ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

BEDERNA ZSOLT

A kiberbiztonság az Európai Unió szabályrendszerében. A kockázatok és incidensek kezelésére vonatkozó elvárások és lehetőségek, az incidensek potenciális hatásainak elemzése

Témavezető: Prof. Dr. Rajnai Zoltán

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. március 17.

Tartalomjegyzék

1 Summary

Generally, cybersecurity capabilities are based on risk management relying on legal, social, and economic processes, to provide proper set of various security controls for defending information systems, cyber personality, and processed data. In many cases, organisations and companies must follow external obligations, especially laws, meanwhile dealing with threat actors' actions. However, despite of the preventive security controls, incidents occur occasionally, which analysis and precise understanding may refine the perceiving risks. The conducted research covers the analysis of laws regarding the European Union, human-based threat actors, and risks and incidents analysis methodologies supported by incident case studies.

Based on the literature and the usage of EURLEX, I reviewed and analysed the EU legislative and policy development regarding cybersecurity since the cyberattack campaign that took place against Estonia in 2007. Based on the current and planned legislation, such as NIS 2 directive, CER, and DORA, I analysed the related legal entities, their obligations, and the targeted capabilities. I also examined the Hungarian implementation based on the National Legislation Database. I have verified that there are organisations and for-profit companies that, although they may perform a significant social or economic function, are not subject to the cybersecurity requirements stipulated in EU legislation.

Regarding human-origin threat actors, I used the structure of the Business Model of Information Security (BMIS) to analyse their attributes. Based on the results of the characterisation, I created the "Model of the attributes and relationship of threats and stakeholders" to define interaction points between threat actors and legal entities, for which I also present "Modelling possibilities of threats and stakeholders". Comparing the first model with STIX standard, I found that the dissemination of information about incidents is an integral part of STIX and the MISP platform, although it is currently not carried out according to official requirements.

Regarding the third topic, I defined a possible methodology for the financial analysis of cybersecurity risks and especially of cybersecurity incidents. I showed that an incident can affect the targeted company, its customer, business partners, owners, the state, and even the performance of the macro economy and international finance. In order to analyse the effects on the organisation, I determined the Impact of Incidents and the Impact of Incidents metrics. Based on the investigated cases, I found that the impact of an incident and the occurrence of the incident can occur in different calendar and financial years, and the impact can occur over several years. I also hypothetically drew the conclusion that as part of the impact on the company and company owners, an incident can also affect the company's financial riskiness, and the shareholders may tend to overreact to the extent of the incidents' impacts, which require further research.

2 A kutatás előzményei

Az információs társadalom legelterjedtebb megközelítése az információs és kommunikációs technológiák (IKT) jelentőségének növekedését okozó technológiai szempontokat hangsúlyozza. Az IKT fejlődésével megteremtésre került a kibertér, amely – az információs társadalom fogalmához hasonlatosan – többféle meghatározással bír. E meghatározások azonban egységesen rávilágítanak arra az összefüggésre, hogy az IKT egyik legnagyobb jelentősége az adatok kezelésében, rendszerezésében és feldolgozásában rejlik, amely alapján információt szolgáltatnak kezelője, felhasználója számára. A technológiai fejlődéssel szoros összefüggésben áll az információs társadalom gazdasági és foglalkozási szempontjai, amelyek szerint az információs szektor és az információs jellegű munka uralja a gazdaságot. Ezeket az aspektusokat emeli ki az Európai Unió, mely az információs társadalmat az IKT alkalmazásán alapuló, az információ létrehozására, elosztására, felhasználására és újra felhasználására összpontosító tevékenységként jellemzi.

Ennek megfelelően az Európai Unió számára az egységes közös piac meghatározó jellegű, amely az elmúlt harminc év során lenyűgöző fejlődést ért el, beleértve az ipari termeléstől kezdve minden iparágat és szolgáltatási szektort, például a közműszolgáltatásokat és az állami szolgáltatásokat, amelyekben meghatározó szerep jut az IKT rendszereknek. Mindez jól jelzi, hogy az IKT manapság már nem egy specifikus ágazat, hanem minden modern innovatív gazdasági rendszer alapja. Azaz az IKT az információs társadalom zavartalan működéséhez számos nélkülözhetetlen rendszert és eszközt, kritikus infrastruktúrát és szolgáltatást biztosít. Az egyik az információs technológia (information technology – IT) megoldásokra épülve az állampolgárokat közvetlenül célzó szolgáltatásokat (pénzügyek, kommunikáció, segélyszolgálatok, egészségügy stb.) kínáló kritikus infrastruktúra rendszerek, amelyek az üzleti folyamatokat, adatgyűjtést és -feldolgozást támogatják. A másik az ipari tevékenységekhez (kitermelés, gyártás, feldolgozás stb.) kapcsolódó kritikus infrastruktúrákat megvalósító információs infrastruktúrák, amelyekben az üzemeltetési rendszerek (operational technology – OT) játszanak kulcsszerepet (pl. üzemek vízkezelése, vízgazdálkodás, műtrágya és mezőgazdasági vegyipar, vegyi üzemek, üzemi szennyvízkezelés, bányák és fémek, energiaterv és kazánvezérlés, autógyártás, kohászati feldolgozó üzemek, papírmérföldek és cellulóz, minőségellenőrzés, finomítók, élelmiszer-feldolgozás és gyógyszergyártás).

Ennek következtében a jogalkotók részéről megjelenő igény a kiberbiztonság szintjének növelése, a vonatkozó képességek fejlesztése. Másrészről az évekkel ezelőtt megjelent bűnözői réteg is felfigyelt e függőségekre és a tevékenységüket tekintve mind mennyiségében, mind minőségében fejlődött és folyamatosan fejlődik. E képességek a szervezetek és vállalatok esetében az ügymenetre és üzletmenetre gyakorolt hatás fényében eltérő jellegű és mértékű kockázatokként jelennek meg, amelyek alapján a kiberbiztonsági kontrollok kialakításra, fenntartásra és fejlesztésre kerülnek. Azonban a körültekintően kialakított működési környezetekben is olykor a kockázat incidens formájában manifesztálódik. A fenyegetésekre vonatkozó információmegosztás egyik alapfrázisa, hogy míg maga az incidens az incidensben

érintett félnek vagy feleknek egyértelműen negatív hatású esemény, addig másoknak a kibervédelmet erősítő információ.

Egy szervezet vagy vállalat kiberbiztonsági képessége (1) az architektúra, (2) a passzív védelem, (3) az aktív védelem, (4) a felderítés és (5) a visszatámadás képességekből tevődik össze, amelyeket az Emberek, a Folyamat és a Technológia tényezők együttműködése hoz létre és működtet. Az Emberek tényező az emberi erőforrásokat és az őket körülvevő biztonsági körülményeket taglalja, meghatározva belső és külső emberi erőforrások stratégia szerinti működését. A Folyamat formális és informális jelleggel meghatározott feladatokat, feladatcsoportokat foglalja magában, amelyek létfontosságú kapcsolatot biztosítanak az összes többi tényezővel. A Technológia tényező az összes olyan eszközből, alkalmazásból és infrastruktúrából áll, amelyek a folyamatok végrehajtását hatékonyabbá teszik.

A fentiekben megfogalmazott látszólagosan egyszerű összefüggéshalmaz, amely magában foglalja a változatos jogszabályi környezetet, heterogén szervezeti és vállalati megközelítéseket, üzleti hatásokat, valamint fenyegető tényezők együttesét és egymásra hatását, valójában egy komplex struktúrát takar, amely ráadásul temporálisan változó jellegű. A folyamatos változás az a tényező, amely miatt a kockázatelemzés – ha nem is folyamatosan, de rendszeres jelleggel – felülvizsgálatot és fejlesztést igényel. E tevékenységben az incidensek utólagos elemzése, a helyes következtetések levonása és a működési rendszerbe történő visszacsatolása szükséges.

Kutatásom során a fentebb megfogalmazott összefüggésekből és tényezőkből vizsgáltam (1) a kritikus (információs) infrastruktúravédelem fejlődését, (2) a kiberbiztonság fejlesztésére vonatkozóan a politikai szándék és a kapcsolódó jogalkotói megközelítés, valamint szervezetekre és a vállalkozásokra érvényes jogszabályi elvárások változását, (3) a humán eredetű fenyegető tényezőket, valamint az általuk alkalmazott technológiákat (4) a humán eredetű fenyegető tényezők és a társadalmi norma és jogszabályi elvárások szerint működő, legális szervezetek és vállalkozások közötti interakciókat, valamint (5) az incidensek pénzügyi és a működésre vonatkozó stratégiai jellegű hatásait.

A tudományos probléma megfogalmazása

Egy nemzet működése, az állampolgárainak jóléte szempontjából a nyújtott szolgáltatások, a kritikus és kritikusnak nem minősített, de gazdasági szempontból jelentős infrastruktúrák működésének folytonossága, a kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, mindezekkel összefüggésben a defenzív képességek nagy jelentőséggel bírnak.

A tényezőkre vonatkozó biztonsági kontrollok kiválasztásakor gondoskodni kell arról, hogy a befektetési és fenntartási költségek arányosak legyenek a fenyegetések által okozható károk értékével. A kockázatokkal arányos védelem indukálja az összes lehetséges fenyegetés figyelembevételét (zárt védelem), a védelmi képesség a rendszer valamennyi elemére történő kiterjedését (teljes körű védelem), valamint a dinamikusan

változó körülményekhez való alkalmazkodást (folytonos védelem). Ennek következtében a lehetséges biztonsági kontrollok közül azokat a preventív, detektív és kompenzáló kontrollokat magában foglaló kontroll-mixet kell megvalósítani, amelyek a lehetséges kontrollok halmazából nem veszélyeztetik az operatív működést és gazdasági szempontból is az optimumot valósítják meg – vagy legalábbis közelítik azt –, másfelől megakadályozzák a szervezet által nem felvállalható jellegű biztonsági incidensek bekövetkezését. A kontrollok tervezési, működési hiányosságainak vagy teljes hiányának folytán bekövetkezett biztonsági incidensek veszélyeztetik az operatív működést és a szervezet működésben érintett feleket, továbbá az IKT függőség, a fizikai tér és a kibertér egymásra hatásának nyomán különböző mértékű gazdasági, társadalmi és környezeti károkat eredményeznek.

A 2007-ben bekövetkezett Észtországot ért kibertámadási kampány kiválóan szemlélteti az incidensek hatásainak és következményeinek jellegét és volumenét. Az ismeretlen (de feltételezhetően oroszországi) támadók 2007 április 27. és 2007 május 18. között az egész nemzetre hatással lévő kibertámadási kampányt folytattak. Az összetett és hosszabb ideig kitartó kibertámadásban mindössze néhány kritikus online szolgáltatás, illetve a nem jelentős (nem kritikus) szolgáltatások (pl. kormányzati weboldalak és a híroldalak) kiesése nem okozott jelentősebb, maradandó kárt. A közvetett hatások tekintetében az észt Pénzügyminisztérium számítása szerint a tranzitszektort érintő orosz megrendelések elmaradásai az észt GDP 1-3,5 százalékos csökkenését okozta. Ugyanis Észtország tranzitszektorának jövedelme 2007-ben 40 százalékkal csökkent az előző évhez képest, mert Oroszország – a jégmentes balti kikötőktől való függése miatt – az észt fél vádjainak megfogalmazását következtében Tallinn kikötője helyett lettországi és litván kikötőket vett igénybe. 2007. július 2-án az S&P a 2006. július 17-i „A stabil" minősítésről „A negatív" besorolásra módosította Észtország megítélését. Azonban a nyilatkozatok alapján ez nem kapcsolható össze a kibertámadási kampánnyal.

