ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

VÁCZI DÁNIEL

Kiberbiztonsági humán kockázati matematikai modell szenzitív digitális információszivárgás potenciáljának mérésére

Témavezető: Dr. habil. Szádeczky Tamás

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2021. 09. hónap 14. nap

Komplex Vizsga Bizottság:

Elnök:

Prof. Dr. Rajnai Zoltán egyetemi tanár; ÓE

Tagok:

Dr. habil. Kerti András egyetemi docens; külső - NKE

Dr. habil. Farkas Tibor egyetemi docens; külső - NKE

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Rajnai Zoltán egyetemi tanár; ÓE

Titkár:

Dr. Varga Péter János adjunktus; ÓE

Tagok:

Prof. Dr. Kovács László ddtbk. egyetemi tanár; külső - NKE

Dr. Krasznay Csaba egyetemi docens; külső – NKE

Dr. Szűcs Endre; külső

Bírálók:

Dr. Keszthelyi András egyetemi docens; ÓE

Dr. Tóth András egyetemi docens; külső – NKE

Nyilvános védés időpontja

2021. december 15. 10.00

TARTALOMJEGYZÉK

BEVEZETÉS

A szervezetek digitalizációja mára már nem egy jól hangzó hívószó csupán [1], mellyel a vezetők igyekeznek megkülönböztetni a vállalatot a versenytársaktól. Az a piaci vagy állami szereplő, aki nem tesz lépéseket az ilyen irányú fejlesztések implementálása érdekében, annak működése rövid időn belül fenntarthatatlanná válik. Ez a modernizáció mára megkerülhetetlenné vált.

2019. év végétől 2021-ig a Föld gyakorlatilag minden országának vezetője a járványhelyzet miatt hosszabb-rövidebb időre kijárási korlátozásokat vezetett be. Ennek a lépésnek azonban számos mellékhatása lett. A vállalatok hirtelen rákényszerültek arra, hogy átszervezzék a munkafolyamataik jelentős részét. Aki megtehette, otthoni munkavégzést írt elő a munkavállalói számára. A személyes munkabeszélgetések, az értékesítés, a bürokratikus, papíralapú folyamatok, de még az olyan – eddig csak személyesen elképzelhetőnek vélt – közösségi események, mint a konferenciák is online csatornákra terelődtek.

Ez a sok esetben ötletszerű, hirtelen átállás mind a szervezeteknek, mind a munkavállalóknak komoly kihívást jelentett számos területen. Nagy felelősség hárult az informatikai és a kapcsolódó biztonsági szervezeti egységekre és szakemberekre. A szakmaiság mellett szükség volt a jó reagáló képességükre a felhasználóigények és a munka fenntarthatóságának figyelembevételével együtt.

A különböző ártó szándékú személyek és szervezetek a hirtelen káoszt a kibertérben[1] is igyekeztek kihasználni. Az Interpol 2020. augusztusában kiadott riportja [2] szerint a kiberbűnözők a profit és károkozás maximalizálása érdekében a célzott támadások során nem az egyéneket, valamint a kis- és középvállalatokat vették célkeresztbe, hanem a nagyvállalatokat, az állami szereplőket és a kritikus infrastruktúrákat (létfontosságú rendszerelemeket). A hirtelen fókuszváltás hatására az érintett szakembereknek a korábbinál is nagyobb figyelmet kell fordítaniuk a kiberbiztonsági kitettség csökkentésére és az ellenálló-képesség növelésére.

A kiberbiztonság általánosságban egy komplex, kockázatok kezelésén alapuló terület, mely az informatikai- és információbiztonságon túl a kapcsolódó jogi, társadalmi és gazdasági folyamatok megfelelő kezelését is magában foglalja. Kezelését nemzetállam-

[1] Minket körülvevő virtuális tér. Bővebben az 1.1.2 fejezetben kerül definiálásra a kibertér fogalma.

és szövetségirendszer-szinten is kell kezelni. E területet hazánkban a különböző nemzetközi ajánlások, előírások és jógyakorlatok alapján készített 2013. évi L. törvény (Ibtv.) [3], illetve Magyarország Nemzeti Kiberbiztonsági Stratégiáját [4] kiegészítő (a hálózati és információs rendszerekre vonatkozó) szakpolitikai stratégia [5] határozza meg. A különböző piaci és állami szervezetek azonban hajlamosak a kiberbiztonság problematikáját elsősorban informatikai szempontok alapján megközelíteni annak ellenére, hogy a kiberbiztonság egyik legnagyobb nemzetközi szervezete – az ISACA[2] – által kiadott „The Business Model for Information Security[3]" folyamatközpontú üzleti modell [6] is rávilágít a szervezetek és az emberek jelentős szerepére a technológia mellett.

Többek között az is lehet annak az oka, hogy a humán oldalra kevesebb figyelem összpontosul, hogy a kiberbiztonság területén az emberi kockázatot a komplexitása miatt nagyon nehéz felmérni. Az elmúlt évtizedek feltárt, és nem csak szakmai körökben ismert nagyobb incidensei (pl.: Stuxnet, Mirai botnet[4], Wannacry, NotPetya, BlackEnergy, Edward Snowden esete, a Cambridge Analitics botrány stb.) azonban azt mutatják, hogy szükséges foglalkozni ezzel a tényezővel a nehézségek ellenére is. Ahogy nő a digitalizáció mértéke, úgy növekszik a szervezeteknek a kibertérből érkező támadásokkal szembeni kitettsége és úgy nő az igény a kiberbiztonság szintjének növelésére, az ellenálló-képesség fejlesztésére. A Covid-19 világjárvány ráadásul számos területre – többek között a kiberbiztonságra is – nagy hatással volt [7].

2020-ban a pandémiát kihasználó támadások mellett történt más, nagy jelentőségű, a kiberbiztonságot érintő eset is. 2020 decemberében ugyanis a FireEye[5] munkatársai felfedezték a sokak által az eddigi legnagyobb kibertámadásnak titulált, Sunburst néven közismertté vált, az ellátási láncot érő támadást[6], mely feltételezhetően az APT29[7] csoporthoz köthető. Az Amerikai Egyesült Államok állami és védelmi szektora mellett

[2] Az ISACA (Information Systems Audit and Control Association) egy nonprofit szakmai szervezet.
[3] A „The Business Model for Information Security" magyarul „Az információbiztonság üzleti modell"-jét jelenti.
[4] A botnet, más néven bot-hálózat a robot network szóból ered. A hálózatba kötött zombi számítógépekkel vagy más digitális eszközökkel, a tulajdonosuk tudta nélkül, a támadó nagyobb teljesítményű támadást tud végrehajtani.
[5] Amerikai kiberbiztonsági gyártó.
[6] Nemzetközi szakzsargonban: supply chain attack.
[7] Az APT29 (Advanced Persistent Threat 29) vagy más néven Cozy Bear egy olyan hackercsoport, mely orosz hírszerző ügynökségekhez köthető. Az APT-k általában információszerzésre irányuló rejtett, célzott támadásokat hajtanak végre.

a legnagyobb cégek[8] jelentős részét és a biztonsági szakma elismert szereplőit is érintette az eset. A kiterjedt felhasználói bázissal rendelkező SolarWinds Orion platform frissítési csomagjába rejtette azt a malware[9]-t, amely hozzáférési lehetőséget biztosít a támadók részére azoknak a szervezeteknek a rendszereihez, akik az érintett javítást telepítették. Ezeket a cégeket, intézményeket úgy érte ez a hatalmas – a disszertáció írásakor felmérhetetlen – kárt okozó támadás, hogy méretükből és pozíciójukból fakadóan az átlagnál sokkal nagyobb erőforrást fektetnek a saját kiberbiztonságuk fejlesztésére.

A példa jól mutatja, hogy soha nem beszélhetünk száz százalékos biztonságról. Hiába vezetünk be különböző adminisztratív, logikai és fizikai kontrollokat, 2021-ben biztosak lehetünk abban, hogy különböző biztonsági események, incidensek be fognak következni. Éppen ezért egy hozzáállásbeli paradigmaváltás kezd megfigyelhetővé válni. A szervezetek a minél tökéletesebb biztonság megteremtésének kialakítása helyett inkább az ellenálló-képesség[10] növelésére kezdenek fókuszálni. A biztonsági szakemberek abból a feltételezésből kezdenek kiindulni, hogy a védelmi szint nagyságától függetlenül mindenképpen történni fog egy esemény vagy incidens, amire reagálni kell az üzleti folyamatok folyamatosságának fenntartása mellett. Az ellenálló- és a reagálóképesség növelése érdekében egyre nagyobb fókusz helyeződik a különböző automatizált digitális megoldások használata mellett az emberi tényezőre, mint a támadások első frontvonalára. Ahhoz, hogy ezt szabályozottan, tervszerűen lehessen kezelni, szükséges megismerni a kockázatos személyeket. Ez segíti a biztonsági csapatot és a menedzsmentet a megfelelő döntések meghozatalára. Ez lehet egy-egy személy képzése, de szélsőséges esetben áthelyezése vagy elbocsájtása is.

Tudományos probléma megfogalmazása

A szervezeteket ért kibertérből érkező különböző sikeres támadások során számos esetben az emberi tényező meghatározó szerepet játszott. Ennek a kockázati faktornak a meghatározására azonban a mai napig nem létezik egy általánosan elterjedt módszertan, hiszen a kockázatok mérése egyáltalán nem triviális. Az oka az, hogy az emberi lény összetett és az individuumok nagyon különböznek egymástól, illetve a környezeti

[8] A legnagyobb cégek alatt az ún. Fortune Global 500 listán található, a legnagyobb árbevétellel rendelkező cégeket kell érteni.
[9] A malware szó, a malicious software angol kifejezésből származik, ami magyarul rosszindulatú szoftvert, programkódot jelent.
[10] Nemzetközi szakzsargonban: cyber resilience.

körülményeik – mint például az adott szervezetnél betöltött szerepük, felkészültségük, motivációik stb. – nagyon eltérőek. Ezeknek az okoknak köszönhetően a kiberbiztonsági szempontból kockázatos személyek meghatározása jelenleg esetleges és nem támaszkodik konkrét számítások által alátámasztott adatokra. A megfelelő módszertan hiányában a befektetett energia ráadásul nincs arányban a kapott eredmény felhasználhatóságával, mivel az valószínűleg nem közelíti meg megfelelő mértékben a valóságot. Márpedig egy szervezet kiberbiztonsági ellenálló-képességének növelésének érdekében célszerű ismerni, hogy mely munkavállalókra szükséges jobban odafigyelni, kit érdemes fejleszteni vagy más módon kezelni a cél elérése érdekében.

Egy személy kiberbiztonsági szempontú kockázatosságának meghatározása azért is komplex és nehéz feladat, mert a vizsgált tényezők értékeinek meghatározása bizonytalan és sok esetben szubjektív. Mindezek mellett sokszor nem is számszerűsíthetőek a hagyományos értelemben, így pontatlanok is. A vállalatok humánkockázat-elemzése során a valósághoz közelítő eredmény elérése érdekében tehát szükség van egy olyan értékelési módszertanra, amely a szokásosnál jobban kezeli a pontatlanságot, bizonytalanságot, szubjektivitást, és értelmezni képes a nehezen számszerűsíthető bemeneti értékeket, valamint kezeli az egyéni specifikumokat, illetve a szervezetben betöltött szerepüket, helyüket is.

Tovább nehezíti a probléma megfelelő kezelését, hogy – a valós kockázatok megismeréséhez – az egyén szervezetben betöltött helyzete mellett a magánéltét és személyiségét is szükséges megismerni. Ennek fontosságát bizonyítja az, hogy a nemzetállamok a minősített adatokhoz hozzáférő személyek átvilágítása során szintén kitérnek az adott ember magánéletének és környezetének megismerésére is.[11]

Ugyan sok esetben nem áll a munkáltató vagy a biztonsági szakemberek birtokában minden magánjellegű információ a munkavállalókról, de még az adatvédelmi szempontból szigorúan szabályozott Európai Unióban sem példa nélküli az a szervezet, ahol a biztonságért felelős szervezeti egység vagy egy törvényileg meghatározott külső állami szerv rendelkezik ilyen magánjellegű adatokkal. Az értekezésemben ismertetett módszertan ebből az okból kifolyólag ezzel a ténnyel nem foglalkozik, és feltételezem, hogy minden szükséges adat rendelkezésre áll.

[11] A Magyarországon az átvilágítás során használt biztonsági kérdőív a következő helyről tölthető le: https://www.nbf.hu/docs/Bizt_kerdoiv.docx.

Témaválasztás indoklása

Az alap- és mesterképzésben eltöltött tanulmányaim és tudományos tevékenységem során mindig is kiemelt figyelmet fordítottam az informatika- és információbiztonság területeinek megismerésére, azon belül is az emberi tényező veszélyeinek feltárására. Tudományos kíváncsiságom arra motivált, hogy számos elméleti kutatást végezzek ezen a területen, és különböző célirányos gyakorlati feladatot hajtsak végre. Az üzleti életben szerzett szakmai tanácsadói és cégvezetői tapasztalataim megerősítettek abban, hogy a humán faktor kockázatainak megismerése a kiberbiztonság területén egy olyan fennálló probléma, amelynek kezelésére nagy szükség van.

A különböző nemzetközi és hazai ajánlások, szabványok és jogszabályok mind kitérnek arra, hogy a biztonság növelése érdekében nem csak technikai fejlesztésekre van szükség, hanem az emberi tényezőből fakadó kockázatot is csökkenteni kell. A kiber-ellenállóképesség egyik fontos dokumentuma az Amerikai Egyesült Államokban működő ASPENS által kiadott A National Cybersecurity Agenda for Resilient Digital Infrastructure[12] c. kiadvány. Ez a dokumentum ajánlást tesz az adott elnöki ciklus legfontosabb kiberbiztonsági fejlesztési területeire vonatkozóan. A legfrissebb, 2020. decemberi kiadványukban [8] az öt javasolt célkitűzés közül első helyen az oktatást és a munkaerő fejlesztését emelték ki.

A megfogalmazott célok között szerepel a technikai szakemberek foglalkoztatása mellett minél több terület bevonása a megfelelő védelem kialakítása érdekében. Jól látszik, hogy az emberi tényező kezelése nemzetközileg is egyre nagyobb prioritásúvá válik, ráadásul a kiber-ellenállóképesség a digitálisan függő szervezetek életében már nem csak a szűk biztonsági szakember munkáján múlik, hanem a teljes munkaerő felkészültségén. Ezt a felkészültséget az erőforrások optimalizálása érdekében tervezett módon szükséges fejleszteni, melynek alapja egy megfelelő kockázatszámítási módszertan.

Kutatási célkitűzés

A kutatásom célja az, hogy a piacon megjelenő valós igényekre megoldást találjak tudományos munka segítségével. Az emberi tényező különböző aspektusait figyelembe véve létrehoztam egy olyan egzakt matematikai modellt és módszertant, melyet

[12] A cím tükörfordításban a következő: Az ellenálló digitális infrastruktúra nemzeti kiberbiztonsági menetrendje

magukra szabva és alkalmazva a szervezetek – a megfelelő információk birtokában – meg tudják határozni a kiberbiztonsági szempontból kockázatos személyeket. Az eredményeket felhasználva célzottan lehet a munkavállalók biztonságtudatosságát, kiber-higiéniáját növelni. A modell használata által kapott eredményeket a képzésen kívül a valós számszerű adatok segítségével az üzleti oldal is felhasználhatja újabb biztonsági kontrollok bevezetésére, a régiek optimalizálására, illetve adott esetben a kockázatok felvállalására.

Értekezésemben a kiberbiztonsági fenyegetettségek közül a szándékos vagy gondatlan módon elkövetett minősített digitális információszivárgást vizsgálom a modell működésének könnyebb érthetőség miatt. A modellalkotás során e speciális fenyegetettségre fókuszálva a hálózatkutatás területét és a fuzzy logika alkalmazását együttesen alkalmaztam a szervezeten belüli kockázatelemzés elősegítése érdekében.

Kutatási hipotézisek megfogalmazása

H1: Jól körülírható azoknak a különböző kockázati tényezőknek a köre, amelyek befolyásolják azt, hogy egy személy gondatlanságból vagy szándékosan szenzitív információt szivárogtat ki egy szervezetből.

H2: Létezik olyan fuzzy modell, amelyet alkalmazva megfelelő információk (bemenetek) ismeretében megsejthető a kiberbiztonsági kockázata egy egyénnek egy szervezeten belül.

H3: Létezik olyan matematikai (hálózatelemzési módszereket és a fuzzy logikát együttesen alkalmazó) modell, melyet alkalmazva nagy valószínűséggel meghatározható azoknak a személyeknek a köre, akik kiberbiztonsági kockázatot jelentenek egy vállalatnál és ismerve őket, a szervezet kiber-ellenállóképességének hatékonysága növelhető.

Kutatási módszerek

Kutatásom alapját a fuzzy logika és a hálózatelemzés módszereinek vizsgálata, valamint a humán faktor kiberbiztonsági aspektusainak tanulmányozása adta. Értekezésem elkészítése céljából irodalomkutatást végeztem kiberbiztonsági, pszichológiai, matematikai (fuzzy logika, hálózatkutatás), szociológiai, kriminalisztikai területeken, illetve áttekintettem a vonatkozó jogszabályokat, ajánlásokat és szabványokat. A

hiányzó információk elérése érdekében mélyinterjúkat készítettem, és egy specifikus kérdőíves kutatást is végrehajtottam.

A két matematikai módszer pozitív tulajdonságait kihasználva alkottam meg az emberi kockázat vizsgálására alkalmas modellt, ahol az egymásba ágyazott fuzzy rendszerek kimeneti értéke határozza meg az élek száma mellett a hálózat pontjainak súlyát. A modellek elkészítéséhez a MatLab R2020a-t, illetve a Fuzzy Logic Toolboxot és a Simulink kiegészítőket használtam. A fuzzy modell bemeneteit képző kockázati tényezőkön tartalmi szempontból rendezést végeztem és külön-külön tagsági függvényeket határoztam meg.

A kérdőíves kutatás során statisztikai módszerekkel állapítottam meg a számmal jellemezhető értékeket, illetve a speciális szövegkijelölést igénylő kérdéseknél egyesével elemeztem a válaszok gyakoriságát.

1 A DIGITÁLIS INFORMÁCIÓSZIVÁRGÁS CÉLZOTT TÁMADÁSOK ESETÉN

A munkavállalókat folyamatosan érzéktelenítik el az őket körülvevő újabb és újabb technológiák és az egyre növekvő információhalmaz. A munkáltató által munkavégzés céljából biztosított eszközöket és programokat a magánéletükben is sokszor használják, illetve arra is van már lehetőség az ún. BYOD[13] megoldásoknak köszönhetően, hogy saját eszközöket részben felügyelt módon használjanak. Mint mindennek, ennek is megvan a maga kockázata [9]. Ezek a lehetőségek is eredményezik azt, hogy nem mindig tiszta a munkavállalók számára a határ. Noha vannak ezt segítő technológiai megoldások mind mobil eszközökre, mind a klasszikus értelemben vett számítógépekre (PC, notebook), de azok nem képesek teljes védelmet biztosítani. Ennek oka, hogy különböző sérülékenységek kihasználásával meg lehet őket kerülni, illetve a szóbeli szándékos vagy véletlen szivárgás ellen nem védenek. A védelmi megoldások megkerülését segíti elő az okostelefonok elterjedése. Ezeknek az eszközöknek a segítségével könnyen készíthetőek fényképek, videó- és hangfelvételek, melyek különböző titkosított csatornákon a mobilinternet segítségével azonnal, akár visszakövethetetlen módon továbbíthatók.

Mivel az emberek a saját buborékukban élnek, nem is biztos, hogy feltűnik számukra, ha szenzitív információkat árulnak el egy beszélgetés során. Még ha tudják is, hogy a közvetlen munkájuk kapcsán mi számít ilyennek, az már nem biztos, hogy a kollégájuk szakterületét megfelelően ismerik és így árulhatnak el egy célzott social engineering[14] támadás során önkéntelenül a támadók számára hasznos információmorzsákat.

Az információszivárgás elleni védelem és a kiber-ellenállóképesség, azon belül főleg az emberi tényező fejlesztéséhez fontos megismerni az elmúlt évtizedek technológiai fejlődését és a minket körülvevő társadalmi környezetet.

[13] A BYOD rövidítés feloldása a Bring Your Own Device. Ez magyarul annyit tesz, hogy „Hozd a Saját Készülékedet”.

[14] Az emberek manipulációján keresztül történő, általában információszerzésre irányuló támadási formát nevezzük social engineeringnek A kifejezésnek nincs általánosan elterjedt magyar fordítása. A szakma az angol terminológiát vette át, ezért a disszertációmban én is ezt használom.

1.1. A Kiberbiztonsági megközelítés

Az elmúlt 20-30 év digitalizációja fontossá tette nem csak a fizikai, de a kibertér kialakulásával annak védelmét is [10]. Ebben a fejezetben bemutatom a kiberbiztonságot holisztikus nézőpontból.

1.1.1. Információs társadalom és veszélyei

A mai értelemben vett információszerzési gyakorlatokat egy hosszú folyamat előzte meg. Történelmünk korai szakaszában a fő információforrás a közvetlen környezet érzékszerveikkel történő megismerése volt. Később a hangokból és a mutogatásból létrejött a beszéd. Ezt követően elkezdte az emberiség tökéletesíteni az információtárolás eszközeit, kezdve a rajzokkal, majd folytatva az írással, a nyomtatással, és később különböző analóg, illetve digitális tárolási eszközökkel. Az információ értelmezésében az 1948-as év nagy fordulópont volt, hiszen ekkorra datálhatjuk két új tudomány megszületését, mely nagyban elősegítette az információs társadalom létrejöttét. A kibernetika alapjának Norbert Wiener könyvét [11] tekinthetjük, illetve az információtudomány kialakulása Claud Shannon tanulmányának [12] publikálásához köthető [13].

Társadalmunk jelenlegi berendezkedésének egyik alapja, hogy az információhoz nagyon gyorsan hozzá tudunk jutni. Alapjait a nemzetállamok teremtették meg a 80-as években saját analóg mobiltelefon-hálózatuk kiépítésével, melyet a 90-es években a kapacitás és a bitsebesség növelése érdekében felváltottak a 2G[15], később a 3G[16] technológián alapuló rendszerek [14]. A technológiai fejlődés azonban tovább gyorsult. A telekommunikációs cégek a 2010-es évek vége óta már a negyedik generációs hálózatokat is túlszárnyaló 5G technológián és annak bevezetésén dolgoznak.

A hálózatok és az eszközök fejlődése elősegítette a kommunikáció gyorsaságának és annak hatékonyságának növelését, így az információk elérése már nem csak egy szűk elit privilégiuma lett, hanem egyre szélesebb körben bárki megismerheti az érdeklődési körének megfelelő írásos és multimédiás tartalmakat. A hordozható eszközök (laptopok, notebookok, ultrabookok, okostelefonok, tabletek és e-book olvasók) elterjedése lehetővé tette a mindennapok emberei számára az információk folyamatos becsatornázását, melyet a felhő-technológia [15] és a viselhető eszközök (pl.: okosórák,

[15] Négy 2G telekommunikációs technológia van jelenleg használatban. Ezek a következőek: GSM, cdmaOne, TDMA és PDC.
[16] UMTS és cdme2000.

okoskarkötők) térhódítása tovább gyorsított az értesítések azonnali olvashatósága révén. Az újabb és újabb technikai megoldások, a rájuk épülő szolgáltatások [16] és alkalmazások rohamos fejlődése, a hatalmas adatmennyiség (big data[17]) elérhetősége [17] 2021-re azt eredményezte, hogy emberek számára problémát jelent a releváns és hiteles információk kiszűrése az őket érő folyamatos áradatban.

Az információsokaság és annak könnyű elérhetősége nem csak a hétköznapi emberek szempontjából fontos. A kibertér offenzív szereplői is könnyen hozzáférhetnek a számukra érdekes és releváns információkhoz mind a nyílt interneten, mind a kereső motoroktól elrejtett ún. DDW-n[18]. Rövid keresés után megismerhetik azokat a támadó technikákat, bevált megoldásokat, amik segítségével elérhetik céljaikat. Az információáradat ráadásul segít számukra a rejtőzködésben, mely a defenzív oldal munkáját nehezíti meg.

