, az a lenyomatképző eljárás feltörését jelenti.

Az md5, whirpool és az SHA[1-3] variánsok érzékenységét Pittalia írta le, és bár megállapítása szerint az md5 és a whirpool érintettsége a gyakorlati megvalósításban egyértelműen bizonyított, az SHA-1 csak elméleti megfontolások alapján lehet ezzel támadható. Pittalia kizárja az SHA-2 és SHA3 collision attack-kel szembeni érzékenységét. [78]

Az ütközések ténye az md5 esetében a 128 bites eljárást valójában 64 bitre, az 160 bites SHA-1-et pedig 80 bitre gyengíti. „...az MD5 teljes ütközését 2004-ben publikálta egy akadémikusokból álló team. Egy IBM P690-es számítógépen kevesebb mint egy óra alatt találták meg az ütközéseit, ami bizonyította, hogy az MD5 elavult, és a világ minden eszközében annak elkerülésére, hogy az ütközéses támadások ne terjedjenek el, ki kell azt

vezetni” [79]. Hasonló megfontolásokból Chris Celi, a NIST informatikusa így ír az SHA-1-ről: „Azt javasoljuk, hogy mindenki, aki az SHA-1-re támaszkodik a biztonság érdekében, a lehető leghamarabb térjen át az SHA-2 vagy SHA-3 protokollcsaládra” [80]. Bár a NIST a kivezetés dátumát 2030-ban határozta meg, a legelterjedtebb böngészők esetében már 2017-ben megszüntették a támogatását [57] [81].

Az algoritmus kivezetésének folyamata egyszerű azokban a rendszerekben, melyek élő támogatással rendelkeznek, és ismeri azok felhasználóit, mert így a fejlesztés elvégezhető, és a módosított kriptográfiai eljárást implementáló komponens eljuttatható a célhelyre. Sokkal nehezebben áthidalható problémát jelentenek azok a hardver elemek és szoftverek, melyek már nem támogatottak vagy melyek üzemeltetői nem értesíthetők, vagy nem végzik el a frissítést. Külön kategóriát jelentenek azok a berendezések, melyek tervezése során olyan mértékben igyekeztek alacsonyan tartani a gyártási költségeket, hogy az eszköz nem képes nagyobb számítási igényű komponensek elfogadható sebességű futtatására, ennek tipikus példái az IOT eszközök[46].

Az algoritmusok logikai hibái sokkal komolyabb problémát jelentenek azokban az esetekben, amikor a javítás egyáltalán nem, vagy csak hosszú idő elteltével végezhető el. Egy számos rendszert érintő példa a KRACK (Key Reinstallation Attack) néven ismertté vált, a vezetéknélküli hálózati eszközök WPA2 algoritmusának hibáját kihasználó eljárás[47], amelynek publikálása egy időre gyakorlatilag szinte minden eszköz WiFi kapcsolatát aláásta, és bár a hiba javítható, annak megoldására hónapokat kellett várni [82]. Mivel a sebezhetőség magában az algoritmusban, illetve az azt leíró ajánlásokban volt, számos eszköz, az operációs rendszerétől függetlenül egyszerre vált kompromittálhatóvá. A KRACK esetében a helyzetet tovább rontotta, hogy a tulajdonosaik egy része soha nem frissíti a vezetéknélküli hálózati eszközeinek operációs rendszerét, amit tovább súlyosbít az, hogy régi eszközök esetében nem is készül már javítás. Ezekben az esetekben a sérülékenység még éveken át kihasználható lesz.

[46] Az IOT (Internet of Things) eszközök olyan kisteljesítményű informatikai eszközök, melyek jellemzően alacsony áramfogyasztás mellett képesek információ gyűjtésére és továbbítására az Interneten keresztül.

[47] A sebezhetőség lényege a következő. Egy vezeték nélküli hálózati kapcsolat kiépítése során a kliens (számítógép, mobiltelefon stb.) kapcsolódási kérelmet indít a hálózati eszköz (pl. WiFi router) felé. A kapcsolat technikailag egy többlépéses párbeszéd eredményeképp épül fel, melynek harmadik lépésében a két fél megegyezik a használt titkosítási kulcsról. Mivel a kapcsolat kialakítása során bármikor, így ebben a lépésben is történhet hálózati hiba, az eljárás képes arra, hogy ezt a titkosítási kulcsot újra küldje. A támadó ezt használja ki úgy, hogy ezeket a kulcsokat begyűjti, majd újra küldi, ezzel kényszerítve az eszközt arra, hogy a saját belső számlálóját (nounce) nullázza. Mivel az algoritmus csak abban az esetben biztonságos, ha ez a számláló nem ismétlődik, ezzel az eljárással az feltörhető.

Egy titkosított kommunikáció feltörésének egyik metodikája a kulcstér minél nagyobb mértékű redukálása, majd a lehetséges kombinációk minél rövidebb idő alatt történő végig próbálása, utóbbit a nyers erő módszerének (brute force) nevezik. A redukció általában az algoritmus működését megalapozó matematikai eljárások ismeretében végezhető el, ugyanakkor a próbálkozásokhoz szükséges idő nagysága leginkább a használt számítástechnikai eszközök számítási teljesítményén, a nyers erőn múlik.

A kriptovaluták megjelenésével számos hashképzésre optimalizált, korábban elképzelhetetlennek tűnő számítási teljesítményű céleszköz jelent meg a piacon, amely ezt a nyers erő módszerét alkalmazta. Céljuk tömeges lenyomatképzés, melyet a kriptovaluták bányászására használtak. Az Antminer S19 Pro[48] 3500W-os fogyasztás mellett 110 TerraHash/másodperc(!) sebességre képes. Ugyanakkor tömeges hashképzési feladatok megoldására a nagyobb teljesítményű VGA kártyák is jól használhatók, ezek saját processzorai (GPU – Graphical Processing Unit) az általánosan használt számítógépekénél lényegesen gyorsabbak, ezért különösen alkalmasak a brute force alkalmazására.

4.5.A kvantumszámítógép hatása az alkalmazott algoritmusokra

A titkosítási és hashképzési eljárások ereje a kvantumszámítógép fejlődésével jelentős mértékben gyengülhet, kikényszerítve egyes algoritmusok kivezetését, vagy működési paramétereinek módosítását. Napjainkra az első kvantumgépek megépítése és sikeres gyakorlati működése egy olyan, akár már néhány éven belül valósággá váló új jövőképet rajzol fel, melyben a ma használt titkosítási eljárások egy része belátható időn belül megfejthetővé válnak. A kvantumgépek megépítésével megjelent kockázat következtében a 2013. évi L. törvény 2022. évi módosításában megjelent a követelmény az abban meghatározott szervezetek informatikai rendszereinek felkészítésére a posztkvantum algoritmusok fogadására. [83]

A kvantumgépre írt alap algoritmusok egy része nem napjaink tudományos eredményei, de a fizikai gép megépítésének nehézségei miatt megelőzték korukat, ugyanakkor gyakorlati kipróbálásukra nem kerülhetett sor. Az elvárt környezet ismeretében azonban előre kidolgozhatók, és emulátorokban futtathatók voltak, így a működő gépek rendelkezésre állásakor azonnal használatba lehetett venni őket[49].

Kibervédelmi szempontból talán az egyik legfontosabb a kvantumgépre tervezett Shor-algoritmus, mely a nyilvános kulcsú titkosítás egyik, igen széles körben használt

[48] https://miners.eu/product/bitmain-antminer-s19-pro-110th-bitcoin-miner/

[49] Fejlesztési célokra a D-Wave Systems egy 2000, a 2-es verzióban 4000 qubites kvantumgép szimulátort fejlesztett ki, mely alkalmas az algoritmusok tesztelésére, de valójában eredményt elérni nem lehet vele.

algoritmusának, az RSA-nak feltörésében is alkalmazható. Működésének lényege, hogy egy egész szám prímtényezős felbontását adja meg[50] melyre többek közt azért irányultak kiemelt számelméleti kutatások, mert több titkosítási algoritmusban is alapvető szerepe van. [84] Bár a probléma első megközelítésben nem tűnik különösebben nehéznek, nagy számok esetében a feladat komoly algoritmikus kihívást jelent, ez alapozza meg a többek közt az RSA ellenállóképességét is. Az eljárás védelme érdekében az RSA Laboratories egy pénzdíjas felhívás keretében vizsgálja, hogy mekkora különböző nagyságú számok esetében sikerül a prímtényezős felbontást megtalálni, és ezzel a titkosítást feltörni, ez jelen sorok írásakor egy 250 számjegyű szám esetében volt sikeres[51].

Egy kvantumszámítógépen a Shor-algoritmus által biztosított prímfelbontási képesség minden olyan titkosítási eljárást feltöréséhez vezet, amely a védettségét a prímfaktorizációnak köszönheti. De ugyanígy veszélyeztetettek azok az eljárások, amelyek a diszkrét logaritmuson alapulnak – e probléma megoldására is készült a kvantum algoritmus. Az ezeket alkalmazó algoritmusok tehát a jövőben nem tekinthetők biztonságosnak, míg mások esetében paraméterek változtatásával (tipikusan az alkalmazott kulcshossz növelésével) a biztonság a posztkvantum korban is megtartható lehet. A felkészülést jól jellemzi, hogy a NIST már egy 2016-os jelentésben összefoglalta egy kvantumszámítógép megépítésének hatását a leggyakrabban alkalmazott algoritmusokra és abban az SHA-2 és az SHA-3 lenyomatképző eljárásokat is érintettként hivatkozza [85].

Algoritmus	Alkalmazási terület	Biztonság fenntarthatósága
AES	Titkosítás	Nagyobb kulccsal biztonságos marad.
SHA-2, SHA-3	Lenyomatképzés	Hosszabb kimenet szükséges.
RSA	Digitális aláírás, kulcs egyeztetés	Nem biztonságos.
ECDSA, ECDH	Digitális aláírás, kulcscsere	Nem biztonságos.
DSA	Digitális aláírás, kulcscsere	Nem biztonságos.

19. táblázat. Kriptográfiai algoritmusok és érintettségük. A szerző szerkesztése [85, p. 2] felhasználásával.

A kvantumszámítógépek tehát elsősorban az aszimmetrikus titkosítási protokollokat fenyegetik, így várható, hogy a támadók az ezekre épülő alkalmazásokat támadják majd. A védelem érdekében módosítani kell az X509-es tanúsítványokat, az IKEv2, a TLS, S/MIME és az SSH protokollok egyes részeit is. A széles körben elterjedt SSL és TLS protokollok mai

[50] Minden összetett szám felbontható néhány prímszám szorzatára (pl. a 15 az 5-re és a 3-ra), ez a prímtényezős felbontás. A prímszámok olyan számok, amelyek 1-en és önmagukon kívül más egész számmal nem oszthatók el maradék nélkül, és már az ókorban is bizonyított volt, hogy végtelen sok ilyen létezik.

[51] A bejelentés a https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html oldalon érhető el.

változatukban nem lesznek többé megbízhatók. Ez szinte minden ma használt böngésző-alapú alkalmazást érint majd, és komoly gazdasági hatása lesz. Az alkalmazott eljárástól függően kvantumgéppel feltörhetővé válhatnak titkosított adathordozók, hálózati kommunikációs eljárások, VPN-csatornák, és a távoli bejelentkezéseket megvalósító eljárások. A Bitcoin bányászata során is alkalmazott SHA-256 lenyomatképzési algoritmus szintén szerepel a NIST figyelmeztetésében, így az esetleges egyéb célú blokkláncok alkalmazását is újra kell gondolni. A blokklánc alkalmazása a Bitcoin kriptovaluta esetében is kritikus pont, mivel a blokklánc visszamenőleges megváltoztatásának képessége garantálja egy új lánc létrehozását, melynek következménye bizonyos feltételek fennállása mellett a Bitcoin tulajdonok elvesztése. Az RSA 2048 bites titkosításának feltörésének jelenlegi időigényét pedig egyes források 8 órára teszik [86].

Posztkvantum algoritmusokon a tradicionális gépeken alkalmazható, de a kvantumteljesítménynek is ellenálló algoritmusokat értünk (használatos még a q-algoritmus elnevezés is). A kvantumszámítógépek fejlesztésének újabb és újabb sikerét jelentő mérföldkövek igen értékessé teszik ezeket az algoritmusokat, melyek kidolgozása két fő módszer mentén történik. Az egyszerűbb eljárás a kiterjesztés, amely a jelenlegi algoritmusokat teszi biztonságossá, amennyiben az lehetséges – a megoldások lényege legtöbbször a korábbi eljárások kulcsméreteinek növelése. Ennek következtében a lehetséges permutációk száma oly mértékben növekszik meg, hogy feldolgozása egy kvantumgép számára is megoldhatatlan feladatot jelentsen. Ez az eljárás sikeresen alkalmazható az AES esetében, de alkalmatlan pl. az RSA vagy a DSA javítására. Ezért ezeket a jövőben más eljárásokkal kell helyettesíteni.

Annak érdekében, hogy az így kiesett algoritmusok pótolhatók legyenek, teljesen új eljárások kifejlesztését kezdték meg. A NIST Post Quantum Cryptograhy Projekt[52] számos új eljárást vizsgál, melyben jelensorok írásakor 17 titkosítást és 9 digitális aláírást megvalósító kvantumbiztos algoritmus szerepel, de ez a szám folyamatosan változik[53].

Az új módszerek teszteléséhez végső soron szintén kvantumszámítógépet kell használni, ezért a NIST koordinálásával indult egy együttműködés a kormányzati és a gazdasági-üzleti szféra közt. 2022-re várták az első olyan szabványtervezeteket, amelyek a posztkvantum algoritmusok elleni védekezés alapjait definiálták, ezek részben elkészültek.

Az algoritmusok gyakorlati implementálása is megkezdődött. A New Hope egy posztkvantum algoritmus a TLS kiváltására, amit a Google *Combined Elliptic-Curve and Post-Quantum*

[52] https://csrc.nist.gov/projects/post-quantum-cryptography
[53] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions

(CECPQ) néven implementálta a Chrome Canary változatában[54]. A DigiCert *post-quantum cryptographic* (PQC) hibrid tanúsítványok előállításához használt szoftver fejlesztett ki, mely a visszamenőleges kompatibilitás érdekében a hagyományos kriptográfiai eljárás mellett egy posztkvantum algoritmust is tartalmaz.