Észtország, miután elemezte az incidens körülményeit, a kiberstratégiájában a stratégiai célok elérése érdekében nemzeti és vállalati szinten határozott meg megvalósítandó feladatokat. A nemzeti szinten értelmezett feladatok a kiberbiztonság, a kibervédelem és a bűnüldözés területére vonatkozó hatás elérését célozták a hírszerzés és offenzív jellegű kiberképességek fejlesztése érdekében, valamint vállalati szinten értelmezett feladatok a kiberbiztonság, a kibervédelem és a kiberrezilienca szintjének emelése érdekében kerültek meghatározásra. Továbbá a kampány során mind az Európai Unió, mind a NATO elkezdte felkutatni a lehetséges új módszereket a kiberbiztonság szintjének fokozására és a megfelelő lehetséges válaszlépéseket és szankciókat a digitális hadviselésben részt vevő államok számára. A NATO 2008 áprilisban megalapította a Kooperatív Kibervédelmi Kiválósági Központot (Cooperative Cyber Defence Centre of Excellence – CCDCoE) Tallinnban, Észtország fővárosában. A NATO CCDCoE Tallinnban történő megalapítása összefüggésben állt Észtország kiberbiztonsági kompetencia növelését célzó törekvéseivel. Valamint felmerült a Washingtoni Szerződés 5. cikkének – miszerint az egyik vagy több tagállam ellen intézett

fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek – kiterjesztése a kibertérre, azaz annak lehetősége, hogy a NATO a kiberteret is műveleti térnek tekintse. A 2016. júliusi varsói csúcstalálkozón kiberteret a műveletek egyik területének nyilvánították a felek, így a kibertér lett az ötödik műveleti tér.

Az immáron tizenhét évvel ezelőtti példa az incidensek operatív kezelésének fontosságát, valamint a következtetések helyes levonását és szükség szerint a stratégiai szintű fejlesztésekbe történő visszacsatolás indokoltságát. Az évek során pediglen számos nagy hatású incidens történt, így, bár a kiberbiztonsági incidensek (és kockázatok) kutatása nem új vagy újszerű terület, elemzésük és a vonatkozó eredmények visszacsatolása operatív, taktikai és stratégiai szinten a dinamikusan változó belső működés és a külső környezet következtében nem csak célszerű, hanem szükségszerű is.

3 Célkitűzések

A kutatásommal a teljes körű, zárt, valamint a kockázatokkal arányos védelemre vonatkozó elvárásokra fókuszálok az Európai Unió tekintetében. Kutatásommal az általános érvényű, széles körben alkalmazható megoldások azonosítását és elemzését célzom meg, kiemelt figyelmet fordítva a jogszabályi követelményeknek, a humán eredetű fenyegető tényezőknek, valamint az általuk okozott incidenseknek, melyek a jövőbeni jogszabályok kialakításában és kockázatelemzési módszertanok kialakításában is bemenetet jelenthet. Ennek érdekében a kutatás célkitűzéseit az alábbiak szerint definiálom:

KC1 Áttekinteni és elemezni a vonatkozó aktuális uniós jogszabályokat, amelyek befolyásolják a szupranacionális és nemzeti védelmi képességeket, valamint determinálják az érdekelt feleket és azok kötelezettségeit. Az érdekelt feleket a tagállami nonprofit szervezetek és profitorientált vállalkozások tekintetében vizsgálom.

KC2 Azonosítani és elemezni a fenyegetettségelemzést jellemző modern módszert vagy módszereket és a vonatkozó információ megosztásának lehetőségeit.

KC3 Meghatározni a felmerülő kiberbiztonság incidensek gazdasági összefüggéseit.

A téma kutatásának hipotézisei

A kutatásomra vonatkozóan az Európai Unió tekintetében a jogszabályi, a fenyegetettségek és a pénzügyi-gazdasági jellegű összefüggéseket vizsgálom a kiberbiztonsággal összefüggésben. A kutatást alapjaiban meghatározó hipotéziseket e három témakör kapcsán határozom meg:

H1: Léteznek olyan szervezetek, illetve profitorientált vállalkozások, amelyek bár jelentős társadalmi vagy gazdasági funkciót töltenek be, nem vonatkoznak rájuk az uniós jogszabályokban előírt kiberbiztonsági elvárások.

H2: A kiberbiztonsági incidensek menedzselésére vonatkozóan az Európai Unió jogszabályai egymással átfedésben határozzák meg a szabályokat, beleértve a hatóságok tájékoztatását is. A kiberfenyegetettségre vonatkozó információk megosztását szolgáló célrendszerek az incidensek hatósági bejelentési kötelezettség támogatására is alkalmasak.

H3: Annak meghatározása, hogy egy szervezetre egy kiberbiztonsági incidens milyen gazdasági hatással van, többféle szempont alapján is lehetséges. A hatályos jogszabályok helytelenül határozzák meg a kiberbiztonsági incidensek pénzügyi jellegű üzleti hatások vizsgálatára vonatkozó elvárásokat, amelyet a kockázatok elemzésekor figyelembe kell venni.

4 Vizsgálati módszerek

A jogszabályi, a kiberbiztonsági és a gazdasági összefüggések következtében a téma összetettsége interdiszciplináris megközelítést kíván, ennek megfelelően a kutatási módszerek területén elengedhetetlen a komplex megközelítés a kutatási témám vizsgálatakor. Felhasználva az indukció és dedukció, valamint az analízis és a szintézis módszereit, a kutatásom során a következő módszereket alkalmaztam:

KM1: A szakirodalom alapján, valamint az EURLEX, mint az uniós joganyagokhoz hivatalos online hozzáférést biztosító szolgáltatást felhasználva áttekintettem és elemeztem a 2007-ben bekövetkezett, Észtországot ért kibertámadási kampány óta eszközölt uniós jogszabályi és szakpolitikai fejlődést a kiberbiztonság tekintetében. Az aktuális és a tervezett jogszabályokat alapul véve elemeztem a jogalkotói szándék eredményeként előálló kiberbiztonsági képességeket, a jogalanyok körét és kötelezettségeiket. A magyarországi vonatkozású összefüggéseket a Nemzeti Jogszabálytár adatbázisa alapján vizsgáltam.

KM2: Szakirodalmi összefüggéseket felhasználva azonosítottam és rendszereztem a szervezeti szintű kiberbiztonsági, kiváltképp a humán eredetű fenyegető tényezők támadói képességeit az információbiztonság üzleti modell modellje (BMIS) modell szerinti struktúra alapján. Az iparági megoldások és szabványok alapján vizsgáltam a humán eredetű fenyegető tényezők tevékenységeiről szóló információk megosztásának módszereit.

KM3: A szakirodalmat felhasználva meghatároztam a kiberbiztonsági incidensek pénzügyi-elemzési lehetőségeit és a kapcsolódó módszertani elemeket. Szekunder kutatást végezve konkrét eseteket (incidenseket) elemeztem, amelyek során alkalmaztam a megalkotott elemzési módszertant, vizsgálva annak megfelelőségét.

5 Új tudományos eredmények

Kutatásom során a vonatkozó stratégiai, technológiai és pénzügyi összefüggéseket vizsgáltam, amely eredményeként a doktori képzés folyamán tizenhét tudományos besorolású publikációt jegyeztem.

Az Európai Unió kiberbiztonságának vizsgálatához a jogszabályi, a fenyegetettségek és a pénzügyi-gazdasági jellegű összefüggések elemzését célzó hipotézisre vonatkozóan az alábbi téziseket fogalmazom meg, a H2 és H3 hipotéziseket összetett jellegükből kifolyólag ketté bontva kezelve:

T1: Igazoltam, hogy léteznek olyan szervezetek, illetve profitorientált vállalkozások, amelyek bár jelentős társadalmi vagy gazdasági funkciót töltenek be, nem vonatkoznak rájuk az uniós jogszabályokban előírt kiberbiztonsági elvárások. [BZs2] [BZs3] [BZs4] [BZs5] [BZs6] [BZs7]

A KC1 kutatási céllal összefüggésben áttekintettem a jelentős, Észtországot 2007-ben ért kibertámadási kampány utáni időszakra vonatkozóan az uniós politikai elköteleződés fejlődését, illetve az ennek következtében manifesztálódott jogszabályokat. Az aktuális uniós jogszabályok egyértelműen befolyásolják a szupranacionális és nemzeti kiberbiztonsági és kibervédelmi képességeket, valamint determinálják az érdekelt feleket és azok kötelezettségeit. Ez a meghatározás a NIS 2 irányelv által „kellő mértékben" bonyolult módon valósult meg, alapozva a hatályba tartozás jellegére (ágazat/alágazat, a szervezet mérete, a kockázati besorolás stb. függvénye) vagy a joghatóság megvalósítására. A NIS 2 irányelv megteremti a lehetőséget a tagállamok számára, hogy a gazdasági szempontból fontos szereplőket az irányelv hatálya alá helyezze. Azonban az irányelv nem határozza meg a vizsgálandó gazdasági szempontok jellegét, így a tagállamokra hagyja a módszertan meghatározását (ezzel fokozva a tagállami eltérések mértékét). A jogalanyok számára a NIS 2 irányelv és további jogszabályok (pl. DORA) tételesen előírják egyes kiberbiztonsági kontrollok kialakítását és fenntartását. A tagállami jogszabályok továbbá kijelölik a felügyeleti hatóságot, illetve hatóságokat és az uniós jogszabályokra alapulva meghatározzák a kapcsolódó feladatokat és felügyeleti lehetőségeket, amely a bírságolást is magában foglalja. Mindez azt jelenti, hogy a szervezeti és vállalati szintű szereplők számára jelentős elvárások jelentkeznek irányukban.

T2.1: Az aktuális jogszabályok elemzése alapján **igazoltam, hogy a kiberbiztonsági incidensek menedzselése kapcsán az Európai Unió hatályos jogszabályai átfedésben határozzák meg a vonatkozó szabályokat.** [BZs1] [BZs2] [BZs3] [BZs6]

T2.2: Az elemzés során megállapítottam, hogy a kiberfenyegetettségre vonatkozó információk megosztását szolgáló célrendszerek az incidensek hatósági bejelentési kötelezettség támogatására is alkalmasak. [BZs1] [BZs7] [BZs8] [BZs9]

hA KC2 kutatási céllal összefüggésben azonosítottam azokat a megközelítéseket, amelyek elősegíthetik a fenyegetések szisztematikus azonosítását és elemzését. Ide soroltam például az általános kockázati kereteket és módszereket (NIST SP 800-39, ISO/IEC 27005), (2) a fenyegetés modellezési keretrendszereket (Attack tree modelling) és az eszközök, taktikák, folyamatok (TTP) alapú modellezéseket (MITRE ATT&CK, MITRE CAPEC). Az elemzés részeként a kibertérbeli műveletekre

és képességekre alapozva azonosítottam és analizáltam a kiberfenyegetések jellemzőit, illetve elemeztem a kiberfenyegetésekhez kapcsolódó TTP és IoC információk megosztási lehetőségeit. A rendszerezett információkat felhasználva megalkottam „A fenyegetések és az érintettek attribútumainak és kapcsolatának modelljét", illetve arra alapozva vizualizáltam „A fenyegetések és az érintettek modellezési lehetőségeit".

„A fenyegetések és az érintettek attribútumainak és kapcsolatának modelljét" felhasználva vizsgáltam a STIX 2.1 képességeivel, amelyet az Európai Unióban megvalósított és támogatott MISP platform is implementál. Megállapítottam, hogy a STIX, valamint a MISP platform szerves részét képezi az incidensekről szóló információk disszeminációja is. Ugyanakkor az incidensek kezelése jelenleg nem a hatósági bejelentések szerint valósul meg. Azonban ahogy a MISP platform a pénzügyi csalásokkal kapcsolatos információk és a terrorizmusellenes információk megosztására alkalmassá vált, úgy a hatósági bejelentések kezelésére is képessé tehető.