A megfelelő információk szelekcióját tovább nehezíti, hogy nem csupán hiteles, lektorált, hivatalos médiumokhoz, forrásokhoz férhetnek hozzá az emberek. Az internet és főleg a közösségi média adta lehetőségek segítségével bárki létrehozhat írásos és multimédiás tartalmakat [18], mely elősegíti az álhírek gyártását és terjedését. Ez már önmagában nagy veszélyt hordoz [19]. Az álhírek és a különböző tartalomjavasló algoritmusok által létrejövő ún. szűrőbuborék hatás [20] és a közösségi hálózatokon történ információ terjedésének [21] eredményeképpen egy megfelelően előkészített kampánynak akár választásokat is befolyásoló hatása is lehet [22].

A gyors technológiai fejlődésnek azonban más, a biztonságot érintő árnyoldala is van. Az egyre növekvő fogyasztói elvárások nagy nyomást gyakorolnak a szoftver- és hardvergyártókra. Minél gyorsabban újabb és újabb termékekkel kell, hogy előálljanak, így nincs elegendő idejük minden részletre kiterjedő fejlesztésre, és a megfelelő teszteléseket sem tudják elvégezni. A biztonság a legtöbb esetben nem számít prioritásnak, és így nem valósul meg az ún. safety-by-design[19] elv sem a tervezés során. Ennek eredménye, hogy különböző sérülékenységek maradnak a szoftverekben és hardverekben, melyeket a rosszindulatú támadók ki tudnak használni, illetve meg

[17] A big data kifejezést a nagy mennyiségű és komplex adatok feldolgozására használják.
[18] DDW, azaz Deep and Dark Web. Az ún. Deep Web az internet nem kereshető (nem indexelt) tartománya, mely becslések szerint a teljes online tér 90%-át teszi ki. Ennek egy apró, védett részegysége a Dark Web.
[19] A safety-by-design elv célja, hogy egy hardver, szoftver vagy rendszer tervezése során törekednek a lehető legmagasabb szintű biztonság elérésére a tervezők.

tudnak osztani egymással úgy, hogy a felderítésükre szakosodott cégek, szervezetek reális időn belül ne tudják pontosan beazonosítani őket [23].

Mivel a piac felől folyamatos újítási és fejlesztési nyomás érkezik, ezért bizonyos esetekben a javítás helyett inkább az új termék bevezetésére koncentrálnak a gyártók. Így maradhatnak évekig, akár évtizedekig sérülékeny eszközök és programok a piacon. Ráadásul a felhasználók többsége nincs tisztában a kockázatokkal és veszélyekkel, így a gyártók többsége nem fordít energiát a probléma kezelésére, megoldására. Ez a mentalitás is hozzájárul számos támadás sikeréhez, holott könnyű szerrel megelőzhetőek lennének [24]. A leghíresebb támadás a 2016-os ún. IoT eszközök[20] segítségével elkövetett korábban említett Mirai botnet támadás [25], ahol kb. 20 óra alatt több százezer eszköz fertőződött meg [26].

A különböző szoftverek, hardverek és az ezeket összekötő firmware-ek szorosan összefüggenek, ezért nem beszélhetünk csupán egy-egy különálló termékről, hanem összetett rendszerekben kell gondolkodni, úgy, hogy az elemek külön-külön és egyben is a lehető legbiztonságosabbak legyenek [27].

1.1.2. Kiberbiztonság múltja és jelene

A kiberbiztonság létrejöttének alapjait azok a támadások eredményezték, melyek a különböző informatikai eszközöket érték. A legelső internetes kártevő felbukkanását a disszertáció írása előtt több mint 30 évvel, 1988. november 2-án jegyzik. Ez volt a Morris-féreg [28]. Az internet létrejöttekor azonban még korántsem volt a maihoz hasonló méretű a „világháló”. Ekkor főleg egyetemi és katonai végpontok alkották a közel sem tökéletes, számos hibával rendelkező hálózatot. Ezekre a problémákra világított rá tudományos célokkal a Cornell Egyetemen a Morris-féreg megalkotója, Robert Tappan Morris Jr. [29].

Az elmúlt évtizedekben azonban sokat változott a kibertér. Számos, történelmileg is fontos esemény történt azóta, mely nem csak lokális problémát jelentett, de kihatással volt a világ hozzáállására a kiberbiztonság kezelésével kapcsolatban. Ahhoz, hogy értelmezni tudjuk a különböző eseményeket, azok összefüggéseit és következményeit fontos meghatározni, mit értünk e fogalom alatt. A kibertér *„…az elektronikus kommunikációs eszközök és rendszerek (számítógép-hálózatok, telefonvonalak,*

[20] Internet of Things – dolgok internete: Az internetre kötött „okos” eszközök gyűjtőneve (IP kamerák, routerek stb.).

műholdas rendszerek stb.) és a rajtuk található szolgáltatások, információk alkotta virtuális tér vagy világ összefoglaló neve" [30]. Ennek a térnek azonban nincsenek nemzetállamokhoz vagy szervezetekhez köthető fizikai határai, ezért más megközelítés szükséges a támadások vizsgálatakor és a különböző védelmi kontrollok bevezetésekor. Mindezek mellett a különböző rejtő, anonimizáló technikák miatt soha nem lehetnek száz százalékig biztosak a biztonsági szakemberek a támadók kilétében.

A kezdetekhez képest több, nagyságrendekkel nagyobb internetes hálózat, a sokkal összetettebb alkalmazások, a számtalan elterjedt technikai és technológiai újítás hatására újabb és újabb, a minket körülvevő digitális infrastruktúrák ellen irányuló fenyegetettségek jelentek meg. A 2001. november 23-án Budapesten az ún. Cybercrime[21] egyezmény [31] aláírásának a ténye is megmutatja, hogy egyre nagyobb teret kapott a haszonszerzés céljából elkövetett kiberbűnözés az elmúlt évtizedekben. Az illegális pénzszerzésnek számos fajtáját lehet tetten érni manapság a kibertérhez köthetően.

Fontos megemlíteni azonban azokat a támadásokat is, melyek nem csak a technikai szakemberek körében voltak számottevőek, de politikai, diplomáciai szempontból, történelmileg is jelentősek voltak. 2007-ben Észtország ellen irányuló megosztott túlterheléses támadás (DDoS[22]) elindított egy folyamatot, mely hatására 2016-ban a varsói csúcstalálkozón a NATO[23] a kiberteret a 4. műveleti terévé emelte be. Ez a gyakorlatban azt jelenti, hogy a szövetség elleni támadásnak tekintik a tagállamok elleni koordinált kibertámadást [32]. A mai napig úgy sejtik az elemzők, hogy az észtek elleni támadás mögött Oroszország állt, azonban ezt Moszkva soha nem ismerte be. Az oroszokhoz köthető az első olyan kibertámadás is, melyet egy konkrét (orosz-grúz) háborús konfliktusban indítottak 2008-ban egy kinetikus harc megsegítésére [33]. Fontosnak tartom még megemlíteni a 2010-es Stuxnet fizikai térben is károkat okozó esetét [34], [35], mely az első olyan kibertámadás volt, ahol konkrét fizikai kárt okozott egy rosszindulatú számítógépes kód. Az iráni atomdúsító turbináit túlpörgető malware évekre vetette vissza az ország atomprogramját.

[21] Magyarul Számítástechnikai Bűnözés Elleni Egyezmény.
[22] A DDoS (Distributed Denial of Service), azaz elosztott túlterheléses támadás célja, hogy a támadó olyan mennyiségű adatcsomaggal támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, hogy a fogadó oldal elérhetetlenné válik, mivel nem tudja feldolgozni a beérkező adatmennyiséget.
[23] A NATO a North Atlantic Treaty Organization rövidítése, melyet magyarul az Észak-atlanti Szerződés Szervezetének hívnak. Célja az észak-amerikai és európai tagállamok szabadságának és biztonságának megőrzése politikai és katonai eszközökkel.

Noha több nagy incidens történt az elmúlt évtizedben is, aminek akár globális érintettsége van, a szakembereknek általában kisebb horderejű támadásokkal kell megküzdeniük. Ennek ellenére fontos azt látni, hogy akár nemzetállamok, szövetségi rendszerek egymás elleni tevékenységéről, akár egy-egy szervezet incidenséről is van szó, a támadók által kihasznált támadási módok gyakorlatilag ugyanazok. Az ENISA által minden évben kiadott riport [36] alapján a legkritikusabb fenyegetettségek az elmúlt években gyakorlatilag nem változtak. A különböző malwarek okozta károk, a webalapú, illetve webes alkalmazásokat célzó támadások, valamint a phishing[24] kampányok évek óta a toplista tetején helyezkednek el.

Ezek a támadások azért is lehetnek sikeresek, mert a technológia gyors fejlődését az emberek nem tudják követni. Az átlagember nem érti és nem is akarja megérteni, hogyan működnek a különböző eszközök és alkalmazások, hiszen mindennapi életét nem befolyásolja jelentősen ennek az ismeretnek a hiánya.

Jellemző az a gondolkodás is, hogy ők nem elég érdekesek vagy fontosak, ezért őket nem fenyegeti – az általuk sokszor nem is ismert – veszély. Természetesen minden vállalatnak, állami szervnek más és más a fenyegetettségi profilja a tevékenységi körétől, a geopolitikai szerepvállalásától, a digitális fejlettségétől függően. Éppen ezért kell kockázatarányosan fejleszteni a védekező és reagáló képességeket úgy a technológia, mind az emberi tényező oldaláról. Mindezeket a kockázatokat ráadásul nem csak statikus értelemben kell kezelni, hanem figyelembe kell venni az egyre elterjedtebb dinamikus, agilis szervezetfejlesztés által keletkező problémákat.

1.1.3. A kibertámadások mögötti motivációk

Számos motiváció lakozhat a különböző károkozó tettek között a kibertérben. Legegyszerűbb, de sokszor a legveszélyesebb fajtája azok az egyéni tettek, melyeket egy sértett munkavállaló követ el az aktuális vagy korábbi munkahelye ellen. Ezekben az esetekben az elkövetőnek konkrét ismerete van a belső folyamatokról, rendszerekről, így célzottan tud akár helyreállíthatatlan kárt is okozni. A sértettség mellett az egyszerű tudás vagy hatalom fitogtatástól kezdve, a ranglétrán történő előrejutás megsegítésén át a nyerészkedésig vagy a szexuális motivációig számos más motiváció is lehetnek akár

[24] Más néven adathalász támadások.

egy úgynevezett script kiddie[25] vagy egy fehér, szürke, vagy fekete kalapos [37] egyén által elkövetett támadás mögött.

A különböző internetes csalások, a jogtalan felhasználások a szervezett bűnözés egyre közkedveltebb módszereivé váltak. Ilyen tevékenységre alkalmazzák például – az eredetileg más célokra készült – TOR (The Onion Router) böngészőt, az általa kínált lehetőségeket kihasználva a DDW-en virágzik az illegális fegyverek, emberek, egzotikus állatok, lopott áruk és információk haszonszerzés céljából történő értékesítése. Gyakorlatilag minden területen, ahol pénz cserél gazdát, megjelentek a kiberbűnözők, így elérhetők illegális szerencsejáték-oldalak, felbérelhetünk tolvajokat, bérgyilkosokat, rosszindulatú hackereket és az illegális szexkereskedelemnek is nagy piaca van [38], mint ahogy a pedofil tartalmaknak is [39].

A kiberbűnözők mellett beszélhetünk még hacktivizmusról, kiberterrorizmusról, kiberhírszerzésről és kiberhadviselésről is [40]. Az ún. hacktivista csoportok olyan aktivista tagokból álló csoportok, akik valamilyen politikai, nemzeti, vallási, szociális vagy más világnézeti véleményüket vagy ellenvéleményüket, nemtetszésüket a kibertéren keresztül próbálják kifejezni és eljuttatni másokhoz. A hacktivizmusnak jellemzően kevésbé káros eszközei vannak. Ilyen lehet például weblapok kompromittálása vagy elérhetetlenné tétele, de vannak ez alól is kivételek. Az egyik legismertebb ilyen szervezet a nemzetközi Anonymus hackercsoport, akik nem csak egy, hanem több különböző témában is aktívak. 2017-ben Magyarország kormánya ellen hirdettek politikai háborút, de 2015-ben az Iszlám Állam (ISIS) aktív tevékenységeire reagálva a terrorizmusnak üzentek hadat a közösségi médián keresztül.

Az ipari és nemzetállami szintű kiberhírszerző tevékenység, a nemzetközi szakzsargonban ún. CYBINT fő célja a védett információk megszerzése különböző nyílt vagy zár számítógépes hálózatokból [41]. Ezeket a támadásokat általában közvetlen módon követik el, azaz valamilyen ún. backdoor[26] segítségével konkrétan hozzáférnek a kívánt információforráshoz. Egy 2018-ban napvilágot látott ilyen eset például a holland AIVD beépülése a korábban említett APT29 hackercsoport rendszereibe [42]. Akadnak azonban olyan nem szokványos, ún. side channel[27] támadások, melyek során közvetett

[25] Automatizált eszközökkel dolgozó, kisebb hacker tudással rendelkező egyén elnevezése.
[26] A back door kifejezést magyarul hátsó kapunak szokták fordítani.
[27] A side channel támadásokat oldalsó csatornás támadásnak lehet fordítani. Ezek nem egy algoritmus gyengeségén alapszanak, hanem a konkrét informatikai eszköz vagy rendszer megvalósításából fakadó gyengeséget használják ki.

módon különböző elektromágneses, akusztikus vagy optikai jelek segítségével dekódolnak információkat vagy egy előzetes sikeres, szoftverek vagy hardverek normál működését módosító támadás után direkt sugároznak ki információkat. A kiberhírszerző műveletek célja általában, hogy minél hosszabb ideig rejtve maradjon a konkrét tevékenység, így minél sikeresebben, a lehető legtöbb információt szivárogtathassák ki a támadók.

A kiberterrorizmus fő célja valamilyen radikális ideológiai vagy vallási kinyilatkoztatás [43]. Általában ezek a csoportok egy fizikai térben működő terrorista szervezethez tartoznak. Ténykedésüket összhangban az „anyaszervezet" munkájával, azt kiegészítve végeznek propaganda-, toborzó- és hittérítő tevékenységeket. A különböző titkosított és/vagy rejtett csatornák segítségével tudnak kommunikálni egymással, illetve a működéshez szükséges adományok egy részét is a kibertéren keresztül gyűjtik be. Az aktív támadások közül leginkább a pszichológiai hadviselésre épülő technikákat alkalmazzák [44], mint például az Iszlám Államhoz köthető United Cyber Califhate szervezet Egyesült Államok és Egyiptom ellenes plakátkampánya [45].

Kiberhadviselésnek nevezzük azokat a különböző (pl. információs [46]) kiber műveletekből álló tevékenységeket, melyeket egy nemzetállam egy másik ellen háborús céljainak megsegítésére követ el [47]. Mivel ilyen típusú támadást konkrétan még soha egy nemzetállam sem vállalt magára, ezért nagyon óvatosan kell a politikai és katonai döntéshozóknak reagálni egy-egy ilyen támadásra, még akkor is, ha a különböző modus operandik alapján erősen sejthetőek az elkövetők.

Az elmúlt évtizedben egyfajta hidegháború alakult ki a kiberfegyverek fejlesztésével kapcsolatban. Egyre több nemzetállam és szövetségi rendszer nyilvánosan vállalja fel védekezőképességének fejlesztését. Ráadásul több nagyhatalomról lehet tudni publikus stratégiákból, kinyilatkoztatásokból, hogy nem csak defenzív, hanem offenzív képességei is vannak.

1.2. A célzott támadások

Nyilvánvalóan a halászó típusú támadásoktól az különbözteti meg a célzott eseteket, hogy a támadónak valamilyen konkrét indítéka és célja van az adott szervezet (vagy személy) megtámadására. Nagyon fontos körülmény, hogy a rosszindulatú félnek általában elegendő ideje van megfelelő mennyiségű és minőségű információt gyűjteni a védelmi megoldásokról, a különböző informatikai eszközökről és a munkaerőről is.

Ezek birtokában specifikusan tud lépéseket tenni a célja elérésére. Az ilyen esetekben a hatékonyság jóval magasabb tud lenni, mint általában [27]. Egy megfelelően előkészített célzott támadás szinte kivédhetetlen, hiszen a célszemélynél önkéntelen reakciók lépnek működésbe.

1.2.1. A célzott támadások általános felépítése

A humán kockázat megismeréséhez szükséges megérteni az informatikai infrastruktúrák elleni támadások felépítését. Az értekezésen túlmutat ezek részletes, különálló ismertetése a számosságuk miatt, ezért általánosságban, néhány ismertebb példán keresztül mutatom be a fő lépéseket.

A célzott kibertámadás első lépése az információszerzés (*felderítés*), amit a támadási eszközök előkészítése (*fegyverkezés*), majd azoknak a célrendszerhez történő eljuttatása (*szállítás*) követi. Itt a kód lefuttatásra kerül (*sérülékenységek kihasználása*), mely segítségével a támadó egy hátsó ajtót telepít (*telepítés*), mely lehetővé teszi az áldozat eszközéhez történő minél hosszabb ideig tartó, szabad átjárást. Ezután kerül sor annak a kétirányú csatornának a kiépítésére (*irányítás*), melyet alkalmazva a céljainak megfelelően tud tevékenykedni (cselekvés) [48]. Ezt a jellemző felépítést nevezzük Cyber (Security) Kill Chain[28]-nek, melyet az *1. ábra* szemléltet.

1. ábra - A Cyber (Security) Kill Chain (saját szerkesztés)

Minden célzott támadás alapja, hogy a támadó a lehető legtöbb információt gyűjtse össze a szervezetről, a célszemély(ek)ről, a célobjektumról és annak fizikai környezetéről és IT[29] infrastruktúrájáról, a hálózati topológiájáról, az azt alkotó eszközökről, a számítógépek operációs rendszeréről, böngészőjének verziójáról, a nyitott portokról, az elérhető szolgáltatásokról, az alkalmazott biztonsági megoldásokról és kontrollokról. Amennyiben feltételezhető, hogy a megtámadni kívánt szervezetnél

[28] A kifejezésnek nincs elterjedt magyar megfelelője. A katonai terminológiából átvett kifejezés a kibertámadások jellemző felépítésének fázisait jelenti.
[29] Az IT (Information Technology) az informatikai rendszereket jelöli.

ún. Operation Technology (OT)[30] eszközök is előfordulnak, akkor azokról is a lehető legtöbb információt szükséges begyűjteni [49]. Ezeknek az eszközöknek a biztonságára ugyanis általában kevesebb figyelmet fordítanak, pedig jelentős károk okozhatók [50], ha sikerül a támadónak átjutni a 0. és 1. szintig – a Purdue modell[31] szerinti – ún. DMZ[32]-n keresztül.

Miután a támadó rendelkezésére áll a lehető legtöbb információ, eldönti, hogy (a) technológiák, eszközök, programok sérülékenységeit használja ki, (b) a nem megfelelően kialakított biztonsági kontrollokat játssza ki vagy (c) egy eredetileg más felhasználásra szánt technológiát vagy szolgáltatást nem rendeltetésszerűen, ártó szándékkal alkalmaz [27].

Egy informatikai rendszer hackelésének is megvannak az általános lépései [51], melyeket el tudunk helyezni a Cyber Kill Chain-en is (1. *táblázat*). A felderítés szakaszának első lépése a passzív információgyűjtés. A támadók itt az internet adta lehetőségek miatt számtalan lehetőséget vehetnek igénybe. Jellemző információforrások például a közösségi média, whois[33] rekordok vagy kereső motorok célzott használatával (pl. GHDB[34] segítségével) megkapott eredmények. Szintén a felderítés szakaszába tartoznak a szkennelési eljárások, melyek eredményeképpen a támadó megismerheti az elérhető szolgáltatásokat, eszközöket, a szervezet által alkalmazott operációs rendszerek, böngészők pontos típusát, esetleg a biztonsági megoldások egy részét vagy adott esetben a hálózati topológiát. Az így megszerzett ismeretek alapján olyan információkat (jellemzően felhasználó név – jelszó párosokat, felhasználói csoportokat és a hozzájuk tartozó jogosultságokat, nyitott TCP/UDP portokat[35] vagy a futó lokális és rendszerszintű alkalmazások listáját) próbálnak megszerezni, amely segítségével hozzáférhetnek a cél a rendszer(ek)hez.

Ezt követő lépések már sokkal összetettebbek és többnyire magasabb szintű szaktudást igényelnek. Itt már konkrétan az a cél, hogy a támadó „bejusson” a rendszerbe. Ha

[30] Az OT (Operation Technology) az ipari irányítási rendszereket jelöli.
[31] A Purdue modell a biztonságos architektúrát mutatja be az ipari irányítási rendszerekben. 4 biztonsági zóna és 6 szint található benne.
[32] A DMZ (demilitarized zone, azaz magyarul demilitarizált zóna) egy olyan fizikai vagy logikai alhálózat, amely az internet és a szervezet belső hálózata között helyezkedik el.
[33] A whois rekordok tartalmazzák többek között egy-egy domainhez tartozó alapinformációkat.
[34] A GHDB (Google Hacking Database) egy olyan adatbázis, amely a Google keresőmotorjának célzott alkalmazásához szükséges kulcsszavakat, keresési kifejezéseket tartalmazza.
[35] A TCP/IP (Transmission Control Protocol) és UDP (User Datagram Protocol) hálózatok logikai csatlakozási pontjai.

korábban nem sikerült konkrét felhasználó név-jelszó párosokat szereznie, akkor ebben a szakaszban használhat különböző jelszótörő vagy hozzáférést segítő más technikákat. Utóbbira példák a különböző ún. MitM[36] módszerek (pl. SL Strip, Burp Suite, Browser Exploitation Framework[37] stb.) vagy trójai falovak, kémprogramok[38], keyloggerek[39], jelszó hashek[40] bejuttatása a célrendszerbe. Ezeket a lépéseket követi a támadó céljához szükséges hozzáférések és jogosultságok megszerzése, majd a támadás után a nyomok eltűntetése. Abban az esetben, ha a támadó szeretné biztosítani, hogy a jövőben is hozzáférhessen a rendszerhez, akkor utolsó lépésként olyan hátsó kapukat hagy nyitva maga után, amelyet feltételezhetően később is feltűnésmentesen használni tud.

<table>
<tr><td rowspan="3">Felderítés (Reconnaissance)</td><td>Passzív információszerzés (Footprinting)</td></tr>
<tr><td>Szkennelés (Scanning)</td></tr>
<tr><td rowspan="2">Behatolási kísérletek (Enumeration)</td></tr>
<tr><td rowspan="2">Fegyverkezés (Weaponization)</td><td rowspan="5">A rendszerbe történő bejutás (System Hacking)</td></tr>
<tr><td>Szállítás (Delivery)</td></tr>
<tr><td>Sérülékenységek kihasználása (Intrusion, Exploitation)</td></tr>
<tr><td>Telepítés (Installation)</td></tr>
<tr><td>Irányítás (Command and Control)</td></tr>
<tr><td rowspan="3">Cselekvés (Actions on Objective)</td><td>Jogosultságok kiterjesztése (Escalation of Privilege)</td></tr>
<tr><td>A nyomok eltűntetése (Covering Tracks)</td></tr>
<tr><td>Hátsó kapuk nyitva hagyása (Planting of Backdoors)</td></tr>
</table>

1. táblázat - A hackelés lépései a Cyber Kill Chain-en (saját szerkesztés)

[36] A MitM (Man int he Middle) közbeékelődéses támadást jelent.
[37] SL Strip, Burp Suite, Browser Exploitation Framework támadási technikák.
[38] A kémprogramok olyan malwarek, amik információk gyűjtésére és adott esetben továbbítására szolgálnak.
[39] A keylogger kifejezést eredetileg a billentyűzet leütését naplózó szoftverekre és hardverekre használták. Ma az okostelefonok idejében sokszor ehelyett képernyőképeket készítenek.
[40] A hash egy olyan egyedi karaktersorozat, amely valamilyen digitális tartalomból egy algoritmus segítségével lenyomatként keletkezik.

1.2.2. A social engineering, azaz emberek ellen irányuló célzott támadások művészete

Douglas P. Twitchell a social engineeringet[41] általánosságban a csalásnak vagy a rábeszélésnek az információ vagy az ingóságok megszerzésére irányuló cselekvéseként értelmezi, kitér arra, hogy a fogalmat gyakran használják számítógépes rendszer, vagy annak információtartalmával kapcsolatban [52]. Christopher Hadnagy könyvében kicsit tovább megy ezen az értelmezésen. Ő azt írja, hogy a social engineering a művészete, sőt a tudománya az emberi lények gyakorlatias műveletekkel történő befolyásolásának annak céljából, hogy az alany a kivitelező célja érdekében cselekedjen. Ez alatt érthetjük a rosszindulatú támadók mellett a hisztivel manipuláló kisgyerekeket és azokat a pszichológusokat, orvosokat is, akik egy jó cél érdekében a pácienseket befolyásolják [53]. A módszer egyik kiemelkedő alakja, Kevin D. Mitnick *A megtévesztés művészete* című könyvében [54] így értelmezi a kifejezést:

„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer[42] *tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy a nélkül – képes az embereket információszerzés érdekében kihasználni.”*

A fenti megfogalmazásokból is látszik, hogy a fogalomnak számos aspektusa lehet. Értekezésem során továbbiakban a social engineering alatt azonban én csak azokat a – főleg információszerzés céljából elkövetett – támadásokat értem a kiberbiztonsággal összefüggésben, amelyek az agy manipulációjával az emberi tényezőt használják ki a rendszerek technikai sérülékenységei helyett.