A Digicert megoldása az egyik legnagyobb nehézséget teszi világossá: amellett, hogy a kriptográfiai protokollok kifejlesztése, szabványosítása és bevezetése nagyon hosszú időt vesz igénybe, kivezetése a meglevő rendszerekből még több időt igényel, ezért a meglevő rendszerekben jelenlevő régi elemek mindegyike biztonsági rést jelenthet.

4.6.Jelszó lenyomatok feltörésének vizsgálata hagyományos eszközökkel

A tudományos kutatási eredmények eltérően ítélik meg az egyes titkosítási eljárások feltörésének esélyeit, illetve az ismertté vált lenyomatok ismeretében az eredeti jelszavak előállításának lehetséges módjait. Internetes források közölnek mérési eredményeket arról, hogy adott hardver- és szoftver környezet mentén kialakított rendszerek milyen sebességgel képesek jelszóhash-ek előállítására, de ezek elsősorban a számítási erőre koncentrálnak [87].

A cél elérésére alkalmazott algoritmusok esetében a hatékonyság növelésének egyik lehetséges útja a felesleges előképek eliminálása, mellyel egyúttal a szükséges számítási erőforrás mennyisége is redukálható. A tudományos kutatások több ilyen célú eljárást ismertetnek, melyek működése elsősorban a felhasználók számára ajánlott metodikák ismeretén alapul.

Az egyik legígéretesebb alternatíva, melynek gyökerei már 1999-ben ismertek voltak, a hagyományos karakter-alapú jelszó helyett valamilyen grafikus megoldáson alapul. Különböző grafikus jelszó megoldások ismertek, mint például a PassPoints, vagy a Cued Click Points. Fintech alkalmazásokhoz egy térkép megfelelő pontjainak megérintésével történő azonosítást javasoltak. [88] Az ilyen típusú eljárások gyengesége olyan hotspotok kialakulásában van, melyeket a felhasználók előszeretettel választanak ki. A hatékonyság javítását a felhasználók meggyőzése jelentheti, melyben minél változatosabb és több véletlenszerű jelszó választására ösztönözik a felhasználókat [89]. Bár a grafikus jelszavak javítják a megjegyezhetőséget, összességében a jelszótér méretét a gyakorlatban jelentősen redukálják, ezzel javítva a feltörésük eredményességének valószínűségét.

Több kutatás irányult a jelszavakban használt karakterek vagy karakterkombinációk alapján a jelszótér méretének redukciójára. Kávrestad és társai munkájukban rámutatnak, hogy „az amerikai kisbetűk és számok szinte minden jelszóban jelen vannak, és úgy tűnik, hogy a

[54] https://www.google.com/chrome/canary/

felhasználók, ha tehetik, kerülik a speciális karakterek használatát.” Méréseik során a billentyűzetminták alkalmazását is vizsgálták, melyek a „a billentyűzeten beütött, egymás melletti billentyűk sorozataként” definiáltak. Megállapították, hogy az adataik titkosítását magas prioritással kezelő felhasználók 17%-a, a felmérésben résztvevők 10%-a részesítette előnyben a billentyűzetminták alkalmazását [90].

Az ismertetett technikák mellett számos más eljárás is ismert a jelszavak memorizálásának megkönnyítésére. Ezek beépítése a feltörésre irányuló, a nyers erő módszerét alkalmazó algoritmusba, jelentősen javíthatja annak hatásfokát.

Nem leltem fel olyan tudományos forrást, mely a felhasználók jelszóképzési szokásait a numerikus és speciális karakterek jelszón belüli pozíciója alapján vizsgálta volna. A jelszavak előképeinek meghatározásának vizsgálatát az Eszterházy Károly Egyetem valós jelszólenyomatait tartalmazó címtáron végeztem úgy, hogy azokat olyan minták alkalmazásával finomhangoltam, melyek feltételezték, hogy a jelszóban a numerikus és speciális karakterek inkább a jelszó második felében helyezkednek el[55].

Mivel az egyetem központi informatikai szervezete számos különböző rendszerrel nyújt komplex szolgáltatási kört, ezért a központi címtárban a jelszavak több különböző lenyomata is rögzítésre került. Ez biztosította annak lehetőségét, hogy megvizsgálhassam az NTLM és az SHA-1 lenyomatképzés ellenállóképességét a nyers erő módszerével szemben.

A vizsgálat elvégzésére egy I5-ös processzorú, SSD-vel rendelkező Linux operációs rendszerű asztali számítógép szolgált, melyben a szükséges számítási kapacitást egy NVidia GTX Titan VGA kártya GPU-ja biztosította. A lenyomatok visszafejtését a HashCat szoftverrel végeztem. Ez egy több platformon is futásképes, MIT licenc alatt elérhető alkalmazás, mely internetes keresések alapján az egyik leggyorsabb előképkeresési szoftver. A mérés idején aktuális verzió 377 különböző lenyomat-variánst és több különböző módot támogat az előképek megtalálására, emellett ki tudja használni a különböző OpenCL-kompatibilis (Open Computing Language) CPU-k, GPU-k és társprocesszorok számítási teljesítményét is, így ideális eszköznek bizonyult az alkalmazott hash kódok visszafejtehetőségének tesztelésére. A HashCat nem csak egy lenyomathoz tartozó jelszó keresésére alkalmas. Kötegelt működési üzemmódjában képes egy lenyomatokat tartalmazó fájl elemeinek egy működési ciklusban történő elemzésére és feltörésének megkísérlésére.

A mérés során kiemelt szerepet kapott a jelszavak feltörésére szolgáló stratégia helyes megválasztása. A nyers erő hagyományos alkalmazása esetén a lehetséges előképeket generáló

[55] A mérésekben Vertike László rendszermérnök nyújtott támogatást.

algoritmus az összes lehetséges változat előállításával keresi azok előképeit. A jelszavak kulcsterének csökkentésére a HashCat ún. maszkok definiálását teszi lehetővé. Ezek olyan reguláris kifejezések, amelyek jelszó mintákat (patterneket) definiálnak oly módon, hogy meghatározzák az egyes pozíciókon alkalmazható karaktereket. A méréseket a hagyományos stratégia alkalmazása mellett több különféle maszkra alapozva is elvégeztem, és a metodika sikerességének meghatározását a rendelkezésre álló idő függvényében vizsgáltam. Az egyes mérési sorozatokhoz felhasználható idő maximumát négy napban határoztam meg, ennek lejártakor a szoftver működését leállítottam és regisztráltam a kimenetét.

Az egyetem címtárszolgáltatásában szereplő jelszavak nagy része két, különféle lenyomat formájában is elérhető, melynek oka a ráépülő különböző háttérrendszerek eltérő követelményeiben van. A vizsgálatot ezért NTLM és SHA-1 hash-ekre is elvégeztem. Mivel az SHA-1-es jelszavakat az egyetemi szolgáltatások fejlesztésének egy későbbi fázisában vezettük be, így azok esetében, akik ezeket nem vették igénybe, nem képeztük egy jelszócsere során az SHA-1 változatot. A vizsgálat első fázisában 2650 NTLM jelszó lenyomatot vizsgáltam öt, különböző konfigurációban:

- Az első beállítás szerint elvégzett vizsgálatban nem végeztem finomhangolást. Az előkép megtalálásához a teljes ASCII névteret felhasználtam úgy, hogy egyetlen lehetséges kombinációt sem hagytam ki.
- A szoftverbe épített alapértelmezett maszk alkalmazása már jelentősen csökkentette a névtér méretét, így a szükséges próbálkozások számát.
- Egyedi maszkok alkalmazásakor három különböző változatot alkalmaztam, a legjobb eredményt a harmadik adta, melyben a hat karakteres vagy rövidebb jelszavak esetén feltételeztem, hogy bármelyik pozícióban állhat kis- és nagybetű, számjegy és speciális karakter is. Az ennél hosszabbak esetén már csak két pozícióban feltételeztem, hogy ott a felhasználó speciális karaktert alkalmaz, a többiben pedig csak kisbetű vagy szám használatát valószínűsítettem. 3-as számú saját maszkként az alábbi mintakészletet alkalmaztam:

```
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?1
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?1?1
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?1?1?1
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?1?1?1?1
```

```
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?2?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?3?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?3?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?3?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?3?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?2?3

?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?2?2?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?3?2?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?3?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?3?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?3?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?2?3?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?2?2?3

?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?1?2?2?2?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?3?2?2?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?3?2?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?3?2?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?3?2?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?2?3?2?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?2?2?3?2
?l?u?d*!$@+-%\,,?l?d,?u*!$@+-%\,,,?1?2?2?2?2?2?2?2?3
```

A jelszavak hosszának függvényében feltört jelszavak számát az alábbi táblázat foglalja össze:

Találatok száma	Jelszó hossza						Össz.
	4 kar.	5 kar.	6 kar.	7 kar.	8 kar.	9 kar.	
Teljes ASCII névtér	2	11	28	26	-	-	**67**
Alapértelmezett maszk	2	11	26	25	186	117	**367**
Saját maszk 1	2	10	27	24	25	13	**101**
Saját maszk 2	2	11	28	25	435	-	**501**
Saját maszk 3	2	11	28	25	435	154	**655**

20. táblázat. Feltört NTLM jelszavak hossza és száma. Készítette a szerző.

A mérés eredményéből megállapítottam, hogy a jelszó hosszára vonatkozó megkötéseknek meghatározó szerepe van egy előkép megtalálásának sikerességében, és a névtér szűkítésére szolgáló stratégia kiválasztásának még hétkarakteres hosszig sincs valódi jelentősége. (A táblázat adataiban hét karakterig az egyes stratégiák esetén alig olvasható ki eltérés.) A maszk alkalmazása a vizsgált jelszavak esetén 8 karakteres hossztól kapott jelentőséget, itt az eltérések száma ugrásszerűen megnőtt, és a teljes névtér vizsgálata a rendelkezésre álló időn belül már

egyetlen érvényes találatot sem adott. A 9 karakteres jelszavak esetében a 2-es típusú maszk sem volt képes egyetlen előkép megtalálására sem, miközben a legjobb eredményt nyújtó 3. típusú még 154 találatot adott. **Ez a minta összesen 655 jelszót volt képes visszafejteni, ami a teljes jelszótér 24,7%-a.**

Érdemes megvizsgálni a konkrét mérési időket és az idő lejártának következtében megszakított mérések feltételezett időigényét is, melyeket az alábbi táblázat tartalmaz. Ennek normál cellái az időkorláton belüli méréseket tartalmazzák. Az inverz cellák értékei feltételezett eredmények, melyeket az alkalmazott jelszóterek nagyságának arányosításával becsültem meg úgy, hogy az egyes találatokhoz szükséges időt egyenlő részekre osztottam fel.

	Jelszó hossza					
Futási idők	**4 kar.**	**5 kar.**	**6 kar.**	**7 kar.**	**8 kar.**	**9 kar.**
Teljes ASCII névtér	0 mp	3 mp	134 mp	3 óra 39 perc	~ 15 nap	-
Alapértelmezett maszk	0 mp	0 mp	0 mp	23 mp	18 perc 35 mp	12 óra 41 perc
Saját maszk 1	0 mp	2 mp	5 mp	154 mp	1 óra 54 perc	3 nap 5 óra
Saját maszk 2	0 mp	0 mp	19 mp	340 mp	4 óra 8 perc	~1 hét.
Saját maszk 3	0 mp	1 mp	19 mp	193 mp	2 óra 18 perc	3 nap 21 óra

21. táblázat. NTLM jelszavak feltöréséhez szükséges idők. Készítette a szerző.

Egy előkép megtalálásának ideje a maszktól függetlenül egy másodpercen belül volt a négykarakteres jelszavak esetén, és az ötkarakteres jelszóhosszig sem érte el az egy másodpercet. A nyolckarakteres jelszavakon, a 3-as saját maszk alapján mért több mint 2 órás idő magas érték, de 435 visszafejtett jelszóval ez az egyik leghatékonyabbnak bizonyuló támadási stratégia volt. Az egyetemi adatbázisban NTLM jelszavak esetén is a 3-as jelölésű maszk volt a legsikeresebb, mely bizonyítja, hogy a speciális karaktereket a jelszó vége felé tartalmazó minták nagyobb gyakorisággal fordulnak elő, ezeket a felhasználók előszeretettel alkalmazzák – feltehetően részben azért, mert a komplex jelszavakat megkövetelő rendszerek hibaüzenetei során ezeket kényelmi okokból a jelszó végéhez adják hozzá.
Összességében, a vizsgált mérési hardveren az időadatok alapján még a 9 karakteres jelszavak sem tekinthetők biztonságosnak. Ez alapján, figyelembe véve az alkalmazott gép számítási teljesítményét, az informatikai rendszerek jelszóra alapozott védelme esetén ennél határozottan hosszabbat, vagy magasabb komplexitásút kell megkövetelni.

A 2194 db. SHA-1-es lenyomat feltörése már nehezebb feladatnak bizonyult, mivel a lenyomatképző eljárás komplexitása következtében az alkalmazott VGA kártya GPU-ja egységnyi idő alatt kevesebb lenyomat előállítására volt képes. Itt a kilenc karakteres jelszavak visszafejtésére a rendelkezésre álló idő nem volt elég, és az NTLM feltörésének korábbi

értékeivel összehasonlítva is megállapítható, hogy sikerességében nem sokkal marad el attól, de az visszafejtéshez szükséges idő kb. háromszoros. Mivel az NTLM jelszavak mérésekor már meghatároztam a rendelkezésre álló leghatékonyabb maszkot, így ebben már csak ennek hatékonyságát vizsgáltam. A sikeresen előállított előképek száma és az előállításukhoz szükséges időt a jelszavak hosszának függvényében az alábbi táblázat tartalmazza:

	Jelszó hossza				
	4 kar.	**5 kar.**	**6 kar.**	**7 kar.**	**8 kar.**
Futási idő	0 mp	2 mp	66 mp	10 perc 55 mp	7 óra 24 perc
Találatok száma	2	11	21	22	414

22. táblázat. A feltört SHA-1 kódolású jelszavak hossza és száma. Készítette a szerző.