T3.1: Igazoltam, hogy egy szervezet esetén egy kiberbiztonsági incidens gazdasági hatásának vizsgálata többféle szempont alapján is lehetséges. [BZs10] [BZs11] [BZs12] [BZs13] [BZs14] [BZs15]

A KC3 kutatási céllal összefüggésben meghatároztam a kiberbiztonsági incidensek pénzügyi elemzésének egy lehetséges módszertanát, amely alapján megmutattam, hogy egy kiberbiztonsági incidens vállalatra (és a vállalat kockázatosságának megítélésére), ügyfeleire (beleértve a magánszemélyeket), a vállalat üzleti partnereire, tulajdonosaira, az államra és összességében a makrogazdaság teljesítményére és a nemzetközi pénzügyekre is hatással lehet. A szervezetre gyakorolt hatások elemzéséhez meghatároztam az $Incidens\ hatása$ és az $Incidensek\ hatása$ mérőszámokat. A vizsgált esetek alapján megállapítottam, hogy egy incidens hatása és az incidens bekövetkezte eltérő naptári és pénzügyi évben is megvalósulhat, a hatás több éven át is jelentkezhet. Továbbá hipotetikus jelleggel azt a következtetést vontam le, hogy a vállalatra és vállalattulajdonosokra gyakorolt hatás részeként egy incidens a vállalat kockázatosságára is hatással lehet, valamint a részvényesek, mint vállalattulajdonosok, hajlamosak lehetnek a kiberbiztonsági incidensek által okozott hatás mértékét túlreagálni. Mindezek tényszerű megállapítása további kutatást igényel.

T3.2: Az aktuális jogszabályok elemzését alapul véve **a Magyarországon hatályos jogszabályokra korlátozódva igazoltam, hogy a hatályos jogszabályok helytelenül határozzák meg a kiberbiztonsági incidensek pénzügyi jellegű üzleti hatások vizsgálatára vonatkozó elvárásokat, amelyet a kockázatok elemzésekor figyelembe kell venni.** [BZs10] [BZs11] [BZs12] [BZs13] [BZs14]

6 Az eredmények hasznosítási lehetősége

A kutatásom eredményeképp a következő ajánlásokat fogalmaztam meg:

A1.1: Javaslom a későbbiekben a NIS 2 irányelv utódja esetén („NIS 3 irányelv") a kiberbiztonságban érintettek körének további szélesítését.

A1.2: Javaslom a gazdasági érintettség alapján történő kijelölés feltételeinek szabályozását egy Európai Unióban egységes szempontrendszer alkalmazása mellett.

A2: Javaslom az Európai Unió jogszabályaiban a hatósági incidensbejelentési kötelezettség szabályozásának felülvizsgálatát, valamint az incidensbejelentési kötelezettség technikai támogatásának (pl. MISP platform alapon történő) kialakítását.

A3.1: Javaslom az üzleti hatások vizsgálati szempontjait az Európai Unió egészére vonatkozóan egységes jelleggel kezelését, minimálisan vizsgálandó szempontok és értékintervallumok megadása mellett. Ezzel összefüggésben az incidensek pénzügyi hatásainak időbelisége, a több évben jelentkező negatív pénzáramok, a bekövetkezés és a jelentkező hatás közötti időbeli differencia kezelése elengedhetetlen.

A3.2: Javaslom a vállalatok kockázatosságának (beta) többfaktor modell alapú számítása során a kiberbiztonsági és adatvédelmi incidensek hatásainak figyelembevételét. E javaslat egyben meghatározza a későbbi kutatásaim alapjait.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] Karvalics L., 'Információs társadalom – mi az? Egy kifejezés jelentése, története és fogalomkörnyezete', in Az információs társadalom. Az elmélettől a politikai gyakorlatig, L. Pintér, Ed., Budapest: Gondolat Kiadó, 2007, pp. 29–46.

[2] F. Webster, 'What information society?', Information Society, vol. 10, no. 1, pp. 1–23, 1994, doi: 10.1080/01972243.1994.9960154.

[3] R. Kurzweil, 'The Law of Accelerating Returns', in Alan Turing: Life and Legacy of a Great Thinker, C. Teuscher, Ed., Berlin, Heidelberg: Springer, 2004, pp. 381–416. doi: 10.1007/978-3-662-05642-4_16.

[4] Molnár Sz., Kollányi B. és Székely L., 'Társadalmi hálózatok, hálózati társadalom', in Az információs társadalom. Az elmélettől a politikai gyakorlatig, Pintér L., Ed., Budapest: Gondolat Kiadó, 2007, pp. 64–81.

[5] D. Bell, 'The Coming of the Post-Industrial Society', Educ Forum, vol. 40, no. 4, pp. 574–579, 1976, doi: 10.1080/00131727609336501.

[6] European Union, ‘Information society’. Hozzáférés: 2020.12.09. [Online]. Elérhető: https://eur-lex.europa.eu/summary/glossary/information_society.html

[7] S. Micossi, ‘30 Years of the Single European Market’, Bruges European Economic Policy Briefings, vol. 41, pp. 1–36, 2016, Hozzáférés: 2023.02.26. [Online]. Elérhető: https://www.coleurope.eu/sites/default/files/research-paper/beep41_0.pdf

[8] Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Európai digitális egységes piaci stratégia. 2015. Hozzáférés: 2022.10.16. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52015DC0192

[9] Munk S., ‘A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései’, Hadtudomány, vol. 28, no. 1, pp. 113–131, 2018, doi: 10.17047/HADTUD.2018.28.1.113.

[10] ENISA, ‘ENISA overview of cybersecurity and related terminology’. Hozzáférés: 2019.02.17. [Online]. Elérhető: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[11] D. T. Kuehl, ‘From Cyberspace to Cyberpower: Defining the Problem’, in Cyberpower and National Security, Potomac Books and National Defense University, 2009, pp. 24–42. doi: 10.2307/j.ctt1djmhj1.7.

[12] Kovács L., A kibertér védelme. Budapest: Dialóg Campus Kiadó, 2018. [Online]. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/Kovács László.pdf

[13] Haig Zs., Információs műveletek a kibertérben. Budapest: Dialóg Campus Kiadó, 2018. Hozzáférés: 2023.02.26. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf

[14] Munk S., ‘Információs színtér, információs környezet, információs infrastruktúra’, Nemzetvédelmi egyetemi közlemények, vol. VI, no. 2, pp. 133–154, 2002, doi: 20.500.12944/1083.

[15] Berzsenyi D., ‘Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában’, Nemzet és Biztonság, no. 3, pp. 69–79, 2017, Hozzáférés: 2022.12.04. [Online]. Elérhető: https://folyoirat.ludovika.hu/index.php/neb/article/view/3721/2999

[16] Szörényi A., ‘A nem-állami szereplők befolyásának növekedése a nemzetközi kapcsolatok különböző területein’, Corvinus University of Budapest, Budapest, 2014. doi: 10.14267/phd.2014080.

[17] Haig Zs., Hajnal B., Kovács L., Muha L. és Sik Z. N., A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Advisory Kft., 2009. Hozzáférés: 2022.07.23. [Online]. Elérhető: https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf

[18] Haig Zs. és Kovács L., Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Nemzeti Közszolgálati Egyetem, 2012. [Online]. Elérhető: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf

[19] M. Ryba, 'The role of ICT components in the functioning of critical infrastructure', in Critical Infrastructure Security - the ICT Dimension, J. Świątkowska, Ed., Kraków: The Kosciuszko Institute, 2014, pp. 59–62.

[20] S. Kumar, A. K. Singh és M. A. Kalam, 'Intelligent electronic device functionality and interfacing: An experimental examination of smart grid', International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special Issue 11, 2019, doi: 10.35940/ijrte.B1523.0982S1119.

[21] Y. Maleh, 'IT/OT convergence and cyber security', Computer Fraud & Security, vol. 2021, no. 12, pp. 13–16, 2021, doi: https://doi.org/10.1016/S1361-3723(21)00129-9.

[22] Muha L. és Krasznay Cs., Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem, 2018. Hozzáférés: 2023.02.26. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf

[23] M. Dunn Cavelty és M. Suter, 'The Art of CIIP Strategy: Tacking Stock of Content and Processes', in Critical Infrastructure Protection, J. Lopez, R. Setola, and S. D. Wolthusen, Eds., Springer, 2012, pp. 15–38. doi: 10.1007/978-3-642-28920-0_2.

[24] A. Sarri és K. Moulinos, Stocktaking, Analysis and Recommendations on the Protection of CIIs. ENISA, 2016. doi: 10.2824/534303.

[25] D. Štrucl, 'Comparative study on the cyber defence of NATO Member States', NATO CCDCOE. Hozzáférés: 2022.07.27. [Online]. Elérhető: https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

[26] A. Ekelhart, S. Fenz, M. D. Klemen és E. R. Weippl, 'Security ontology: Simulating threats to corporate assets', in Information Systems Security, A. Bagchi and V. Atluri, Eds., Kolkata, India: Springer, 2006. doi: 10.1007/11961635_17.

[27] R. von Solms és J. van Niekerk, ‘From information security to cyber security’, Comput Secur, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[28] Európai Tanács és Az Európai Unió Tanácsa, ‘Információvédelem’. Hozzáférés: 2022.08.14. [Online]. Elérhető: https://www.consilium.europa.eu/hu/general-secretariat/corporate-policies/classified-information/information-assurance/

[29] International Organization for Standardization, ISO/IEC 27000:2018, 5th ed. 2018.

[30] Európai Központi Bank, ‘What is cyber resilience?’ Hozzáférés: 2022.08.14. [Online]. Elérhető: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.hu.html

[31] International Organization for Standardization, ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements. 2019.

[32] T. Bonnyai, ‘Kritikus infrastruktúrák védelme’, in Kritikus információs infrastruktúrák védelme, V. Deák, Ed., Budapest: Nemzeti Közszolgálati Egyetem, 2019, pp. 56–83.

[33] L. Robert M., ‘The Sliding Scale of Cyber Security’, SANS Institute. Hozzáférés: 2022.08.16. [Online]. Elérhető: https://sansorg.egnyte.com/dl/GJEumszLQX

[34] R. M. von Roessing, The Business Model for Information Security. ISACA, 2010.

[35] International Organization for Standardization, ‘ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements’, 2013.

[36] International Organization for Standardization, ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. 2022.

[37] National Institute of Standards and Technology, ‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1’, Gaithersburg, MD, 2018. doi: 10.6028/NIST.CSWP.04162018.

[38] National Institute of Standards and Technology, ‘NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations’, Gaithersburg, MD, 2020. doi: 10.6028/NIST.SP.800-53r5.

[39] Wimmer Á., ‘Üzleti teljesítménymérés az értékteremtés szolgálatában’, Vezetéstudomány - Budapest Management Review, vol. 35, no. 9, pp. 2–11, 2004.

[40] National Institute of Standards and Technology, ‘NIST Special Publication 800-207 - Zero Trust Architecture’, 2020. doi: https://doi.org/10.6028/NIST.SP.800-207.

[41] International Organization for Standardization, ‘ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model’. 2022.

[42] A Bizottság (EU) 2024/482 végrehajtási rendelete a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról. 2024. Hozzáférés: 2024.03.03. [Online]. Elérhető: http://data.europa.eu/eli/reg_impl/2024/482/oj

[43] OWASP, ‘Application Security Verification Standard 4.0.3’. Hozzáférés: 2022.08.27. [Online]. Elérhető: https://raw.githubusercontent.com/OWASP/ASVS/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

[44] American Psychological Association, ‘APA Dictionary of Psychology’. Hozzáférés: 2022.09.15. [Online]. Elérhető: https://dictionary.apa.org

[45] ISACA Magyarországi Egyesület, ISACA magyar szakkifejezés-gyűjtemény. 2014. Hozzáférés: 2023.02.26. [Online]. Elérhető: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-hungarian_1213.pdf

[46] A. Tversky és D. Kahneman, ‘The framing of decisions and the psychology of choice’, Science (1979), vol. 211, no. 4481, pp. 453–458, 1981, doi: 10.1126/science.7455683.

[47] D. Kahneman, Thinking, Fast and Slow. New York: Farrar, Straus and Giroux, 2011.