Ezek a módszerek azért is tudnak hatékonyan működni, mert az emberek alapvetően szeretik minél jobban megkönnyíteni az életüket és a munkájukat, így viszonylag gyakran hágnak át egy-egy szabályt vagy hagynak figyelmen kívül egy útmutatást éppen csak egy kis mértékben. Jó példa erre a közlekedési lámpa sárga jelzése utáni „átcsúszás”. Tulajdonképpen az elkövető ebben az esetben is érezheti azt, hogy csak kis hibát követett el. Mivel saját magának nem akar senki sem rosszat, ezért értelemszerűen ebben az esetben nem fogja felhívni a szabályszegő a rendőrséget, hogy bevallja a piros lámpán történő áthajtás tényét.

[41] A kifejezésnek nincsen megfelelő magyar fordítása
[42] A social engineering tevékenységet folytató személy.

Ez az analógia értelmezhető az informatikai rendszerek használata és az esetleges szándékos vagy vétlen információszivárogtatással kapcsolatban is. A social engineer úgy építi fel a támadásait, hogy a célszemély agya nagy valószínűséggel az adott pillanatban éppen figyelmen kívül hagyjon egy furcsaságot, vagy, hasonlóan a piros lámpán történő átcsúszáshoz, az eset ne tűnjön olyan súlyosságú esetnek, amivel foglalkozni kellene. A támadók mindent megtesznek, hogy minimalizálják a kockázatát annak, hogy a célszemélyben tudatosuljon az illetéktelen segítség ténye, vagy az estet ne lépje át a szakmai szervezetek felé történő bejelentési szándék küszöbét. A tervezés szakaszában arra is odafigyelhetnek, hogy bizonyos személyek egyszerűen nem érzik komfortosan magukat, ha másoknak el kell mondani valamit [55].

A támadók dolgát segíti a korábbi fejezetben ismertetett információdömping, amely remek alapja egy jól felépített támadásnak vagy támadássorozatnak. Ráadásul a sokszor rohanó világban a gyakran túlterhelt emberek szeretnének minél hamarabb túlesni egy-egy gyorsan elvégezhető feladaton. A támadók ezekre a körülményekre jól tudják felépíteni a célzott szándékuk szerinti befolyásoló, meggyőző, irányító támadásokat, melyek az alapvető emberi tulajdonságokra épülnek. Ilyen lehet például a segítőkészség, jóhiszeműség, megtéveszthetőség, naivitás mellett számos más jellemvonás, melyek megfelelő, tudatos alkalmazásához a támadónak tisztában kell lenni a személyiségpszichológia által ismertetett embertípusokkal [56] és a szociálpszichológia egymásra hatásainak [57] területével, és, mivel általában egy szervezet munkatársa ellen irányulnak, a munkapszichológiával [58] is, a technikai tudás mellett.

A social engineerek a támadás típusától, a célszemélytől és az adott helyzettől függően számos kommunikációs technikát alkalmaznak a céljuk eléréséhez [53]. A manipuláció során a profi támadók a személyiségfelvétel mellett [59] jó benyomást próbálnak kelteni [60], illetve figyelik a verbális és nonverbális jelzéseket, a cél eléréséhez leginkább megfelelő kérdezési technikákat alkalmaznak, és megpróbálják megismerni a célszemély információbefogadására használt domináns érzékszervét (látás, hallás, tapintás) [61], hogy a lehető legjobban tudjanak rá hatni. A befolyásolás hatékonyságának növelése érdekében folyamatosan figyelik a velük szemben álló fél reakcióit, mimikáját és gesztusait [62], valamint igyekeznek összhangot és szimpátiát teremteni a célszemély pszichológiai szükségletei alapján [63]. A jobb eredmények

elérése érdekében az ismereteik alapján különböző befolyásolási technikákat is alkalmaznak [64] figyelembe véve akár a célszemély nemét is [65].

A támadók számára nagy előny, hogy általában nincsenek időkorláthoz kötve, így egy-egy információmorzsa megszerzése közben napok, hetek, de akár hónapok is eltelhetnek. A célzott támadásoknál a támadók igyekeznek minél jobban feltérképezni a támadási pontokat, és a lehető legnagyobb precizitással építik fel a social engineering során felhasználandó történeteket, hamis személyiségeket. Az ilyen alapos tervezés után végrehajtott támadásoknak még a legfelkészültebb szakemberek is áldozatul eshetnek.

A social engineering módszerek alapvetően két, egymástól elkülöníthető csoportba sorolhatók. A humán alapú technikák alkalmazása során a támadónak nincsen szüksége informatikai eszközökre. Ezek olyan cselekedetek, amelyek általában visszakövethetetlenek, vagy visszakövetésük nagy kihívást jelent. Az áldozat sokszor fel sem fogja, hogy egy támadást hajtottak végre vele szemben. Ezeknek az általában egyszeri eseteknek a rekonstruálása nehéz, hiszen a legtöbb esetben csak az áldozat agya által szelektíven tárolt emlékekre hagyatkozhatnak a szakemberek, ha egyáltalán az incidens kiderül, és annak rekonstruálására van szükség. A humán alapú social engineering támadások gyakori ismertetője, hogy a támadók igyekeznek a célszemély környezetére jellemző szlenget és szakkifejezéseket használni.

A másik támadási csoportba az IT alapú technikák tartoznak. Ez esetben ugyan informatikai és technikai eszközöket alkalmaznak, de mégsem azok sérülékenysége, hanem az emberi mulasztás, hiszékenység és más tulajdonságok kihasználásával éri el a támadó a célját. A social engineerek ezeknél a támadásoknál nem „hackelnek” meg a kifejezés klasszikus értelmében rendszereket, csupán kihasználják a technológia adta lehetőségeket.

A fő cél mindkét csoport alkalmazásánál általában az információszerzés vagy a folyamatos információáramoltatás biztosítása. Gyakoriak azok az esetek, amikor nem csak egy technikát alkalmaznak. Több, csak humán vagy csak IT alapú módszer egymással kombinálva sokszor növeli a hatékonyságot, ráadásul vegyes alkalmazásukkal adott esetben még jobb eredmény érhető el. A social engineering alapú technikák alkalmazása során vagy önmagában hasznos, konkrét információ megszerzése a cél, vagy ez egy konkrét technikai sérülékenység kihasználását előkészítő szakasz. Ez utóbbi esetekben a támadó a szervezetnél található informatikai rendszer vagy hálózat

pontos felépítését, egy szoftver vagy hardver bizonyos tulajdonságát szeretné megismerni vagy egyszerűen csak megtudni, hogy bizonyos célra milyen céleszközt vagy célprogramot használnak, esetleg milyenek az árnyékinformatikai megoldások[43]. Előfordulhat tehát, hogy egy hosszú bizalomépítési folyamatnak vagy egy beszélgetésnek csupán annyi a célja, hogy egy IP címet, egy verziószámot vagy egy termék nevét megismerje a támadó.

1.2.3. Humán és IT alapú social engineering technikák

Számtalan különböző social engineering technika létezik, és a technológiai szektor fejlődése újabb és újabb módszereknek biztosít alapot. Ebben a fejezetben éppen ezért inkább tájékoztató jelleggel, magas szinten ismertetem a fontosabb, ismertebb támadási metódusokat.

A humán alapú technikák nagy része azon alapszik, hogy a támadó egy valós vagy fiktív személynek adja ki magát. Egy identitás megszemélyesítése történhet személyesen, hanghívással, üzenetküldő alkalmazások segítségével, e-mail használatával, illetve bármilyen más online vagy offline kommunikáció útján.

A támadók az esetek nagy részében olyan szerepkörbe bújnak, melyekkel kapcsolatos sztereotípiák egy hozzáállási mechanizmust is elindítanak a célszemélyben. Ilyen szerepkör lehet például a mindenki által jól ismert szerelő, takarító vagy ételfutár. Léteznek természetesen más megszemélyesítések is: a támadók kiadhatják magukat a célszervezet vezetőjének, alkalmazottjának, informatikusának vagy egy segítségre szoruló gyakornokának. Felvehetik a partner cég vagy beszállító munkatársának a szerepét, esetleg megszemélyesíthetnek egy hatósági személyt, külső auditort vagy NAV ellenőrt. Amennyiben az adott szituáció úgy kívánja, szélsőséges esetben egy elhunyt ember identitását is felvehetik.

A támadók hatékony manipulációs technikája a célszeméllyel szemben, amikor nem egy konkrét identitást lopnak el, hanem egy harmadik személyre hivatkozva kérnek segítséget. Emellett hatásos eszköz lehet a hamis hatalomfitogtatás, a flörtölés és a pozitív benyomást keltés is. Jó eséllyel vezet eredményre, ha a támadó valamilyen módon az áldozat tudomására juttatja, hogy ő egy probléma megoldásának a szakértője, amit később manipulatív szándékkal elő is idéz. Mivel a célszemély már ismeri, hogy

[43] Az ún. Shadow IT olyan, a szervezet vezetősége, informatikai vagy biztonsági osztálya által jóvá nem hagyott informatikai megoldások, melyek a hivatalos engedély hiánya ellenére használatban vannak a szervezetnél.

kire lehet számítani a megoldásban, ezért könnyen bizalmat szavazhat különösebb előzmény nélkül, és önként belesétál a csapdába. Ez nem feltétlen jelenti azt, hogy az a konkrét informatikai rendszer vagy eszköz hibásodik meg, amihez a támadó hozzá kíván férni. Elegendő azt az érzést keltetni, hogy egy hiba megoldása miatt (pl. áramkimaradás megszüntetése, parkolóhely biztosítása stb.) tartozik az áldozat egy szívességgel. Ezért cserébe a támadó olyan cselekvésre bírja rávenni a célszemélyt (pl. egy idegen pendrive behelyezése a számítógépbe egy oldal nyomtatása végett), amelyre normál esetben nemleges választ kapna.

Lehetséges az, hogy kezdetben nincs lehetősége a támadónak egy konkrét informatikai rendszerhez történő hozzáféréshez. Például ilyenkor fordulhat elő, hogy egy objektumba kell először bejutniuk. A gyakorlott social engineerek számára ez jó eséllyel könnyen megléphető feladat egy kevésbé őrzött helyen, de egy komoly fizikai biztonsággal és őrzésvédelemmel biztosított épületben sem feltétlen lehetetlen. Az ún. tailgating technika lényege, hogy bejutáskor a támadó úgy tesz, mintha egy csoporthoz tartozna és velük együtt surran be. Ennek előkészülete során előfordulhat, hogy egy odaillő ruházatot (öltönyt vagy munkaruhát) használ a tömegbe történő beolvadás segítésére. Másik mód lehet az engedély nélküli belépésre a késés színlelése egy hamis beléptető kártya használatával. A (természetesen) nem működő eszközre hivatkozva gyors bejutási lehetőséget kérhetnek a támadók. A bejutáshoz az ún. piggybacking technikát is alkalmazzák, mely más jogosultságának felhasználásával történő belépést jelenti.

A humán alapú technikák közé tartoznak a gyenge jelszavak [66] kitalálására irányuló támadások, melyeket az emberi tudatlanságot, figyelmetlenséget, nemtörődömséget kihasználva könnyen megfejtenek a támadók. Az alapértelmezett jelszavak (pl. admin, password, jelszó, 0000, 1234, 123456, qwerty stb.) kipróbálása rutinmunkának számít. Egy célzott támadásnál előfordulhat, hogy a közösségi médiában és máshol megadott adatok (pl. születési időpont, rokonok és háziállatok neve, hobbi, kedvenc csapat, sportoló, sztár neve stb.) alapján egy úgynevezett szivárványtáblát építenek fel a jelszavak feltöréséhez [67]. Ennek a nyílt szövegből vagy azok hash értékéből álló adatbázis segítségével nem kell minden lehetséges karaktervariációt kipróbálnia a támadóknak, hanem a célszemélyről gyűjtött adatok kombinálásával a próbálkozási lehetőségeket töredékére tudják csökkenteni. A jelszavak vagy PIN kódokat úgy is megszerezhetik, akár egy generált szituációban is, hogy egyszerűen lelesik azokat a bevitelkor. Ezt a technikát shoulder surfingnek, azaz „váll szörfölésnek” nevezzük.

Mivel sokszor nem figyelnek arra az emberek, hogy mit dobnak ki a kukába, ezért a szemét átvizsgálása számos hasznos feljegyzést, dokumentumot rejtegethet a támadók részére. Ezek vagy teljes dokumentumok, vagy lehetnek olyan papírcetlire írt részinformációk, amelyről az átlagember azt gondolja, hogy nem értékes, azonban a korábban megszerzett információkkal együtt mégis hasznos lehet. Ez az úgynevezett dumpster diving, azaz kukabúvárkodás. A cégeknél található iratmegsemmisítő gép lehet a legjobb védekezési technika ez ellen, de érdemes figyelembe venni, hogy amennyiben a támadónak érdeke fűződik hozzá, még az összeaprított papírt is össze tudja illeszteni.

Ahogy korábban említettem, az IT alapú technikákat a social engineering kapcsán nem egy adott szoftver vagy hardver sérülékenységének kihasználásaként értelmezzük. Ezekben az esetekben arról van szó, hogy egy adott technológia, platform nyújtotta lehetőségeket alkalmazzák a támadók köztes lépcsőként. Hatékony módszer például a klasszikus OSINT kutatás, amely általában az előzetes információszerzés alapja is egyben. Mivel ezekben az esetekben nincs közvetlen kapcsolat a célszeméllyel, így a támadónak kiindulásképpen ez egy kézenfekvőbb módszer. Azért működik nagyon hatékonyan, mert az egyének és a szervezetek rengeteg információt közölnek publikusan a saját honlapjukon. Alkalmanként azonban a webszervereken a látható tartalmakon kívül meglehetősen sok információ található a tulajdonos tudta vagy szándéka nélkül. A kereső oldalak motorjainak megfelelő paraméterezésével könnyen listázhatók ezek az adatbázisok, táblázatok, média vagy más formátumú fájlok, dokumentumok. Egyik legelterjedtebben használt keresőmotorkihasználó-gyűjtemény a korábban említett Google-t kihasználó GHDB.

A weboldalakon kívül a közösségimédia-oldalak és a blogok is valóságos kincsesbányaként szolgálhatnak egy-egy célzott támadás előkészítésekor. A posztok, megosztások, reakciók és a „story” funkcióban kommunikáltak alapján sokszor a célszemély szokásai, személyisége, kedvencei, érdeklődése is megismerhető. Ráadásul akár olyan zsarolásra vagy más módon történő kihasználásra alkalmas érzékeny információk is megtudhatók, mint a vallási és politikai nézet, szexualitás, vagy egészségügyi és anyagi helyzet. Előfordul ráadásul, hogy bizonyos felhasználók olyan fényképeket, videókat osztanak meg, ami alapján egy fizikai támadás is előkészíthető. Ilyen információ lehet például a munkaruha, a beléptető eszköz kinézete vagy az objektumban található konkrét biztonsági megoldások, esetleg azok hiányának ténye.

Az internet és főleg a közösségi médiumok böngészésével megszerzett információk a jelszó töréséhez használt rainbowtábla-építés mellett, például a phishing (adathalász) és ennek célzott típusához, a spearphishing kampányok előkészítéséhez is hasznosak lehetnek. Ezeknek a támadásoknak a lényege, hogy a támadók valamilyen elektronikus csatornán keresztül olyan üzenetet juttatnak el az áldozathoz, ami egy manipulált weboldalra mutató linket vagy fertőzött csatolmányt tartalmaz. Az adathalászatnak a hagyományos e-mail alapú mellett sok változata ismert. Használták korábban csatornának az üzenetrögzítőt, azonban a technológia elavultsága miatt manapság veszített a relevanciájából. Ehelyett ma már inkább az SMS, és főleg az üzenetküldő alkalmazásokon keresztüli üzenetek jellemzőbbek, de létezik az ún. pharming is, ahol a DNS szervert használják erre a célra. A klasszikus phishing (vagy bármelyik változatának) cégvezetők elleni alkalmazását a szakma külön névvel, whalinggel illeti.

A social engineerek munkáját segíthetik olyan malwarek, mint például kémprogramok, leütést figyelő szoftverek (keyloggerek), képernyőképet készítő programok. Közvetett információszerzésre bizonyos esetekben a felhasználó tudta nélkül be tudják kapcsolni az adott eszközbe integrált kamerát vagy mikrofont, de egy okostelefon többi szenzorát is kihasználhatják az eredeti funkcionalitástól eltérően. Ezek a megoldások általában akkor sikeresek, ha nincs megfelelő szerver- és/vagy végpontvédelem kialakítva, nem elég körültekintő, biztonságtudatos a felhasználó vagy ún. nulladik napi (zero-day) sérülékenységeket[44] használnak ki a támadók.

Gyakori social engineering támadás az ún. baiting. A kifejezés alatt azt a malware bejuttatási technikát értjük, amikor valamilyen fertőzött adathordozót (pl. CD-t, pendrive-ot, memóriakártyát stb.) helyeznek el a támadók úgy, hogy a gyanútlan célszemély nagy valószínűséggel megtalálja azt. A rosszindulatú kód lefuthat automatikusan a csatlakoztatást vagy valamilyen felhasználói interakciót (pl. egy fájl megnyitását) követően. Ezeken az adathordozókon a figyelemfelkeltés érdekében gyakori a különböző szövegek (pl.: „érdekes képek”, „bizalmas” stb.) vagy céges logók elhelyezése.

Ugyan a hálózatok klasszikusan vett vizsgálata nem teljesen tartozik a social engineering technikákhoz, de célalkalmazásokkal vagy parancsokkal, illetve céleszközökkel jó hatékonysággal deríthetők fel hasznos információk egy-egy

[44]A zero-day, azaz nulladik napi támadások jellemzője, hogy egy rendszer olyan sérülékenységét használnak ki, amit még nem publikáltak.

célrendszerről. Nagy problémát jelenthet a Wi-Fi, Bluetooth vagy más vezeték nélküli technológia nem körültekintő használata is a felhasználók számára. Ezt kihasználó jellemző támadási módszer a publikus WLAN hálózati hozzáférési pontok hamisítása, melyre a gyanútlan célszemély mit sem sejtve csatlakozik [68], de az okosotthonokban is biztonsági rést jelenthet [69].

1.3. Kritikus infrastruktúrák kibervédelme

Az elmúlt évtizedekben a korábban biztonságosnak hitt információs rendszereken alapuló ipari áramszolgáltató, közlekedésirányító és más létfontosságú rendszerelemek is veszélybe kerültek [70]. Azért tartom fontosnak kiemelni ezeket a szervezeteket, mert két szempont miatt is potenciális felhasználói lehetnek a 4. fejezetben ismertetett modellnek. Egyrészt a kibertámadások egyik kedvelt célpontjai. Másrészt a modellem tartalmaz olyan személyek magánéletére vonatkozó információkat, amelyek egy átlagos piaci szervezetnél (pl. a GDPR[45] [71] megfelelés miatt) nem érhetők el a munkáltató számára.

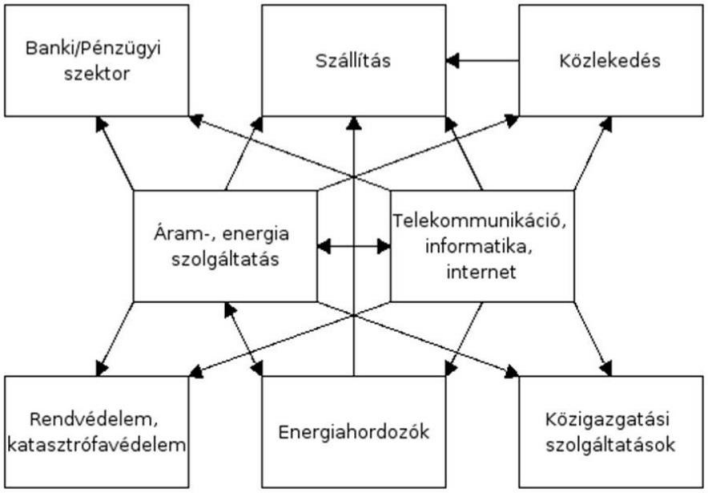
1.3.1. A kritikus infrastruktúrák kibervédelméről általában

Azok a szektorok és szervezetek, amelyek szolgáltatásainak kiesése az egész társadalomra vagy annak egy jelentős részére jelentős hatással lennének, minden országban kiemelt figyelmet kapnak. Ezeket összefoglaló néven kritikus infrastruktúrának, vagy a magyar jogszabályok szerint létfontosságú rendszerelemeknek hívjuk. Beazonosításuk és védelmük a 2001. szeptember 11-ei terrortámadás után még fontosabbá vált a világon mindenhol [72]. Először az Amerikai Egyesült Államok emelte törvényi szintre [73] az 1998-as direktíváját [74], majd a különböző nemzetállamok – így Magyarország [75] – és az Európai Unió (például a 2005-ös Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó európai programról [76] kiadásával) igényeiknek megfelelően ezt átalakítva beemelték ezt saját jogrendjükbe.

A nemzetközi gyakorlatban az energetika, az információtechnológia, a telekommunikáció, a kémiai anyagok és vegyi üzemek, a közlekedési rendszerek, a vészhelyzeti mentőszervek, a mezőgazdaság és élelmiszeripar, a közegészségügy, a vízellátás, a banki és pénzügyi szektor, a nemzeti emlékművek, valamint a védelmi szféra került a védendő ágazatok közé [77]. A területet szabályzó, 2012-ben megalkotott

[45] A General Data Protection Regulation, röviden: GDPR, magyar megfelelője az Általános Adatvédelmi Rendelet, mely célja az EU-n belül élő természetes személyeknek a személyes adatok kezelése tekintetében történő védelme.

magyarországi törvény 1. melléklete [78] a nemzetközi trendeknek megfelelően gyakorlatilag a felsorolt ágazatokat szerepelteti. Ahhoz, hogy valamit kritikus infrastruktúraként lehessen azonosítani Magyarországon, annak a területet szabályzó 2013-as kormányrendelet [79] alapján kockázatelemzést kell végrehajtani a veszteségek, a gazdasági-, a társadalmi-, a politikai- és környezeti hatás és a védelem kritérium mentén.



2. ábra - A kritikus infrastruktúra elemeinek interdependenciája [80]

A különböző kritikus infrastruktúrákat az internet[46] és a technológia fejlődésének hatására egyre nagyobb mértékű, korábban nem létező összefonódás jellemzi, ahogy az a 2. ábrán is szerepel. Emiatt komplex, rendszerszintű kibervédelem kialakítására van szükség. Ennek elősegítése érdekében hozta létre 2014-ben a NIST[47] a specifikus keretrendszerét [82], mely a kormányzati és a magánszektor közös munkája alapján készült ágazat és technológia függetlenül.

Számos szervezet jött létre vagy alakult át az elmúlt években a kibervédelem – és közvetve az összetett kritikus információs infrastruktúrák biztonságának [70] – növelése céljából. Magyarország szempontjából legfontosabb szervezetek az Európai Unió hálózat- és információbiztonságának biztosításáért felelős ENISA, az EU Rendőrségi Hivatalának Európai Kiberbűnözés Elleni Központja (EC3) és a NATO [83], amelynek 2011-es új kibervédelmi politikája is hatással van az országra [84].

[46] Az Egyesült Nemzetek (ENSZ) legrégebbi szervezete, a telekommunikációs szektort összefogó International Telecommunication Union (ITU) 2020-as riportja [81] szerint a világ régiói közül Európában a legnagyobb az internet felhasználók aránya: a kontinens teljes lakosságának 83%-a, a fiatalok (15-24 éves) 96%-a használja.

[47] A NIST (National Institute of Standards and Technology) azaz a Nemzeti Szabványügyi és Technológiai Intézet, az Amerikai Egyesült Államok Kereskedelmi Minisztériumának szabványügyekkel foglalkozó intézménye.