A vizsgált mintán tehát 470 SHA-1 kódolású jelszót sikerült feltörni, ami 21,4%-os eredményt jelent.

Az NTLM és SHA-1-es hashképző algoritmusok összehasonlításakor egyértelműen leolvasható, hogy a 3-as saját maszk alkalmazása esetén a találati eredmények száma lényegében alig különbözik, a 6 karakternél ráadásul épp az erősebbnek tartott SHA-1 bizonyult gyengébbnek. Amennyiben eltekintünk a 9 karakteres jelszavaktól, a két eljárás közti hatékonyságának különbsége nem tekinthető relevánsnak, az mindössze 93% (470/501). A két táblázat időadatainak összevetésével megállapítható, hogy az NTLM algoritmusa lényegesen kisebb időigényű, a jelszótér azonos stratégiájú redukciója rövidebb idő alatt szolgáltatott az SHA-1-gyel hozzávetőleg azonos eredményeket. Az SHA-1 magasabb erőforrás igénye a vizsgált konfigurációban a 9 karakteres jelszavaktól mutatkozott meg, a rendelkezésre álló idő nem volt elégséges ezen jelszavak visszafejtésének befejezésére, így erre a hosszra már nem állt rendelkezésemre adat.

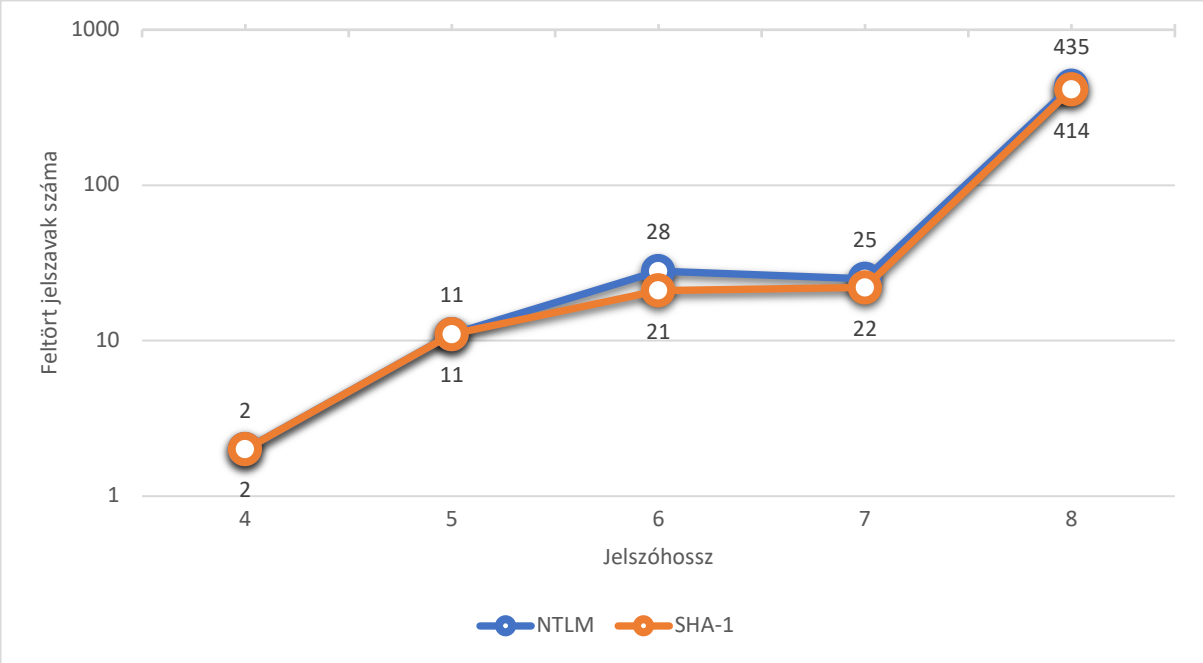
Annak érdekében, hogy az összehasonlítás azonos környezeti feltételek mellett is összehasonlítható legyen, elhagytam a 9 karakteres jelszóhosszhoz tartozó mérési értékeket. Mivel az egyes jelszótípusokra nézve a bemeneti adathalmaz mérete különböző volt, így képeztem a visszafejtett és a rendelkezésre álló jelszavak hányadosát. Ez az NTLM jelszavak esetében:

$$\frac{501}{2650} = 0{,}1890 = 18{,}9\%$$

Míg az SHA-1 alkalmazásakor:

$$\frac{470}{2194} = 0{,}2142 = 21{,}42\%$$

Amennyiben a vizsgálat eredményeinek elemzése során csak a rendelkezésre álló idő alatt lefutott méréseket vesszük figyelembe, **megállapítható, hogy az előképek megtalálásának elsődleges forrása a jelszótér redukciójára irányuló stratégia, az alkalmazott lenyomatképzési eljárásnak csak a futási időre nézve van jelentősége**. A nyers erő módszerének végeredménye eltérő időigénnyel ugyan, de azonos lesz. A bemutatott pattern alkalmazásával a vizsgált felsőoktatási rendszer esetében ez az arány 18,9% és 21,42% közé tehető.



8. ábra. Az NTLM és az SHA-1 jelszavak feltörésének eredményessége.
Forrás: saját szerkesztés.

Az eredmény értelmezése során figyelembe kell a két jelszó adatbázis eltérő méretéből adódó különbségeket. A vizsgált NTLM jelszavak magasabb számának következményeként a meghatározott idő alatt több jelszó vizsgálata volt elvégezhető, melyek azokra is kiterjedtek, amelyeknek nem állt rendelkezésre az SHA-1-es megfelelőjük. Ezért nem várható el, hogy az alkalmazott algoritmustól függetlenül a mérés azonos hosszúságú jelszavakra azonos találati számot adjon, és a mért adatok minden esetben az SHA-1 jelszavak azonos, vagy alacsonyabb értékét mutatják.

A felsőoktatási rendszerek jelszóképzési eljárásai az alkalmazott rendszerek hasonlósága, és a dolgozói kör azonos jelszóképzési attitűdje következtében valószínűsíthetően azonosak, így indukció útján az egyetemi vizsgálat során kapott eredmények további más intézményekre is

kiterjeszthetők. Az indukció helyességének igazolása a kutatásban alkalmazott mérési eljárás megismétlésével bámely felsőoktatási intézmény elvégezheti.

Ezzel bizonyítottam a H6. hipotézis első részállítását: **A felsőoktatás saját rendszereiben működő e-mail címek jelszavai egy brute force előkép-meghatározási eljárással szemben csak részlegesen védettek, melynek eredményességét elsősorban a támadó előkép meghatározási stratégiája határozza meg.**

4.7.Adatsértésben érintett intézményi e-mail címek vizsgálata

A jelszavak biztonságának vizsgálata során kézenfekvő kérdés az is, hogy egy intézményi e-mail címekhez tartozó jelszavak milyen mennyiségben találhatók meg olyan adatbázisokban, amelyek valamilyen adatszivárgás következményeként kerültek ki az azokat kezelő szervezetektől. Ezek a címek nem csak a kéretlen levelek forrásául szolgáló címlistákban jelennek meg, hanem egyéb adatokkal, akár obfuszkált, akár olvasható jelszavakat tartalmazó adatbázisok kínálatában pl. a darkneten. Annak vizsgálatára, hogy a felsőoktatási intézmények e-mail címei milyen mértékben váltak érintetté ilyen jellegű támadásokban, a HIBP adatbázisát alkalmaztam, amely a vizsgálat elvégzésekor valamivel több, mint tízmilliárd rekordot tartalmazott.

A site internetes adatlopások kapcsán nyilvánossá vált e-mail címek és valamilyen rendszerben ahhoz tartozó egyéb személyes adatok, főleg jelszavak tömegét tartalmazza. Adatbázisában a vizsgálat idején 485 különböző adatszivárgásból 10,5 milliárd hozzáférési adatot tartalmazott, melyben bárki ellenőrizheti, hogy az e-mail címe mely incidensben vagy gyűjteményben[56] volt érintett. A források közt neves szoftvercégek (Adobe, Dropbox, Sony) szolgáltatásainak adatszivárgásai éppúgy megtalálhatók, mint az interneten árusított gyűjtemények tartalma – az egyik legnagyobb gyűjteményt a Collection#1-nak nevezik. Ezt a hozzávetőleg 2,9 milliárd rekordot tartalmazó listát 2019-ben fedezték fel egy népszerű hackerfórumon, mely több ezer különböző adatlopásból származó adatok gyűjteménye. A Collection#1 1.160.253.228 egyedi e-mail cím és jelszó kombinációját tartalmazza [91].

A HIBP rendszer adatbázisát alkotó források egy rosszindulatú támadó számára további rendszerekhez történő hozzáférést is biztosíthatnak, az ismertté vált bejelentkezési adatokat felhasználva megkísérelhetik a postafiókon túl más rendszerekbe történő belépést is. Bár az előbbi kompromittálásának következményeit a felhasználók egy része hajlamos alábecsülni:

[56] A site adatbázisa több konkrét támadás során megszerzett adatok mellett egyéb, esetenként ismeretlen incidensből származó adatokat is tartalmaz. A támadók ezeket gyűjteményekként értékesítettek, melyeket ők, vagy a site üzemeltetője nevezett el.

egy sikeresen feltört mailbox az első és lényeges eleme lehet különféle Man in the Middle típusú csalások elkövetésének, vagy más, pl. jelszóemlékeztető kérésével indított támadás sikeres kivitelezésének. A támadási lehetőségek további kiterjesztését teszik lehetővé a föderációban működő azonosítási szolgáltatások. A magyar közép- és felsőoktatásban dolgozók és tanulók számára biztosított EduRoam szolgáltatás a világ több mint száz országában és kísérleti helyszínén érhető el és biztosít vezetéknélküli hálózati hozzáférést. A szintén föderációban működő EduID egységes azonosítási rendszert kínál a felsőoktatásban tanulók és dolgozók számára, és számos könyvtár, tudományos adatbázis és folyóirat rendszeréhez biztosít hozzáférést. A kiszivárgott jelszavak súlyos incidensek kiindulási pontjai lehetnek minden olyan szervezet esetén, melyek valamilyen központi címtárszolgáltatásra alapozva több szolgáltatáshoz is biztosítanak hozzáférést. Az ilyen típusú megoldások kényelmi és biztonsági szempontból is elterjedtek, ugyanakkor az egy pontba koncentrált belépési azonosítások az informatikai védelem achillesi sarkát jelentik.

A felhasználók gyakorlati szempontból előnyben részesítik az azonos jelszavak különböző rendszerekben való alkalmazását, ezirányú motivációjukat több kutatás is vizsgálta. Adams és Sasse [92] megállapították, hogy a felhasználók számára nem elfogadható jelszószabályok elégedetlenséget váltanak ki, így azok kontraproduktívak lesznek – alacsony biztonsági motivációkhoz és a szabályok kijátszásához vezetnek. A valós életkörnyezetben a jelszó használatának kényszere megszakítja a felhasználó elsődleges feladatát [93], Bonneau pedig kutatásában megállapította, hogy a vizsgálatában résztvevők egyetlen, a jelszavak helyett alkalmazható alternatív megoldást sem tartottak teljeskörűen elfogadhatónak [94]. Inglesant és Sasse arra a következtetésre jutottak, hogy a jelszóval kapcsolatos szabályzások a jelszó erősségének maximalizálására és a gyakori cserére összpontosítanak, így ehelyett az adott használati kontextushoz megfelelő erősségű jelszó alkalmazását javasolták. Kutatásukban megállapították, hogy a jelszavak gyakori megváltoztatásának követelménye nem növelte a biztonságot [95]. Herley betekintést nyújt az felhasználók implicit költség/haszon számításaiba, amikor egy biztonsági szabály betartásáról vagy megszegéséről döntenek. Gondolatmenetében a gyenge jelszó választása a felhasználó szempontjából racionális lépés abban az esetben, ha egy támadás valószínűségét a felhasználók alacsonynak ítélik meg, miközben a szabályok betartásának akadályozó hatását azonnalinak és biztosnak tartják [96].

A felsorolt problémák megoldást gyakran valamilyen jelszószéf alkalmazásában látják, azonban ezek alkalmazásában is merülnek fel kockázati tényezők. Mivel ezek a rendszerek nagy számú felhasználó szinte minden hozzáférési adatait egyetlen adatbázisba koncentrálják, ezért a támadók kiemelt célpontjainak számítanak, a rendszerelemek hibája pedig egyszerre

nagymennyiségű és várhatóan érvényes hozzáférés kiszivárgását teszi lehetővé. A jelszótárolási szolgáltatóknál bekövetkezett adatszivárgásra a magas szintű védelmi eljárások alkalmazásának ellenére is van példa, 2022-ben például a Lastpass szolgáltatásában keletkezett, felhőben tárolt mentések titkosított adatfájljai kerültek ki. Bár a szolgáltató tájékoztatása alapján csak abban az esetben tudják garantálni a feltörhetetlenségét, ha az alkalmazott mesterjelszót máshol nem használták, annak erőssége az előírásoknak megfelelő, vagy az ún. Federated Login Services szolgáltatást használták az azonosításhoz, egy ilyen eset alapjában rendíti meg a harmadik fél felé irányuló bizalmat [71].

A fentiek alapján H.5. figyelembevételével (egy felsőoktatási rendszerben tárolt jelszó hash-ek az alkalmazott algoritmusok függvényében jelentős arányban dekódolhatók) kijelenthető, hogy az e-mail címek jelszavainak nyilvánosságra kerülésének hatása nem csak az elektronikus levelezésre terjed ki.

H.5-2. bizonyításához megállapítom, hogy milyen arányban találhatók meg felsőoktatási intézmények domain névterébe tartozó e-mail cím és jelszó párosok az HIBP adatbázisában, valamint összehasonlítom azt egy másik magyar egyetemével.