[48] A. Chariri, ‘Cognitive Limitations and Decision Making’, Jurnal Bisnis Strategi, vol. 3, pp. 21–28, 1999.

[49] Barabási A. L., The Formula: The Universal Laws of Success. New York: Little, Brown and Company, 2018.

[50] A. Anastasios, ‘The 2019 SANS Security Awareness Report: Awareness Training Is Rising’. Hozzáférés: 27, 2022.02.27. [Online]. Elérhető: https://www.tripwire.com/state-of-security/sans-security-awareness-training-rising

[51] L. Spitzner, ‘Applying Security Awareness to the Cyber Kill Chain | SANS Security Awareness’, SANS Institute. Hozzáférés: 2020.02.01. [Online]. Elérhető: https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

[52] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. 2013. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-50-00-00

[53] Michelberger P. és Horváth Z., 'Biztonságorientált folyamatmenedzsment', International Journal of Engineering and Management Sciences, vol. 2, no. 4, 2017, doi: 10.21791/ijems.2017.4.28.

[54] A. Schmidt, 'The Estonian Cyberattacks', in A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, J. Healey, Ed., Vienna: Cyber Conflict Studies Association, 2013, pp. 174–193.

[55] D. K. Bohl, B. B. Hughes, M. T. Irfan, E. S. Margolese-Malin és J. R. Solórzano, 'Cyber Benefits and Risks: Quantitatively Understanding and Forecasting the Balance', University of Denver, Zurich Insurance and Atlantic Council, 2015. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://korbel.du.edu/pardee/resources/cyber-benefits-and-risks-quantitatively-understanding-and-forecasting-balance

[56] Trading Economics, 'Estonia - Credit Rating'. Hozzáférés: 2020.10.15. [Online]. Elérhető: https://tradingeconomics.com/estonia/rating

[57] The Baltic Times, 'S&P's slams Estonia with negative outlooks', 2007.07.04. [Online]. Elérhető: https://www.baltictimes.com/news/articles/18203/

[58] Republic of Estonia, 'Estonian National Strategic Reference Framework 2007-2013'. Hozzáférés: 2023.02.16. [Online]. Elérhető: https://vana.struktuurifondid.ee/sites/default/files/estonian_national_strategic_reference_framework_2007-2013.pdf

[59] Ministry of Defence - Estonia, 'Cyber Security Strategy'. [Online]. Elérhető: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en

[60] S. Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses', Journal of Strategic Security, vol. 4, no. 2, pp. 49–60, 2011, doi: 10.5038/1944-0472.4.2.3.

[61] Paráda I., 'A NATO kibervédelmi irányelveinek fejlődése', Honvédségi Szemle – Hungarian Defence Review, vol. 146, no. 3, pp. 3–13, 2018, Hozzáférés: 2023.02.27. [Online]. Elérhető: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/373

[62] Európai Tanács Főtitkársága, Európai biztonsági stratégia - Biztonságos Európa egy jobb világban. Luxembourg: Az Európai Unió Kiadóhivatala, 2009. doi: 10.2860/15719.

[63] Ármás J. és Nagy L., 'Hibrid hadviselés: a befolyás megtartásának-megszerzésének új eszköze a posztszovjet térségben?', Honvédségi Szemle – Hungarian Defence Review, vol. 148, no. 2, pp. 74–88, 2020, doi: 10.35926/hsz.2020.2.8.

[64] Az Európai Parlament és a Tanács 1007/2008/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az Ügynökség megbízatási ideje tekintetében történő módosításáról. 2008. Hozzáférés: 2022.10.05. [Online]. Elérhető: http://data.europa.eu/eli/reg/2008/1007/oj

[65] Az Európai Közösségek Bizottsága, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről. 2009. Hozzáférés: 2022.10.07. [Online]. Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:hu:PDF

[66] Európai Bizottság, EURÓPA 2020 Az intelligens, fenntartható és inkluzív növekedés stratégiája. 2010. Hozzáférés: 2022.10.07. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/ALL/?uri=CELEX%3A52010DC2020

[67] Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az európai digitális menetrend. 2010. Hozzáférés: 2022.10.07. [Online]. Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:HU:PDF

[68] Megállapodás az Európai Parlament, az Európai Tanács, az Európai Unió Tanácsa, az Európai Bizottság, az Európai Unió Bírósága, az Európai Központi Bank, az Európai Számvevőszék, az Európai Külügyi Szolgálat, az Európai Gazdasági és Szociális Bizottság, a Régiók Európai Bizottsága és az Európai Beruházási Bank között az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) szervezetéről és működéséről. 2018. Hozzáférés: 2022.10.08. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:32018Q0113(01)

[69] Az Európai Parlament és a Tanács 580/2011/EU rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az ügynökség megbízatási ideje tekintetében történő módosításáról. 2011. Hozzáférés: 2022.10.05. [Online]. Elérhető: http://data.europa.eu/eli/reg/2011/580/oj

[70] Az Európai Parlament és a Tanács 526/2013/EU rendelete az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről. 2013. Hozzáférés: 2022.10.08. [Online]. Elérhető: http://data.europa.eu/eli/reg/2013/526/oj

[71] Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. 2013. Hozzáférés: 2022.10.08. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52013JC0001

[72] L. Dupré, EP3R 2010-2013 - Four Years of Pan-European Public Private Cooperation. ENISA, 2014. doi: 10.2824/565581.

[73] Európai Unió, 'Számítástechnikai Bűnözés Elleni Európai Központ az Europolon belül'. Hozzáférés: 2022.10.10. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:230806_1

[74] Európai Bizottság, A Bizottság közleménye a Tanácsnak és az Európai Parlamentnek - Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása. 2012. Hozzáférés: 2022.10.10. [Online]. Elérhető: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:HU:PDF

[75] Az Európai Unió Tanácsa, Uniós kibervédelmi szakpolitikai keret. 2014. [Online]. Elérhető: http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/hu/pdf

[76] Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának - Az európai biztonsági stratégia. 2015. Hozzáférés: 2022.10.09. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52015DC0185

[77] Európai Külügyi Szolgálat, Közös jövőkép, közös fellépés: Erősebb Európa - Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan. Luxembourg: Az Európai Unió Kiadóhivatala, 2016. doi: 10.2871/695883.

[78] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. 2016. Hozzáférés: 2022.10.08. [Online]. Elérhető: http://data.europa.eu/eli/dir/2016/1148/oj

[79] Európai Bizottság, Közös közlemény az Európai Parlamentnek és a Tanácsnak - Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése. 2017. Hozzáférés: 2022.10.10. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450

[80] D. E. Sanger, 'As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy', The New York Times, 2016.06.17. [Online]. Elérhető: https://www.nytimes.com/2016/06/17/world/europe/nato-russia-cyberwarfare.html

[81] Molnár A., 'Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége', in Kritikus információs infrastruktúrák védelme, Deák V., Ed., Budapest: Nemzeti Közszolgálati Egyetem, 2019, pp. 35–55.

[82] Az Európai Unió Tanácsa, Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat). 2018. [Online]. Elérhető: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

[83] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). 2019. Hozzáférés: 2022.10.12. [Online]. Elérhető: http://data.europa.eu/eli/reg/2019/881/oj

[84] A Tanács (EU) 2019/796 rendelete az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. 2019. Hozzáférés: 2022.10.12. [Online]. Elérhető: http://data.europa.eu/eli/reg/2019/796/oj

[85] Az Európai Unió Tanácsa, 'Az első uniós szankciók kibertámadások elkövetőivel szemben'. Hozzáférés: 2022.10.12. [Online]. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/pdf

[86] Európai Tanács, 'A Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról'. Hozzáférés: 2022.10.13. [Online]. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/pdf

[87] Közös közlemény az Európai Parlamentnek és a Tanácsnak - Az EU kiberbiztonsági stratégiája a digitális évtizedre. 2020. Hozzáférés: 2022.10.14. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX:52020JC0018

[88] Az Európai Parlament és a Tanács (EU) 2021/887 rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról. 2021. Hozzáférés: 2022.10.14. [Online]. Elérhető: http://data.europa.eu/eli/reg/2021/887/oj

[89] Európai Bizottság, Javaslat – Az Európai Parlament és a Tanács irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről. 2020. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=COM:2020:823:FIN

[90] Az Európai Unió Tanácsa, Javaslat – Az Európai Parlament és a Tanács irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről – Általános megközelítés. 2021. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/hu/pdf

[91] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). 2022. Hozzáférés: 2023.01.12. [Online]. Elérhető: http://data.europa.eu/eli/dir/2022/2555/oj

[92] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának - Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja. 2021. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52021DC0118

[93] S. Backman, 'Risk vs. threat-based cybersecurity: the case of the EU', European Security, vol. 32, no. 1, pp. 85–103, 2022.05., doi: 10.1080/09662839.2022.2069464.

[94] A Tanács 2008/114/EK irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. 2008. Hozzáférés: 2022.09.30. [Online]. Elérhető: http://data.europa.eu/eli/dir/2008/114/oj

[95] Európai Bizottság, Javaslat Az Európai Parlament és a Tanács irányelve a kritikus fontosságú szervezetek rezilienciájáról. 2020. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020PC0829

[96] Európai Bizottság, Javaslat – Az Európai Parlament és a Tanács rendelete a pénzügyi ágazat digitális működési rezilienciájáról és az 1060/2009/EK rendelet, a 648/2012/EU rendelet, a 600/2014/EU rendelet, valamint a 909/2014/EU rendelet módosításáról. 2020. Hozzáférés: 2022.10.15. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020PC0595

[97] Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről. 2014. Hozzáférés: 2022.11.02. [Online]. Elérhető: http://data.europa.eu/eli/reg/2014/910/oj

[98] Európai Bizottság, Javaslat az Európai Parlament és a Tanács rendelete a 910/2014/EU rendeletnek az európai digitális személyazonosság keretének létrehozása tekintetében történő módosításáról. 2021. Hozzáférés: 2022.10.17. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0281

[99] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). 2016. Hozzáférés: 2022.09.16. [Online]. Elérhető: http://data.europa.eu/eli/reg/2016/679/oj

[100] Az Európai Parlament és a Tanács 575/2013/EU rendelete a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról. 2013. Hozzáférés: 2024.05.09. [Online]. Elérhető: http://data.europa.eu/eli/reg/2013/575/oj

[101] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve a belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről. 2015. Hozzáférés: 2022.11.02. [Online]. Elérhető: http://data.europa.eu/eli/dir/2015/2366/oj

[102] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról. 2013. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-237-00-00

[103] 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről. 2015. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-42-20-22

[104] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2012-166-00-00

[105] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól. 2015. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-222-00-00

[106] 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól. 2023. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2023-103-00-00

[107] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról jogszabály tartalmazza. 2011. Hozzáférés: 2023.03.27. [Online]. Elérhető: https://njt.hu/jogszabaly/2011-112-00-00

[108] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről. 2023. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2023-23-00-00

[109] 2013. évi CCXXXV. törvény az egyes fizetési szolgáltatókról. 2013. Hozzáférés: 2024.03.10. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-235-00-00

[110] Centre for Cybersecurity Belgium, 'The NIS 2 Directive: what does it mean for my organization?' Hozzáférés: 2024.03.12. [Online]. Elérhető: https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

[111] Európai Parlament, Jelentés a 2016–2020-as időszakra vonatkozó uniós e-kormányzati cselekvési tervről. 2017. Hozzáférés: 2022.10.12. [Online]. Elérhető: https://www.europarl.europa.eu/doceo/document/A-8-2017-0178_HU.pdf

[112] Anomali, ‘APT28 Timeline of Malicious Activity’. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.anomali.com/blog/a-timeline-of-apt28-activity

[113] J. Orr, ‘Incident Of The Week: 4 Million Bulgarian Citizens Affected By Tax Agency Data Breach’, CYBER Security Hub, 2019.07.26. [Online]. Elérhető: https://www.cshub.com/attacks/articles/incident-of-the-week-4-million-bulgarian-citizens-affected-by-tax-agency-data-breach

[114] A Tanács 904/2010/EU rendelete a hozzáadottérték-adó területén történő közigazgatási együttműködésről és csalás elleni küzdelemről (átdolgozás). 2010. Hozzáférés: 2022.10.11. [Online]. Elérhető: http://data.europa.eu/eli/reg/2010/904/oj

[115] 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról. 2015. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-187-20-22

[116] 2013. évi CXXXIX. törvény a Magyar Nemzeti Bankról. 2013. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://njt.hu/jogszabaly/2013-139-00-00.62

[117] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről. 2018. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://njt.hu/jogszabaly/2015-41-20-0A

[118] National Institute of Standards and Technology, NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. 2013. doi: 10.6028/NIST.SP.800-53Ar4.