A megfelelő védelmi képességek kialakítása céljából alakultak ki nemzetközi és nemzeti, illetve szektorspecifikus (pl. tudományos, üzleti, kritikus (információs) infrastruktúrákat segítő, kormányzati, katonai stb.) reagáló csapatok (CERT[48]-ek, CSIRT[49]-ek vagy más csoportok[50]) is. Magyarországon jelenleg a *3. ábrán* látható szervezeti struktúrában működnek ezek a szervezetek, mely Magyarország Kiberbiztonsági Stratégiáját [85] kiegészítő (Hálózati és információs rendszerekre vonatkozó) szakpolitikai stratégiája [86], mely az Európai Parlament által kiadott NIS direktíva [87] alapján készült.

3. ábra - Magyarország kiberbiztonsági struktúrája (2019) [88]

Ezek a szervezetek segítik a létfontosságú rendszerelemeket a kibertérből érkező támadások elleni válaszintézkedésekkel, megelőző szolgáltatásokkal, torzulások kezelésével, biztonsági minőségirányítással [89], de a védelem és az ellenálló-képesség kialakítása és folyamatos fejlesztése mindig az adott cég vagy intézet feladata. Ennek érdekében a felsővezetésnek kell mindenek előtt elköteleződnie a terület mellett. Csak így biztosítható, hogy a sokszor ellentétes üzleti, informatikai (üzemeltetési) és biztonsági érdekek megfelelő módon legyenek figyelembe véve.

[48] A CERT-ek (Computer Emergency Response Team), azaz Számítógép Vészhelyzet Kezelő Csoportok olyan szervezeteket takarnak, mely a kiberbiztonság területén különböző szolgáltatásokat nyújtanak megfelelő időben és minőségben. A kifejezést az amerikai CERT Coordination Center (CERT/CC) védette le.

[49] A CSIRT (Computer Security Incident Response Team), azaz Számítógép-biztonsági Incidenskezelő Csoport a CERT európai megfelelője.

[50]Előfordulnak a CERT-eken és a CSIRT-eken kívül más elnevezések is, mint például az IRT (Incident Respons Team) azaz Incidenskezelő Csoport), a CIRT (Computer Incident Response Team) azaz Számítógép Incidenskezelő Csoport) és a SERT (Security Emergeny Response Team) azaz Biztonsági Vészhelyzet Kezelő Csoport).

1.3.2. Egy szervezet kibervédelmi eszközrendszere

Egy szervezet kiberbiztonsága alatt annak információbiztonságának komplex értelmezése értendő, amely védelmi intézkedésekkel és folyamatokkal emelhető egyre magasabb szintre [90]. Alapja a bizalmasság, a sértetlenség és a rendelkezésre állás[51] megteremtése, de fontos elemei a kommunikáció megvalósulása során a letagadhatatlanság, a hitelesség és a jogszerűség is. E célok elérése több dimenzióban lehetséges, melynek fő területei a személyi biztonság, a fizikai biztonság, az adminisztratív biztonság és az elektronikus információbiztonság [91], azonban egy kritikus infrastruktúra esetén ennek más dimenziói is vannak, hiszen felmerülhetnek a kiberteret és annak biztonságát érintő nemzetbiztonsági, katasztrófavédelemi, belbiztonsági, honvédelemi vagy éppen nemzetközi biztonságpolitikai kihívások is [92]. Mindezek mellett a területet állami oldalról jogszabályokkal kell szabályozni, szervezeti szinten külön oda kell figyelni speciális menedzsment szempontokra, oktatásra és nem utolsó sorban a szakemberek mentális egészségére [93]. Magyarország e területet szabályzó 2013. L. törvénye a következőképpen fogalmazza meg a kiberbiztonságot:

„*...a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez működtetéséhez*” [94].

A kiberbiztonság kiépítése nem lehet önkényes, hanem kockázatok mentén szükséges a különböző védelmi intézkedéseket és folyamatokat bevezetni. Egy szervezetnél a biztonságért felelős vezetők feladata az, hogy az üzleti víziót és stratégiát értékeljék és kialakítsák az ezt szolgáló (ha lehet, a humán faktort is figyelembe vevő [95]) kiberbiztonsági politikát, stratégiát, majd akciótervek segítségével mérhető célokat tűzzenek ki az operatív munkát végző kollégák számára. Ehhez azonban a menedzsmentnek mindenekelőtt reális képpel kell rendelkeznie az őket érhető károkról és fenyegetettségekről. A kockázatok ismeretében meg kell határozni, hogy mit és miért kívánnak megvédeni, majd csak ezek tudatában célszerű a megfelelő eszközöket, kontrollokat bevezetni, figyelembe véve a szervezet kiberbiztonsági érettségi szintjét.

[51] E három fogalom angol megfelelőjéből (sorban:confidentiality, integrity, availability) ered az információbiztonság alapjaként használt CIA triád.

A kockázatalapú kezelés azért fontos, mert manapság minden szervezet – legyen szó kis-, közép- vagy nagyvállalatról, államigazgatási szervről – ki van téve a kibertérből érkező veszélyeknek. Nem biztos, hogy célzott támadás áldozata lesz, de a nagyfokú digitalizációból fakadóan jó eséllyel érni fogja valamilyen halászó rosszindulatú tevékenység. Egy nagy kárt okozó incidensnél csak az a rosszabb, ha egy szervezet nem tud az őt érő támadásról, és hamis biztonságtudatban tevékenykedik tovább. Ennek a veszélynek, mint kedvelt célpontnak, a létfontosságú rendszerelemek még jobban ki vannak téve.

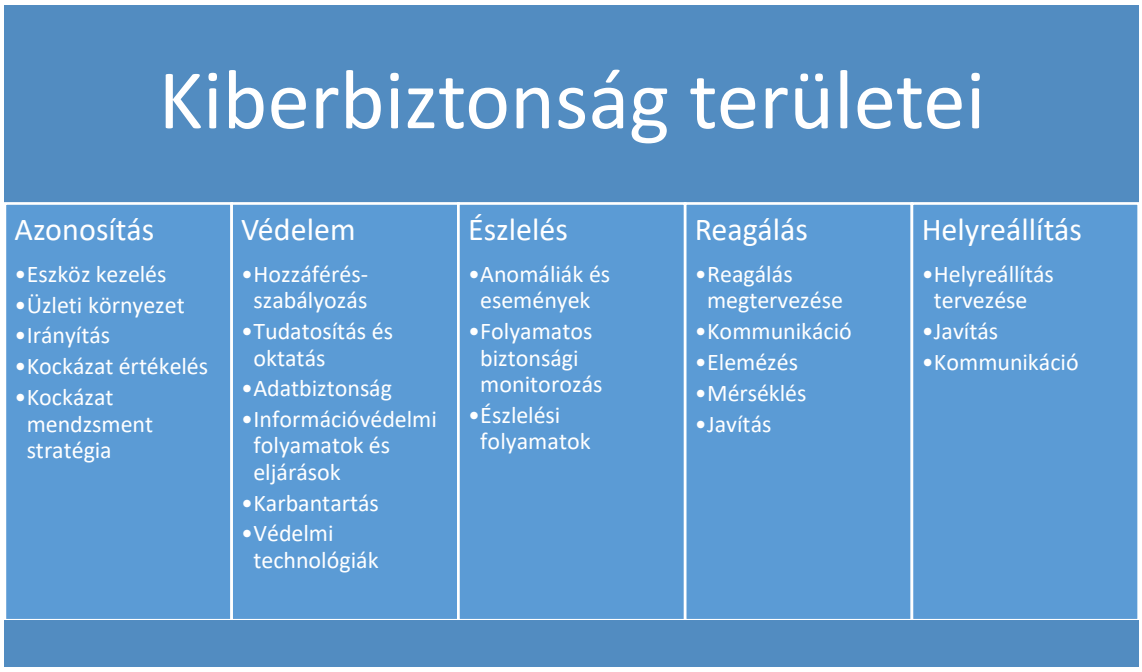
A kockázatok értékelése után természetesen az is lehet egy döntés, hogy nem fordítanak preventív kontrollok bevezetésére, hanem egy incidens bekövetkezése után ad hoc reagálnak az incidensekre. A károk minimalizálása érdekében ennek a stratégiának azonban tudatos döntés alapján kell megtörténnie. Akármelyik utat is választja egy szervezet menedzsmentje, a kár mértéke nagyban függ a reakcióidő mértékétől. Akkor ellenálló egy szervezet, ha a munkavállalók a hétköznapi munkájuk során felismerik a veszélyt, és utána megfelelően reagálnak. Tudniuk kell, hogy a védekezés nem csak a biztonságért felelős szervezeti egység munkatársainak a feladata. Ezért érdemes minden esetben hangsúlyt fektetni az érzékenyítésre, tudatosításra és a kritikus gondolkodás kialakítására.

A konkrét operatív intézkedésekhez, a biztonsági kontrollok kialakítására számos szabvány és ajánlás létezik. Ezek közül fontosabb szabványok [96] az információtechnikai termékek biztonsági szempontjainak értelmezésének közös követelményrendszerét leíró ún. Common Criteria[52], az Információs Irányítási Rendszer (IBIR) bevezetésével, fenntartásával és fejlesztésével ISO/IEC 27000-es szabványcsalád és az informatikaszolgáltatás módszertana (ITIL[53]). A témakörben megkerülhetetlen a NIST által megfogalmazott információbiztonsági és adatvédelmi irányítási elveket tartalmazó NIST SP 800-53 és az ISACA, valamint az IT Governance Institute által kiadott, aktuálisan a 2019-es verziójánál tartó COBIT[54]. Érdemesnek

[52] A szabvány teljes neve Common Criteria for Information Technology Security Evaluation, azaz Közös Követelményrendszer az Információtechnológia Biztonsági Értékeléséhez. Röviden Common Criteria-nak szokás nevezni.
[53] ITIL (Information Technology Infrastructure Library), azaz Az informatikaszolgáltatás módszertana
[54] COBIT (Control Objectives for Information and Related Technology), azaz Informatikai Irányítási és Ellenőrzési Módszertan

tartom még megemlíteni a bankkártyás fizetések biztonságát irányzó PCI DSS[55] szabványt is.

Ugyan különböző dokumentumokról beszélünk, de lényegében mind azt a célt szolgálja, hogy útmutatást biztosítsanak a kiberbiztonság növelésére. A különböző fenyegetettségek ráadásul szektortól, geolokációtól, mérettől és más egyéb szemponttól függenek. Ezeket nevezzük fenyegetettségi profilnak, melynek függvényében különböző védelmi megoldásokat kell kialakítani. A következő *4. ábrában* a NIST kiberbiztonsági keretrendszer [82] segítségével bemutatom a legfontosabb kiberbiztonsági területeket, amelyre potenciálisan egy szervezetnek figyelmet kell fordítania:



4. ábra - A kiberbiztonság fő funkciói és alkategóriái (saját szerkesztés)

1.4. Információszivárgás mint kockázat a kibertérben

A lehető legtöbb információ megszerzésére valószínűleg azóta törekszik az emberiség, amióta létezik. Minél többet birtokol valaki egy adott témával kapcsolatban, annál jobb döntéseket tud hozni a különböző szituációkban. Az információs előnyt felhasználva egy adott személy, szervezet vagy nemzetállam jobb pozícióba hozhatja magát és akár magához is ragadhatja a hatalmat vagy más előnyökre válthatja a tudását.

[55] A PCI DSS (Payment Card Industry Data Security Standard)

1.4.1. Az információ megszerzésének és védelmének módszertani-történeti áttekintése

Az információk megszerzésének intézményesítésére már az ókori mezopotámiaiak, görögök és rómaiak is törekedtek [97], de a klasszikus hírszerzés alapjai a középkorban gyökereznek [98]. Az információgyűjtési módszerek az emberiséget körülvevő világhoz igazodtak, és annak ütemével fejlődtek. Napjainkban a megszerzés módja szerint hat különböző területet különböztethetünk meg, amellyel – jellemzően nemzetállamok, de sokszor ipari szereplők is – információt gyűjtenek. Beszélhetünk a klasszikus emberi erőforrásokkal folytatott (HUMINT[56]), a nyílt forrásokat használó (OSINT[57]), a mérésen és jelmeghatározáson alapuló (MESINT[58]) és a kibertérben lévő (CYBINT[59]) hírszerzésről, illetve létezik még a rádióelektronikai (SIGINT[60]) és képfelderítés (IMINT[61]).

A felsorolásban található CYBINT a legújabb hírszerzési ág, amely a 20. századtól egyre nagyobb hangsúlyt kap. Célja a célország (vagy célszervezet) különböző nyílt és zárt hálózatain keresztül vagy a számítógépek és a hálózatok által kisugárzott jelek visszafejtéséből történő olyan adatok elérése, melyeket különböző módszerekkel a tulajdonosai védeni kívánnak [99].

A különböző állami, piaci, akadémiai szervezetek bizonyos része – de egyre több magánszemély is – felismerte az adataik ellopását célzó fenyegetettséget, ezért igyekeznek különböző lépéseket tenni a védelem kialakítása érdekében. A szakemberek kifejlesztettek olyan kódolási technikákat, melyeket alkalmazva az ellenérdekelt fél akkor sem tudja azt értelmezni, ha sikerült is a kívánt adathoz, jelhez, üzenethez hozzáférnie. Ezt, a titkosítás tudományát nevezzük kriptológiának.

Alapjai az ókorban gyökereznek, ahol különböző titkosírásokat alkalmaztak annak érdekében, hogy csak az arra hivatott személyek olvashassák el az érzékeny információkat. Ezekben az időkben különböző egyszerű titkosító algoritmusok segítségével próbálták elrejteni az információkat. A mono- és polialfabetikus helyettesítések (ún. szubsztitúciók) során egy kulcs-tábla segítségével cserélték ki a

[56] A „Human Inteligence” angol szakkifejezés rövidítése.
[57] Az „Open Source Inteligence” angol szakkifejezés rövidítése.
[58] A „Measurement and Signature Inteligence” angol szakkifejezés rövidítése.
[59] Az „Inteligence geatherd from Cyber Space” angol szakkifejezés rövidítése.
[60] A „Signal Inteligence” angol szakkifejezés rövidítése.
[61] Az „Imagery Inteligence” angol szakkifejezés rövidítése.

nyílt szöveg jeleit a rejtett szöveg egységeire, illetve alkalmaztak még átrendezéses (ún. transzpozíciós) eljárásokat, ahol egy kulcs-permutáció szerint a nyílt szöveg azonos hosszúságú blokkjait felcserélték. Tulajdonképpen a modern kriptológia is használja ezeket a módszereket a mai napig.

A kriptográfia a kriptológia azon ága, amely az információkat különböző algoritmusokkal és protokollokkal el kívánta rejteni [100]. Az elsőgenerációs kriptográfiai megoldásnak tekinthetjük például a Ceasar-rejtjelzést, a Kriptogramot vagy a pálcára tekert szövegcsíkot, az ún. Szkütala-t. Ezt követően a XV-XVI. század folyamán új módszereket fejlesztettek ki, amiből a leghíresebb talán a DeVigenere titkosítás. A technológia tovább fejlődött, és ennek köszönhetően elkészítették az elektromechanikus elven működő rejtjelző eszközöket. A II. világháború során ilyen, harmadik generációs eszköz volt a Német Birodalom által fejlesztett Enigma. A titkosító megoldások fejlesztését az is inspirálta, hogy a titkosított üzenetek megfejtésére szakosodott – kriptoanalízissel foglalkozó – személyek és szervezetek számára is egyre hatékonyabb eszközök, technológiai vívmányok álltak rendelkezésre.

A modern kriptográfia a számítógépek nyújtotta számítási kapacitásnak köszönhetően kezdett kialakulni és egyre nagyobb ütemben fejlődni. Ezek a negyedik generációs módszerek már az egyszerű titkosító algoritmusok sorozatából állnak. Kódolásukhoz és dekódolásukhoz szükség van – a módszertől függően – szimmetrikus vagy aszimmetrikus kulcsokra. Ha a támadónak sikerül is elfognia vagy megszereznie az így titkosított adatokat, a jó algoritmussal létrehozott fájlok esetén a kulcs nélkül a jelenlegi számítási kapacitással évmilliók kellenek a visszafejtéshez.

Érdemes azonban megemlíteni, hogy már több cég is bejelentette, hogy működő kvantumszámítógéppel rendelkezik. Ebből kiindulva feltételezhetjük, hogy belátható időn belül elég nagy számítási kapacitás fog rendelkezésre állni bizonyos állami és ipari szereplők számára, s hogy a kriptoanalitikus módszerek számára a negyedik generációs titkosító módszerek törésének nehézségét okozó a faktorizálást és a diszkrét logaritmus problémákat megoldják polinomiális időben. A klasszikus modernkori módszerekkel (pl. RSA[62], a DSA[63] vagy az ECDSA[64]) titkosított adatok tehát veszélyben vannak, de már most dolgoznak kriptográfusok olyan módszereken, amelyeket alkalmazva

[62] Rivest-Shamir-Adleman által megalkotott aszimmetrikus algoritmus.
[63] A DSA, azaz Digital Signature Algorithm egy digitális aláíró séma.
[64] Az ECDSA, azaz Elliptic Curve Digital Signature Algorithm egy elliptikus görbék elméletére épülő digitális aláíró séma.

továbbra is biztonságban maradnak a rejteni kívánt adatok a kvantumgépekkel szemben [101].

Az információkat azonban nem csak titkosítással lehet megvédeni az ellenérdekelt felekhez történő hozzájutás megakadályozása érdekében. Az ún. szteganográfia az információk elrejtésének módszere, ahol a cél nem az üzenet vagy adat olvasatlanná tétele, hanem az üzenet meglétének elfedése. Gyökerei a titkosításhoz hasonlóan az ókorban erednek. Ismert módszer ebből az időből, hogy a rabszolga kopasz fejbőrére tetováltak üzenetet, majd megvárták, amíg annak újra kinő a haja, és úgy küldték el őt a célszemélyhez. Később egyre finomabb módszereket kezdtek használni. Készítettek hő hatására láthatóvá váló „láthatatlan" tintát pitypang tejéből, de írtak főtt tojás héjára timsó és ecet elegyével üzenet, mely a hámozás után a fehérjén láthatóvá vált. Bevált gyakorlat volt különböző textúrákra írt nyílt szövegek betűinek alig észrevehető módon történő megjelölése, melyeket összeolvasva megismerhetővé vált az igazi üzenet. A nyomtatás és a fényképezés hőskorában használtak olyan mikropontokat is levelekben, melyek valójában gépelt oldalak milliméternél kisebbre zsugorított változatai voltak.

A digitalizáció, és a tény, hogy ez a technológia „0"-k és „1"-ek különböző sorrendjén és azok blokkokba történő rendezésén alapszik, számos új szteganográfiai módszer kialakítását hordozza magában. Elterjedt módszer a multimédiás tartalmakba vagy más fájlokba történő rejtés bizonyos bitek megváltoztatásával, de az online tér, a közösségi médiumok, a különböző számítógépes és konzolos játékok, az instant üzenetküldő és más alkalmazások nem rendeltetésszerű alkalmazásával a korunkat jellemző információáradat miatt csak a képzelet szab határt újabb és újabb szteganográfiai megoldások létrehozásának. A rejtést nagyban elősegíti a korunkat jellemző információáradat, mely teljes körű analizálása, feldolgozása követhetetlen.

1.4.2. Digitális minősített információszivárgás

Egy adott szervezet digitális információs rendszereiben lévő temérdek adat olyan hatalmas tud lenni, hogy az összes megszerzése és elemzése az ellenérdekelt félnek mára már általában nem célja. Ekkora mennyiség feldolgozása kihívást jelentene még a fejlett technikai háttérrel rendelkező támadóknak is, ha egyáltalán minden védelmi megoldást sikerrel ki tudnának játszani. Hiába vannak különböző automatizáló rendszerek, a végén az emberi erőforrás az, ami különbséget tud tenni egy-egy adat

hasznosságának megítélésében. Reálisabb cél lehet tehát eleve kevesebb, de olyan értékes információ megszerzése, aminek a birtokában valódi előnyre lehet szert tenni.

Ilyenek adatok lehetnek a vállalatok üzleti vagy a szervezet tevékenységi körétől függően banki, orvosi, jogi vagy más titkai. A közfeladatokat ellátó szervezetek esetében pedig a 2009-es Mavtv. [102] által szabályozott nemzeti minősített adatok vagy a szövetségi rendszereken belüli (például NATO [79], EU [103]) titkok is. Ezeknek az érzékeny információknak az informatikai rendszerekből történő véletlen (emberi mulasztásból származó) vagy szándékos (adatlopás, kémkedés) kiszivárgásának bekövetkezési valószínűségét a legtöbb szervezet – legalábbis nagyvállalati és állami szereplő – igyekszik komplex védelmi intézkedésekkel minimalizálni [104]. Minden védelmi intézkedés ellenére nem ritka a minősített adatok szivárgása, melyet a Wikileaks nemzetközi nonprofit szervezet által publikált anyagok is bizonyítanak. A különböző minősítésű anyagokat az értekezésem során homogén egységként kezelem, függetlenül a minősítő szervezettől vagy annak besorolásától.

Mivel kiberbiztonsági szempontból vizsgálom a területet, ezért csak a digitális formában előforduló adatok szivárgását tekintem fenyegetésnek. A kizárólag papíralapú dokumentumokat, jegyzeteket és a szóban elhangzott információkat csak akkor tekintem a kutatásom tárgyának, ha azok szorosan kapcsolódnak valamilyen manipulációs technikához (bővebben a 1.2.3 fejezetben), hiszen ebben az esetben a szervezet digitális infrastruktúráját veszélyeztetik.

A minősített információk online szivárgása az internetre kötött eszközök és rendszerek számos sérülékenysége miatt könnyen értelmezhető. Ezekbe tartoznak azok a rosszindulatú tevékenységek, amelyek valamilyen malware vagy más megoldás segítségével a rendszer tulajdonosa tudta és engedélye nélkül történnek. Azok az esetek, amikor például valaki egy számítógép képernyőjéről okostelefonnal vagy más eszközzel képet készít, offline támadásnak tekintendőek, hiszen nincs élő internetes kapcsolat.

Fontos megkülönböztetni azokat az eseteket, amelyek során a támadók maguk használják fel az információt, illetve azokat, amikor mások számára biztosítanak hozzáférést egy rendszerhez [105]. Ez utóbbi eset lehet például egy lefizetett személy, akinek a pénzért cserébe csupán az a feladata, hogy egy adathordozót csatlakoztasson egy számítógépbe. Az elkövetők különböző motivációval rendelkezhetnek mindkét esetben. Néhány példa ezek közül az anyagi javakhoz történő hozzáférés, a bosszúvágy

kielégítése, a tudásuk vagy hatalmuk fitogtatása, a szervezeti vagy társadalmi ranglétrán történő előbbre jutás elősegítése, de szexuális motiváció vagy féltékenység is vezetheti az elkövetőt a tette végrehajtásakor [106].

A kibertámadások és így az információszivárgás mögött is a leggyakrabban külső támadókra asszociálnak az emberek, azonban nagyon fontos kiemelni, hogy a szervezeten belülről sokszor sokkal nagyobb károk okozhatók. Ezekben az esetekben a támadó tisztában van a belső folyamatokkal, szokásokkal, rendszerekkel, így könnyebben megkerülheti a biztonsági védelmi intézkedéseket.

Az 1. fejezet összefoglalása

Az 1. fejezetben a célom az értekezés eredményeinek megalapozása volt. Összefoglaltam a 4. fejezetben található modell szempontjából releváns ismereteket a kiberbiztonság területén. Ennek céljából létrehoztam egy összefoglaló táblázatot, amely segít megérteni a kiberbiztonsági támadásokat a cyber kill chain és a hackelés lépéseinek összehasonlításával.

A később bemutatott modell megmutatja annak a kockázatát, hogy egy illető milyen potenciállal esik áldozatul egy célzott, minősített digitális információszerzés céljából elkövetett támadásnak, ezért ebben a fejezetben tisztáztam a releváns fogalomköröket.

2 KIBERBIZTONSÁGI HUMÁN KOCKÁZATOK AZONOSÍTÁSA FUZZY LOGIKA ÉS HÁLÓZATELMÉLET SEGÍTSÉGÉVEL

A gyanús magatartási formák (mint például a sunnyogás vagy az indokolatlan szorongás) vizsgálata különböző viselkedéselemző profilalkotó megoldásokkal működik a rendvédelmi szervek preventív tevékenységében [107]. Hasonló módon az emberi kockázatokból eredő károk csökkentése érdekében a különböző szervezetek más és más metodológiát használnak az új munkavállalók kiválasztásakor e célra. Általában ilyenkor nem a munkaerő technikai tudását vagy kiberbiztonsági tudatosságát vizsgálják, hanem a potenciális munkavállaló személyiségét, külső körülményeit és annak mértékét, hogy feltételezhetően mennyire illik bele a céges kultúrába. Bizonyos szervezetek, mint például bankok, telekommunikációs vagy nagy könyvvizsgáló, tanácsadó cégek a felvételi eljárás során a biztonsági kockázatok kiértékelésit is elvégzik.