Annak érdekében, hogy a mérési környezet a lehető legszorosabban egyezzen meg egy valódi támadó által elérhetővel, első lépésként azt vizsgáltam meg, hogy az egyetemek kínálnak-e olyan publikusan elérhető szolgáltatást, mely lehetővé teszi a személyes e-mail címek tömeges begyűjtését. Ennek megállapításhoz áttekintettem az első fejezetben kiválasztott egyetemeket és manuális kereséssel próbáltam megtalálni a kérdéses szolgáltatást.
A kapott eredményeket összevetettem a 2018-ban elvégzett mérésemmel, akkor 32 magyar egyetem weblapját vizsgáltam meg olyan publikus forrást keresve, mely lehetővé teszi dolgozók neveinek, e-mail címeinek és munkakörük megnevezését tartalmazó adatforrás szüretelését. Hét egyetem esetében akkor nem találtam ennek módját, vagy a lista felhasználói azonosításhoz kötött volt, 25 intézmény esetében a dolgozói listát letölthetőnek ítéltem meg. 2022-ben a felsorolt intézmények áttekintése során megállapítottam, hogy ez az állapot nem sokat változott, a legnagyobb egyetemek adatai OSINT útján továbbra is beszerezhető.
Azok esetében, amelyek kínáltak ilyen szolgáltatást, megvizsgáltam, hogy azok milyen korlátozásokat alkalmaznak a teljes címlista letöltésére és hogy azok milyen módszerekkel kerülhetők meg. Megítélésem szerint csak azok a megoldások elfogadhatók, melyek személyes e-mail címekről a publikus internet felé nem nyújtanak információt, vagy melyek kizárólag

szervezeti egységek címeit publikálják. Minden olyan vizsgált esetben, melyben a tömeges letöltést a keresőkérdésben meghatározott minimális karakterszámmal kívánták megakadályozni, egy 10–50 soros, az adott forrás megkötéseinek megkerülésére létrehozott shell scripttel meg tudtam volna kerülni. Az adatok begyűjtését végző programjaim a potenciális támadó kilétének rejtésére a darkneten keresztül kommunikáltak a szolgáltatást nyújtó szerverekkel.

A címek begyűjtését két magyar egyetemen és egy akadémiai kutatóintézetben végeztem el. Tekintettel arra, hogy a kutatásetikai megfelelőség érdekében a mérés elvégzéséhez az adott intézmény kifejezetten nehezen megszerezhető engedélye szükséges, a további egyetemek e-mail címeinek mérésétől annak ellenére tekintettem el, hogy többségük esetében az láthatóan megoldható lett volna. Így e hipotézis esetében is az indukció módszerét alkalmazva fogalmazok meg általános következtetést.

Az adatsértésekben érintett címeket a HIBP egy előfizetéses szolgáltatására alapozva határoztam meg. A tömeges ellenőrzések elvégzését egy ún. REST API[57] híváson keresztül lehet elvégezni, ezt alkalmaztam az általam készített, ellenőrzést végző szoftverben. A módszer hátránya, hogy az ellenőrzés során az e-mail címek a HIPB szolgáltatása számára abban az esetben is megismerhetők, ha azok korábban nem szerepeltek az adatbázisában. Ez a tény egyes üzemeltetők részéről az ellenőrzéssel szembeni ellenállást vált ki.

A saját intézményem vizsgálatakor a teljes címlistáját használtam, amely nem csak az élő, hanem a kivezetett címeket is tartalmazta, ideértve az intézmény korábbi domainjét is[58], ez indokolja az e-mail címek viszonylagos magas számát. A mérés eredménye rendkívül kedvező képet mutatott, 6.386 e-mail címből csupán 50 volt megtalálható ebben az adatbázisban, mely 87 adatszivárgásban volt érintett, és az incidensek száma is csak 11 volt. Ez alapján megállapítható, hogy az érintett e-mailek száma nem éri el ez 1%-ot sem, és az előfordulásuk arányában is csak **1,36%-os eredményt kaptam** (87/6.386). Utóbbi értelmezése kérdéses, mivel nem egyértelmű, hogy az egyes adatszivárgások azonos e-mail címhez ugyanazokat a hozzáféréseket és járulékos adatokat hozták nyilvánosságra. Az érintett címek túlnyomó része személyes használatra készült, szervezeti egység címét összesen 3 esetben azonosítottam. Összességében tehát megállapítottam, hogy az egri egyetem e-mail címei csak minimális

[57] Az API (Application Programming Interface) egy olyan kapcsolódási felület, amelyet programok közti kommunikációra fejlesztettek ki. A REST API e felület de facto szabványa.

[58] Az EKE az egyetemmé alakulása előtt az ektf.hu domain alatt működtette a levelezését, amelyet 2015-ben az uni-eszterhazy.hu-ra cserélt. Az ilyen típusú változások jellemzők voltak az egyetemek jelenleg zajló átszervezése következtében.

mértékben voltak jelen ezekben az adatbázisokban. A részletes eredményeket az alábbi táblázat foglalja össze:

#	Forrás	Darabszám
1.	Collection #1 [Collection1] 2019-01-07	52
2.	2,844 Separate Data Breaches [2844Breaches] 2018-02-19	11
3.	Canva [Canva] 2019-05-24	6
4.	Covve [db8151dd] 2020-02-20	5
5.	Apollo [Apollo] 2018-07-23	4
6.	Onliner Spambot [OnlinerSpambot] 2017-08-28	2
7.	Exploit.In [ExploitIn] 2016-10-13	2
8.	Anti Public Combo List [AntiPublic] 2016-12-16	2
9.	LinkedIn [LinkedIn] 2012-05-05	1
10.	Edmodo [Edmodo] 2017-05-11	1
11.	Data Enrichment Exposure From PDL Customer [PDL] 2019-10-16	1

23. táblázat. Adatszivárgások és az érintett e-mail címek száma. Készítette a szerző.

A mérést egy magyar tudományegyetem publikusan elérhető e-mail adatbázisán is elvégeztem. Ennek során először elkészítettem azt a shell scriptet, mely a darkneten keresztül begyűjtötte az egyetem e-mail címeit, majd a már ismertetett módon ezek jelenlétét is lekérdeztem a HIPB adatbázisában.

Ez a mérés már sokkal nagyobb arányban mutatta ki a címek és kapcsolódó adatainak érintettségét. A megszerzett 2.849 címből 551 volt megtalálható legalább egy adatforrásban, ami 19,3%-os előfordulási gyakoriságot jelent. Az érintett címek túlnyomórészt esetükben is személynevekhez köthetők voltak, de elvétve előfordultak hivatali címek is (pl. office@ kezdetűek az egyetem által használt különböző aldomainekben). Összesen 51 különböző adatszivárgásban vagy gyűjteményben fordultak elő hozzáférési adataik, melyek közül az első helyet itt is a Collection#1 foglalta el. Az előfordulási arány ezen az egyetemen lényegesen rosszabb képet mutatott: a az említett 551 cím 1.396 alkalommal volt kimutatható 53 különböző adatszivárgásban, **ami 49%-os eredményt jelent** (1.396/2.849).

Harmadik lépésként a vizsgálatot egy kutatóintézet nyilvános adatain végeztem el. A 676 e-mail cím begyűjtése itt sem jelentett problémát, melyből csak 40 volt megtalálható a HIBP adatbázisában, ez 5,9%-os sikerességi rátát jelent. Mivel a kutatóintézet e-mail címei 21 különböző adatszivárgásban 100 alkalommal fordultak elő**, az előfordulási arány esetükben is magasabb: 14%** (100/676).

A mért adatok ismeretében megállapítható, hogy **a felsőoktatási rendszerek e-mail címeinek védelme során kockázatot jelent a különböző internetes jelszógyűjteményekben hozzájuk társított jelszavak mennyisége, ezzel a H.5-2 hipotézist azzal a kitétellel igazoltam, hogy a kockázat mértéke intézményenként jelentős eltérést mutathat**. A fiatal, elektronikus levelezésre használt domainek esetében az érintettség mértéke értelemszerűen kisebb, és az intézmények védelmi módszereikkel is csökkenthetik az érintettség növekedésének mértékét (az említett kutatóintézetben nem lehet olyan jelszót beállítani, amely valamilyen adatszivárgási incidensben érintett volt.)

Annak megállapítására, hogy az egyetemek mely incidensekben érintettek leginkább, előállítottam azok összesítő táblázatát, mely azokat az adatszivárgásokat vagy gyűjteményeket tartalmazza, melyben 10-nél magasabb számban fordulnak elő a vizsgált intézmények e-mail címei. Annak ellenére, hogy a kutatóintézetben a Collection#1 csak a harmadik helyen szerepelt, egyértelműen leolvasható, hogy ez tartalmazza a szféra legtöbb adatát. Az összesített lista második helyen szereplő PDL (Data Enrichment Exposure From PDL Customer) 1,2 milliárd személyes adatot tartalmazó adatszivárgás, mely az e-mail címek és telefonszámok mellett munkáltatók és beosztások, nevek és közösségi média profilok is megtalálhatók voltak. A harmadik helyen szereplő LinkedIn adatszivárgásában pedig természetes a felsőoktatás és a kutatók adatainak jelenléte, mint ahogyan a Dropbox és az Adobe esetében is. A teljes táblázatot a 4. sz. melléklet tartalmazza.

Sorsz.	Darab	Név
1	272	Collection #1 [Collection1]
2	169	Data Enrichment Exposure From PDL Customer [PDL]
3	155	LinkedIn [LinkedIn]
4	137	Anti Public Combo List [AntiPublic]
5	112	Exploit.In [ExploitIn]
6	99	Verifications.io [VerificationsIO]
7	96	MDPI [MDPI]
8	90	2,844 Separate Data Breaches [2844Breaches]
9	71	Dropbox [Dropbox]
10	55	Onliner Spambot [OnlinerSpambot]
11	51	Covve [db8151dd]
12	49	Adobe [Adobe]
13	38	Trik Spam Botnet [TrikSpamBotnet]
14	34	MyHeritage [MyHeritage]
15	21	Exactis [Exactis]
16	20	Canva [Canva]
17	17	Kayo.moe Credential Stuffing List [KayoMoe]

Sorsz.	Darab	Név
18	16	Apollo [Apollo]

24. táblázat. A felsőoktatási e-mail címek nyilvánosságra kerülésében érintett adatszivárgások. Készítette a szerző.

A korábban hivatkozott 10.5 milliárd adat kiszivárgása nem jelenti azt, hogy azok olvasható formátumú jelszavakat tartalmaznak. Ezekben gyakran a már tárgyalt jelszóhash-ek szerepelnek, így azok nem használhatók azonnal. Az egyetemi jelszó adatbázis vizsgálata során viszont megmutattam, hogy az algoritmusoktól várt biztonság nem szükségszerűen működik jól a gyakorlatban.

A titkosítás hatékonyságának javítása érdekében az iparági vezető cégek számos biztonsági módosítást alkalmaznak a szoftvereikben. A Google a Chrome böngészőben lehetetlenné tette, hogy a https-t használó oldalakról titkosítatlanul (http protokollon) lehessen fájlokat letölteni[59]. Az Apple a Safari böngésző tanúsítványainak érvényességét két évről egyre csökkentette, ezzel lerövidítve az esetlegesen kompromittálódott kulcsok használhatóságának időtartamát[60]. Elsőként a Safari, azóta már a legnépszerűbb böngészők mindegyike képes a felhasználói profilban tárolt jelszavak ellenőrzésére és figyelmeztetést küldenek, ha azok közt szerepel olyan, mely korábban már nyilvánosságra került.

4.8.Adathalászati módszerek eredményességének vizsgálata

Egy felhasználó hozzáférési adatainak megszerzésére a bemutatott előképképzési eljárások elsősorban nagy mennyiségű titkosított jelszavakat tartalmazó adatbázisok nyilvánosságra kerülése esetén lehetnek eredményesek, ugyanakkor a hozzáférések megszerzésére az egyik leginkább ismert módszer az adathalász levelek alkalmazása. A hackmageddon.com adatainak feldolgozásával készített adatbázisomban a 2016 és 2022 között az oktatási intézmények ellen sikeresen indított, adathalász levelekkel (a Hackmageddon nevezékében: account takeover) végrehajtott sikeres támadások aránya 4,24%, a hozzáférés-eltérítéssel (account hijacking) kivitelezetteké pedig 12,2% volt[61]. Az ismeretlen jellegű (26,3%), és malware támadások (43,9%) után ez a módszer fordult elő a legnagyobb arányban. Ezért célszerűnek tartottam annak vizsgálatát, hogy milyen hatékonysággal vehetők rá egy felsőoktatási intézmény

[59] https://blog.chromium.org/2020/02/protecting-users-from-insecure.html
[60] https://www.thesslstore.com/blog/ssl-certificate-validity-will-be-limited-to-one-year-by-apples-safari-browser/
[61] Az oktatási intézmények ellen indított legnépszerűbb támadási forma a malware (43,9%). A támadások eszköze az esetek 26,3%-ában ismeretlen maradt.

munkatársai egy-egy ismeretlen melléklet megnyitására, illetve egy megtévesztő weboldal felhasználásával hozzáférési adataik megadására. Feltételezésem szerint a munkatársak jelentős, legalább 20%-a egy célzott támadás során megtéveszthető. H.5-3. bizonyításához, mely szerint **egyetemi környezetben pedig egy OSINT információk alapján felépített, phishing támadással kicsalható legfeljebb 9 karakteres jelszavak mennyisége alacsonyabb, mint a jelszó adatbázis általam javasolt stratégiára optimalizált brute force technikával megszerezhetőké**, bemutatom azt a módszert, melyet egyetemi oktatók és dolgozók ilyen típusú támadási helyzetben adott reakcióinak mérésére dolgoztam ki, és annak eredményességét összevetettem jelszavak feltörésével elértekkel.

4.9.A social engineering

A social engineering (SE) „egy személy manipulálása azért, hogy olyan cselekedetet hajtson végre, […] amely a támadó érdekeit szolgálja, s mely magában foglalhatja az információszerzést, hozzáférés megszerzését, vagy a célszemély rávezetését bizonyos lépések megtételére” [97]. A módszer tehát a technikai eszközök hibáinak felkutatása és kihasználása helyett az emberi oldal hibáját vagy gyengeségét használja ki, lényege a megtévesztés. A számítógépek korai időszakában a SE eszköztárának fő irányát a hagyományos kommunikációs csatornák, tipikusan a telefonos megtévesztések jelentették. Ma a SE ereje főként olyan nagy szervezetekben érvényesül, ahol a dolgozók nem ismerik egymást, így egy támadó viszonylag egyszerűen képes olyan helyzet előállítására, melyben a célszemélyt információ átadására vagy más nem kívánatos tevékenység elvégzésére tudja rávenni.
A social engineeringnek több, jellegzetes eszköztára van. Ezek egy része a hipotézisem igazolása érdekében könnyen megvalósítható, míg mások csak nehezen, vagy egyáltalán nem. Kutatásomban két különböző típusú SE támadás működőképességét vizsgáltam. Az elsőben egy malware típusú támadást indítottam, mellyel a célcsoport tagjait egy ismeretlen forrásból származó melléklet megnyitására igyekeztem rávenni. A második mérésben egy jelszó megszerzésére irányuló adathalász technikát (phishing – Password Harvesting Fishing) alkalmazva próbáltam elérni, hogy a munkatársak megadják a hivatali e-mail hozzáférésüket.