[119] Miniszterelnöki Kabinetirodát vezető miniszter, A Miniszterelnöki Kabinetirodát vezető miniszter ---------- MK rendelete a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. 2024. Hozzáférés: 2024.03.11. [Online]. Elérhető: https://cdn.kormany.hu/uploads/document/2/25/25e/25e5d729f900acc21babb2d22da8cc03aa810a71.pdf

[120] Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81. Hozzáférés: 2022.10.29. [Online]. Elérhető: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.del.consiglio.dei.ministri:2021-04-14;81!vig=2021-06-30

[121] S. Schmitz-Berndt and P. G. Chiara, ‘One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive’, International Cybersecurity Law Review, vol. 3, pp. 289–311, 2022. doi: 10.1365/s43439-022-00058-7.

[122] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist. Hozzáférés: 2022.10.29. [Online]. Elérhető: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[123] ENISA, ‘Best practices for cyber crisis management’, 2024. doi: 10.2824/767828.

[124] J. De Muynck and S. Portesi, ‘Strategies for Incident Response and Cyber Crisis Cooperation’, 2016. doi: 10.2824/967546.

[125] NIS Cooperation Group, ‘Synergies in Cybersecurity Incident Reporting’. 2020.12. Hozzáférés: 2023.01.19. [Online]. Elérhető: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72147

[126] C. Lambrinoudakis et al., Interoperable EU risk management framework. ENISA, 2022. doi: 10.2824/07253.

[127] D. J. Bodeau, C. D. McCollum, and D. B. Fox, ‘Cyber Threat Modeling: Survey, Assessment, and Representative Framework’, 2018.04. Hozzáférés: 2022.11.23. [Online]. Elérhető: https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf

[128] Joint Task Force Transformation Initiative, NIST SP 800-39 Managing Information Security Risk. National Institute of Standards and Technology, 2011. doi: 10.6028/NIST.SP.800-39.

[129] ‘ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks’, 2022.

[130] National Institute of Standards and Technology, NIST SP 800-30 R1 - Guide for conducting risk assessments. 2012. doi: 10.6028/NIST.SP.800-30r1.

[131] Office of the Director of National Intelligence, ‘Building Blocks of Cyber Intelligence’. Hozzáférés: 2023.02.23. [Online]. Elérhető: https://www.dni.gov/index.php/cyber-threat-framework

[132] B. Schneier, ‘Attack trees: Modeling security threats’, Dr. Dobb’s Journal, 1999.12., Hozzáférés: 2022.11.23. [Online]. Elérhető: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

[133] L. Zhang, A. Taal, R. Cushing, C. de Laat, and P. Grosso, ‘A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces’, Int J Inf Secur, vol. 21, pp. 509–525, 2021, doi: 10.1007/s10207-021-00566-3.

[134] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, 'MITRE ATT&CK: Design and Philosophy'. Hozzáférés: 2021.12.11. [Online]. Elérhető: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[135] MITRE, 'Common Attack Pattern Enumeration and Classification'. Hozzáférés: 2022.11.24. [Online]. Elérhető: https://capec.mitre.org/index.html

[136] T. Ucedavélez and M. M. Morana, Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons, Inc, 2015. doi: 10.1002/9781118988374.

[137] ENISA, 'Cyber Security and Resilience of smart cars', 2016. doi: 10.2824/87614.

[138] ENISA, 'Glossary'. Hozzáférés: 2022.11.29. [Online]. Elérhető: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary

[139] National Institute of Standards and Technology, FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems. 2006, doi: 10.6028/NIST.FIPS.200.

[140] ENISA, 'Threat Taxonomy'. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[141] NIS Cooperation Group, 'Cybersecurity Incident Taxonomy'. 2018. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

[142] M. Theocharidou, A. Malatras, I. Lella, and E. Tsekmezoglou, 'Threat Landscape 2021'. ENISA, 2021. doi: 10.2824/324797.

[143] G. Alblas és E. Wijsman, Organisational Behaviour, 2nd Edition. London: Routledge, 2021. doi: 10.4324/9781003194736.

[144] D. Gervasi, G. Faldetta, M. M. Pellegrini és J. Maley, 'Reciprocity in organizational behavior studies: A systematic literature review of contents, types, and directions', European Management Journal, vol. 40, no. 3, pp. 441–457, 2022, doi: 10.1016/j.emj.2021.07.008.

[145] R. A. Gandhi, Anup Sharma, W. Mahoney, W. Sousan, Q. Zhu és P. A. Laplante, 'Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political', IEEE Technology and Society Magazine, vol. 30, no. 1, pp. 28–38, 2011, doi: 10.1109/MTS.2011.940293.

[146] Verizon, ‘Data Breach Investigations Report 2020’. Hozzáférés: 2021.03.23. [Online]. Elérhető: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[147] M. Lee, ‘Russia Is Losing a War Against Hackers Stealing Huge Amounts of Data’, The Intercept. Hozzáférés: 2022.12.09. [Online]. Elérhető: https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/

[148] W. Chang, A. Mohaisen, A. Wang, and S. Chen, ‘Measuring botnets in the wild: Some new trends’, in ASIACCS 2015 - Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015, pp. 645–650. doi: 10.1145/2714576.2714637.

[149] C. Cimpanu, ‘Hacker takes over 29 IoT botnets’, ZDNet. Hozzáférés: 2020.03.10. [Online]. Elérhető: https://www.zdnet.com/article/hacker-takes-over-29-iot-botnets/

[150] IBM Corporation, ‘The inside story on botnets’. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://securityintelligence.com/inside-story-on-botnets/

[151] K.-L. Hui and J. Zhou, ‘The Economics of Hacking’, Oxford Research Encyclopedia of Business and Management, 2020, doi: 10.2139/ssrn.3695381.

[152] D. Manky, ‘Cybercrime as a service: A very modern business’, Computer Fraud and Security, vol. 2013, no. 6, pp. 9–13, 2013, doi: 10.1016/S1361-3723(13)70053-8.

[153] Szőr P., The Art of Computer Virus Research and Defense. New Jersey: Pearson Education (US), 2005.

[154] C. G. J. Putman, A. Abhishta és L. J. M. Nieuwenhuis, ‘Business Model of a Botnet’, in Proceedings - 26th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2018, 2018, pp. 441–445. doi: 10.1109/PDP2018.2018.00077.

[155] MITRE, ‘Develop Capabilities’. Hozzáférés: 2023.01.05. [Online]. Elérhető: https://attack.mitre.org/techniques/T1587/

[156] MITRE, ‘Obtain Capabilities’. Hozzáférés: 2023.01.05. [Online]. Elérhető: https://attack.mitre.org/techniques/T1588/

[157] CERT-FR, ‘The malware-as-a-service Emotet’, 2021.02. Hozzáférés: 2023.01.27. [Online]. Elérhető: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

[158] R. M. Ryan és E. L. Deci, ‘Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions’, Contemp Educ Psychol, vol. 25, no. 1, pp. 54–67, 2000, doi: 10.1006/ceps.1999.1020.

[159] H. Rhee, ‘Comparison of Process Theories to Content Theories in Motivating Workforces’, International Journal of Human Resource Studies, vol. 9, no. 4, pp. 267–274, 2019, doi: 10.5296/ijhrs.v9i4.15620.

[160] M. F. Washburn, ‘Dynamic Psychology . By Robert Sessions Woodworth. New York, Columbia University Press. 1918. Pp. 210.’, Science (1979), vol. 48, no. 1241, 1918, doi: 10.1126/science.48.1241.372.

[161] S. B. Klein, Motivation: Biosocial Approaches. McGraw-Hill, 1982.

[162] E. N. és C. L. Hull, ‘Principles of Behavior. An Introduction to Behavior Theory’, J Philos, vol. 40, no. 20, pp. 558–559, 1943, doi: 10.2307/2019960.

[163] O. Guy-Evans, ‘Drive-Reduction Theory and Human Behavior’, SimplyPschichology. Hozzáférés: 2022.12.12. [Online]. Elérhető: https://www.simplypsychology.org/drive-reduction-theory.html

[164] A. H. Maslow, ‘A theory of human motivation’, Psychol Rev, vol. 50, no. 4, pp. 370–396, 1943, doi: 10.1037/h0054346.

[165] A. H. Maslow, Motivation and Personality, 2nd Edition. Harper & Row, 1970.

[166] A. H. Maslow, ‘New Introduction: Religions, Values, and Peak-Experiences’, Journal of Transpersonal Psychology, vol. 2, no. 2, pp. 83–90, 1970.

[167] A. H. Maslow, Motivation és personality, 3rd Edition. Delhi, India: Pearson Education, 1987.

[168] C. Miller, ‘Kim Jong-il and me: How to build a cyber army to attack the U.S.’, in DEF CON 18, 2010. Hozzáférés: 2022.12.21. [Online]. Elérhető: https://defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf

[169] E. Hutchins, M. Cloppert és R. Amin, ‘Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains’, Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, pp. 1–14, 2011, Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

[170] MITRE, ‘MITRE ATT&CK - Enterprise Matrix’. Hozzáférés: 2021.12.11. [Online]. Elérhető: https://attack.mitre.org/matrices/enterprise/

[171] MITRE, ‘MITRE ATT&CK - Mobile Matrix’. Hozzáférés: 2022.12.23. [Online]. Elérhető: https://attack.mitre.org/matrices/mobile/

[172] MITRE, ‘MITRE ATT&CK - ICS Matrix’. Hozzáférés: 2022.12.23. [Online]. Elérhető: https://attack.mitre.org/matrices/ics/

[173] MITRE, ‘Common Weakness Enumeration’. Hozzáférés: 2023.01.04. [Online]. Elérhető: https://cwe.mitre.org/

[174] MITRE, ‘Common Vulnerabilities and Exposures’. Hozzáférés: 2023.01.04. [Online]. Elérhető: https://cve.mitre.org/

[175] N. Y. Conteh és P. J. Schmick, ‘Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks’, International Journal of Advanced Computer Research (IJACR), vol. 6, no. 23, pp. 31–38, 2016, doi: 10.19101/IJACR.2016.623006.

[176] ENISA, ‘ENISA Threat Landscape Report 2018’, 2019. doi: 10.2824/622757.

[177] ENISA, ‘Threat Landscape 2022’, 2022. doi: 10.2824/764318.

[178] J. Aycock, Spyware and adware. New York, NY: Springer, 2011. doi: 10.1007/978-0-387-77741-2.

[179] S. Eskandari, A. Leoutsarakos, T. Mursch és J. Clark, ‘A First Look at Browser-Based Cryptojacking’, in Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018, 2018. doi: 10.1109/EuroSPW.2018.00014.

[180] J. R. Youngblood, ‘Ransomware’, in Business Theft and Fraud, 1st Edition., J. R. Youngblood, Ed., Boca Raton, FL: Taylor & Francis Group, 2016, pp. 307–310. doi: 10.1201/9781315380780.