Az egyének biztonsági értékelése során alkalmazott tényezők azonban természetüknél fogva a vizsgálati módszertől függően mindig kicsit bizonytalanok. Ezáltal egzaktan egy 1-5-ös skálán nem meghatározhatóak, mint ahogy azt a kiberbiztonsági kockázatok mérésének általános módszertanában használják. Ennek kiküszöbölése érdekében egy fuzzy logika alapján készített értékelési modellt hoztam létre, mely képes kezelni a rendszerben lévő bizonytalanságot.

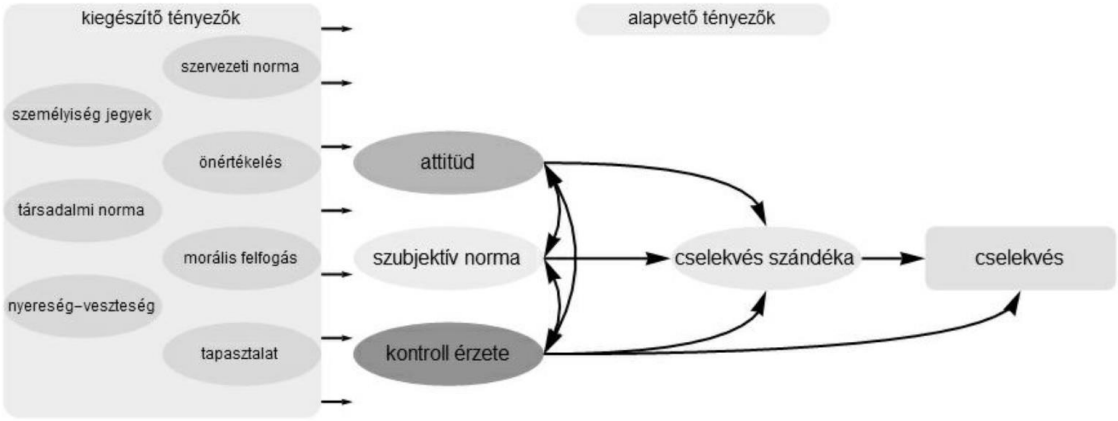
Célom, az volt, hogy létrehozzak egy olyan fuzzy modellt, amely segítségével bárki el tud végezni egy ilyen kockázati értékelést. A tényezőket (bemenetek) különböző forrásokból gyűjtöttem össze, majd szintetizáltam azokat egy bemeneti mátrixban, majd hozzárendeltem az úgynevezett tagsági függvényeit, azaz skálájukat. A modell, melyet létrehoztam, egy olyan alapot képez, melyet minden szervezet a maga igényei szerint, akár tényezők (bemenetek) vagy teljes modulok (fuzzy alrendszerek) kivételével vagy újak hozzáadásával módosítani tud. Nem volt célom egy minden szervezetre alkalmazható univerzális séma létrehozása, mivel ez többek között a szervezetek kockázatvállalási küszöbétől, fenyegetettségi helyzetétől nagyon eltérő lehet.

A disszertáció során egy konkrét fenyegetettségre, a digitális minősített információszivárgásra koncentráltam. A bemeneti tényezők újragondolásával azonban

létrehozható akár általánosságban a kiberbiztonsági kockázat mérésére vagy egy másik fenyegetettség mérésére alkalmas modell. Fontos hangsúlyozni, hogy a modell egy adott személy kockázatát méri. Az értékelés végén kapott szám ugyan önmagában is hasznos információt nyújthat a kiértékelők számára, azonban a részeredmények, így például a szándék vagy a véletlen elkövetés külön vizsgálva valószínűleg hasznosabb információt hordoz, mint maga a kockázati érték. A modellt érdemes komplexen, annak értékeit nem kiemelve értelmezni, figyelembe véve az adott szervezet fenyegetettségét az informatikai és védelmi infrastruktúra, valamint a munkatársakhoz történő viszonyítás segítségével. Így a szervezet még hasznosabb eredményt kaphat.

2.1 A kockázati tényezők azonosításának forrásai

A digitális információ szivárogtatása egy olyan cselekmény, amely alapvetően tervezett magatartáson alapul. Ettől eltérhetnek a véletlen esetek, melyek összefüggenek egy adott személy figyelmességével (vagy annak hiányával) és digitális kompetencia szintjével. Ajzen és Fishbein Tervezett Viselkedés Elméletét (TVE)[65] [108] alapul vége Hunyady és Münnich alkotta meg a szilárd erkölcsiség mutatót (SZEM) [109] (*5. ábra*) Alapfeltevésük, hogy a szilárd erkölcsiség nem magától született tulajdonsága az embernek, hanem azt az egyéniségek tágabb és szűkebb környezetből tanultak szintetizálása alapján építik be a személyiségükbe.



5. ábra - A SZEM-modell belső összefüggéseinek jellemzői [109]

A gyenge erkölccsel rendelkező egyének a belső morális integritásuk hiánya miatt nagyobb valószínűséggel követnek el titoksértést is, ezért a szándékos digitális információszivárogtatás kockázatainak elemzése során ezt a modellt vettem alapul.

[65] Az angol nyelvű szakirodalmak TPB-nek rövidítik az eredeti The Theory of Planned Behavior kifejezést használva.

Megvizsgáltam a Hunyady és Münnich által javasolt kiegészítő tényezőket, és a konkrét vizsgált fenyegetettségnek megfelelően módosítottam, bővítettem és kockázati tényezővé alakítottam őket a kockázati modellemben. Azért fontos külön értékelni a specifikus tényezőket, mert korábbi kutatások [110], [111] alapján kijelenthető, hogy az összevont vizsgálatok nem alkalmasak konkrét viselkedés predikciójára.

A tényezők összeállításánál Hunyady és Münnich kutatását alapul véve pozitív pólusú prototípusból indultam ki. Feltételezem, hogy az adott személy érzékeli a jogi-erkölcsi normákat és felfogja azok szigorát és racionális következményeit, valamint megvizsgálja a szivárogtatás (a SZEM esetében a korrupció) kitudódásának valószínűségét is. A TVE, így a SZEM is figyelembe veszi az egyének személyiségjellemzőit, attitűdrendszerét a konkrét cselekedettel kapcsolatosan, valamint az egyén percepcióit a cselekedetre és a közösség-cselekedet relációjára. A kockázati tényezők kialakítása során én magam is vizsgáltam ezeket, és figyelembe vettem a Belügyminisztérium empirikus vizsgálatát [112], a Debreceni Egyetem Pszichológiai Intézetének irányításával készült tanulmánykötetét [113], Chun-Hua Susan Lin és Chun-Fei Chen munkahelyi tisztességtelenséget vizsgáló tanulmányát [114] is. Fontos azonban hangsúlyozni, hogy disszertációmban nem a TVE modellt módosítom, hanem azt (és mások által specifikált változatait) vizsgálva egy fuzzy modell bemeneteit határoztam csupán meg, ezeket alapul véve.

Meghatározó forrás volt továbbá az úgynevezett Biztonsági Kérdőív is. A kritikus infrastruktúrákban, mint például a rend- és honvédelmi, illetve energetikai szektorban, az államigazgatás bizonyos területein vagy éppen a titkosszolgálatoknál a személyek kiválasztására még nagyobb figyelmet fordítanak, mint általában a privát szférában. Magyarországon az ilyen helyeken dolgozni kívánó egyéneknek sok esetben a törvénynek [115] megfelelően a nemzetbiztonsági átvilágítás folyamatán kell átesni, ahol beosztástól függő mértékben végeznek kockázatértékelést. Mivel ezeket a tényezőket évtizedek óta vizsgálják a magyar nemzet szempontjából legbizalmasabb munkakörökben, ezért véleményem szerint megfelelő alapot képez a kiberbiztonság szempontjából kockázatos munkavállalók körének megismeréséhez is. A kiértékelés módja ugyan nem nyilvános, azonban az eljárásnak az alapját képző kérdőív [116] igen, ezért ezt dolgoztam fel a tényezők megállapításához.

A modell alkotásakor alapul vettem még egy korábbi konferenciacikkeimben [106] [117] publikált fuzzy modelleket is. Az itt ismertetett tényezők megállapítása és validálása az információszivárgást különböző aspektusokból ismerő, neves szakemberekkel készített mélyinterjúk alapján történt. Hegyi Krisztián, a Belügyminisztérium Titokvédelmi Irodájának volt helyettes vezetője főleg a minősített adatokkal kapcsolatos incidensek kapcsán, Hegedűs Judit, a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészeti Magatartástudományi Tanszékén dolgozó egyetemi docens az emberi hajlandósággal kapcsolatban, és Fehér Sándor, a White Hat IT Security ügyvezetője a kiberbiztonsági incidenskezelésben jártas. A mélyinterjúkon megismert, de a konferenciacikk írásakor nem felhasznált információkat szintén beépítettem a modellbe.

Végül utolsó forrásként egy célzott kérdőívet készítettem (*3. függelék*), ahol a korábbi kutatómunkám (irodalomkutatás és a mélyinterjúk) alapján főleg olyan kockázati elemeket és összefüggéseket vizsgáltam, amelyekre nem találtam konkrét irodalmi forrást, vagy megerősítést szerettem volna egy-egy kockázat kapcsán. A kérdőívet összesen 174-en töltötték ki. Nem törekedtem a kitöltők összetétele esetén a magyar társadalom demográfiai helyzetének megfelelő reprezentativitásra, mivel ez esetben a szakma véleményére fektettem hangsúlyt. A kérdőív részletesen kiértékelése a 2.2 fejezetben található, mely eredményeinek egy részét már korábban publikáltam szerzőtársaimmal [118]. A kapott releváns adatokat az egyes tényezők ismertetésénél ismertetem.

A kockázati elemek az átlagemberekre vonatkoznak egy szervezeten belül. A különböző személyiségzavarban szenvedő vagy patológiai esetek (pl. narcisztikus személyiség, pszichopaták) nem képzik a vizsgálat tárgyát. Az értekezésben elkészített modell kiemelt személyek (pl. közjogi méltóságok, világvállalatok vezetői stb.) elemzésére sem, vagy csak nagyon korlátozott mértékben alkalmas.

Az elkészült modell további empirikus kutatások és specifikus ismeretek alapján bővíthető. A fuzzy modell – sajátosságai miatt – képes kezelni, ha bizonyos bemenetek bizonytalanul állnak rendelkezésre. Ezek főleg a munkavállaló privát szféráját érintő információk lehetnek. A modellező szoftver korlátai miatt az értekezésben bemutatott verzió nem alkalmas konkrét bemenetek hiányának kezelésére, azonban egy külön szoftverként továbbfejlesztett változat ezt is képes lenne kezelni, hiszen a fuzzy logika

önmagában alkalmas erre. A modell bemeneteit kifejezetten az információszivárgás szempontjából hoztam létre. Bizonyos tényezők átalakításával azonban más fenyegetettségek esetén is alkalmazható.

2.2 Kutatási kérdőív részletes kiértékelése

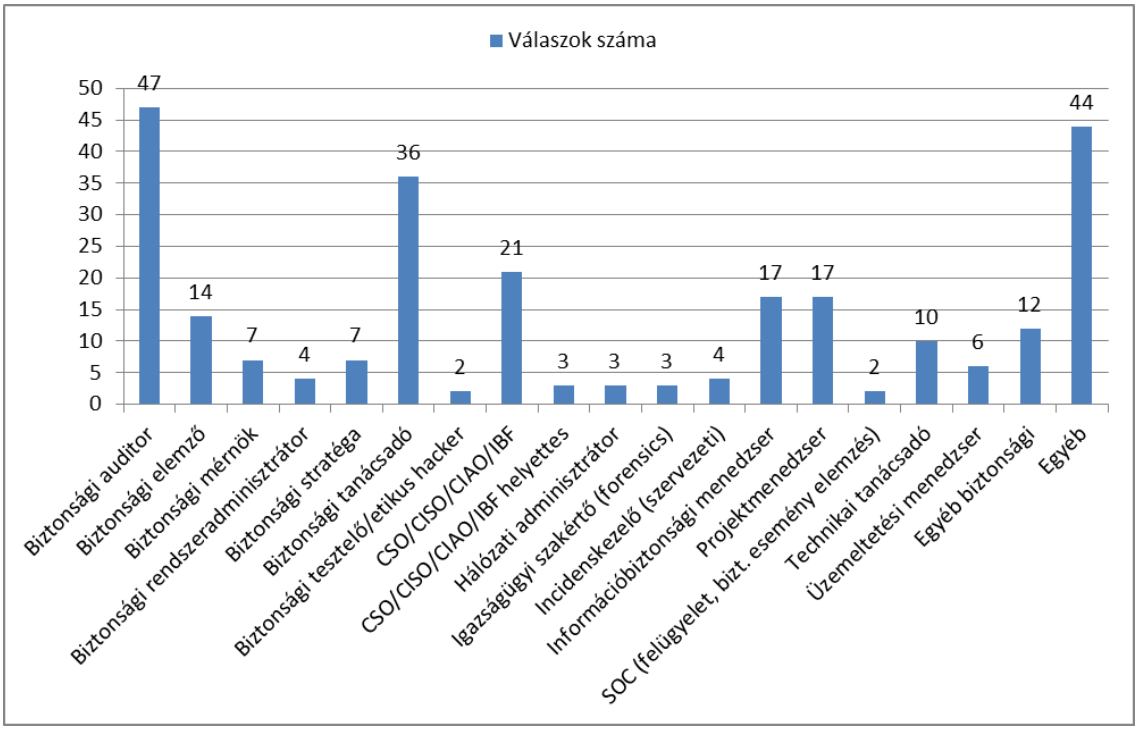
A kérdőív célja a kockázati tényezők megállapítása és a modell validálása volt. A válaszok begyűjtésének 4 szakasza volt. Először elkészítettem az irodalomkutatás és gyakorlati tapasztalatok alapján az első verziót az Alchemer (a kutatás kezdeti szakaszában még SurveyGizmo néven működő) online-kérdőívalkalmazás segítségével. Ennek a verziónak a kitöltésére felkértem tizenhét olyan személyt, akik különböző aspektusokból ismerik a témát, és bízom az értékítéletükben és szakmaiságukban. Az ő javaslataik alapján minimálisan módosítottam stilisztikailag és tartalmilag a kérdéseken, majd ezt publikáltuk különböző szakmai fórumokon, mint például Facebook és LinkedIn csoportok, egyetemek, a Hétpecsét Információbiztonsági Egyesület és az ISACA Budapest Chapter levelezőlistáin.

Összesen 341-en kezdték kitölteni a kérdőív második verzióját, melyből 162-en fejezték be azt. A kiértékelés során csak azokat a válaszokat vettem figyelembe, akik az összes kérdést befejezték. További ötöt érvénytelennek ítéltem meg az irreálisan rövid kitöltési idő miatt. Így végül 157 második körös eredménnyel tudtam dolgozni az első 18 mellett. Ugyan a két kérdőív között van eltérés, azonban ez minimális, és az első verzióban módosítottak egyértelműen megfeleltethetőek a másodikban találhatóknak, hiszen csak stilisztikailag változtak. Lényegi különbség a kettő között csak új kérdések bekerülésével volt. Ezeket a későbbiek során külön fogom jelölni. Végül tehát összesen 174 érvényes válasz alapján tudtam dolgozni.

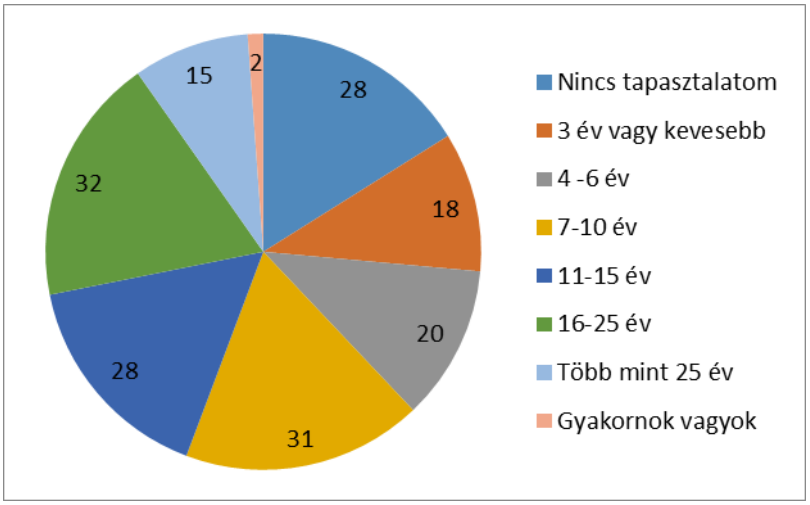
A kérdőív első része a kitöltőkre vonatkozott. Első kérdésként arra voltam kíváncsi, hogy a kitöltők mennyire lehetnek kompetensek a vizsgált témában. 18 kapcsolódó területet határoztam meg, melyből többet is bejelölhettek a kitöltők. Az eredményeket a *6. ábra* szemlélteti.

A kitöltők közül bizonyos célelemzés során két halmazt alkottam. Vizsgáltam, hogy összesen mennyien adtak választ, és megkülönböztettem egy kiemelt csoportot. Ezek közé nem kerültek be azok, akik csak projektmenedzserek, technikai tanácsadók, üzemeltetési menedzserek és az „Egyéb” kategóriában egyértelműen nem biztonsági szakembereknek (pl. értékesítő, gazdasági szakember stb.) jelölték be magukat. A

kiemelt csoportba azok a személyek sem kerültek be, akik a *7. ábrán* látható módon a tapasztalatnál a „*Nincs tapasztalat*” opciót jelölték be, még akkor sem, ha egyébként releváns területen is dolgoznak.

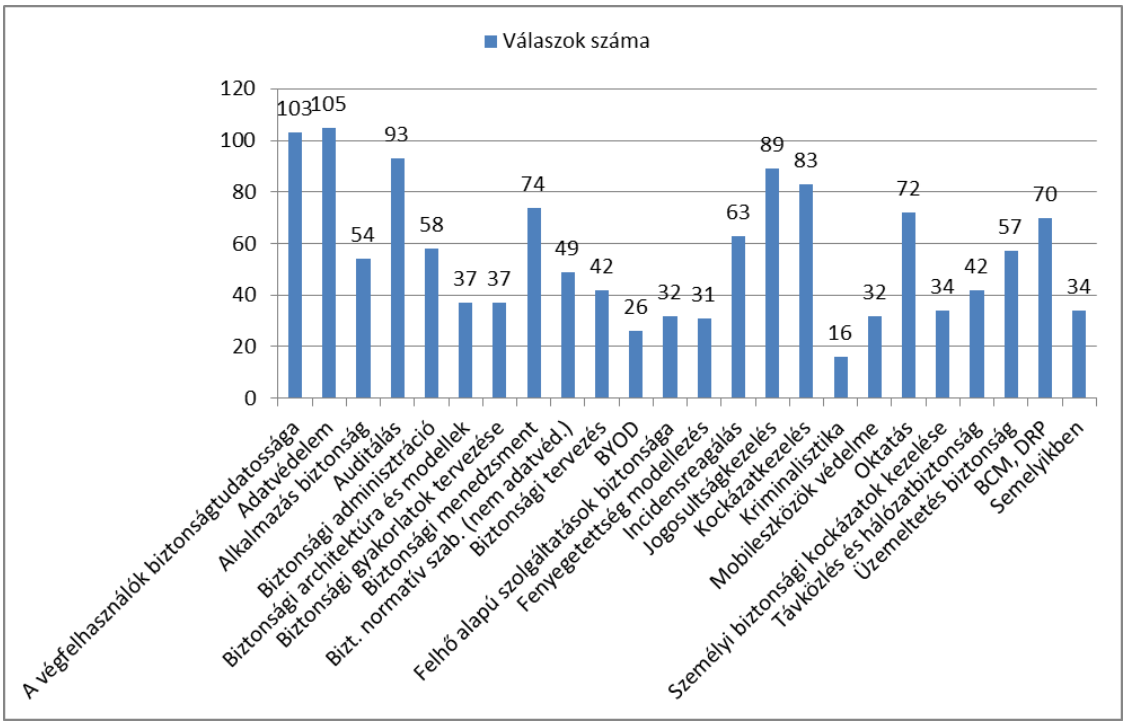


6. ábra - Területek, ahol a kitöltők dolgoznak (saját szerkesztés)



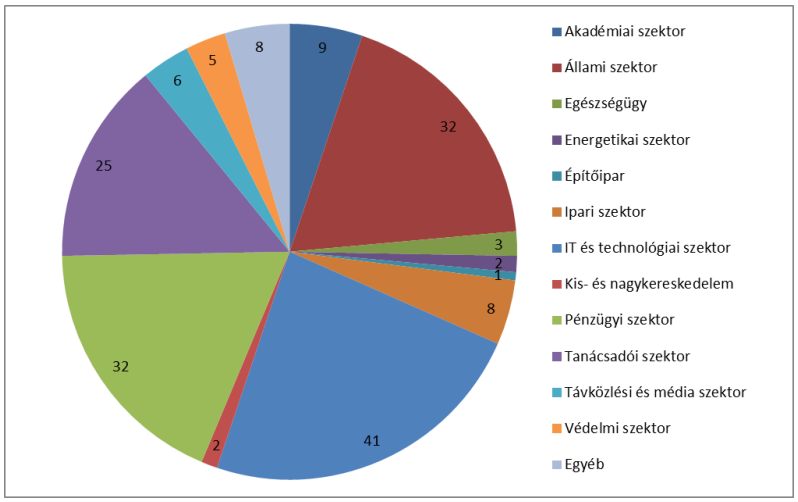
7. ábra - Kitöltők biztonsági munkatapasztalata (saját szerkesztés)

A kérdezők szakmai tapasztalata elég vegyes, de kiterjed a szakma egészére. Ennek összetételét a *8. ábra* szemlélteti. A kitöltők egyszerre több lehetőséget is meg tudtak jelölni.

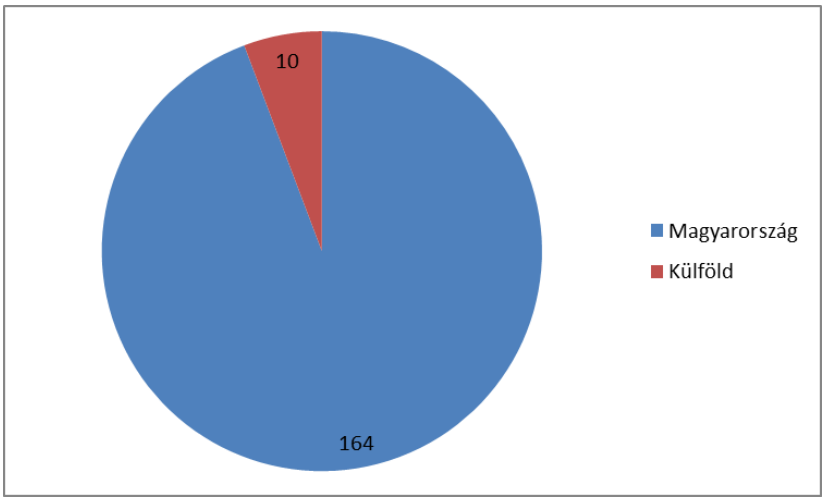


8. ábra - Biztonsági területeken szerzett tapasztalatok (saját szerkesztés)

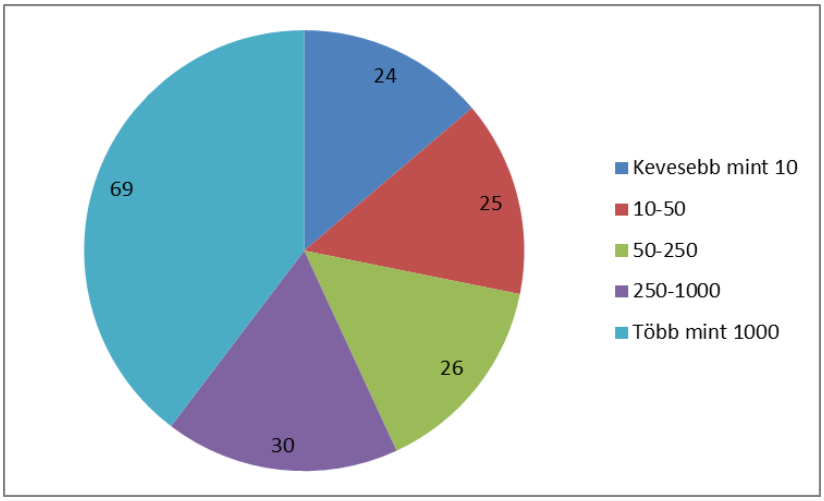
A *9. ábrán* látható, hogy milyen szektorban dolgoznak a kitöltők (az idegenforgalmi, a közlekedési és a mezőgazdasági szektorokra nem érkezett válasz), a *10. ábrán* a Magyarországon és a külföldön dolgozók aránya, a *11. ábrán* a munkahelyükön dolgozók száma, valamint a *12. ábrán*, hogy lokális vagy multinacionális szervezetnél dolgoznak-e.