A phishing értelmezését különböző források eltérően magyarázzák, Lastdrager szisztematikus szakirodalmi elemzésében 113 definíciót kutatott fel és gyűjtötte össze a fogalom értelmezésének fő kritériumait [98]. Vizsgálatom szempontjából Lastdrager által bemutatott jellemzők közül olyan, az áldozat által ismert, vagy megbízhatónak tekintett e-mail címet és website-ot használtam fel, melyet a célszemély hitelesként fogad el, s ezen keresztül

megtéveszthető úgy, hogy megadja hozzáférési adatait. A módszer alkalmazása esetén az így kicsalt adatokat jellegüktől függően további célokra használják fel, mivel a már bemutatott adatok alapján a támadók tevékenységének fő célja általában valamilyen anyagi előny megszerzése. Jellemző célpontok a bankszámlák, a bankkártya adatok megadását megkövetelő szolgáltatások (Paypal, AppleID), de egy megszerzett hozzáférés birtokában elemezhető a postafiók korábbi tartalma, melyből így további értékes források mellett egyéb hozzáférési adatok kutathatók fel, vagy pl. jelszóemlékeztetők kérésével továbbiak szerezhetők meg.

A phishing gyakori eleme egy valódinak látszó webhivatkozás felkínálása a célszemély számára. Ennek hiteles közlése a módszer kritikus pontja, melyet célzottan, az adott személyekre adaptálva küld ki a támadó[62], vagy pedig tömegesen, a találatot a véletlenre bízva juttatja el felhasználókhoz. A magyar nyelv nehézsége és viszonylagos ritkasága korábban előnyt jelentett – a lándzsás halászat leveleinek hibás magyarsága az egyetemen dolgozó külföldiek mellett csak néhány magyar kollégának nem tűnt fel. A nyelvi modellek utóbbi időben tapasztalt rendkívüli fejlődése a fordítóprogramokra is komoly hatást gyakorolt, ezeket, illetve a chatGPT-t felhasználva a támadók hibátlan magyar nyelvű szövegeket tudnak előállítani.

A phishing weblapokon történő alkalmazásának ellehetetlenítését többek közt a tanúsítvány alapú védelem jelenthetné. A módszer elméleti és technikai szempontól is kidolgozott, de tapasztalataim szerint a tanúsítványok feladatát és helyességének ellenőrzési módját az átlagos felhasználók többsége nem ismeri, az erre vonatkozó információkat nem képes értelmezni, így azok nem érik el eredeti céljukat. Az olcsó tanúsítványt nyújtó szervezetek ebből a szempontból tovább rontották a helyzetet (egy nameCheap tanúsítványának ára 8.88 dollár évente[63], a LetsEncrypt pedig ingyenes). Tekintettel arra, hogy a megrendelők és üzemeltetők is az adatlopási (lehallgatási) kísérletek megakadályozásában érdekeltek, ezért lehetőség szerint minden website-ot tanúsítvánnyal látnak el, hogy azok titkosított https protokollon legyenek elérhetők. A hangsúly ezzel egy site eredetiségének igazolásáról eltolódott a titkosított átvitel megvalósítására anélkül, hogy a felhasználó tanúsítvánnyal kapcsolatos hibajelzéseket kapna. A minimális ellenőrzési eljárást alkalmazó tanúsítványkiadók ezzel nagyban hozzájárulnak az adattovábbítás biztonságához, egyúttal viszont lehetővé tették, hogy támadó website-ok is hitelesként legyenek feltüntethetők. Ezt a módszert a kutatásomban én is alkalmaztam.

[62] A megtévesztő e-mailek mellett jellemzők az SMS-ben küldött online vásárlással vagy szállítással kapcsolatos értesítések, lejáró bankkártyákról, szolgáltatásokban fennálló hátralékról értesítő üzenetek.
[63] https://www.namecheap.com/security/ssl-certificates/comodo.aspx

H.5-3. bizonyítására egy célzott támadást valósítottam meg úgy, hogy kizárólag olyan nyilvános adatforrásokat használtam fel, melyeket a vizsgálat idején bárki képes volt összegyűjteni. Ezek az információk internetes keresés eredményei, illetve az egyetemi weblap mérést megelőző állapotából származnak. A két mérésben az alábbi feladatot határoztam meg[64]:

1. Excel táblázat letöltésére buzdító e-mail kiküldése az egyetemi tudakozóban szereplő felhasználók számára, a mérés során a letöltések számának és a letöltő e-mail címének rögzítése.
2. E-mail-ben küldött figyelmeztetés a hivatali hozzáférésekben használt jelszó ellenőrzésére, egyúttal a felhasználó csaló weblapra terelése és hozzáférési adatainak kicsalása. Az érvényes hozzáférést megadók számának és e-mail címének rögzítése.

4.10. Műszaki környezet

A vizsgálat elvégzése előtt áttekintettem azokat a szoftvereket, amelyekkel a feladat elvégezhető. A legegyszerűbben alkalmazhatónak a GoPhish-t tartom[65], mely a phishing tesztek elvégzését egyszerűsíti le úgy, hogy a tesztelő a feladat lényegére koncentrálhat. A Metasploit talán az egyik legnépszerűbb, de az ingyenes változat erősen korlátozott, a professzionális csomag alkalmazását az árazása miatt elvetettem. A szoftver a phishing mellett számos más sérülékenység vizsgálatára és kihasználására alkalmas elemet tartalmaz, ennek megfelelően a kezelése bonyolult és mélyebb hálózati és rendszerszintű ismereteket feltételez. A Social Engineering Toolkit (SET) egy alkalmazáscsomag, mellyel különböző típusú SE támadások végezhetők. Bár a SET eszközkészletében szereplő Mass mailer attack alkalmazhatónak tűnt, végül a körülményesen konfigurálható SET alkalmazását is elvetettem, és a feladat viszonylagos egyszerűsége és a konfigurálhatóság megtartása érdekében egy virtuális szerverre saját rendszert telepítettem, és kidolgoztam a mérésekhez szükséges programokat.

Mindkét támadás első fázisa megtévesztő levelek tömeges célba juttatását igényelte. Mivel a kéretlen levelek forgalmának megakadályozása érdekében a levélküldés eljárásait az elmúlt

[64] Bár dolgozatom témája szempontjából nem releváns, de a teljesség kedvéért megemlítem, hogy a felhasználók vizsgálata előtt az informatikai üzemeltetők megtéveszthetőségét is vizsgáltam. Ennek fő pontjai: 1. Fiktív új felhasználót felvétele a rendszerbe. 2. A fiktív felhasználó számára virtuális szerver létrehozásának elérése az egyetem infrastruktúráján. 3. A szerverrel kapcsolatos megszorítások, tűzfalszabályok fellazításának elérése, külső hozzáférési csatornák (portok) megnyitása.

[65] https://getgophish.com

évtizedekben számos védelmi megoldással egészítették ki, a terjesztés megvalósítására olyan műszaki megoldást kerestem, mely műszaki szempontból koherens és teljes, ezért nem alkalmaztam technikai értelemben vett hamis címeket, megtévesztő url-eket. OSINT módszerrel begyűjthető valódi e-mail címekkel operáltam, és a qov.hu-hoz hasonlóan olyan valódi domain nevet alkalmaztam, amely az egyetem eredeti nevével könnyen összetéveszthető [99]. Az alkalmazott metodika, mely egy valódi domain regisztrációján alapul, biztosította a munkatársak reakciójának monitorozását úgy, hogy közben minimalizáltam a megtévesztő levelek és url-ek felismeérésének kockázatát úgy, hogy az alkalmazott szoftverek (böngészők, e-mail kliensprogramok) sem adjanak figyelmeztető jelzést számukra.

A mérések elvégzéséhez egy új, az egyetem nevéhez nagyon hasonlító domain nevet választottam, az *uni-esztehazy.hu*-t, mely az egyetem által használt névtől csak egy *r* karakterben különbözik. Mivel az olvasás során egy szó felismerését a szavak elején és végén levő karakterek alapján végezzük, feltételeztem, hogy a név középső részében levő „r” hiánya csak kevés felhasználó számára tűnik majd fel.

A műszaki megvalósításhoz egy saját, Linux operációs rendszerű szervert készítettem, melyen egy DNS szervert, valamint egy SMTP és IMAP szervert telepítettem fel – ezek feltételei a domain regisztrációs folyamat sikeres lebonyolításának. Üzemeltetési tapasztalataim alapján állítom, hogy a jól működő megtévesztés a gyakorlatban ma már csak valódi domain nevek és jól konfigurált levelező szerverek használatával lehetséges. A spammel szembeni harcban az MTA-k[66] üzemeltetői számos ellenőrzést végeznek, és csak egy teljesen szabályosan felkonfigurált, valódi domain névre alapozott, tanúsítvánnyal rendelkező levelező szerver beállítása után tudtam elérni, hogy a teszt levelem célba jusson.

A domain regisztrációja egy támadó számára a legkockázatosabb követelmény, mivel ennek során a legtöbb esetben a személyazonosság igazolására van szükség. A jelenlegi magyar domain regisztrációs gyakorlat bárki számára lehetővé teszi, hogy szinte tetszőleges domain nevet regisztráljon és működtessen[67]. A magyar eljárásrend követte az amerikai gyakorlatot: a korábban csak írásban, cégek esetében cégszerűen aláírt igénylőlap kitöltése után induló regisztrációs folyamatot hazánkban is fellazították, így a regisztráció a tulajdonos személyének szigorú ellenőrzése nélkül is elvégezhető. A korábbi kéthetes kötelező várakozással szemben ma már egy igény benyújtását követő rövid időn belül a domain ideiglenesen használatba vehető, bár a végleges tulajdonába csak két hét után kerül[68]. Ebben a fázisban már bármilyen

[66] MTA: Mail Transfer Agent, a levelek küldését végző szerver szoftver.
[67] Kivételt jelentenek a személynevek, melyek regisztrációjához névhasználati igazolást kell benyújtani.
[68] A prioritásos domain nevek esetében ez a feltétel nem áll fenn.

szolgáltatás felépíthető a domain név alatt, így akár a domain regisztráció igényének benyújtása után, annak kifizetése nélkül is le lehet bonyolítani egy támadást. Ebben az esetben a két hét, vagy a fizetési határidő lejárta után a regisztrátor a domaint valószínűleg törölni fogja, megnehezítve ezzel a forenzikus vizsgálatokat, és a támadó kilétének megállapítását.
A regisztrációs folyamat lefutásához egy másodlagos DNS szervert is biztosítani kell, melyre a későbbiekben egy támadó célú, ideiglenes működésre szánt infrastruktúra esetén már nincs szükség.
A domaint az Eszterházy Károly Egyetem nevére regisztráltam be, ehhez az egyetem weblapjáról OSINT módszerrel minden szükséges adat összegyűjthető volt. A magánszemélyként történő regisztrációhoz személyi igazolvány számot kellett volna megadni, és igyekeztem megmaradni a törvényesség talaján – inkább a céges regisztráció mellett maradtam úgy, hogy a regisztráció során sehol sem igazoltam, hogy bármilyen kapcsolatban állnék az egyetemmel. Kapcsolattartóként az egyetem informatikai vezetőjének nevét adtam meg (ez a bárki számára elérhető telefonkönyvből származik) e-mail címként viszont egy ellenőrzötten nem létező egyetemi e-mail címet használtam.
A regisztrációt saját magam végeztem, melyhez a már meglevő bejegyzési gyakorlatomat alkalmaztam. A nagyszámú domain bejegyzését végző szervezetek szigorú folyamatok mentén működnek, így valós szituációban inkább kisebb, domain bejegyzésre jogosult vállalkozást érdemes a bejegyzéssel megbízni. Ezek általában nem rendelkeznek szigorú ügyviteli szabályokkal így egy támadó akár telefonos megbízással is elindíthatja a domain felvételét, és hozzáférést kaphat annak a DNS szerverhez. A legnagyobb problémát a szolgáltatás kifizetése jelentheti, a kis szolgáltatók esetben akár készpénzes fizetésre is lehetőség van.
A domain regisztrációja során nem jelentett akadályt annak nyilvánvalóan megtévesztő jellege. Sem a rendszer, sem a bejegyzést végző személyzet nem jelezte a hibát, feltételezhetően az automatizált folyamat nem tartalmazott erre vonatkozó ellenőrzést.

Az SMTP szerver konfigurálásakor szintén a műszaki szempontból teljesen szabályos eljárást követtem, biztosítva, hogy a szerver ne szolgálhasson ugródeszkaként mások számára, melynek következtében feketelistára kerülhet az általa használt IP cím, lehetetlenné téve így a megtévesztő levelek célba juttatását. A konfiguráció részeként megvalósítottam a Domainkeys Identified Mail (DKIM) védelmi rendszer előírásait, mely egy PKI infrastruktúra alkalmazásával biztosítja a feladó ellenőrizhetőségét. Ez a védelem (hasonlóan az SPF-hez)

elsősorban az idegen domainek alá tartozó e-mail címekről küldött levelek kiszűrésére alkalmas, a saját kezelésben levő domainek esetében egyszerűen kijátszhatók[69,70].

A tesztelését a www.mail-checker.com oldalon elérhető szolgáltatással végeztem el, mely a szerverről küldött leveleket megfelelőségük szerint pontozza. A teszt levelek tartalmi hiányosságai következtében nem értem el tökéletes eredményt, de a kapott 8 pont feletti érték több mint elégséges a levelek célba juttatásához.