[181] P. Brichant, Ryan; Eftekhari, ‘The rise of disruptionware’, ICIT & Forescout. Hozzáférés: 2019.09.29. [Online]. Elérhető: https://icitech.org/wp-content/uploads/2019/09/ICIT-Brief-The-Rise-of-Disruptionware.pdf

[182] P. Ravali, ‘A Comparative Evaluation of OSI and TCP/IP Models’, International Journal of Science and Research, vol. 4, no. 7, pp. 514–521, 2013.

[183] S. M. Specht és R. B. Lee, ‘Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures’, in Proceedings of the International Workshop on Security in Parallel and Distributed Systems, San Francisco, 2004, pp. 543–550. Hozzáférés: 2023.02.27. [Online]. Elérhető: http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf

[184] E. C. Tandoc, Z. W. Lim és R. Ling, ‘Defining “Fake News”: A typology of scholarly definitions’, Digital Journalism, vol. 6, no. 2. pp. 137–153, 2018. doi: 10.1080/21670811.2017.1360143.

[185] H. Siddiqui, E. Healy és A. Olmsted, ‘Bot or not’, in 2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017, Cambridge, UK, 2018, pp. 462–463. doi: 10.23919/ICITST.2017.8356448.

[186] M. Khonji, Y. Iraqi és A. Jones, ‘Phishing Detection: A Literature Survey’, IEEE Communications Surveys and Tutorials, vol. 15, no. 4. pp. 2091–2121, 2013. doi: 10.1109/SURV.2013.032213.00009.

[187] Object Management Group, OMG Unified Modeling Language. 2017. Hozzáférés: 2023.01.10. [Online]. Elérhető: https://www.omg.org/spec/UML/2.5.1/PDF

[188] E. Hemberg et al., ‘Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting’. 2020. doi: 10.48550/arXiv.2010.00533.

[189] R. McMillan, ‘Definition: Threat Intelligence’, Gartner Research. 2013. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.gartner.com/en/documents/2487216

[190] K. Baker, ‘What is Cyber Threat Intelligence?’, Crowdstrike. Hozzáférés: 2022.12.01. [Online]. Elérhető: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

[191] W. Tounsi és H. Rais, ‘A survey on technical threat intelligence in the age of sophisticated cyber attacks’, Comput Secur, vol. 72, pp. 212–233, 2018, doi: 10.1016/j.cose.2017.09.001.

[192] D. Chismon és M. Ruks, Threat Intelligence: Collecting, Analysing, Evaluating. MWR Infosecurity & CERT-UK, 2015. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

[193] M. E. Korstanje, Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities. IGI Global, 2016. doi: 10.4018/978-1-5225-1938-6.

[194] G. Manco, ‘Threat Intelligence Platforms’, in The European Network for Cybersecurity (NeCS) PhD School, Trento, 2022. Hozzáférés: 2022.12.03. [Online]. Elérhető: https://gmanco.github.io/talk_trento_gen22.pdf

[195] Gartner, ‘CrowdStrike Reviews’. Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendor/crowdstrike

[196] Gartner, ‘Check Point Software Technologies Reviews’. Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.gartner.com/reviews/market/network-firewalls/vendor/check-point-software-tech

[197] Gartner, ‘Recorded Future Reviews’. Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.gartner.com/reviews/market/security-threat-intelligence-services/vendor/recorded-future

[198] Check Point, ‘What is Cyber Threat Intelligence?’ Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-threat-intelligence/

[199] Recorded Future, ‘What is Threat Intelligence?’ Hozzáférés: 2022.12.04. [Online]. Elérhető: https://www.recordedfuture.com/threat-intelligence

[200] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder és C. Skorupka, Guide to Cyber Threat Information Sharing. Gaithersburg, MD: National Institute of Standards and Technology, 2016. doi: 10.6028/NIST.SP.800-150.

[201] T. D. Wagner, K. Mahbub, E. Palomar és A. E. Abdallah, ‘Cyber threat intelligence sharing: Survey and research directions’, Comput Secur, vol. 87, p. 101589, Nov. 2019, doi: 10.1016/j.cose.2019.101589.

[202] MISP Project, ‘MISP Threat Sharing’. Hozzáférés: 2023.10.20. [Online]. Elérhető: https://www.misp-project.org/

[203] ETSI, ETSI TR 103 456 V1.1.1 (2017-10) CYBER; Implementation of the Network and Information Security (NIS) Directive. 2017. Hozzáférés: 2023.01.20. [Online]. Elérhető: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

[204] G. Settanni et al., ‘A collaborative cyber incident management system for European interconnected critical infrastructures’, Journal of Information Security and Applications, vol. 34, no. 2, pp. 166–182, 2017.06., doi: 10.1016/j.jisa.2016.05.005.

[205] K. Satlas, ‘CTI-EU event’, in Cyber Threat Intelligence CERT-EU vision, Róma: CERT-EU, 2017.10. Hozzáférés: 2023.01.20. [Online]. Elérhető: https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cert-eu-presentation/

[206] B. Stojkovski, G. Lenzini, V. Koenig és S. Rivas, ‘What’s in a Cyber Threat Intelligence sharing platform?’, in Annual Computer Security Applications Conference, New York, NY, USA: ACM, Dec. 2021, pp. 385–398. doi: 10.1145/3485832.3488030.

[207] A. Michota, A. Mitrakas, C. Patsakis és V. Stupka, ‘Technical aspects of cooperation between CSIRTS and LE’. ENISA, Dec. 2019. doi: 10.2824/28206.

[208] MISP Project, ‘How MISP enables stakeholders identified by the NISD to perform key activities’. Hozzáférés: 2023.01.20. [Online]. Elérhető: https://www.misp-project.org/compliance/NISD/

[209] FIRST, ‘TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0’. Hozzáférés: 2023.01.22. [Online]. Elérhető: https://www.first.org/tlp/

[210] ENISA, ‘Considerations on the Traffic Light Protocol’. Hozzáférés: 2023.01.22. [Online]. Elérhető: https://www.enisa.europa.eu/topics/incident-response/glossary/considerations-on-the-traffic-light-protocol

[211] FireEye, ‘OpenIOC_1.1’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://github.com/fireeye/OpenIOC_1.1

[212] Internet Engineering Task Force (IETF), ‘The Incident Object Description Exchange Format Version 2’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://www.rfc-editor.org/rfc/rfc7970

[213] Verizon, ‘Vocabulary for Event Recording and Incident Sharing (VERIS)’. Hozzáférés: 2023.01.16. [Online]. Elérhető: https://github.com/vz-risk/veris

[214] MITRE, ‘STIX Release Archive’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://stixproject.github.io/releases/archive/

[215] MITRE, ‘Cyber Observable eXpression (CybOXTM) Archive Website’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://cyboxproject.github.io/

[216] OASIS, ‘OASIS Cyber Threat Intelligence (CTI) TC’. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

[217] OASIS Open, ‘STIX Best Practices Guide Version 1.0.0’. 2022.09.15. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://docs.oasis-open.org/cti/stix-bp/v1.0.0/stix-bp-v1.0.0.pdf

[218] MITRE, ‘Malware Attribute Enumeration and Characterization (MAEC)’. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://maecproject.github.io/

[219] OASIS, ‘TAXII Version 2.1’. 2021.06.10. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html

[220] A. Ramsdale, S. Shiaeles és N. Kolokotronis, ‘A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages’, Electronics (Basel), vol. 9, no. 5, p. 824, 2020, doi: 10.3390/electronics9050824.

[221] ENISA, ‘Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy’. 2016. doi: 10.2824/975760.

[222] Európai Bizottság, A Bizottság (EU) 2017/2288 végrehajtási határozata a közbeszerzésben hivatkozható IKT műszaki előírások azonosításáról. 2017. Hozzáférés: 2023.01.18. [Online]. Elérhető: http://data.europa.eu/eli/dec_impl/2017/2288/oj

[223] DIGITALEUROPE, ‘The EU-US Trade & Technology Council: from ambitious work plans to concrete outcomes’. 2022. Hozzáférés: 2023.01.18. [Online]. Elérhető: https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/09/TTC_from_ambition_to_outcome.pdf

[224] A. Malatras, E. Tsekmezoglou, M. Theocharidou és R. Naydenov, Cybersecurity Threat Landscape Methodology. ENISA, 2022. doi: 10.2824/339396.

[225] MISP Project, 'MISP Published Standards'. Hozzáférés: 2023.01.22. [Online]. Elérhető: https://www.misp-standard.org/standards/

[226] OASIS, 'STIX Version 2.1'. Hozzáférés: 2023.01.17. [Online]. Elérhető: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

[227] C. Oral és G. CenkAkkaya, 'Cash Flow at Risk: A Tool for Financial Planning', Procedia Economics and Finance, vol. 23, pp. 262–266, 2015, doi: 10.1016/s2212-5671(15)00358-5.

[228] IFRS, 'IAS 7 Statement of Cash Flows'. 2022. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.ifrs.org/content/dam/ifrs/publications/pdf-standards/english/2022/issued/part-a/ias-7-statement-of-cash-flows.pdf?bypass=on

[229] O. Žižlavský, 'Net Present Value Approach: Method for Economic Assessment of Innovation Projects', Procedia Soc Behav Sci, vol. 156, pp. 506–512, 2014, doi: 10.1016/j.sbspro.2014.11.230.

[230] I. Fisher, The theory of interest. New York: Macmillan, 1930.

[231] F. Modigliani és M. H. Miller, 'The Cost of Capital, Corporation Finance and the Theory of Investment', Am Econ Rev, vol. 48, no. 3, pp. 261–297, 1958.

[232] F. Modigliani és M. H. Miller, 'Corporate Income Taxes and the Cost of Capital: A Correction', Am Econ Rev, vol. 53, no. 3, pp. 433–443, 1963.

[233] S. C. Myers, 'Interactions of Corporate Financing and Investment Decisions-Implications for Capital Budgeting', J Finance, vol. 29, no. 1, pp. 1–25, 1974, doi: 10.2307/2978211.

[234] P. Fernández, 'Valuing companies by cash flow discounting: ten methods and nine theories', Managerial Finance, vol. 33, no. 11, pp. 853–876, 2007, doi: 10.1108/03074350710823827.

[235] A. Beccarini, 'Investment sensitivity to interest rates in an uncertain context: is a positive relationship possible?', Economic Change and Restructuring, vol. 40, pp. 223–234, 2007.09., doi: 10.1007/s10644-007-9025-1.

[236] M. Rossi, 'The capital asset pricing model: A critical literature review', Global Business and Economics Review, vol. 18, no. 5, pp. 604–617, 2016, doi: 10.1504/GBER.2016.078682.

[237] M. A. Elbannan, 'The Capital Asset Pricing Model: An Overview of the Theory', Int J Econ Finance, vol. 7, no. 1, pp. 216–228, 2014, doi: 10.5539/ijef.v7n1p216.

[238] A. Damodaran, Investment Valuation: Tools and Techniques for Determining the Value of Any Asset, 3rd edition. John Wiley & Sons, 2012.

[239] P. Fernández, 'WACC: Definition, Misconceptions, and Errors', Business Valuation Review, vol. 29, no. 4, pp. 138–144, 2010, doi: 10.5791/0897-1781-29.4.138.

[240] E. F. FAMA and K. R. FRENCH, 'The Cross-Section of Expected Stock Returns', J Finance, vol. 47, no. 2, pp. 427–465, 1992, doi: 10.1111/j.1540-6261.1992.tb04398.x.

[241] M. M. Carhart, 'On Persistence in Mutual Fund Performance', J Finance, vol. 52, no. 1, pp. 57–82, 1997, doi: 10.1111/j.1540-6261.1997.tb03808.x.

[242] Ľ. Pástor és R. F. Stambaugh, 'Liquidity Risk and Expected Stock Returns', Journal of Political Economy, vol. 111, no. 3, pp. 642–685, 2003, doi: 10.1086/374184.

[243] E. F. Fama és K. R. French, 'A five-factor asset pricing model', J financ econ, vol. 116, no. 1, pp. 1–22, 2015, doi: 10.1016/j.jfineco.2014.10.010.