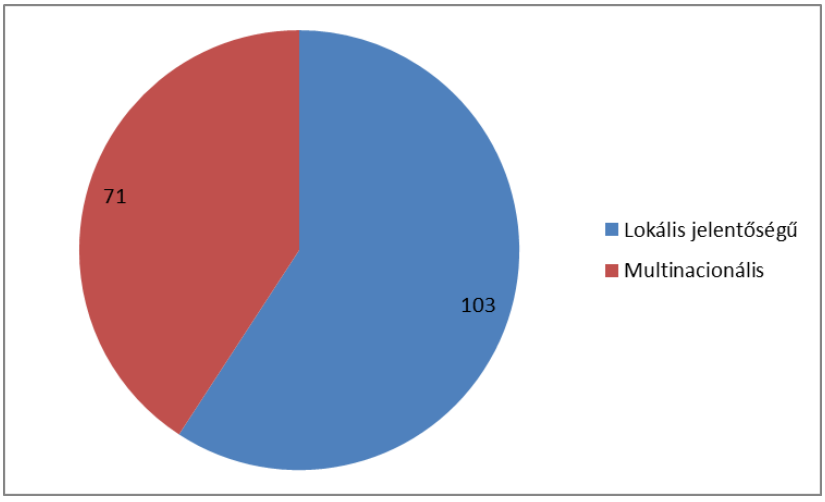
9. ábra - Szektorok aránya (saját szerkesztés)



10. ábra - Magyarországon és külföldön dolgozók aránya (saját szerkesztés)

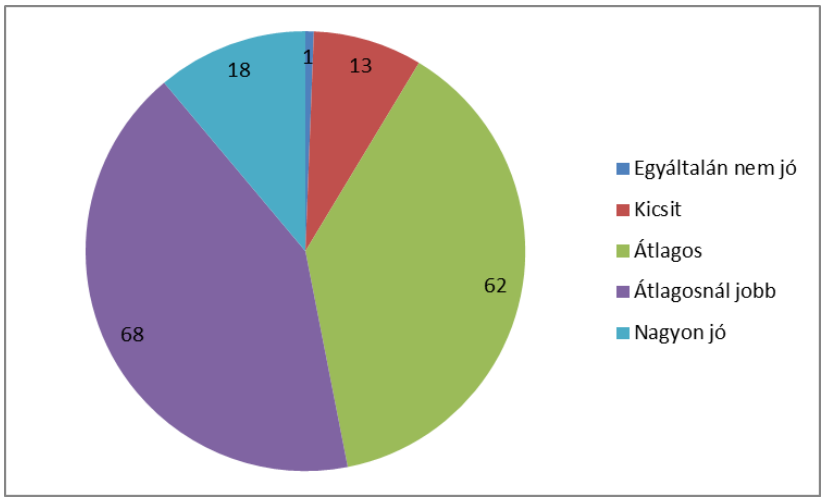


11. ábra - Munkavállalók száma a kitöltők munkahelyein (saját szerkesztés)



12. ábra - Lokális jelentőségű és multinacionális vállalatoknál dolgozó kitöltők aránya (saját szerkesztés)

Mivel emberi karaktereket és azok kockázatait vizsgáltam, ezért kíváncsi voltam a kitöltők emberismeretére. Ennek célja az volt, hogy a kitöltés eredményét mennyire tudom figyelembe venni. Ahogy a *13. ábrán* is látható, önbevallás szerint összesen 85%-ban átlagos, átlagosnál jobb vagy nagyon jó emberismerőnek tartja magát.



13. ábra - A kitöltők emberismerete (saját szerkesztés)

Az általános adatok után kitértem a konkrét célzott kérdésekre. Első feltételezésem, amit szerettem volna igazolni, hogy a különböző szakmák kiberbiztonsági kockázatai között van különbség. Konkrét, felhasználható forrást nem találtam erre vonatkozóan, ezért a kérdőívem első szakmai kérdése erre vonatkozott. Meghatároztam egy olyan munkakörlistát, ami feltételezésem szerint magas szinten lefedi egy nagyvállalat munkaerejét.

Az értekezésen túlmutat egy feladatkörök szintjén részletezett lista elkészítése, hiszen ez minden szervezetnél teljesen egyedi. Ennek értelmében csak általánosan határoztam meg a vizsgált munkaköröket. Habár információszivárgás szempontjából nagy különbség van például a felhasználói támogatást végző munkatárs, a szoftverfejlesztő, vagy éppen az adatbázis-adminisztrátor között, a fent ismertetett ok miatt én egységesen informatikusként vizsgáltam őket. Az egyszerűsítést az is indokolja, hogy a 3. fejezetben ismertetett bemenetek lehetőséget biztosítanak a mélyebb szintű specifikációra.

Az elkészített listát egy multinacionális bank magyarországi HR specialistájával készített mélyinterjú keretén belül validáltam, és az ott elhangzottak alapján módosítottam, így kialakítva a végleges munkakörmátrixot (*2. táblázat*). Minden elemhez rendeltem a gyakorlati tapasztalataim alapján egy kockázati értéket úgy, hogy

közben figyelembe vettem az interjúalany véleményét is. Annak érdekében, hogy az általam meghatározott kockázati értéket validáljam, a kérdőíves kutatásom során az alábbi kérdést tettem fel: „*Mennyire tartja általában kockázatosnak az adott munkakörben dolgozó személyeket kiberbiztonsági szempontból?"*

A válaszadók egy 1-től 10-es skálán adhatták meg az általuk helyesnek vélt értéket. A következő táblázat 3-6. oszlopában található számok a válaszok móduszát, azaz a legtöbb válaszadó által megadott azonos értéket tartalmazzák.

A *végleges kockázati értéket* (VK - 6. oszlop) úgy határoztam meg, hogy az általam meghatározott *tapasztalati kockázati értéket* (TK – 2. oszlop) vettem a leginkább relevánsnak. Ennek egyik oka, hogy a kérdőívben nem volt lehetőségem részletesen elmagyarázni a kitöltés célját. Másik oka pedig, hogy social engineering tesztek végzése egy speciális terület, amit a szakmában is kevesen szoktak elvégezni. Így feltételezhetően a kitöltők válasza kevésbé mérvadó. A következő releváns értéket a kérdőív kitöltői közül azok adják, akik bejelölték, hogy *személyi biztonsági kockázatok* (SZBK – 3. oszlop) kezelésében van tapasztalatuk. Fontosnak tartottam külön súlyozni azoknak a személyeknek a véleményét, akik nem tartoznak az SZBK csoportba, de valamilyen *kiberbiztonsági* területen van tapasztalatuk (KK – 4. oszlop) és külön, akiknek nincs (egyéb kategória=EK – 5. oszlop). A végleges kockázati érték a súlyozott átlag egész számra kerekített eredménye:

$$VK = (5 * TK + 3 * SZBK + 2 * KK + EK)/11$$

Munkakör	**TK**	**SZBK**	**KK**	**EK**	**VK**
Asszisztens (nem vezetői)	4	4	5	4	**4**
Biztonsági őr a recepción	7	5	3	3	**5**
Kontroller	7	3	4	4	**5**
Gyakornok	3	3	3	3	**3**
Hosztesz	2	2	2	2	**2**
HR-es	7	5	6	5	**6**
Informatikus	8	6	6	6	**7**
IT biztonsági munkatárs	8	6	6	6	**7**
Jogász	6	3	3	3	**4**
Kirendeltség vezető (fióktelep)	7	5	5	5	**6**
Könyvelő (pénzügyes, bérszámfejtő)	7	5	5	5	**6**
Marketinges	4	3	3	3	**3**
Takarító/ karbantartó munkatárs	8	4	4	4	**6**
Ügyfélszolgálati munkatárs	6	4	4	4	**5**
Vezetői asszisztens	8	5	5	5	**6**

2. táblázat - Munkaköri kockázati mátrix (saját szerkesztés)

A kérdőívben szerepel egy plusz, a táblázatban be nem mutatott szerepkör: *Külsős munkavállaló (hosztesz)*. Ezt azért nem jelenítem meg, mert eredetileg más szöveg került volna ide. Így viszont megegyezik a *Hosztesz* értékeivel.

A következő feladata a kitöltőknek az volt, hogy tizenhat, előre megadott karakter leírása alapján válasszák ki, hogy véleményük szerint milyen tényezők teszik kockázatossá azokat a személyeket (karaktereket) abból a szempontból, hogy külső megkeresésre vagy önszántukból, esetleg gondatlanságból szenzitív információt szivárogtathatnak ki. A válaszokat kiértékeltem és elemeztem az alábbi módon. Az első szám azt mutatja meg, hogy a 174 kitöltő közül mennyien jelölték összesen az előtte lévő aláhúzott szót vagy kifejezést kockázatosnak. A második érték kifejezi, hogy ebből mennyien rendelkeznek releváns kiberbiztonsági tapasztalattal:

Agilis (7;5), egyetemista (6;0), van párja (7;4), de gyakran flörtöl a cégen belül másokkal (45;35). Anyagi háttere gyenge (64;42), szegényebb családból származik (6;4). Korából fakadóan a technológiára fogékonyabb (11;8), átlagos aktív felhasználó (9;7), aki a közösségi médiát is sokat használja (53;41). Monoton munkát végez precízen (13;10), ami nincs megbecsülve (77;53), sokkal több munkát is el tudna végezni (7;5). Nem sikerült teljesen beilleszkednie (26;14), a teljes állású munkavállalók „csak egy gyakornok"-ként kezelik (24;16). Nem alakult még ki teljesen az erkölcsi értékrendje (87;69). Dohányzik (6;5), sokat jár bulizni (11;8).

Mind a tizenhat karakter és a hozzájuk tartozó elemzés megtalálható a *4. függelékben*. A kapott értékek alapján megállapítottam, hogy melyek azok a tényezők, amelyeket fontos kockázatként jelöltek be. Erre a darabszámot jelöltem ki. Ha az összes kitöltőből vagy a szakemberből 20%-nál többen jelölték az adott kifejezést kockázatosnak, akkor érdemesnek tartottam beilleszteni a fuzzy modell bemenetei (*3. fejezet*) közé. A 35, illetve 25 feletti értékek alapján a következő bemeneteket határoztam meg a korábban (*2.1. fejezet*) bemutatott források alapján végzett kutatásokon kívül:

- Pletykásság (Személyiségi jegyek);
- Machiavellizmus (Személyiségi jegyek);
- Munkahelyi frusztráció (Belső munkahelyi tényezők);
- Közösségbe történő beilleszkedés (Belső munkahelyi tényezők);
- Képességekhez képesti leterheltség (Belső munkahelyi tényezők);
- Munkájának megbecsültsége (Belső munkahelyi tényezők);

- Figyelmetlenség (Véletlen elkövetés lehetséges mértéke).

Kérdőívemben kíváncsi voltam arra is, hogy bizonyos tényezőket mennyire ítélnek kockázatosnak a kitöltők. Megkérdeztem tehát, hogy az alábbi lista elemei[66] közül egy 1-6-os skálán[67] véleményük szerint melyik és milyen mértékben növeli annak a kockázatát, hogy egy személy zsarolhatóvá válik, így szenzitív információkat szivárogtathasson ki. A lista elemei a megadott kockázatok átlagának két tizedes jegyre történő kerekítésével növekvő sorrendben a következőek:

- A tény, hogy az illető párkapcsolatban van, így a párjáért is felel (2,37)
- Nagy munkatapasztalat az adott helyen és pozícióban* (2,45)
- A tény, hogy az illető külsős munkatárs (2,74)
- Rossz egészségügyi állapot (3,05)
- Kevés élettapasztalat (3,15)
- Megfelelő, figyelmes vezető hiánya* (3,25)
- Pszichés terhelhetőség (feszültségtűrés, frusztrációtolerancia)* (3,26)
- Munkahelyi közösségbe történő be nem illeszkedés (3,28)
- Önismeret hiánya (3,29)
- Alacsony EQ szint (3,31)
- Negatív véleményt formáló társas közeg* (3,34)
- Figyelmetlenség (3,67)
- Alacsony IQ szint (3,81)
- Az illetőnek több gyermeket kell eltartania (3,81)
- Az illető már követett el apróbb szabályszegéseket* (3,84)
- Nagyarányú hozzáférés érzékeny adatokhoz (4,05)
- Társadalmi normától való titkos eltérés (vallás, szexualitás, politikai nézet stb.) (4,10)
- Rossz pénzügyi helyzet (vélt vagy valós egzisztenciális problémák (4,13)
- Szervezet iránti lojalitás hiánya (4,26)
- Sértettség (fizetésemelés, előléptetés hiánya) (4,41)

[66] A *-al jelölt tényezőket a kérdőív első verziója nem tartalmazta.
[67] Az első kérdőívben egy 1-10-es skála segítségével tudtak a válaszadók erre a kérdésre válaszolni, azonban a visszajelzések alapján ez túl széles spektrum volt, viszont mindenképpen páros számú lehetőséget szerettem volna megadni a középérték elkerülése miatt.
A közös értékelhetőség érdekében ezt egy 1-6-os skálára vetítettem rá úgy, hogy vettem a 6/10-ét a megadott értékeknek, majd egész számra kerekítettem azokat.

- Gyenge értékítélet/értékrend* (4,64)
- Függőség (4,79)
- Gyenge erkölcs* (5,06)

A négyes értéket meghaladó egységek közül a zsarolhatóság tényezője alá illesztettem a *Társadalmi normától való titkos eltérés (vallás, szexualitás, politikai nézet stb.)* és *Függőség* kockázatát, mivel azokat az eredetileg elkészített modellemben máshol nem szerepeltettem. Az anyagi helyzet/ anyagi kiszolgáltatottság tényezőjét szintén az itteni eredmények alapján helyeztem el a modellemben a végleges helyére.

A *Gyenge erkölcs* és a *Gyenge értékítélet/értékrend* egybeolvadt a morális felfogással, a sértettség a belső munkahelyi tényezők közé került annak szoros kapcsolata miatt, illetve az érzékeny adatokhoz való hozzáférést a külső tényezőkön belül a lehetőség tartalmazza.

2.3 Kiberbiztonsági kockázatkezelés általában

Egy szervezet akkor tud ellenálló lenni a kibertérből érkező fenyegetésekkel szemben, ha preventív és reaktív biztonsági intézkedései kockázatarányosak és költségoptimalizáltak. Nem kivétel ez alól a humán faktorból eredő kockázatok kezelése sem. A szervezeteknek nincs elegendő kapacitása a teljes kontrollra, és az üzleti folyamatok sem működnének megfelelően egy túlszabályozott technológiai környezetben. Ezért szükséges megtalálni az optimumot az információs rendszer funkcionalitásában, használhatóságában és a biztonságban.

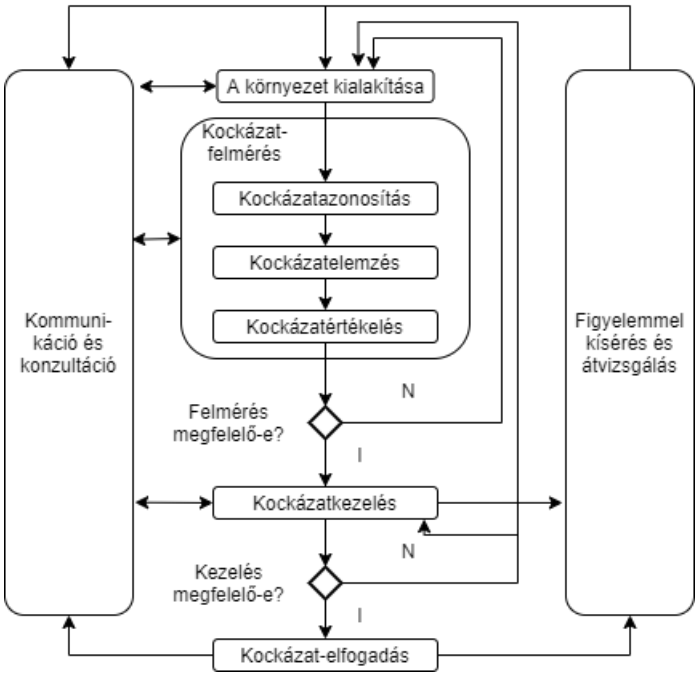
A humán faktor nyújtotta kockázatok előtt azonban szükséges megismerni a kockázatkezelést (kockázatmenedzsmentet) általánosan, és a kiberbiztonságra vetítve. Egy szervezet életében számos kockázati tényező található meg, mint például a stratégiai, a környezeti, a piaci, a pénzügyi, a működési vagy épp a megfelelőségi kockázatok. A digitalizált életünkben ezek mindegyike közvetve vagy közvetlenül érintett az informatikai és egyben a kiberbiztonsági kockázatokkal egyaránt.

A megfelelő kezeléshez először azonosítani kell a lehetséges bekövetkezhető eseményeket azok mechanizmusával és kárhatásával együtt. Ezt követően az összehasonlíthatóság miatt meg kell becsülni és számszerűsíteni a szervezetre vonatkoztatott potenciált az ajánlások és a korábbi tapasztalatok alapján [119]. Ez jellemzően a következő számítással történik:

*Kockázat = Valószínűség * Hatás nagysága*

A már számszerűsített kockázatok alapján – a szervezet kockázatvállalási hajlandóságától függően – intézkedéseket kell megfogalmazni a potenciális károk minimalizálására, majd végre kell hajtani azokat. Bizonyos esetekben a menedzsment döntése alapján fel is lehet ezeket vállalni. Bármilyen döntés is születik egy kockázatról, a folyamatos visszamérés és megfigyelés elengedhetetlen.

Ennek a folyamatnak a specifikus, információbiztonságra leképzett változatát foglalja magában az ISO/IEC 27005 ajánlás, melynek jelenleg a 2018-as verziója a legfrissebb. Az általános modellhez képest a kockázat elfogadásának lépését külön kiemeli a maradvány-kockázat kezelése érdekében, valamint plusz két döntési pontot vezet be, melyet az alábbi 14. *ábra* mutat be [120]:



14. ábra - Az információbiztonsági kockázatfelmérés és -kezelés folyamata [120]

Az információ- és így a kiberbiztonsági kockázatkezelés tehát azt az alapvetést kívánja kezelni, hogy nem áll rendelkezésre elegendő erőforrás egy adott szervezet fenyegetettségi profiljának teljeskörű kezelésére. Fontos, hogy a kockázatmenedzsment folyamatába be legyen vonva a teljes vezetői testület. Ezen belül az ügyvezető igazgatónak, az információbiztonsági és informatikai vezetőknek kiemelkedő a szerepe. A biztonsági területnek továbbá fontos bevonni a rendszerfelelősöket és az adatgazdákat is, hiszen többnyire ők ismerik megfelelően a saját rendszereiket és azok tartalmát. Amennyiben NATO (és EU) minősített adatokról van szó, abban az esetben szükséges a

kommunikációs és információs rendszerek tervezőinek, kivitelezőinek, üzemeltetőinek, a biztonsági felügyeletnek, a rejtjelfelügyelőnek, illetve a projekttagoknak és a biztonságot jóváhagyó hatóság(ok)nak a bevonása is [104].

A kiberbiztonsági kockázatkezelést üzleti célokon alapuló, folyamatosan fejlesztett stratégia mentén kell végrehajtani [121] annak érdekében, hogy a megfelelő hatást érhesse el. A célok megfogalmazása után először fel kell állítani azokat a mérőszámokat, amelyek segítségével nyomon követhető a fejlődés (vagy a visszaesés), és csak ez után szabad megkezdeni az üzemeltetni kívánt megoldások bevezetését.

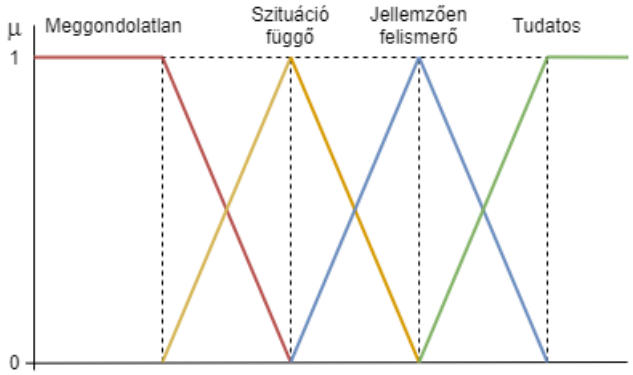
Ezeket a kockázat értékeléseket Patel szerint [122] végezhetjük kvalitatív és bonyolultabb esetekben matematikai eszközök (pl. fuzzy elmélet, hibafák stb.) segítségével, kvantitatív módszerekkel. Ez utóbbi a valószínűségi kockázatértékelés (PRA[68]) kategóriájába tartozik, mely alapvetően nem tér ki a kockázatok azonosítására [124]. Különböző megközelítésben készítettek már kiberbiztonsági kockázati modellt. Létezik például Bayesi hálózat [125] vagy fuzzy és FMEA[69] [126] alapú, kiberbiztonsági hatások előrejelzését [127], a támadások biztonsági rendszerekre gyakorolt hatásainak mérését [128] célzó és egy adott kiberbiztonsági rendszer sebezhetőségét meghatározó [129] módszerek. A következőkben egy a humán kockázatokra fókuszáló fuzzy modellt ismertetek, melynek egyes elemeit a *3. fejezet* tartalmazza. Azonban mielőtt ezeket részletezném, fontos megismerni a fuzzy logika alapjait.

2.4 Fuzzy logika általában

Egy szervezet által a bevezetett fizikai, logikai és adminisztratív védelmi intézkedések ellenére a munkaerő tagjai különböző mértékben – személyiségüktől, személyes hátterüktől, a szervezetben betöltött pozíciójuktól függően – kockázatot jelentenek kiberbiztonsági szempontból. Ezt a tényezőt azonban szükséges minél hatékonyabban kezelni. Hiába van sok szabvány és elterjedt gyakorlat a kiberbiztonsági kockázatok általános kezelésére, a szakmában jelenleg nincs egy széles körben elterjedt módszertan, amely kifejezetten a humán oldalra koncentrál.

[68] PRA (probabilistic risk assessment), azaz valószínűségi kockázatértékelés. Magában foglalja az összes hiba/támadási fa elemzést, eseményfa elemzést, hibamód- és hatáselemzést, valamint ok-következmény elemzést. Ezek a módszerek irányított grafikonokat és logikai diagramokat használnak [123].
[69] FMEA (Failure Mode Effects Analysis), azaz hibamód- és hatáselemzés.

Ennek véleményem szerint több oka van. Sok szubjektív és/vagy egzakt számokkal nem leírható kockázati tényezőt szükséges figyelembe venni úgy, hogy ezek együttes hatása nem mindig átlátható. Emiatt az emberi kockázatok kiértékelése és kezelése aránytalanul sok energiát emészt fel a szakma nagy részét adó olyan szakemberek számára, akik főleg technológiai háttérrel rendelkeznek. A tényezők ráadásul sok esetben nem mennyiségi adatok, hanem olyan jellemzők, amelyre nyelvi leírásokat tudunk adni konkrét számok helyett. A biztonságtudatosság esetén a *15. ábrán* látható módon például ez lehet meggondolatlan, szituációfüggő, jellemzően felismerő és tudatos, nem pedig 1-2-3-4.



15. ábra - A biztonságtudatosság nyelvi változói (saját szerkesztés)

Kiértékeléskor számításba kell venni sok külső tényezőt is. Ilyen például a szektor, ahol a szervezet tevékenykedik, a vállalat nagysága, annak ténye, hogy lokális vagy nemzetközi tevékenységet folytat. Befolyásoló tényező még a kiberbiztonsági érettségi szint, és az is, hogy a működés országának jogszabályai milyen mennyiségű és minőségű adatot engednek a munkavállalókról kezelni. Tehát kezelni kell azt a problémát is, hogy hiányosak lehetnek a bemeneti értékeink.