Egy megbízható levelezési és a webszerver megköveteli a már említett tanúsítványok alkalmazását. Ennek beszerzésére a magyar szolgáltatók az azonosítási követelmények miatt nem jöhettek szóba, és a külföldiek esetében sem találtam anonim lehetőséget. Így a már említett Letsencrypt szolgáltatását választottam, mely három hónapig érvényes, könnyen és önműködően megújítható tanúsítvány biztosít, melyhez csak azt várja el, hogy a tanúsítvány igénylése az azt felhasználó szerverről történjen. A tanúsítvány birtokában a levelek küldése biztonságos csatornán keresztül valósítható meg, a „jelszóellenőrzést" végző weblap pedig tanúsított, biztonságos webhely benyomását kelti a felhasználóban.

Hosszú távon az elkészített szerver egy virtuális gépben, esetleg egy docker image-ben akár egy notebookon is futtatható, vagy a támadás folyamata egy demonstrációs céllal pár napra akár ingyenesen igénybe vett virtuális szerverszolgáltatónál lebonyolítható[71].

4.11. Phishing teszt

Az első mérés célpontja egyetem összes olyan munkatársa volt, akiknek e-mail címei OSINT módszerekkel összegyűjthetők voltak. A mérés célja egy ismeretlen forrásból származó e-mailben található link mentén egy idegen weblapról származó Excel táblázatot megnyitása volt. Az MS Office adatfájljainak megnyitásakor különösen óvatosan kell eljárni, hiszen az azokban elhelyezhető makrók ideális helyet biztosíthatnak a kártékony programok számára, bár erre a legtöbb esetben a védelmi rendszerek figyelmeztetést adnak.

A levél elkészítése során igyekeztem minden olyan lehetőséget kihasználni, hogy a munkatárs lássa, hogy a levelet **nem** számára küldték. A címzett látszólag az egyetem egyik levelezési listája volt[72], a címzett számára azt a benyomást keltve, hogy a levelet rossz címre küldték. Már

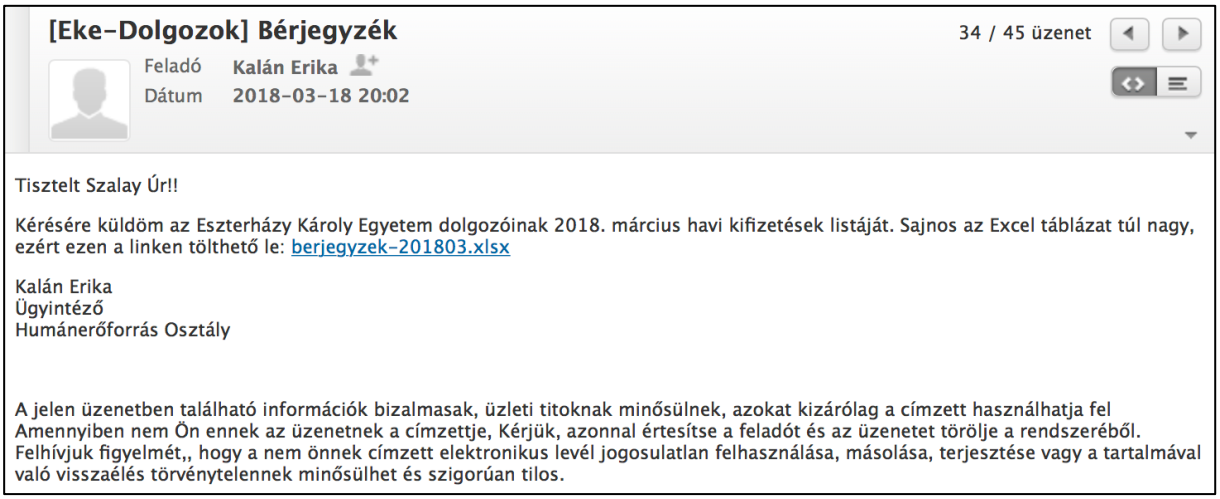
[69] A DKIM alkalmazása során a levél küldését végző szerver digitálisan aláírja a levelet, melynek érvényességét a domain zónájában egy TXT rekordban elérhető publikus kulccsal lehet ellenőrizni. A DKIM alkalmazásával egyértelművé tehető, hogy melyik szerver küldte az adott elektronikus levelet.

[70] Az SPF rekordban az adott domain alá tartozó e-mail címek legális szerverei sorolhatók fel, így más szerverektől érkező leveleket a rendszerek nem fogadnak be.

[71] Egy példa: https://www.arubacloud.hu/ingyenes-probaverzio.aspx

[72] Az egyetemi levelezőlisták nevét és címeit az első lépésben, az üzemeltetés által létrehozott e-mail cím használatával könnyen ki lehetett deríteni, naponta két-három listás levél is érkezett rá.

a megszólítás is nyilvánvalóvá tette a téves címzést, ami a levél tartalma alapján is egyértelmű volt. A levél egy záradékot is tartalmazott, melyben a feladó megtiltja a levél jogosulatlan felhasználását. A levél tartalma az alábbi volt:


[Eke-Dolgozok] Bérjegyzék

34 / 45 üzenet

Feladó Kalán Erika

Dátum 2018-03-18 20:02

Tisztelt Szalay Úr!!

Kérésére küldöm az Eszterházy Károly Egyetem dolgozóinak 2018. március havi kifizetések listáját. Sajnos az Excel táblázat túl nagy, ezért ezen a linken tölthető le: berjegyzek-201803.xlsx

Kalán Erika
Ügyintéző
Humánerőforrás Osztály

A jelen üzenetben található információk bizalmasak, üzleti titoknak minősülnek, azokat kizárólag a címzett használhatja fel Amennyiben nem Ön ennek az üzenetnek a címzettje, Kérjük, azonnal értesítse a feladót és az üzenetet törölje a rendszeréből. Felhívjuk figyelmét,, hogy a nem önnek címzett elektronikus levél jogosulatlan felhasználása, másolása, terjesztése vagy a tartalmával való visszaélés törvénytelennek minősülhet és szigorúan tilos.

9. ábra. A mérés során alkalmazott adathalász levél. Forrás: saját szerkesztés.

Annak érdekében, hogy a informatikai rendszerek adminisztrátorai minél később vegyék észre a megtévesztő levelek beérkezését, őket a címzettek listájában nem szerepeltettem. Mivel a telefonkönyv a dolgozók szervezeti egységét és a beosztását is tartalmazta, azokat a címeket, melyek leírásai tartalmazták az *informatikai, hálózatüzemeltetési, klienstámogatás, informatikus, rendszergazda* szavakat, eltávolítottam a címzettek listájáról. A levélhez kapcsolódóan egy Excel táblát készítettem, amely tartalmazta az intézmény dolgozóinak neveit, illetve az Excel *véletlen.között()* függvényét használva generált a nevek mellett egy-egy megfelelően formázott adószámot, illetve egy kifizetés adatot tüntetett fel. Ezzel a módszerrel kliens oldalon biztosítottam, hogy mindenki eltérő táblázatot kapjon, és az minden egyes megnyitáskor eltérő tartalmat lásson. Az oszlopok fejléceiben egyértelműsítettem, hogy a táblázat az egyetem dolgozóinak aktuális havi illetményét tartalmazza.

A mérhetőség érdekében a táblázatot nem a levél melléklete volt, hanem letölthető dokumentumként hivatkoztam rá a levélben. A forrás a már korábban regisztrált megtévesztő domainre, az *uni-esztehazy.hu*-ra mutatott. Ehhez a szerveren létrehoztam egy aldomaint, a *letoltes.uni-esztehazy.hu*-t. Az ide feltelepített, szabályosan bekonfigurált webszerver a már említett LetsEncrypt tanúsítvánnyal igazolta a hitelességét. A letöltést végző személyek azonosításához először mindegyikük számára generáltam egy véletlenszerű karakterláncot (pl. *rECJ3lSwENJVWYDx9J2PVuhmBIsGjWIx)*. A kiküldött levelek ezt felhasználva nem voltak azonosak, a karakterlánc alkalmazásával a letöltés linkjét minden levélre nézve egyedivé tettem, így a letöltést végző személyek azonosíthatók voltak.

A szerver oldalon az Apache *url rewriting* mechanizmusára alapozva egy .htaccess állományban összerendeltem ezeket és a hozzájuk tartozó e-mail címeket, így amikor egy munkatárs a rá nézve egyedileg létrehozott linkre kattintott, a véletlenszerű karakterekből „dekódoltam" és naplóztam a letöltést végző személy e-mail címét[73]. A kiértékelést a fájl letöltését biztosító program automatikusan végezte, az eredményeket folyamatosan egy fájlba rögzítve.

A levelek kiküldését egy hétfői munkanapon reggel 7:20-kor indítottam, és összesen 1.750 címre küldtem ki. Maga a küldési folyamat közel 45 percet vehetett igénybe. A letöltéseket folyamatosan nyomon követtem, ezek üteme az alábbi volt:

Idő	Letöltések
07:00-08:00	27
08:00-09:00	264
09:00-10:00	121
10:00-11:00	40
11:00-12:00	24
12:00-13:00	17
13:00-14:00	16
14:00-15:00	9

25. táblázat. A táblázat letöltésének időbeni eloszlása. Készítette a szerző.

A teljes letöltések száma 969, az ismétlések nélkülieké 532 volt, ez 30.4%-os arányt jelent (a felhasználók egy része a levele más személyeknek is megküldtek, amelyet ők is letöltöttek).

4.12. Jelszó megadásának tesztje

Az e-mail címekhez tartozó jelszavak kicsalhatóságának mérését ugyanezen a napon végeztem el. Ehhez egy, az egyetem arculatához illeszkedő weblapot készítettem elő, amely a munkatársak jelszavainak helyességét ellenőrizte. Erről újabb e-mail értesítést küldtem, szintén a csaló domain névről. A levél állítása szerint néhány jelszó nyilvánosságra került, ezért az informatikai személyzet nevében arra kértem a címzetteket, ellenőrizzék jelszavukat megadott link mentén. A levelek kiküldését az első mérésben használt úton küldtem ki ugyanarra a címlistára.

A jelszóellenőrző űrlap mögött futó program nem csak a kitöltés tényét rögzítette, hanem a jelszó helyességét is ellenőrizte oly módon, hogy a megadott paraméterekkel felépített egy hálózati kapcsolatot a postafiókhoz tartozó IMAP szerverrel, és megkísérelte a bejelentkezést

[73] pl. RewriteRule rECJ3lSwENJVWYDx9J2PVuhmBIsGjWIx.html /index.php?mail=koczka.ferenc@uni-eszterhazy.hu [L]

– ennek eredménye alapján végezte el az esemény értékelését és rögzítését. A módszer alkalmazásával a mérés a jelszavak tárolása nélkül is lefolytatható, így azok nem okozhatnak adatszivárgást. A megvalósítást szintén egy virtualhosttal végeztem, melyhez a https://jelszoellenorzes.uni-esztehazy.hu címet rendeltem. A titkosított protokoll használata ebben az esetben elkerülhetetlen: ha egy támadó a mérés során képes lehallgatni az ide irányuló adatforgalmat, az a mérést incidenssé változtatta volna. A hitelesség látszatát ebben az esetben is egy Letsencrypt tanúsítvány biztosította.

10. ábra. Adathalász weboldal a https://jelszoellenorzes.uni-eszterhazy.hu oldalon. Forrás: saját szerkesztés.

A mérés eredményeként 1.750 felhasználóból 304-en adták meg a jelszavukat, ez 17,37%-os sikerességi arányt jelent. Ez alapján megállapítható, hogy a sokkal kisebb befektetéssel megvalósítható, a jelszavak kicsalására irányuló SE módszer 17.37%-os eredményessége alacsonyabb, mint a jelszóállomány visszafejtésével kapott 24.7 és 21.4%-os eredmény. Ezzel **H6-3. bizonyításra került: egyetemi környezetben egy OSINT információk alapján felépített, phishing támadással kicsalható legfeljebb 9 karakteres jelszavak mennyisége alacsonyabb, mint a jelszó adatbázis általam javasolt stratégiára optimalizált brute force technikával megszerezhetőké**.

4.13. Összegzés

A fejezet hipotéziseit az azokban foglalt korlátozások mellett igazoltam. A brute force támadás az egyetemi jelszó adatbázison működőképesnek bizonyult, és hatékonyságát a jelszótér szűkítésére irányuló stratégia határozta meg. Bizonyítottam az az OSINT információforrásból megszerezhető egyetemi jelszavak jelenlétét a HIBP adatbázisában, megmutattam azok eltérő mértékét és magyarázatot adtam a különbségekre. Végül bizonyítottam, hogy az egyetemi környezetben végrehajtott phishing támadások eredményesek, és kilenc karakteres jelszavakig a brute force módszerével történő feltörésük eredményesebb, mint a phishing alkalmazása.

A fejezetben bemutattam, a jelszavakkal kapcsolatos elméleti és gyakorlati hátteret, a különféle titkosítási eljárások vonatkozó részeit, a hashképzési eljárásokat, sebezhetőségeik lehetőségeit. Kitértem a kvantumszámítógép kriptográfiára gyakorolt hatására, a posztkvantum algoritmusokra és a titkosítási eljárások jövőbeni lehetőségeire. Mérés útján bizonyítottam, hogy egy, a mérés időpontjában hozzávetőleg 200.000 Ft-os számítógép konfigurációval és a feltörést végző szoftver konfigurálásával **a szervezet teljes jelszóállományának több mint egyötöde feltörhető négy napon belül.** A mérés további fontos megállapítása, hogy a 8 karakteres jelszavak egy ilyen egyszerű konfiguráció alkalmazása mellett sem jelentenek elégséges védelmet, ennél határozottan magasabb jelszószám javasolt, ajánlásom szerint ez 12 karakter. A jelszavak feltörésére irányuló vizsgálatom a rendelkezésre álló hardverrel kilenc karakteres jelszavakig volt hatékony, nagyobb anyagi ráfordítással ezt további karakterekkel tolható ki, de a szükséges számítási kapacitás minden egyes karakterrel többszörösére nő.