[244] F. P. Ramsey, 'A Mathematical Theory of Saving', The Economic Journal, vol. 38, no. 152, pp. 543–559, 1928, doi: 10.2307/2224098.

[245] V. Kazlauskienė, 'Application of Social Discount Rate for Assessment of Public Investment Projects', Procedia Soc Behav Sci, vol. 213, pp. 461–467, 2015, doi: 10.1016/j.sbspro.2015.11.434.

[246] M. A. Moore, A. E. Boardman, A. R. Vining, D. L. Weimer és D. H. Greenberg, '"Just give me a number!" Practical values for the social discount rate', Journal of Policy Analysis and Management, vol. 23, no. 4, pp. 789–812, 2004, doi: 10.1002/pam.20047.

[247] J. Zhuang, Z. Liang, T. Lin és F. D. xDe Guzman, 'Theory and practice in the choice of social discount rate for cost-benefit analysis: a survey', 2007. Hozzáférés: 2023.01.26. [Online]. Elérhető: http://hdl.handle.net/11540/1853

[248] N. Sklavos és P. Souras, 'Economic models and approaches in information security for computer networks', International Journal of Network Security, vol. 2, no. 1, pp. 14–20, 2006, Hozzáférés: 2023.02.01. [Online]. Elérhető: ijns.jalaxy.com.tw/download_paper.jsp?PaperID=IJNS-2005-07-08-1&PaperName=ijns-v2-n1/ijns-2006-v2-n1-p14-20.pdf

[249] L. A. Gordon és Martin P. Loeb, 'The economics of information security investment', ACM Transactions on Information and System Security, vol. 5, no. 4, pp. 438–457, 2002, doi: 10.1145/581271.581274.

[250] Z. Bederna és T. Szadeczky, ‘Industry 4.0-based critical infrastructure and the NIS Directive’, in Central and Eastern European eDem and eGov Days, New York, NY, USA: ACM, 2022, pp. 93–99. doi: 10.1145/3551504.3551546.

[251] T. Szádeczky és Z. Bederna, ‘The Economic Measurement of Cyber Incidents’, Periodica Polytechnica Social and Management Sciences, 2023, doi: 10.3311/PPso.22150.

[252] T. Olovsson, ‘A structured approach to computer security’, Chalmers University of Technology, Gothenburg, 1992. Hozzáférés: 2023.02.27. [Online]. Elérhető: https://research.chalmers.se/en/publication/166411

[253] K. Ruan, ‘Introducing cybernomics: A unifying economic framework for measuring cyber risk’, Comput Secur, vol. 65, pp. 77–89, 2017, doi: 10.1016/j.cose.2016.10.009.

[254] J. Freund és J. Jones, Measuring and Managing Information Risk. Elsevier, Butterworth-Heinemann, 2015. doi: 10.1016/C2013-0-09966-5.

[255] A. Erola, I. Agrafiotis, J. R. C. Nurse, L. Axon, M. Goldsmith és S. Creese, ‘A system to calculate Cyber Value-at-Risk’, Comput Secur, vol. 113, p. 102545, 2022, doi: 10.1016/j.cose.2021.102545.

[256] M. Talabis és J. Martin, ‘Information Security Risk Assessments’, in Information Security Risk Assessments, Elsevier, 2013, pp. 1–26. doi: 10.1016/B978-1-59-749735-0.00001-4.

[257] W. K. Brotby, Information Security Management Metrics, 1st Edition. New York: Auerbach Publications, 2009.

[258] EY, ‘Applying IFRS Accounting for the financial impact of natural disasters’. Hozzáférés: 2023.02.17. [Online]. Elérhető: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-applying-ifrs-natural-disasters.pdf

[259] M. Rabin, ‘Psychology and Economics’, J Econ Lit, vol. 36, no. 1, pp. 11–46, 1998, Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.jstor.org/stable/2564950

[260] A. Tversky és D. Kahneman, ‘Judgment under uncertainty: Heuristics and biases’, Science (1979), vol. 185, no. 4157, pp. 1124–1131, 1974, doi: 10.1126/science.185.4157.1124.

[261] N. Ambady és R. Rosenthal, ‘Thin slices of expressive behavior as predictors of interpersonal consequences: A meta-analysis’, Psychol Bull, vol. 111, no. 2, pp. 256–274, 1992, doi: 10.1037/0033-2909.111.2.256.

[262] B. Schwartz, The Paradox of Choice. New York, USA: HarperCollins Publishers Inc, 2004.

[263] International Monetary Fund, Balance of Payments and International Investment Position Manual, 6th Edition. Washington, D.C: International Monetary Fund, 2009. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.imf.org/external/pubs/ft/bop/2007/pdf/bpm6.pdf

[264] United Nations, System of National Accounts 2008. New York, [Brussels/Luxembourg], [Washington, D.C.], [Paris], [Washington, D.C.]: United Nations; Commission of the European Communities; International Monetary Fund; Organisation for Economic Co-operation and Development; World Bank, 2010. doi: 10.18356/4fa11624-en.

[265] European Commission, European system of accounts ESA 2010. Luxembourg: Publications Office of the European Union, 2010. doi: 10.2785/16644.

[266] Az Európai Parlament és a Tanács 549/2013/EU rendelete az Európai Unió-beli nemzeti és regionális számlák európai rendszeréről. 2013. Hozzáférés: 2023.02.06. [Online]. Elérhető: http://data.europa.eu/eli/reg/2013/549/oj

[267] S. Suranovic, International Finance: Theory and Policy. Saylor Foundation 2010, 2010.

[268] BBC, 'Tesco Bank attack: What do we know?', 2016.11.07. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://www.bbc.com/news/technology-37896273

[269] Tesco PLC, 'Tesco PLC Annual Report and Financial Statements 2017'. Hozzáférés: 2022.04.28. [Online]. Elérhető: https://www.tescoplc.com/media/474467/16-tesco-annual-report-2017.pdf

[270] L. Botter, 'Tesco Shares Fall After Cyber Attack at its Online Banking Group Hits 40,000 Customers', TheStreet, 2016.11.07. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://www.thestreet.com/investing/tesco-shares-drop-on-bank-hack-13882530

[271] M. Kumar, 'Tesco Bank Hacked — Cyber Fraudsters Stole Money From 20,000 Accounts', The Hacker News, 2016.11.07. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://thehackernews.com/2016/11/tesco-bank-hack.html

[272] Financial Conduct Authority, 'FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack'. Hozzáférés: 2022.04.25. [Online]. Elérhető: https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack

[273] A. Damodaran, 'Data:Archives, Discount Rate Estimation'. Hozzáférés: 2022.06.12. [Online]. Elérhető: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html#discrate

[274] D. Wolpoff, 'After the FireEye and SolarWinds breaches, what's your failsafe?', TechCrunch, 2020.12.21. [Online]. Elérhető: https://techcrunch.com/2020/12/21/after-the-fireeye-and-solarwinds-breaches-whats-your-failsafe

[275] S. Oladimeji és S. M. Kerner, ‘SolarWinds hack explained: Everything you need to know’, TechTarget, 2021.06.16. Hozzáférés: 2022.05.02. [Online]. Elérhető: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[276] SolarWinds, ‘Form 10-K 2019’. Hozzáférés: 2022.05.02. [Online]. Elérhető: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

[277] I. Jibilian és K. Canales, ‘The US is readying sanctions against Russia over the SolarWinds cyber attack. Here’s a simple explanation of how the massive hack happened and why it’s such a big deal’, Insider, 2021.04.15. Hozzáférés: 2022.05.02. [Online]. Elérhető: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[278] S. Shah, ‘The Financial Impact of SolarWinds Breach’, BitSight, 2021.01.12. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided

[279] SolarWinds, ‘Form 10-K 2020’. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://www.sec.gov/Archives/edgar/data/1739942/000173994221000043/swi-20201231.htm

[280] SolarWinds, ‘Form 10-Q’, 2021.09. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://www.sec.gov/Archives/edgar/data/0001739942/000173994221000154/swi-20210930.htm

[281] G. Ratnam, ‘Cleaning up SolarWinds hack may cost as much as $100 billion’, Roll Call, 2021.01.11. Hozzáférés: 2022.06.11. [Online]. Elérhető: https://rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

[282] M. Akbanov, V. G. Vassilakis és M. D. Logothetis, ‘WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms’, Journal of Telecommunications and Information Technology, vol. 1, no. 2019, pp. 113–124, 2019.04., doi: 10.26636/jtit.2019.130218.

[283] L. Rosencrance, ‘WannaCry ransomware’, TechTarget, 2021.09. Hozzáférés: 2022.06.16. [Online]. Elérhető: https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

[284] S. Barlyn, ‘Global cyber attack could spur $53 billion in losses: Lloyd’s of London’, Reuters, 2017.07.17. Hozzáférés: 2022.06.16. [Online]. Elérhető: https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB

[285] National Audit Office, ‘Investigation: WannaCry cyber attack and the NHS’, 2018.04. Hozzáférés: 2019.03.15. [Online]. Elérhető: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

[286] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi és P. Aylin, 'A retrospective impact analysis of the WannaCry cyberattack on the NHS', NPJ Digit Med, vol. 2, no. 1, p. 98, 2019.12., doi: 10.1038/s41746-019-0161-6.

[287] Krasznay Cs., 'Case Study: The NotPetya Campaign', in Információ- és kiberbiztonság, T. Bernát, Ed., Ludovika Egyetemi Kiadó, 2020, pp. 485–499. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16195/TKP_Kiberbiztonsag_01_25.pdf

[288] A. Hern, 'Hackers who targeted Ukraine clean out bitcoin ransom wallet', The Guardian, 2017.07.05. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://www.theguardian.com/technology/2017/jul/05/notpetya-ransomware-hackers-ukraine-bitcoin-ransom-wallet-motives

[289] A. Greenburg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, 2018.08.22. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[290] C. Pownall, 'The Context and Impact of Maerk's NotPetya cyber attack'. Hozzáférés: 2022.06.17. [Online]. Elérhető: https://www.researchgate.net/publication/346080185_The_Context_and_Impact_of_Maerk's_NotPetya_cyber_attack

[291] M. van Hees, 'The 2017 MAERSK Cyber Incident'. Hozzáférés: 2022.07.17. [Online]. Elérhető: https://fhi.nl/app/uploads/sites/75/2020/10/201029-FHI_Maersk.pdf

[292] E. Sagonowsky, 'Merck, insurers fight over $1.3B in damages from cyberattack: Bloomberg', Fierce Pharma. Hozzáférés: 2022.06.18. [Online]. Elérhető: https://www.fiercepharma.com/pharma/merck-insurers-fight-over-1-3-billion-damages-from-cyberattack-bloomberg

[293] M. Erman és J. Finkle, 'Merck says cyber attack halted production, will hurt profits', Reuters, 2017.07.28. Hozzáférés: 2022.06.18. [Online]. Elérhető: https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurt-profits-idUSKBN1AD1AO

[294] Merck, 'Form 10-K'. Hozzáférés: 2022.06.18. [Online]. Elérhető: https://www.sec.gov/Archives/edgar/data/310158/000031015819000014/mrk1231201810k.htm

[295] Merck & Co. Inc. v. ACE American Ins. Co., UNN-L-002682-18. US: N.J. Super. Ct. Law Div., 2022. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.documentcloud.org/documents/21183337-merck-v-ace-american

[296] The Guardian, ‘Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach’, 2018.03.17. [Online]. Elérhető: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[297] Business Insider, ‘Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Here’s everything that’s happened up until now.’, 2019. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3

[298] S. Meredith, ‘Facebook-Cambridge Analytica: A timeline of the data hijacking scandal’, CNBC, 2018.04.10. Hozzáférés: 2023.03.01. [Online]. Elérhető: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

[299] CNBC, ‘Here are the scandals and other incidents that have sent Facebook’s share price tanking in 2018’, 2018.10.20. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html

[300] MarketWatch, ‘Facebook stock drops roughly 20%, loses $120 billion in value after warning that revenue growth will take a hit’, 2018. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.marketwatch.com/story/facebook-stock-crushed-after-revenue-user-growth-miss-2018-07-25

[301] Business Insider, ‘Facebook just announced it was hacked, and almost 50 million users have been affected’. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.businessinsider.com.au/facebook-security-attack-affecting-50-million-users-2018-9

[302] International Business Times, ‘Facebook Stock Suffers Biggest Drop Of 2019, Loses $37B In 4 Trading Days’, 2019.03.18. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.ibtimes.com/facebook-stock-suffers-biggest-drop-2019-loses-37b-4-trading-days-2776826

[303] Liao Shannon, ‘Facebook, Instagram, and WhatsApp are still down for some users around the world’, The Verge, 2019.03.13. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.theverge.com/2019/3/13/18264092/facebook-instagram-down-partially-post-messages-profile-loading

[304] Facebook, ‘Keeping Passwords Secure’. Hozzáférés: 2020.08.10. [Online]. Elérhető: https://about.fb.com/news/2019/03/keeping-passwords-secure/

[305] Markets Insider, ‘Facebook shares drop sharply after unearthed emails reportedly show Mark Zuckerberg is aware of “problematic privacy practices”’, 2019.06.12. Hozzáférés: 2021.03.01. [Online].