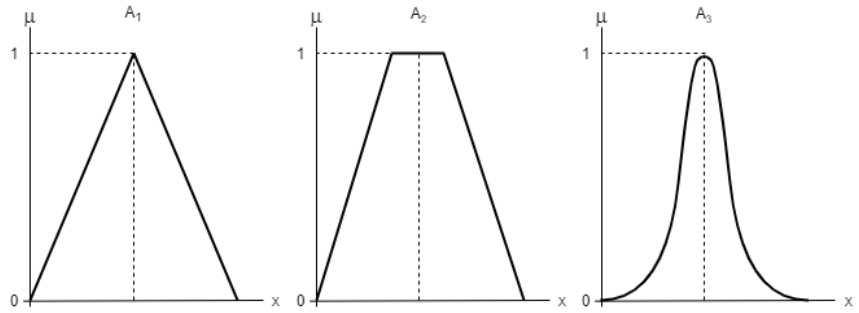
Ezeknek a problémának a kezelésére a lágy számítási módszereket és azon belül is a fuzzy logikát tartom a legalkalmasabbnak. Létrehoztam egy olyan fuzzy modellt, amely figyelembe veszi az egyéni adottságokat és a kockázati tényezők kölcsönhatását. A célom az volt, hogy egy könnyen bővíthető és átlátható, moduláris felépítésű modellt hozzak létre, hiszen a kiberbiztonságban az emberi tényező jelentette kockázatok mérése nem szabad, hogy statikus mérés legyen.

A fuzzy logika egy matematikai apparátus. Nagy bonyolultságú esetekben alkalmazható jól, ahol matematikailag nehezen leírható problémák mellett nyelvi változók kezelésére van szükség, és az esetekre jellemző az információhiányból fakadó bizonytalanság, a

kétértelműség, illetve a pontatlanság. Az adatok és a kiértékelés folyamata sokszor szubjektív, így az általános statisztikai értékelés nem hoz megfelelő eredményt. A fuzzy logika nagyon közel áll az emberi gondolkodás és döntéshozatal szisztematikájához [130].

Az alapja a fuzzy halmazelmélet, amely a klasszikus halmazelméletből vezethető le. Az alaphalmazhoz ($X \neq \emptyset$) történő hozzátartozás mértékét egy [0,1] intervallumból választott érték megadásával (vagy az ún. type 2 fuzzy halmaz esetében intervallummal) tudjuk definiálni, melyet tagsági függvényekkel ($\mu A: X \rightarrow [0,1]$), azaz fuzzy halmazokkal tudunk leírni. Gyakran használjuk a $\mu_A(x)$ jelölés helyett az $A(x)$ formát. Gyakorlatilag úgy rendelünk függvényeket bizonyos fogalmakhoz, hogy azok a halmazhoz tartozás mértékét írják le. Ennek köszönhetően lehetővé teszi olyan tényezők kezelését, amelyek nem rendelkeznek éles határokkal, hanem finom átmenet figyelhető meg két kategória között.

A tagsági függvények különbözőek lehetnek a jellemezni kívánt bemenet tulajdonságainak megfelelően. Leggyakrabban a háromszög (A_1), a trapéz (A_2) vagy a haranggörbe (A_3) alakú függvényeket alkalmazzák, melyeket a következő ábra szemléltet:

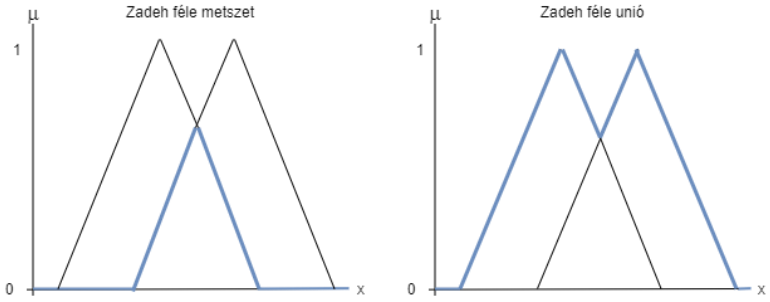


16. ábra - Jellemző tagsági függvények (saját szerkesztés)

A tagsági függvények leírására a karakterisztikus függvény szolgál. A *16. ábra* A_1 esete a következőképpen írható le. Ha *a*, *b* és *c* a háromszög töréspontjait jelentik balról jobbra haladva:

$$A_1 \begin{cases} \dfrac{x-a}{b-a} & ha\ a \leq x \leq b, \\ \dfrac{c-x}{c-b} & ha\ b \leq x < c, \\ 0 & \text{ha x} > \text{c;} \end{cases}$$

A fuzzy logikában is léteznek halmazműveletek, melyek a hagyományos crisp[70] halmazok fuzzy halmazokra történő általánosítása. Itt is értelmezhető, hogy $A(x)$ halmaz $\overline{A}(x)$ komplementere. A konjukció (metszet) fuzzy megfelelője a t-norma, míg a diszjunkciót (uniót) t-konormának vagy s-normának nevezzük. Ezeket a műveleteket különböző operátorok segítségével valósíthatjuk meg. Az adott szituáció határozza meg, hogy melyiket alkalmazzuk. Leggyakrabban a Zadeh-féle komplemens képzést, metszetet (mely mind közül a legnagyobb) és uniót (mely mind közül a legkisebb) használják.



17. ábra - Zadeh féle metszet és unió (saját szerkesztés)

A Zadeh-féle alapműveletek a következőképpen határozhatók meg:

- Komplemens: $\overline{A}(x) = 1 - A(x)$,
- Metszet: $(A \cap B)(x) = \min[A(x), B(x)]$,
- Unió: $(A \cup B)(x) = \max[A(x), B(x)]$.

A t-norma operátorok közül leggyakrabban a fent definiált minimumot (min) és a szorzatot (prod) használjuk, míg az s-norma operátorok közül a maximumot (max) és a probabilisztikus összeget (probor) [131].

Zadeh 1973-ban publikált modellje [132] után különféle fuzzy következtetési (irányítási) rendszereket alkottak meg. Mamdani egyszerűsített modelljét [133] módosította Larsen [134] és a Sugeno-Takagi páros [135]. A különböző modellek más-más előnyökkel és hátrányokkal járnak. A humán kockázatok mérése során, figyelembe véve, hogy az emberi gondolkodáshoz közeli modellre van szükség, ahol az intuíció beépíthető, de a kiértékelésnek nem kell azonnal megtörténnie, a Mamdani módszert fogom alkalmazni. A rendszer *HA állapot, AKKOR következtetés* típusú természetes nyelvi szabályokat alkalmaz:

[70] Crisp értéknek az egyértelműen leírható „éles” értékeket (pl. 0, 1) hívjuk.

$$HA\ x_1 = A_{1,i_1}\ \text{és} \ldots \text{és}\ x_n = A_{n,i_n}\ AKKOR\ y = B_{i_1,\ldots,i_n}$$

ahol $x_1, \ldots, x_n$ a bemeneti paraméterek, A_{k,i_k} az i_k-adik bemenet k-ik tagsági függvénye, $B_{i_1,\ldots,i_n}$ a szabályhoz rendelt kimeneti fuzzy halmaz, $i_j = 1, \ldots, n_j$ és n_j a j bemenethez tartozó tagsági függvények száma [136]. A Mamdani következtetési rendszer a szabályok implikációja helyett logikai „*ÉS*" kapcsolatot modellez, mely hatékonynak bizonyul [131]. Általánosan a következőképpen írható fel t megfelelő tulajdonságokkal rendelkező t-norma esetén:

$$B'(y) = \sup_{x \in X}(t\left(A'(x), t\big(A(x), B(y)\big)\right))$$

A Mamdani-típusú kiértékelés lépései:

- 1) megfigyelés,
- 2) az illeszkedés mértékének meghatározása a tagsági függvény segítségével, a fuzzifikálás,
- 3) a tüzelési szint meghatározása (a szabályok feltétel részének kiértékelése ÉS esetén konjunkciós, VAGY esetén diszjunkciós operátorral),
- 4) az implikáció,
- 5) az egyes szabályok kimeneti halmazainak az egyesítése, az aggregáció,
- 6) a kapott komplex halmazt legjobban jellemző crisp érték meghatározása, a deffuzifikáció. [137].

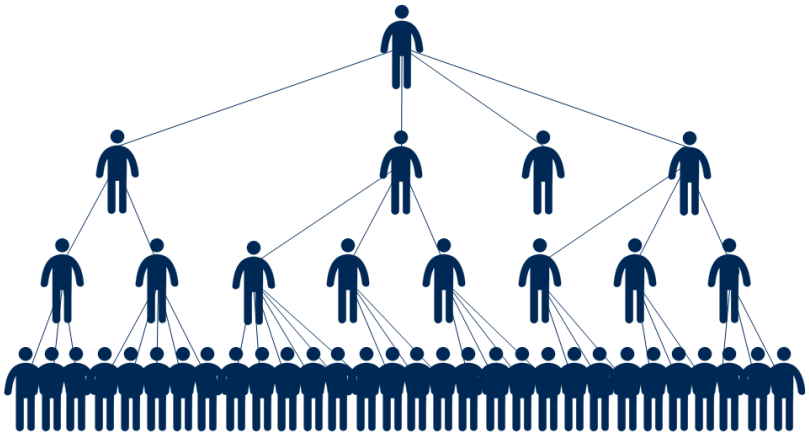
2.5 Szervezeti kapcsolati háló és annak kiberbiztonsági vetületei

A XXI. században a hálózatelemzésre a hálózatok komplexitásának növekedésével egy külön tudományterületként, tudományágként tekinthetünk, mely ugyan a gráfelméletben gyökeredzik, de azon összefüggéseiben jelentősen túlmutat. A hálózatok kutatásának alapkövét 1967-ben Stanley Milgram kísérlete [138] jelentette. Az elhíresült csomagküldő teszt során bebizonyította, hogy az Egyesült Államokban mindenki mindenkit ismer 5-6 ismerősön keresztül. Ez a felfedezés megalapozta az úgynevezett kisvilág elméletet [139], melynek lényege, hogy egy nagy hálózatban a pontok közötti távolság számtani átlaga (átlagos távolsága) viszonylag kicsi.

A következő fontos mérföldkő a terület megismerésében a véletlen gráfok, hálózatok felfedezése volt. Az ezt vizsgáló Erdősi-Rényi modell [140] kimondja, hogy ugyanakkora valószínűséggel csatlakoznak bármely ponthoz a hálózatba bekerülő újak

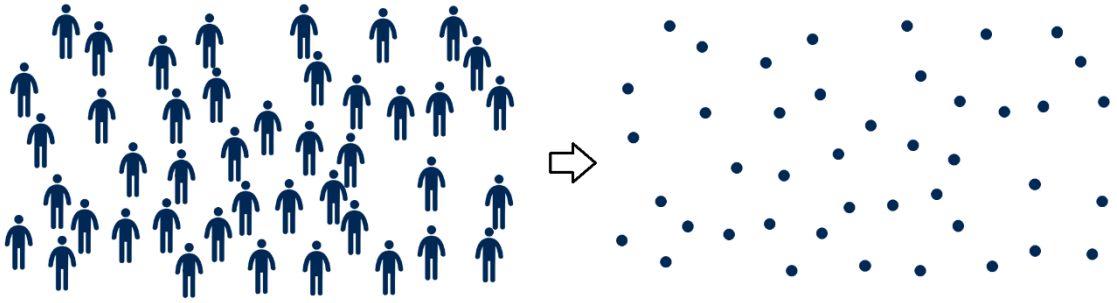
egy véletlen hálózatba. Azaz az egy csúcsba befutó élek számának (fokszámának) eloszlása Gauss görbét mutat. Azonban a hétköznapokban sokkal jellemzőbbek azok az esetek, ahol nem véletlenszerűen csatlakoznak az új pontok, hanem valamilyen szabály mentén. Ezeket nevezzük skálafüggetlen hálózatoknak [141]. A Barabási-Albert modellben bebizonyításra került, hogy kellően nagy hálózatokban vannak nagyobb vonzással rendelkező pontok. Ezekben az esetekben azonban a fokszámok nem normáleloszlást mutatnak, hanem azok negatív hatványfüggvényt követnek.

A hálózatelemzési módszerek olyan területeken hoztak új eredményeket, mint a digitális hálózatok feltérképezése és a társadalmi, szociális hálók megértése. Ezeket vizsgálva a kiberbiztonság humán aspektusával kapcsolatban is felfedezhetünk szabályszerűségeket [142]. Egy vállalat, az élén a tulajdonosokkal, a különböző szintű vezetőkkel és a beosztottakkal, első pillantásra egy hierarchikus rendszer képét kelti, mint ahogy a *18. ábrán* ez a 43 fős cég példája is mutatja.



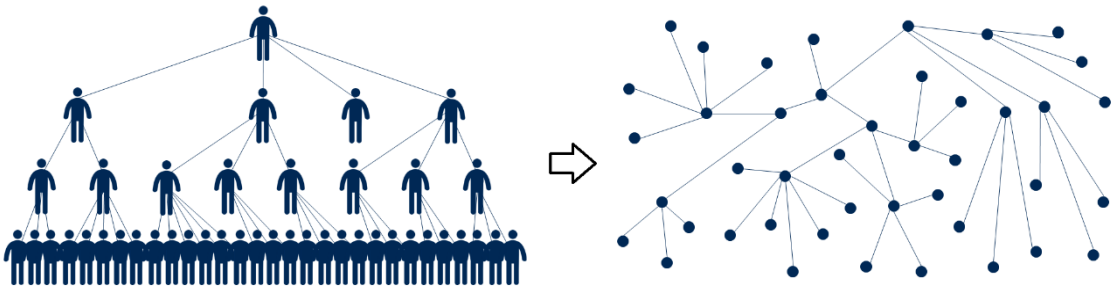
18. ábra - A vállalati hierarchia egy elméleti hálója (saját szerkesztés)

Azonban a szervezeti informális hálózatok ennél sokkal összetettebbek és bonyolultabbak. Ennek megértésére tekintsünk a benne lévő személyekre egy embertömegként, ahol mindenki egy különálló pontként értelmezhető:



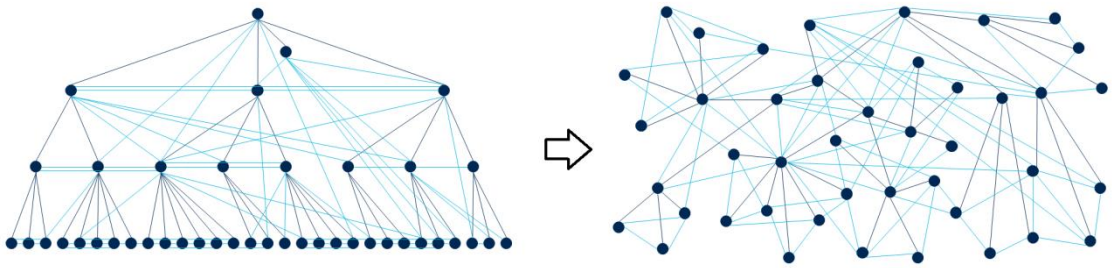
19. ábra - A szervezet tömegként értelmezve, majd azok pontokká konvertálva (saját szerkesztés)

Ha a pontokat élekkel összekötjük a *18. ábrán* szereplő hierarchia mentén, akkor kezd kialakulni az emberek közötti hálózat alapja, melynek így 42 a fokszáma:



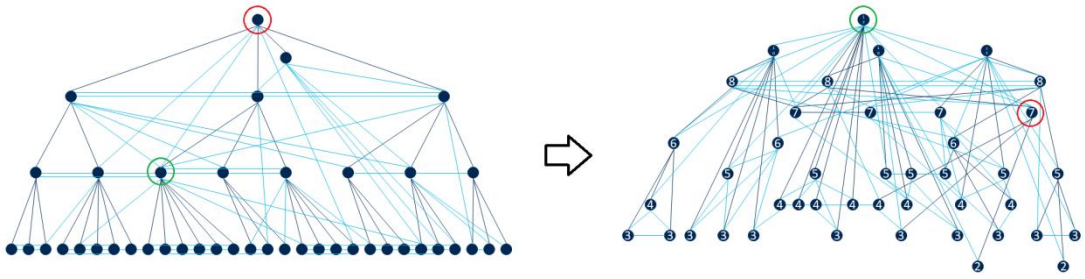
20. ábra- szervezet hálózatba rendezve (saját szerkesztés)

Azonban sokkal bonyolultabb, 113 fokszámú hálózatot kapunk, ha a pontokat összekötjük újabb élekkel, amelyek az informális (személyes- és munkaviszonyon alapuló), illetve a manapság egyre tipikusabb mátrix-, illetve projektalapú szervezeti struktúrák általi kapcsolatokat jelentik:



21. ábra - A szervezet informális kapcsolataival kiegészített hálózata (saját szerkesztés)

Ha továbbá ezt a rendezést a pontok fokszáma alapján átrendezzük, akkor nem egy négyszintű hierarchiát látunk, hanem kilenc, különböző súllyal rendelkező pontot:

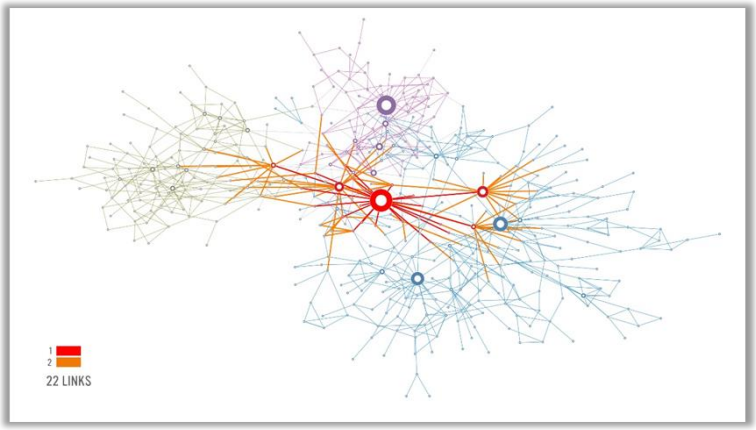


22. ábra - A személyek kapcsolati hálójuk erőssége szerint hierarchiába szervezve (saját szerkesztés)

A *22. ábra* bal felén pirossal jelzett tulajdonos/ügyvezető ugyan a szervezeti hierarchia tetején van, azonban a kapcsolati háló fokszám szerint rendezett verziójában csak a negyedik szinten van. Ezzel szemben a zölddel jelölt, alsóbb szintű vezetőnek a

legkiterjedtebb az ismeretségi köre. Minél nagyobb (több csomóponttal rendelkező) szervezetet vizsgálunk, annál jobban veszi fel az emberek hálózata a skálafüggetlen jelleget.

Ez a gyakorlatban – a fokszámelosztást vizsgálva – azt jelenti, hogy lesz néhány kulcsfontosságú kolléga, akik jelentősen nagyobb fokszámmal fognak rendelkezni a többieknél. Ráadásul a kívülről érkező új személyek nagyobb valószínűséggel fognak ezekkel az egyénekkel kapcsolatot kialakítani. Minél nagyobb egy ponthoz kapcsolódó élek száma, annál hatékonyabbá is válik [143]. Ugyanakkor ezek a személyek egy célzott kibertérből érkező támadás esetén nagyobb kockázatot jelentenek. Egyrészt valószínűleg több információ van a birtokukban, másrészt az ő nevükben végrehajtott támadás nagyobb sikert érhet el.



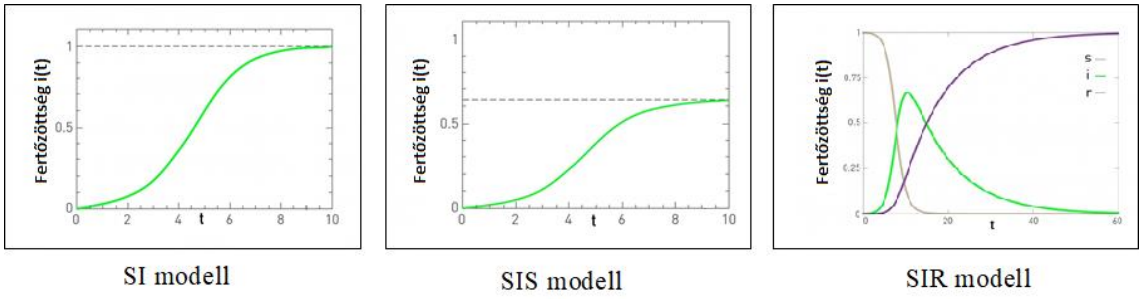
23. ábra - Egy vizsgált vállalat fokszám eloszlása [143]

Barabási *A hálózatok tudománya* c. könyvében egy három telephellyel rendelkező vállalatot vizsgált, ahol a legnagyobb fokszámú személy (a legnagyobb piros kör a *23. ábrában*) a munka- és környezetvédelmi felelős volt. Egy nem megfelelő kiberbiztonsági tudatossággal rendelkező ilyen karakterű személy egy fertőzött adathordozóval jóval gyorsabban (a támadó szemszögéből hatékonyabban) fertőzheti át a vállalatot.

Az, hogy a szociális háló, és az elküldött, illetve fogadott e-mailek között egyértelmű összefüggés van, már bizonyított [125]. Ezt kihasználva fel lehet építeni egy olyan támadást, ahol egy phishing levélben rejtett macro fertőzés van. Lefutás után átnézi az áldozat levelezőrendszerét, és onnan a leggyakrabban használt e-mail címre az (kevésbé szofisztikált) Emotet támadásokhoz hasonlóan egy korábbi levél részletét küldi ki. Így a

fogadó fél azt hiheti, hogy valóban attól a személytől kapta, mint akinek álcázni próbálja magát a malware.

Barabási a vírusok terjedésének 3 típusát (SI, SIS, SIR) is vizsgálja a hálózatokban [143], melyeket a *24. ábra* is szemléltet. Az SI (Susceptible-Infected), azaz Fogékony-Fertőzött modellben a kezdeti időpontban mindenki fogékony, majd a fertőzöttek száma exponenciálisan nő. A SIS (Susceptible-Infected-Susceptible), azaz Fogékony-Fertőzött-Fogékony modell nagyon hasonló az előzőhöz, azzal a különbséggel, hogy a fertőzött pont meggyógyulhat és ismét fogékonnyá válhat. A SIR (Susceptible-Infected-Removed), azaz Fogékony-Fertőzött-Eltávolított modellben bevezetésre kerül egy új, gyógyult állapot, aki nem válik ismét fogékonnyá.



24. ábra - A vírusterjedési modellek ([143] alapján szerkesztve)

A különböző, információszivárogtatásra is alkalmas malwarek ezen modellek mentén tudnak terjedni a szociális és informatikai hálózatok összeforrt rendszerében [144]. Az SI modell a biztonsági kontrollok nélküli állapotnak felel meg. Ugyan a kritikus infrastruktúrákban és a nagyvállalati környezetben manapság szerencsére nem jellemző, hogy ne legyenek kiberbiztonsági megoldások, ettől függetlenül egy zero-day támadás alkalmával, vagy egy nem kontrollált támadással ez a terjedési mód is elképzelhető.

Az SIS terjedési metódusról lehet szó, ha például van egy új sérülékenység, de még nem érkezett a gyártótól frissítés, vagy az adott szervezetben a patch menedzsment szabályok miatt még nem telepítették azokat. Ilyenkor a biztonsági szakemberek felhívhatják a munkaerő figyelmét arra, hogy ha bizonyos jelekkel találkoznak, akkor azt jelezzék számukra, és lehetőség szerint mihamarabb juttassák el az eszközt. Ilyen esetekben a csere vagy az újratelepítés csak azt eredményezi, hogy utána nem lesz fertőzött a készülék, azonban amíg a sérülékenység ki nincs javítva, addig bármikor újra áldozatul eshet a felhasználó.

Az esetek nagy többségében azonban az SIR modell vehető alapul. Ilyen esetekben az adott sérülékenységet befoltozzák, és így az eszköz védetté válik az adott támadás ellen. Ha azonban nem csak egy módon terjed az adott kártékony kód, hanem a támadó több különböző lehetőséget is kihasznál, akkor egyfajta SIS-SIR hibrid modellt lehet alapul venni.

A védekezési stratégiákat segítő elemzések mellett ráadásul a szervezeti szociális háló elemzése akár olyan klikkek, csoportok felfedezésére is alkalmas [145], amelyek szervezetfejlesztési lépésekkel vagy adminisztratív kontrollok bevezetésével, módosításával kezelhetővé válnak. De emellett számos, főleg üzleti szempontból fontos eredménye is lehet, mint a csapatok hatékony munkájának segítése [146], vagy a vállalati pletyka terjedési útjának követése, mely akár minősített információkat is tartalmazhat.