Az adathalászat sikerességére vonatkozó vizsgálatom 30%-os eredménye bizonyítja, hogy egy potenciális támadó megtévesztő levelekkel képes lehet az egyetemi infrastruktúra megbénítására és egy cryptovírus aktiválásával az adatvagyon számottevő részének elveszítésére [100]. Ez, és a csaló jelszóellenőrzést célzó weboldal 17,3%-os sikerességi aránya egyaránt alátámasztja azt a feltételezést, hogy a felsőoktatásban dolgozók megtéveszthetősége meglehetősen magas, ugyanakkor a 9 karakteres jelszavakig a jelszó adatbázis megszerzése és a jelszavak előképeinek brute force technológiára alapozott visszafejtetése nagyobb eredményességű lehet. A jelszavak hosszának és komplexitásának növelése értelemszerűen megváltoztatja ezt az arányt, a javasolt 12 karakteres jelszóhossz kötelező érvényre juttatása esetén lényegesen magasabb számítási kapacitás szükséges.

A méréssel kapcsolatban érdemes kiemelni annak belső, szervezeti hatását, a mérés során több esemény egészen másképp történt, mint ahogyan azt feltételeztem. A felhasználók a megtévesztő levelek vételét nem jelezték az informatikai igazgatóság felé, így ők csak akkor szereztek erről tudomást, amikor a munkatársak már tömegesen letöltötték a megtévesztő mellékletet. Ez egy valós támadás esetén a lehetséges veszteségeket megtöbbszörözte volna. A

munkatársak kollégáikat vagy barátaikat figyelmeztették, esetleg a saját vezetőiknek jeleztek. Emellett a mérést sok, főleg oktatói és kutatói munkakörben dolgozó kolléga nehezményezte, és személyes támadásnak tekintette. Megfelelő erős vezetői támogatás hiánya nélkül ezért ilyen mérés lebonyolítását nem tartom elvégezhetőnek.

5. Összegzett következtetések

Értekezésem hipotéziseinek tárgyát a felsőoktatási rendszerek néhány informatikai védelmi kérdései adják. Elsőként megmutattam, hogy a magyar felsőoktatási intézmények jelentős adatvagyonnal rendelkeznek, az azokat kezelő informatikai rendszereken keresztül bemutattam azok jellegét és hozzávetőleges mennyiségét. Főként nemzetközi adatok elemzésével bizonyítottam, hogy az oktatási rendszerek ellen indított támadások száma a teljes támadási kör hozzávetőleg 6–9%-a között van, emellett kimutattam, hogy hazai viszonylatban nem állnak rendelkezésre a szférát ért informatikai incidenseket leíró adatbázisok vagy nyilvántartások. Bemutattam, hogy a magyar jogszabályi környezet nem rendelkezik a szektorra vonatkozó szabályzással, ezzel szemben más olyan, állami tulajdonban vagy állami fenntartásban levő szervezet létezik, mely sokkal kevesebb érzékeny adatot kezel, ugyanakkor szigorú jogszabályi előírások szabnak kereteket az informatikai rendszereik kialakítására és üzemeltetésére. Az egyetemek adatvagyonának meghatározására és a szabályzatok homogenitásának megállapítására dokumentumelemzésen alapuló kutatás során elemeztem a magyar egyetemek szabályzatainak reprezentatív mintáját, és megállapítottam, hogy azok jelentős részben OSINT támogatást nyújtanak, kisebb részben elavultak, a kis létszámú egyetemek esetében pedig gyenge kidolgozásúak vagy nem léteznek. A homogenizálás érdekében javaslatot adtam a leggyakoribb egyetemi szakrendszerek 41/2015 BM. rendelet szerinti besorolására.

Miután bizonyítottam, hogy az egyetemi informatikai rendszerek nagymennyiségű érzékeny adatot tartalmaznak, és 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 megállapítottam, hogy az informatikai rendszerelemek sérülékenységi szintje nem különbözik a központi és perifériális campusok közt, viszont számos, sok éve ismert sérülékenység mutatható ki ezekben a rendszerelemekben. Emellett bizonyítottam, hogy a feltárt sebezhetőségek jelentős arányban az üzemelteltető személyzet által javítható konfigurációs hibák, melyek javíthatósága a beállítások szigorúbb szabályzása mellett az elavult szoftver-, és kisebb részben hardver eszközpark cseréjével küszöbölhető ki.

A harmadik fejezetben egy felsőoktatási intézmény jelszó adatbázisának feltörési lehetőségeit vizsgáltam. Mérésem arra irányult, hogy egy egyetemi informatikai rendszer feltörése esetén kiszivárgó jelszó adatbázisban tárolt titkosított jelszavak visszafejtése milyen mértékben végezhető el sikeresen egy bárki számára elérhető hardver- és szoftver konfiguráció

alkalmazásával. Megállapítottam, hogy az SHA1-es és NTLM jelszavak elfogadható időn belül az alkalmas szoftverkörnyezetben egy közepes munkaállomásra alapozva 20-25%-os eredményességgel voltak feltörhetők; ez magasabb érték, mint amelyet a korábban, az EKE-n indított belső adathalász kampány során értem el. Megmutattam, hogy a jelszavak előképeinek brute force technikával történő meghatározásának sikerét nem az adott hashképzési eljárás ereje, hanem a jelszótér csökkentésére irányuló stratégia határozza meg. Emellett bizonyítottam, hogy az egyetemek nagyrésze esetében az alkalmazott e-mail címek OSINT eljárással összegyűjthetők, valamint nyilvános jelszó adatbázisban fellelhetők.

Összességében dolgozatom rávilágít a felsőoktatási informatikai rendszerek néhány általános problémájára, melyekre megoldási javaslatot nyújt, vagy bemutatja annak alkalmazásának módszertanát, így más intézmények is alkalmazhatják azt.

Új tudományos eredmények

Hipotéziseim bizonyításával az alábbi új, tudományos eredményeket értem el:

E1. Bizonyítottam, hogy a magyar felsőoktatási rendszerek jelentős mennyiségű érzékeny adatot tartalmaznak.

E2. Bizonyítottam, hogy külföldi adatok alapján az oktatási intézmények 6–9%-át érik kibertámadások, valamint hazai viszonylatban nem áll rendelkezésre erre vonatkozó hiteles adat.

E3. Bizonyítottam, hogy a felsőoktatási intézmények informatikai szabályzatai nem homogének, részben elavultak és jórészt támogatják az OSINT információk gyűjtését.

E4. Javaslatot adtam az egyetemi informatikai rendszerek besorolására.

E5. Bemutattam az egyetemi informatikai rendszerek sérülékenységvizsgálatának két alkalmazható módszerét, bizonyítottam a sérülékenységek magas számát és magas életkorát, valamint kimutattam, hogy a sebezhetőségek túlnyomórészt konfigurációs hibák eredményei. Bizonyítottam továbbá, hogy a legtöbb támadás a publikus internet felől elérhető, valamint az informatikai infrastruktúra eszközei ellen érkezik.

E6. Kimutattam, hogy egy egyetemi környezetben alkalmazott jelszavak 25% körüli arányban visszafejthetők, mely 9 karakteres jelszavakig meghaladja az adathalász módszerekkel megszerezhető hozzáférések számát.

Ajánlások

PhD értekezésemben megfogalmazott eredményeimet elsősorban az egyetemi informatikai vezetők figyelmébe ajánlom. Áttekintését javaslom továbbá azon kutatóknak, akik a témához kapcsolódó további tudományos vizsgálatok elvégzését és eredményeik hasznosítását tűzik ki célul elsősorban a magyar felsőoktatási intézményekben.

További kutatásra ajánlom az egyes rendszerek sérülékenységei adatait, melyekből megítélésem szerint számos egyéb következtetés levonható, új összefüggések lehetnek megállapíthatók.

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 minden felsőoktatási intézmény számára ajánlom javaslatom alkalmazását a felsőoktatási informatikai rendszerek besorolásainak elkészítésekor.

Témakörből készült publikációim

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.

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

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.

Publikációk és hipotézisek kapcsolata

Tudományos eredmény	Publikáció
H1.	M1, O2
H2.	M2
H3.	M3
H4.	M3, O3
H5.	M4
H6.	K1, K2, O1, O3

Irodalomjegyzék

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

[2] A. I. P. Sudrastawa, Sariyasa és 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.

[3] *2009/2015. (XII. 29.) Kormány határozata nemzetbiztonsági védelem alá eső szervek és létesítmények köréről.,* 2015.

[4] G. Wangen és J. B. Ulven, „A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet,* %1. kötet13, pp. 1-40, 2021.

[5] N. Rahima, Z. Othmanb és F. Z. Hamidc, „Cyber Security and the Higher Education Literature: A Bibliometric Analysis," *International Journal of Innovation, Creativity and Change,* %1. kötet12, %1. szám12, 2020.

[6] *1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról,* 2020.

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

[8] *Stratégiai Koncepció az Észak-atlanti Szerzıdés Szervezete tagállamainak védelméért és biztonságáért.*

[9] NATO, *Defending the networks - The NATO Policy on Cyber Defence,* 2011.

[10] D. Appelman, „California Requires Disclosure of Database Security Breaches," in *Usenix*, Usenix, 2004.

[11] „Australian Government Department of Home Affairs," 11 2020. [Online]. Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf.

[12] *2011. évi CCIV. törvény a nemzeti felsőoktatásról,* 2011.

[13] *2012. évi C. törvény a Büntető Törvénykönyvről,* 2012.

[14] „Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete,” 27. 04. 2016.. [Online]. Available: 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: 01. 2022.].

[15] National Institute of Standards and Technology, „Framework for Improving Critical Infrastructure Cybersecurity,” 16 04 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Hozzáférés dátuma: 23 05 2019].

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

[17] J. J. Giszczak és D. A. Paluzzi, „ass or Fail? Data Privacy and Cybersecurity Risks in Higher Education,” McDonald Hopkins, 2016.

[18] E. K. Kwaa-Aidoo és M. Agbeko, „An Analysis of Information System Security of a Ghanaian University,” *International Journal of Information Security Science,* %1. kötet7, %1. szám2, pp. 90-99, 2017.

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

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

[21] I. G. Butnaru, V. Nita és 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,* %1. kötet13, %1. szám9, pp. 1-20, 2021.

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

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

[24] F. Inc., „Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do about It. White paper.,” Fireeye Inc., 2015.

[25] Verizon, „Educational Services,” 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/2022/data-breaches-in-education/. [Hozzáférés dátuma: 03 04 2022].

[26] M. Z. Zalat, S. M. Hamed és 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,* %1. kötet16, %1. szám3, pp. 1-12.

[27] G. Vámosi, „Ezerhétszáz hallgató adatait vesztette el a veszprémi egyetem,” 10 12 2008. [Online]. Available: https://www.origo.hu/techbazis/20081210-1717-hallgato-adatait-vesztette-el-a-veszpremi-egyetem.html. [Hozzáférés dátuma: 10 01 2022].

[28] „Zsarolóvírus-támadás érte a Pázmányt, leállt a Neptun,” HVG, 24 04 2020. [Online]. Available: https://hvg.hu/tudomany/20200424_pazmany_peter_katolikus_egyetem_zsarolovirus_neptun_tanulmanyi_rendszer_szakdolgozat_leadasi_hatarido. [Hozzáférés dátuma: 10 01 2022].

[29] Nemzeti Adatvédelmi és Információszabadság Hatóság, „Közérdekű adatigénylés,” 08 12 2018. [Online]. Available: https://kimittud.hu/request/12018/response/17739/attach/3/NAIH%202019%20741.pdf. [Hozzáférés dátuma: 10 12 2022].

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

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

[32] S. Vinovski, „Where is Middleware?,” *IEEE Internet Computing,* %1. kötet6, %1. szám2, pp. 83-85, 2002.

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

[34] U.S. Department of Education, „34 CFR PART 99—FAMILY EDUCATIONAL RIGHTS AND PRIVACY,” U.S. Department of Education, 2011.

[35] „2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról,” 11 04 2020. [Online]. Available: https://njt.hu/jogszabaly/2011-112-00-00.29. [Hozzáférés dátuma: 10 04 2023].

[36] A. Adams és 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.

[37] S. Al-Janabi és I. Al-Shourbaji, „A Study of Cyber Security Awareness in Educational Environment in the Middle East,” *Journal of Information & Knowledge Management,* %1. kötet1, 2016.

[38] G. Wangen, „Unrecorded Security Incidents at NTNU. Bachelor’s Thesis.,” Trondheim, Sweden, NTNU Open Gjøvik., Sweden, 2019.

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

[40] A. Patel, M. Taghavi, K. Bakhtiyari és J. J. Celestino, „An intrusion detection and prevention system in cloud computing: A systematic review,” *Journal of Network and Computer Applications,* %1. kötet36, %1. szám1, pp. 25-41, 2013.

[41] F. Zhang, S. Zhou, Z. Qin és 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.

[42] E. D. Mann és M. S. Christey, „Towards a Common Enumeration of Vulnerabilities,” in *The MITRE Corporation*, Bedford , 1999.

[43] „Common Vulnerabilities and Exposures,” [Online]. Available: https://www.cve.org/About/History.

[44] A. Arora, N. Anand és R. Telang, „Does information security attack frequency increase with vulnerability disclosure? An empirical analysis.,” *Information Systems Frontiers,* %1. kötet8, pp. 350-362, 2006.

[45] P. Johnson, R. Lagerström, M. Ekstedt és U. Franke, „Can the common vulnerability scoring system be trusted? A Bayesian analysis,” *IEEE Transactions on Dependable and Secure Computing,* %1. kötet16, %1. szám6, 2018.

[46] A. Murray, „What Is CVSS v3.1? Understanding The New CVSS. Mend Report.,” Mend, Mend.io, 2020.

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

[48] A. M. N. F. Shaker és A. M. Mohamed, „Zero Click Attack,” in *The International Undergraduate Research Conference*, 2021.

[49] A. Tereshkin és 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.

[50] A. Mallik, „Man-In-The-Middle_Attack: Understanding in Simple Words,” *Cyberspace: Jurnal Pendidikan Teknologi Informasi,* %1. kötet2, %1. szám2, pp. 109-134, 2018.

[51] M. Bozorgi, L. Saul, S. Savage és 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.

[52] L. Allodi és F. Massacci, „Comparing vulnerability severity and exploits using case-control studies,” *ACM Transactions on Information and System Security,* %1. kötet17, %1. szám1, pp. 1-20, 2014.