Elérhető: https://markets.businessinsider.com/news/stocks/facebook-stock-price-reaction-to-zuckerberg-reportedly-aware-privacy-issues-2019-6-1028274446

[306] Information Commissioner's Office, 'Statement on an agreement reached between Facebook and the ICO'. Hozzáférés: 2023.02.28. [Online]. Elérhető: https://www.wired-gov.net/wg/news.nsf/articles/Statement+on+an+agreement+reached+between+Facebook+and+the+ICO+30102019151000?open

[307] Federal Trade Commission, 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook'. Hozzáférés: 2020.08.10. [Online]. Elérhető: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[308] Facebook, 'FTC Agreement Brings Rigorous New Standards for Protecting Your Privacy'. Hozzáférés: 2020.11.08. [Online]. Elérhető: https://about.fb.com/news/2019/07/ftc-agreement/

[309] Techcrunch, 'A huge database of Facebook users' phone numbers found online', 2019.09.04. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/

[310] CNBC, 'Facebook stock rises on better-than-expected revenue and earnings', 2019.10.30. Hozzáférés: 2023.02.22. [Online]. Elérhető: https://www.cnbc.com/2019/10/30/facebook-fb-q3-2019-earnings.html

[311] Competition Bureau Canada, 'Facebook to pay $9 million penalty to settle Competition Bureau concerns about misleading privacy claims'. Hozzáférés: 2021.01.08. [Online]. Elérhető: https://www.canada.ca/en/competition-bureau/news/2020/05/facebook-to-pay-9-million-penalty-to-settle-competition-bureau-concerns-about-misleading-privacy-claims.html

[312] HmbBfDI, 'Tätigkeitsbericht datenschutz 2019'. Hozzáférés: 2021.03.06. [Online]. Elérhető: https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf

[313] Facebook, 'Form 10-K 2019'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/2019/ar/2019-Annual-Report.pdf

[314] Facebook, 'Form 10-K 2016'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf

[315] Facebook, 'Form 10-K 2017'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2017_FINAL.pdf

[316] Facebook, 'Form 10-K 2018'. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2018-Annual-Report.pdf

[317] Facebook, ‘Form 10-K 2020’. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://s21.q4cdn.com/399680738/files/doc_financials/2020/ar/2020-Annual-Report.pdf

[318] A. Damodaran, ‘Historical Returns on Stocks, Bonds and Bills: 1928-2020’. Hozzáférés: 2021.07.09. [Online]. Elérhető: https://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/histretSP.html

[319] MSCI, ‘MSCI ACWI Index (USD)’. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://www.msci.com/documents/10199/8d97d244-4685-4200-a24c-3e2942e3adeb

[320] International Monetary Fund, ‘Interest Rates, Government Securities, Government Bonds for United States’. Hozzáférés: 2023.02.01. [Online]. Elérhető: https://fred.stlouisfed.org/series/INTGSBUSM193N#

[321] Coin News, ‘Current US Inflation Rates: 2000-2021’. Hozzáférés: 2021.03.06. [Online]. Elérhető: https://www.usinflationcalculator.com/inflation/current-inflation-rates/

[322] Yahoo! Finance, ‘Meta Platforms, Inc. (META)’. Hozzáférés: 2023.01.07. [Online]. Elérhető: https://finance.yahoo.com/quote/FB/history

[323] Yahoo! Finance, ‘S&P 500 (^GSPC)’. Hozzáférés: 2021.01.07. [Online]. Elérhető: https://finance.yahoo.com/quote/%5EGSPC/history?p=%5EGSPC%0A

[324] J. H. Ahn, ‘The impact of the banking competition in funding and lending markets on lending technology’, Revue Economique, vol. 67, no. 6, pp. 1117–1139, 2016, doi: 10.3917/reco.pr2.0069.

[325] Statista, ‘IT budgets & investments’. Hozzáférés: 2021.01.28. [Online]. Elérhető: https://www.statista.com/study/71560/it-budgets-and-investments/

[326] Flexera, ‘State of tech spend report’. Hozzáférés: 2021.03.14. [Online]. Elérhető: https://info.flexera.com/SLO-REPORT-State-of-Tech-Spend

[327] J. Bernard, D. Golden és M. Nicholson, ‘Reshaping the cybersecurity landscape’, Deloitte Insights. Hozzáférés: 2021.03.20. [Online]. Elérhető: https://www.fsisac.com/hubfs/DI_2020-FS-ISAC-Cybersecurity.pdf

[328] J. Roettgers, ‘Mark Zuckerberg Says Facebook Will Spend More Than $3.7 Billion on Safety, Security in 2019’, Variety, 2019.02.05. Hozzáférés: 2021.03.06. [Online]. Elérhető: https://variety.com/2019/digital/news/facebook-2019-safety-speding-1203128797/

[329] S. Armitage, ‘Event study methods and evidence on their performance’, J Econ Surv, vol. 9, no. 1, pp. 25–52, 1995, doi: 10.1111/j.1467-6419.1995.tb00109.x.

[330] T. S. Breusch és A. R. Pagan, ‘A Simple Test for Heteroscedasticity and Random Coefficient Variation’, Econometrica, vol. 47, no. 5, pp. 1287–1294, Sep. 1979, doi: 10.2307/1911963.

[331] E. I. Obilor és E. C. Amadi, ‘Test for significance of Pearson’s correlation coefficient’, International Journal of Innovative Mathematics, Statistics & Energy Policies, vol. 6, no. 1, pp. 11–23, 2018.

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

[BZs1] Bederna Zs., ‘Bizalom és megbízhatóság’, Katonai Nemzetbiztonsági Szoglálat, vol. XVII., no. 1., pp. 135–149, 2019, [Online]. Elérhető: https://www.knbsz.gov.hu/hu/letoltes/szsz/2019_1_ szam.pdf

[BZs2] Bederna Zs., ‘Critical Information and Communications Technology protection’, in Kiberbiztonság-Cybersecurity 2, Rajnai Z., Ed., Biztonságtudományi Doktori Iskola, 2019, pp. 137–146. [Online]. Elérhető: https://bdi.uni-obuda.hu/sites/default/files/oldal/csatolmany/kiadvany-2019.pdf

[BZs3] Bederna Zs., Rajnai Z. és Szádeczky T., ‘Further Strategy Analysis of Cybersecurity Incidents’, Land Forces Academy Review, vol. 26, no. 3, pp. 251–260, 2021, doi: 10.2478/raft-2021-0032.

[BZs4] Bederna Zs. és Rajnai Z., ‘Review of the advancement of critical information infrastructures and their structural analysis’, National Security Review, pp. 166–175, 2020.

[BZs5] Bederna Zs., ‘Az Általános adatvédelmi rendelet és az információbiztonság kapcsolódási pontjai’, Szakmai Szemle, vol. XVI., no. 3., pp. 76–103, 2018.

[BZs6] Bederna Zs. és Rajnai Z., ‘Analysis of the cybersecurity ecosystem in the European Union’, International Cybersecurity Law Review, vol. 3, pp. 35–49, 2022, doi: 10.1365/s43439-022-00048-9.

[BZs7] Bederna Zs. és Szádeczky T., ‘Cyber espionage through Botnets’, Security Journal, vol. 33, pp. 43–62, 2019, doi: 10.1057/s41284-019-00194-6.

[BZs8] Bederna Zs. és Rajnai Z., ‘Analysis of static and dynamic parameters of players in cyberspace’, in Eighth International Scientific Web-conference of Scientists and PhD. students or candidates, in Trends and Innovations in E-business, Education and Security. Budapest: Obuda University, 2020, pp. 65–80.

[BZs9] Bederna Zs. és Szádeczky T., ‘Effects of botnets – a human-organisational approach’, Security and Defence Quarterly, vol. 35, no. 3, pp. 25–44, 2021, doi: 10.35467/sdq/138588.

[BZs10] Bederna Zs. és Szadeczky T., ‘Industry 4.0-based critical infrastructure and the NIS Directive’, in Central and Eastern European eDem and eGov Days, New York, NY, USA: ACM, 2022, pp. 93–99. doi: 10.1145/3551504.3551546.

[BZ11]Szádeczky T. és Bederna Zs., ‘The Economic Measurement of Cyber Incidents’, Periodica Polytechnica Social and Management Sciences, 2023, doi: 10.3311/PPso.22150.

[BZs12] Bederna Zs., Rajnai Z. és Szádeczky T., ‘Attacks against energy, water and other critical infrastructure in the EU’, in 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE), IEEE, 2021, pp. 000125–000130. doi: 10.1109/cando-epe51100.2020.9337751.

[BZs13] Bederna Zs. és Szádeczky T., ‘Managing the financial impact of cybersecurity incidents’, Security and Defence Quarterly, vol. 41, no. 1, 2023, doi: 10.35467/sdq/159625.

[BZs14] Bederna Zs., Rajnai Z. és Szadeczky T., ‘Business Strategy analysis of Cybersecurity Incidents’, Land Forces Academy Review, vol. 26, no. 2, pp. 139–148, 2021, doi: 10.2478/raft-2021-0020.

[BZs15] Bederna Zs., ‘Analysing the Financial Impact of Cybersecurity Incidents’, Open Science Foundation. 2023. doi: 10.17605/OSF.IO/ZEM8Y.

8.2 További tudományos közlemények

[BZs16] Bederna Zs. és Szádeczky T., ‘Modelling computer networks for further security research’, Security and Defence Quarterly, vol. 36, no. 4, pp. 51–66, 2021, doi: 10.35467/sdq/141572.

[BZs17] Bederna Zs., ‘Fuzzy-based intrusion detection’, Hadmérnök, vol. 10, no. 1, pp. 147–160, 2015, Hozzáférés: 2024.03.11. [Online]. Elérhető: http://hadmernok.hu/151_14_bedernazs.pdf

[BZs18] Bederna Zs., ‘Az informatikai eszközök használatával kapcsolatos attitűdök az egyetemi hallgatók körében ma Magyarországon’, Információs Társadalom, vol. 12, no. 4, p. 106, 2012, doi: 10.22503/inftars.XII.2012.4.4.

[BZs19] Bederna Zs., Váczi D., Pollner P. és Szádeczky T., ‘Támadás hálózatba szervezve’, in Hálózatok a közszolgálatban, Auer Á. és Joó T., Eds., Budapest: Dialóg Campus Kiadó, 2019, pp. 223–247.

[BZs20] Váczi D., Bederna Zs., Szalánczi-Orbán V. és Szádeczky T., ‘Az incidenskezelés szervezeti háttere’, in Hálózatok a közszolgálatban, Auer Á. és Joó T., Eds., Budapest: Dialóg Campus Kiadó, 2019, pp. 205–222.