[53] L. Allodi és F. Massacci, „Security Events and Vulnerability Data for Cybersecurity Risk Estimation,” *Risk Analysis - Special Issue: Advances in Risk Analysis with Big Data.,* %1. kötet37, %1. szám8, 2017.

[54] F. Valeur, G. Vigna, C. Kruegel és R. A. Kemmerer, „A Comprehensive Approach to Intrusion Detection Alert Correlation,” *IEEE Transactions on Dependable and Secure Computing,* %1. kötet1, %1. szám3, pp. 146-169, 2004.

[55] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid és M. Roytman, „Exploit Prediction Scoring System (EPSS),” *Digital Threats: Research and Practice,* %1. kötet2, %1. szám3, pp. 1-17, 2021.

[56] I. Chalvatzis, C. P. Rallis és 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.

[57] Google Inc., „Google Security Blog,” Google Inc., 15 12 2015. [Online]. Available: https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html. [Hozzáférés dátuma: 10 10 2022].

[58] M. A. Dissanayaka, S. Mengel, L. Gittner és 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.

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

[60] 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,* %1. kötet5628, 2009.

[61] D. Ferbrache, „Passwords are broken – the future shape of biometrics," *Biometric Technology Today,* %1. kötet2016, %1. szám3, pp. 5-7, 2016.

[62] „Have I Been Pwned (HIBP)," [Online]. Available: https://haveibeenpwned.com.

[63] R. Bhanot és H. Rahul, „A Review and Comparative Analysis of Various Encryption Algorithms," *International Journal of Security and Its Applications,* %1. kötet9, %1. szám4, pp. 289-306, 2006.

[64] Forces.net, „The First Man To Storm A Nazi U-Boat And Seize An Enigma Machine," 06 01 2016. [Online]. Available: https://www.forces.net/services/navy/first-man-storm-nazi-u-boat-and-seize-enigma-machine. [Hozzáférés dátuma: 01 10 2020].

[65] D. J. Barett and R. Silverman, SSH, The Secure Shell: The Definitive Guide, Sebastopol: O'Reilly, 2001.

[66] A. Chopra, „Comparative Analysis of Key Exchange Algorithms in Cryptography and its Implementation," *IMS Manthan (The Journal of Innovations),* %1. kötet8, %1. szám2, 2015.

[67] D. Knuth, The Art of Computer Programming, Addison-Wesley, 1973.

[68] Adboe Inc., „Customer security alert," Adobe Inc., 28 10 2013. [Online]. Available: https://helpx.adobe.com/x-productkb/policy-pricing/customer-alert.html. [Hozzáférés dátuma: 12 03 2023].

[69] A. Agarwal, „Security update and new features," Dropbox Inc., 31 07 2012. [Online]. Available: https://blog.dropbox.com/topics/company/security-update-new-features. [Hozzáférés dátuma: 12 03 2023].

[70] N. Raymond, „Sony to pay up to $8 million in 'Interview' hacking lawsuit,” Reuters, 20 10 2015. [Online]. Available: https://www.reuters.com/article/us-sony-cyberattack-lawsuit-idUSKCN0SE2JI20151020. [Hozzáférés dátuma: 12 03 2023].

[71] K. Toubba, „Notice of Recent Security Incident,” LastPass Inc., 22 12 2022. [Online]. Available: https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/. [Hozzáférés dátuma: 12 03 2023].

[72] D. Rountree, Cryptography. Security for Microsoft Windows System Administrators, 2011.

[73] Z. N. Sík, „A blockchain filozófiája, avagy a fennálló társadalmi rendek felülvizsgálatának kényszere,” *Új Magyar Közigazgatás,* %1. szám4, pp. 37-56, 2017.

[74] R. Morris és K. Thompson. [Online]. Available: https://rist.tech.cornell.edu/6431papers/MorrisThompson1979.pdf.

[75] S. Boonkrong és C. Somboonpattanakit, „Dynamic Salt Generation and Placement for Secure Password Storing,” *IAENG International Journal of Computer Science,* 29 02 2016.

[76] Y. Yarom és N. Benger, „Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack,” Cryptology ePrint Archive, 2014.

[77] C. Endrődi és K. Csorba, „Kriptográfiai algoritmus implementációjának időalapú támadása,” in *Netowrkshop konferencia*, Budapest, 2004.

[78] P. P. Pittalia, „A Comparative Study of Hash Algorithms in Cryptography,” *International Journal of Computer Science and Mobile Computing,* %1. kötet8, %1. szám6, pp. 147-152, 2019.

[79] J. Lake, „What is a collision attack?,” 30 05 2022. [Online]. Available: https://www.comparitech.com/blog/information-security/what-is-a-collision-attack/.

[80] B. Hayes, „NIST Retires SHA-1 Cryptographic Algorithm,” 15 12 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm. [Hozzáférés dátuma: 14 01 2023].

[81] Mozilla Corporation, „The end of SHA-1 on the Public Web,” Mozilla Corporation, 23 02 2017. [Online]. Available: https://blog.mozilla.org/security/2017/02/23/the-end-of-sha-1-on-the-public-web/. [Hozzáférés dátuma: 10 10 2022].

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

[8 *2013. évi L. törvény az állami és önkormányzati szervek elektronikus*
3] *információbiztonságáról,* 2022.

[8 P. W. Shor, „Polynomial-Time Algorithms for Prime Factorization and Discrete
4] Logarithms on a Quantum Computer," *Society for Industrial and Applied Mathematics,* %1. kötet41, pp. 1484-1509, 1997.

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

[8 S. Jurvetson, „How a quantum computer could break 2048-bit RSA encryption in 8
6] hours," MIT Technology Review, 30 05 2019. [Online]. Available: https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/. [Hozzáférés dátuma: 10 10 2020].

[8 J. Gosney, „8x Nvidia GTX 1080 Hashcat Benchmarks," [Online]. Available:
7] https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40. [Hozzáférés dátuma: 19 06 2022].

[8 W. Meng, L. Zhu, W. Li, J. Han és Y. Li, „Enhancing the security of FinTech applications
8] with map-based graphical password authentication," *Future Generation Computer Systems,* %1. kötet101, pp. 1018-1027, 2019.

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

[9 J. Kävrestad, J. Zaxmy és M. Nohlberg, „Analyzing the usage of character groups and
0] keyboard patterns in password creation," *Information & Computer Security,* %1. kötet28, %1. szám3, pp. 347-358, 2020.

[9 T. Hunt, „The 773 Million Record "Collection #1" Data Breach," 07 01 2019. [Online].
1] Available: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/. [Hozzáférés dátuma: 19 06 2020].

[9 A. Adams és A. M. Sasse, „Users Are Not The Enemy," *Communications of the ACM,*
2] %1. kötet1999, %1. szám42/12, pp. 40-46.

[93] B. S. Sasse, „Safe and sound: A safety-critical approach to security,” in *Proceedings of the workshop on New security paradigms*, New Mexico.

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

[95] P. Inglesant és A. Sasse, „The True Cost of Unusable Password Policies: Password Use in the Wild,” in *CHI 2010: Privacy Behaviors*, Atlanta, 2010.

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

[97] C. Hadnagy, Social Engineering - The Art of Human Hacking, John Wiley & Sons, 2010.

[98] E. E. Lastdrager, „Achieving a consensual definition of phishing,” *Crime Science,* %1. kötet3, pp. 1-10, 2014.

[99] P. Bányász, A. Tóth, S. Magyar és M. Koller, „A videókonferencia-alkalmazások biztonsági,” *Acta Humana,* %1. kötet4, p. 24, 2022.

[100] G. Kapitány, „Hekkerek támadták meg a PTE informatikai rendszereit: a Lázlap is leállt!,” *Pécs Aktuál,* 24 04 2023.

[101] H. Péter, „Ukrajna közösségi finanszírozású, katonai célokat szolgáló oktokoptereinek elemzése,” *Hadmérnök,* %1. kötetXIV, %1. szám2, pp. 34-43, 2019.

[102] The Guardian, “UK has mounted covert attacks against Russian leadership, says ex-mandarin,” The Guardian, 24 10 2020. [Online]. Available: https://www.theguardian.com/technology/2020/oct/24/uk-has-mounted-covert-attacks-against-russian-leadership-says-ex-mandarin. [Accessed 8 11 2020].

[103] R. Klima and N. Sigmon, Cryptology: Classical and Modern, Boca raton: CRC Press, 2019.

[104] Bitport, „A titkosítás tiltása veszélyes,” Bitport, 30 03 2016. [Online]. Available: https://bitport.hu/a-titkositas-tiltasa-veszelyes. [Hozzáférés dátuma: 01 10 2020].

[105] F. Piodi and I. Mombelli, “The ECHELON Affair,” Europena Parliament, Luxembourg, 2014.

[106] L. Chen, S. Jordan, L. Yi-Kai, D. Moody, R. Peralta, R. Perlner és D. Smith-Tone, „https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf,” National Institute of Standards and Technology, 2016.

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

[108] „Unit-Department for ICT and Joint Services in Higher Education and Research,” Direktoratet for IKT og fellestjenester, Norway, 2019.

[109] Australian Government Department of Home Affairs, „Security Legislation Amendment (Critical Infrastructure) Bill 2020. Explanatory Document.,” Australian Government Department of Home Affairs, Australia, 2020.

[110] F. Koczka, „Információbiztonsági teszt az Eszterházy Károly Egyetemen,” in *Hungarnet Egyesület*, Budapest, 2018.

[111] *2009/2015. (XII. 29.) Korm. határozat a nemzetbiztonsági védelem alá eső szervek és létesítmények köréről.,* 2015.

[112] K. Toubba, „Notice of Recent Security Incident,” Lastpass, Lastpass offical website, 2022.

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 egyetemek informatikai szabályzatainak dokumentumelemzése.

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	Du
Publikus szabályzatok			Nem	Nem				
Nemzetvédelmi felügyelet		Igen					Igen	
Informatikai Szabályzat (ISZ) hatály	2007	2022	2009	N/A	-	-	-	
Informatikai Biztonsági Szabályzat (IBSZ) hatály	2007	2022	**2014**	N/A	-	-	2021	
Összevont szabályzat				N/A	2019	2017	-	
Szervezeti egységek besorolása		Igen					Igen	
Rendszerelemek besorolása								
Skála elemszáma	4	4	4	4	5	Nem alkalmaz	5	
Hivatkozás	5. oldal	44.oldal	7. oldal	4. oldal	IBSZ 6-7		62.ol	I
Szakrendszerek konkrét megnevezése	Nem	Igen, IBSZ 44.o.	Igen, ISZ 6.o.	Igen, IBSZ 4.o.	Nem	Nem	Igen, 62.oldal.	
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								
Technológiai rendszerek			2	2				
Nagios Infrastruktúra menedzsment		1						
Határvédelmi rendszerek		1		1				
Könyvtári rendszer		2					2	
Riasztó- és beléptető rendszerek		3						
HPC	3			3				
E-learning rendszerek		3					1	
Hallgatói laborok			3		4			
Virtualizációs rendszerek			2	1				
Egyetemi webszerver szolgáltatás		2	2	2				
Telefonközpont			2	2	2			
Kommunikációs rendszerek	2			1	2			
Központi címtár			1	1	2			
Telefonhálózat	2		2	1	2			
Szerverek	3		3	3	3			
Authentikációs rendszerek	1	2	1	1				
Kutatói rendszerek	3	3	3	3	3		2	
Központi tárhely kiszolgálók	1	2	1	1	2			
Dokumentumkezelési/Iktatási rendszer	1	2		1	2		1	
Számítógép hálózat	2	2	2	2	1			
Middleware rendszerek (DNS)	2	2	2	2	3			
Tanulmányi rendszer	1	1	1	1	1		1	
Bér, és munkaügyi rendszer	1	1	1	1	1		2	
Központi levelező kiszolgálók	1	2	1	2	2		2	
Gazdasági/Gazdálkodási rendszer	1	2	1	1	1		2	

3. 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**

4. sz. melléklet. A Have I Been Pwned adatbázisában előforduló egyetemi jelszavak.

Darab	Név
272	Collection #1 [Collection1]
169	Data Enrichment Exposure From PDL Customer [PDL]
155	LinkedIn [LinkedIn]
137	Anti Public Combo List [AntiPublic]
112	Exploit.In [ExploitIn]
99	Verifications.io [VerificationsIO]
96	MDPI [MDPI]
90	2,844 Separate Data Breaches [2844Breaches]
71	Dropbox [Dropbox]
55	Onliner Spambot [OnlinerSpambot]
51	Covve [db8151dd]
49	Adobe [Adobe]
38	Trik Spam Botnet [TrikSpamBotnet]
34	MyHeritage [MyHeritage]
21	Exactis [Exactis]
20	Canva [Canva]
17	Kayo.moe Credential Stuffing List [KayoMoe]
16	Apollo [Apollo]
9	Netlog [Netlog]
8	MySpace [MySpace]
6	You have Been Scraped [YouveBeenScraped]
5	Last.fm [Lastfm]
3	ShareThis [ShareThis]
3	Promo [Promo]
3	MyFitnessPal [MyFitnessPal]
3	Dailymotion [Dailymotion]
3	500px [500px]
2	VK [VK]
2	Teracod [Teracod]
2	Intelimost [Intelimost]
2	Houzz [Houzz]
2	GeekedIn [GeekedIn]
2	Evite [Evite]
2	Elance [Elance]
2	000webhost [000webhost]
2	Wattpad [Wattpad]
2	River City Media Spam List [RiverCityMedia]
2	Edmodo [Edmodo]
1	Trillian [Trillian]
1	SHEIN [SHEIN]
1	NetEase [NetEase]

Darab	Név
1	mail.ru Dump [MailRu]
1	Lumin PDF [LuminPDF]
1	Kickstarter [Kickstarter]
1	iMesh [iMesh]
1	Evony [Evony]
1	Disqus [Disqus]
1	DaniWeb [DaniWeb]
1	Coupon Mom / Armor Games [CouponMomAndArmorGames]
1	Chegg [Chegg]
1	Bitly [Bitly]
1	Armor Games [ArmorGames]
1	AKP Emails [AKP]
1	LiveJournal [LiveJournal]