A fentiek a hálózatok vizsgálatára vonatkoznak, azonban fontosnak tartom a pontok (vagyis személyek) különböző kockázati tényezőinek vizsgálatát. A kettő együttes alkalmazásával válik láthatóvá, hogy potenciálisan ki vagy kik lehetnek azok, akiken keresztül a legnagyobb eséllyel minősített információ tud kiszivárogni a szervezetből.

A 2. fejezet összefoglalása

A kiberbiztonsági kockázatelemzés általános menetének leírása, és a modellalkotáskor használt halmazelméleti, illetve fuzzy logikai összefüggések bemutatása mellett kielemeztem az értekezés megírásához készített kérdőív eredményeit, mely alapján több kockázati tényezőt azonosítottam. A kérdőív eredménye alapján bizonyítottam, hogy a különböző munkakörök eltérő kockázattal rendelkeznek, így szükséges ezeket is külön bemenetként kezelni.

3 A FUZZY MODELL BEMENETEI

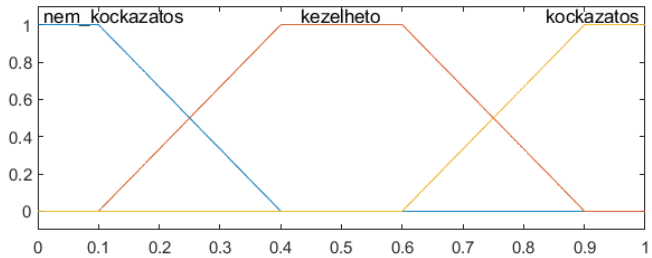
Ezek a kockázati tényezők az általam készített fuzzy modell bemenetei, melyek összeállítását *2.1. fejezetben* említett források és az általam elvégzett social engineering auditok gyakorlati tapasztalatai alapján határoztam meg.

Az értekezés írásakor nem törekedtem arra, hogy könnyen beszerezhető információkon alapuljon a módszertan, a célom az volt, hogy minél alaposabb legyen. Ennek értelmében sok esetben nem áll a munkáltató birtokában minden általam felsorolt bemenet, mégis fontosnak tartom ezeknek a tényezőknek az ismertetését, hiszen indokolt esetben a közvetlen felettes, egy pszichológus, illetve célszoftverek, kérdőívek alkalmazásával ezek az információk begyűjthetők hol könnyebben, hol nehezebben.

A bemenetek alapján egy kockázati értéket fogunk kapni kimenetként, amelynek tagsági függvényei a következőek:

- Nem kockázatos: [0 0 0.1 0.4];
- Kezelhető: [0.1 0.4 0.6 0.9];
- Kockázatos: [0.6 0.9 1 1].

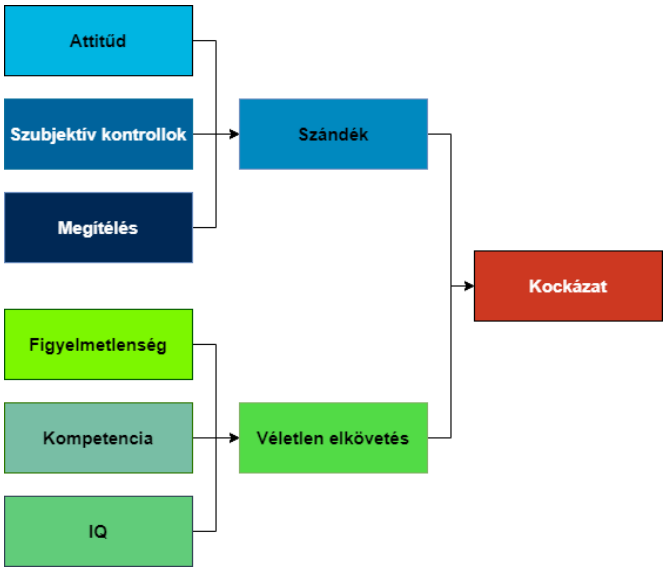
Az értékeket a könnyű használhatóság, szabályalkothatósági jelleg és kiértékelhetőség miatt minden esetben 0 és 1 között határoztam meg. Minden, a jelen fejezetben található be- és kimeneti tagsági függvényt a [szám1 szám2 szám3 szám4] formátumban határozok meg. Az értékek a trapéz alapú tagsági függvények x tengelyen adott értékét jelzik. Az első és a negyedik szám y tengelyen mindig 0, míg a másodiké és a harmadiké 1. A MatLab program a következő módon ábrázolja őket:



25. ábra - A kockázat tagsági föggvényeinek ábrázolása a MatLab rendszer által

3.1 A bemenetek fő struktúrája

A bemenetek fő struktúráját a TVE és a belőle származtatott SZEM modellek adják, azonban a specifikus értelmezés szempontjából módosítottam rajta. A direkt elkövetés fő tényezőit az alábbi, *26. ábra* szerint állítottam össze:



26. ábra - A bemenetek fő struktúrája (saját szerkesztés)

Fontos megkülönböztetni, hogy valaki véletlenül vagy szándékosan követi el a digitális adatok szivárogtatását. A **véletlen elkövetés** kockázatát egyrészről az illető figyelmetlenségének mértéke, intelligenciája, illetve a digitális kompetenciája határozza meg. Ezt, a tényezőnek a lehetséges mértékét három tagsági függvénnyel jellemeztem:

- Alacsony: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Magas: [0.6 0.9 1 1].

A direkt elkövetés, azaz a **szándék** ennél jóval bonyolultabb. Itt szükséges megismerni az illető képességeit, mennyire ítéli el az elkövetést, mennyire zsarolható egy harmadik fél által, vagy milyen a munkahelyi és a személyes környezete. Az elkövetésben fontos megismerni, hogy az illető milyen külső és belső kontrollokkal rendelkezik, hogyan ítéli meg tettét és milyen az alap attitűdje. Ezt a hajlandósági tényezőt az előzőhöz hasonlóan a következő tagsági függvényekkel jellemeztem:

- Alacsony: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Magas: [0.6 0.9 1 1].

Attitűd

Az attitűd gyakorlatilag a „jó-rossz” dimenziójával kifejezett értékelés az információszivárogtatásra (az attitűd tárgyára) vonatkoztatva [147]. Ez az értékelés három fő komponensből épül fel:

- kognitív információs komponens (gondolatok, elképzelések, hitek),
- affektív információs komponens (érzelmek, érzések),
- viselkedéses információs komponens (múltbeli tapasztalatok).

Egy adott személy attitűdjének az ismeretek szervezése, a nyereség-veszteség optimalizálás, az ego védelme és az értékrend kifejezése a fő funkciója [148].

Mivel az attitűd megállapítása nagyban függhet a mérési módszertől, így a szivárogtatással kapcsolatban nagyon körültekintően kell eljárni. Ilyen módon ez egy tipikus fuzzy érték. Felmérésének egyik lehetséges módszere egy kérdőív kitöltése a munkavállalókkal, ahol különböző releváns eseteket vizsgálunk a jó-rossz dimenzióban. A TVE alapmodell szerint ez a következő számítás szerint számolható ki:

$$A = P(k_1) * E(k_1) + .. + P(k_n) * E(k_n)$$

Ahol az *A* az attitűd értékét, a k_i az *i*-edik következmény, *P* a szubjektív bekövetkezési valószínűség és $E(k_i)$ pedig a jó-rossz dimenzió szerinti értékelése az adott következménynek.

A tagsági függvények között a jó attitűd az értelmezésemben azt jelenti, hogy az egyén értékrendjébe nem fér bele egy ilyen tett elkövetése, míg ellenkező esetben igen:

- Jó: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Rossz: [0.6 0.9 1 1].

Szubjektív kontrollok

Azt, hogy mennyire nehéznek vagy könnyűnek ítéli meg az egyén a szivárogtatás végrehajtását, a szubjektív kontroll érzetével jellemezhető. Ide tartozik, hogy rendelkezésére áll-e az illetőnek a megfelelő eszközrendszer, tapasztalat, információ és erőforrás a kivitelezéshez. Ezek a kontrollok lehetnek a munkahelyi környezetből adódó (külső) és saját egyéniségéből, magánéletéből, a munkahelyen betöltött szerepéből (belső) fakadó kontrollok.

Ez gyakorlatilag egy magabiztossági tényezővel is helyettesíthető. Megmutatja, hogy az egyén mennyire bízik abban, hogy kontrollálni tudja a cselekedetét és a környezeti körülményeket. Az, hogy ez utóbbi kategóriában mit és milyen súllyal veszünk figyelembe, szintén az egyén megítélése alapján történik. Az alább (3.2-3.5

fejezetekben) részletezett tényezők esetében ezért javasolt lehet egy pszichológus, a közvetlen vezető, illetve bizonyos esetekben egy specifikus kérdőív elkészítése.

A szubjektív kontrollok esetében a tett elkövetésének nehézsége adja a tagsági függvényeket:

- Nehéz: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Könnyű: [0.6 0.9 1 1].

A tett elkövetésének megítélése

Az ábrán és a fuzzy rendszerben (Megítélés).

Fontos megismerni azt, hogy az egyén hogyan ítéli meg az adott tettet. Ez a SZEM modellben csak szubjektív normaként értelmezett, azonban véleményem szerint egy kiberbiztonsági fenyegetettségnél több dolgot kell értékelni, mint hogy az illető környezetében hogyan vélekednek az információszivárogtatás (vagy más cselekedet) elkövetéséről. Természetesen ez egy nagyon fontos része, azonban figyelembe kell venni az illető morális felfogását, hogy követett-e már el ilyen vagy más hasonló bűncselekményt, szabálysértést. Fontos tényező, hogy milyen (lenne) az önképe egy ilyen tett elkövetése után, és, hogy lebukás esetén a felelősségre vonás és büntetés arányban van-e számára a potenciális nyereséggel. Ezeknek a tényezőknek a mérését az illető munkahelyi, családi, baráti közegének megismerésével, pszichológus és/vagy kérdőív kitöltésével lehet megismerni.

A tagsági függvényeket a következőképpen határoztam meg:

- Elítélendő: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Helyeslő: [0.6 0.9 1 1];

Figyelmetlenség

A figyelmetlenség önmagában is eredményezhet véletlen titoksértést. Egy megfelelő biztonsági háttérrel rendelkező szervezet azonban rendelkezik olyan megoldásokkal, amelyek elősegítik a károk minimalizálását egy véletlen cselekedet esetén. Rohanó világunkban nagyon sokszor találkozhatunk olyan szituációval, amikor nem gondoljuk végig a tettünket, vagy nem vagyunk elég körültekintőek. Ezeket a körülményeket használják ki sok esetben a támadások során.

A figyelmetlenséget a következő skálán értelmezem:

- Figyelmetlen: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Precíz: [0.6 0.9 1 1].

Digitális kompetencia

A digitális kompetencia ismerete segít elkülöníteni a gondatlan elkövetést a szándékos károkozástól. Számos esetben derült ki, hogy egy incidenst egy informatikában jártas munkatárs okozott. Ennek oka, hogy a kiterjedtebb szakmai ismerettel rendelkező egyén tisztában van a tetteivel. Az ő esetükben kevésbé hihető, hogy gondatlanságból követtek el egy olyan tettet, mint például Edward Snowden, a CIA[71] volt rendszergazdája [149].

A digitális kompetencia másfelől kockázatcsökkentő hatású is. Egy megfelelően tájékozott és magas kiberbiztonsági tudatossági szinttel rendelkező alkalmazott időben észlelhet egy rosszindulatú károkozási próbálkozást. A bangladesi bank alkalmazottjának példája jól szemlélteti ezt az esetet: magas fokú biztonságtudatosságának és felkészültségének köszönhetően 800 millió dollár veszteségtől óvta meg a bankot [150].

A digitális kompetencia szintjét a következőképpen határoztam meg:

- Professzionális: [0 0 0.1 0.4];
- Középszintű: [0.1 0.4 0.6 0.9];
- Alapszintű: [0.6 0.9 1 1].

Intelligencia hányados

Az ábrán és a fuzzy rendszerben (IQ).

A készített mélyinterjúk alapján egyértelműen kijelenthető az a logikus tény, hogy az intelligencia fontos tényező. A mentálisan retardált vagy gyenge intelligenciával rendelkező személyek nehezebben tudják értelmezni, hogy egy támadó milyen szándékkal közeledik hozzájuk, míg egy magasabb IQ-val rendelkező egyén könnyebben átlátja az összefüggéseket. Ha az illető találkozott már valamilyen biztonságtudatossági tréninggel, akkor egy valós támadás során szintetizálni tudja az ott tanultakat, és azt felismerve tud cselekedni.

[71] CIA (Central Intelligence Agency), azaz az Amerikai Egyesült Államok Központi Hírszerző Ügynöksége

Az intelligenciát a következő tagsági függvényekkel jellemeztem:

- Magas: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Gyenge: [0.6 0.9 1 1].

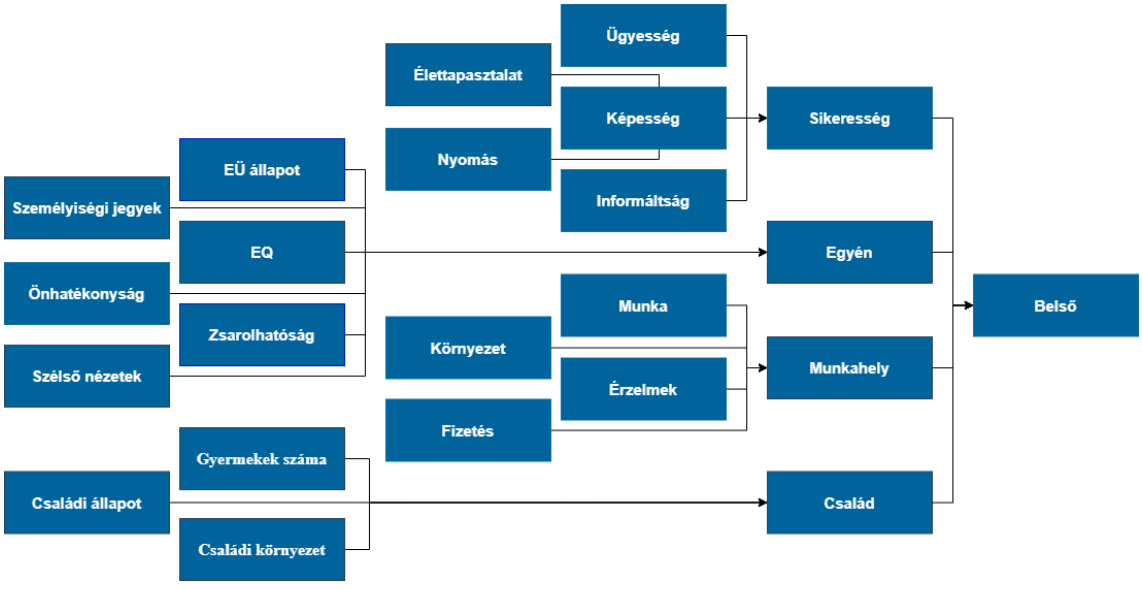
3.2 Belső szubjektív kontrollok

Az ábrán és a fuzzy rendszerben (Belső).

A belső kontrollok megléte vagy azok hiánya megmutatja, hogy az egyén a személyiségéből, személyes környezetéből fakadóan potenciálisan mennyire fogja elkövetni az adott tettet. Ez alapján a tagsági függvények a következőek:

- Nagy: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];
- Kicsi: [0.6 0.9 1 1].

A belső szubjektív kontrollok a legszerteágazóbbak, ezért azok további csoportosítása szükséges, melyet a következő módon tettem meg:



27. ábra - A belső szubjektív kontrollok struktúrája (saját szerkesztés)

3.2.1 A támadás végrehajtásának sikerességi tényezői

Az ábrán és a fuzzy rendszerben (Sikeresség).

A sikerességi faktorok megmutatják, hogy a belső szubjektív kontrollok alapján milyen esélyeit látja az egyén arra, hogy végrehajtsa a titoksértést. Ennek értelmében ez a tényező a következő tagsági függvényekkel jellemezhető:

- Esélytelen: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Esélyes: [0.6 0.9 1 1].

Ügyesség

Az ügyesség elsősorban a lebukás valószínűségének dimenziójaként értelmezhető. Ha valaki kellően ügyes, körültekintő és megvannak a megfelelő információi a nyomok eltüntetéséhez, akkor ez valószínűleg elősegíti a tett elkövetését. Az ügyesség megmutatkozhat abban is, hogy valaki el tudja-e terelni magáról a gyanút vagy megtalálja-e azokat a kiskapukat, amelyekkel nem, vagy nem számottevő mértékben vonható felelősségre.

A következő tagsági függvényekkel jellemezhető ez a tényező:

- Ügyetlen: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Ügyes: [0.6 0.9 1 1].

Élettapasztalat

Az élettapasztalat két alapvető tényezőből tevődik össze. Az illető ***kora*** megmutatja, hogy mennyi tapasztalatot gyűjthetett már össze, míg az ***iskolázottsága*** az elméleti ismeretanyag mennyiségében számíthat. A tagsági függvények ebben az esetben a következők:

- Tapasztalt: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Tapasztalatlan: [0.6 0.9 1 1].

28. ábra - Élettapasztalat tényezői (saját szerkesztés)

A legmagasabb iskolai végzettség véleményem szerint kis mértékben számít, de érdemes vele kalkulálni, hiszen egyszerűen begyűjthető adat. Minimális kockázatot rejt ugyan önmagában az is, hogy ha valaki csak alap- és középszintű tanulmányokat végzett, hiszen feltételezhetően kevesebb elméleti ismeretanyaggal rendelkezik diplomás társainál. Ettől függetlenül számos olyan személy van, aki ugyan soha nem

vett részt felsőoktatásban, mégis több tudással, rátermettséggel, gyakorlati tapasztalattal rendelkezik. Ezt a tényezőt a következő tagsági függvényekkel jellemeztem az elvégzett tanulmányokat alapul véve az **iskolázottságot**:

- Magas: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];
- Alacsony: [0.6 0.9 1 1].

Ami sokkal fontosabb, az a szakismeret. Tudjuk azt, hogy egyre több szakmában használnak számítógépet, de ezek sokszor kimerülnek az alapszintű felhasználói tudásban. A mai napig vannak olyan kétkezi szakmák (pl. építőipari szakmunkások, szépség- vagy a vendéglátóiparban dolgozók stb. egy része), ahol egyszerűen nincs, vagy elhanyagolható mértékben van rá szükség. Ezeknél a személyeknél várhatóan egyszerűbb dolguk lesz a támadóknak. Felmerülhet a kérdés, hogy ők miért lennének kockázatosak, ha munkájuk révén nem is kötődnek a kibertérhez. Az igazság az, hogy a kritikus infrastruktúrákban, nagy vállalatoknál, az államigazgatásban, ha ők nem is dolgoznak IT eszközökkel, szinte biztos, hogy van a környezetükben számítógép. A gondnok, a takarító, a szerződtetett masszőr stb. mind képesek arra, hogy egy egyszerű, jól elmagyarázott cselekedetet végrehajtsanak, ha a támadók valamilyen fogási pontot találnak rajtuk. Mivel nem rendelkeznek megfelelő tudással, ezért a veszélyérzetük sem kellő mértékű. Ezeket a körülményeket részben a digitális kompetenciák kapcsán kezelem. Fontos azonban külön kezelni, hogy egy illető milyen valószínűséggel találkozott különböző, akár kritikus szituációkkal az életében.

Ezt a tényezőt a következőkben ismertetett módon, az emberi élet szakaszai alapján érdemes elkülöníteni, hiszen ez az érés függ az adott személytől:

- Idős: [0 0 0.1 0.4];
- Középkorú: [0.1 0.4 0.6 0.9];
- Fiatal: [0.6 0.9 1 1].

Képesség

Egyik alapvető kontroll, hogy az adott személy képes-e lelkileg arra, hogy egy bűntettet hajtson végre. El kell azonban különíteni a jelenleg bemutatott logikai és figyelmi képességet a digitális kompetencia során tárgyalttól. Jelenleg azt vizsgáljuk, hogy egy konkrét tett elkövetésére lelkileg képes-e az illető, míg a másik esetben értékeljük, hogy konkrét szoftvereket és/vagy hardvereket tud-e használni.

A tagsági függvények a következők:

- Képtelen: [0 0 0.1 0.4];
- Attól függ: [0.1 0.4 0.6 0.9];
- Képes: [0.6 0.9 1 1].

Érzelmi ráhangolódás/nyomás

Az ábrán és a fuzzy rendszerben (Nyomás).

Ez a tényező megmutatja, hogy az illető teljesítőképessége nyomás hatására hogyan változik. Az emberek a komfortzónájuk átlépésével általában jobban teljesítenek, ahogy ezt a Yerkes-Dodson törvény is megmutatja, mely akár a biztonsági szintet is növelheti egy szervezeten belül [151].

29. ábra - Yerkes-Dodson törvény [151]

A kérdés az, hogy egy bizonyos információ kilopása a szervezetből az adott személy stressz-szintjén hol helyezkedik el: még a feszült figyelem állapotát eredményezi-e az illetőnél, vagy már átbillen a kimerülés szakaszába. Ezeket figyelembe véve a teljesítés dimenziójával jellemeztem ezt a tényezőt:

- Alulteljesít: [0 0 0.1 0.4];
- Átlagosan teljesít: [0.1 0.4 0.6 0.9];
- Túlteljesít: [0.6 0.9 1 1].

Informáltság

Az informáltság egy elég tágan értelmezhető tényező. Itt azt fontos figyelembe venni, hogy megfelelő ismeretei vannak-e egy munkavállalónak egy potenciális támadás kivitelezésére. Ismeri-e a szabályzatokat, a kiberbiztonsági kontrollokat, és azok kijátszhatóságát. Tudja-e, hogy konkrétan mit, honnan és hogyan kell neki kilopnia. Ez

az információ származhat a kollégák okos kérdezgetéséből, de külső, harmadik fél által korábban megismert információk alapján is.

Ezt a tényezőt nem szabad összetéveszteni azzal az információhiánnyal, hogy az illető nincs megfelelően tájékoztatva arról, hogy mit lehet és mit nem. Ezeket a biztonságtudatosság (3.5. fejezet) és külső munkahelyi kontrollok (3.3. fejezet) kockázatai közé kell sorolni. Ez alapján a következőképpen határoztam meg a skálát:

- Informálatlan: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Informált: [0.6 0.9 1 1].

3.2.2 Családhoz köthető tényezők

Az ábrán és a fuzzy rendszerben (Család).

Mindenki más és más családi környezetben él. Jelen értekezésben nem célom, hogy a különböző családtípusokat külön-külön vizsgáljam. Az itt ismertetett tényezők általánosságban határozzák meg ezt a kérdéskört, a digitális információszivárogtatást figyelembe véve. Ennek értelmében a családnak a belső szubjektív kontrollok kialakulására fejtett hatása a következő lehet:

- Pozitív: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Negatív: [0.6 0.9 1 1];

A megélhetés és a felelősségvállalás szemszögéből fontos, hogy milyen egy személy **családi állapota**. Egy esetleges célzott támadás során a célszemély döntését befolyásolhatja, hogy van-e rajta kívül olyan személy, akit el kell tartania. Ez szoros összefüggésben van a következőkben ismertetett eltartott gyermekek számával, vagyis azzal, hogy mennyien élnek egy háztartásban.

Az, hogy valaki egyedülálló vagy párkapcsolatban él, egyéb körülményekkel, a személyiségével együtt értelmezve szintén közrejátszhat egy adott cselekedet végrehajtásában. Egy laza, kialakulóban lévő kapcsolat általában kevésbé jelent elköteleződést mások iránt. Amennyiben az illető jogilag is felelős másért (házasság, bejegyzett élettársi kapcsolat), akkor ez erkölcsileg erősítő hatású lehet. Egy egyedülálló nő vagy férfi valószínűleg könnyebben megy bele kockázatos cselekedetekbe. Érdekes helyzetet jelenthet, ha valakinek megromlott a házassága, és

még válás előtt/közben van. Az ilyen különleges helyzeteket minden esetben külön kell vizsgálni. Ráadásul ezekbe a folyamatokba – érthető módon – nem szeretnek az emberek külsősöket bevonni. További kockázatot jelent, ha valakinek szeretője van. Ez az információ azonban szinte soha nem áll rendelkezésre.

Ennek a kockázatnak a tagsági függvényeit a párkapcsolat erősségével tudom jellemezni, hiszen a hivatalos kapcsolati státusz különböző személyeknél mást és mást jelenthet:

- Erős: [0 0 0.1 0.4];
- Köztes: [0.1 0.4 0.6 0.9];
- Gyenge: [0.6 0.9 1 1].

Érdemes foglalkozni azzal az adattal, hogy van-e gyermeke valakinek. Ez a tény főleg a szülő és a gyermek viszonyával és az anyagi helyzettel van összefüggésben. Nélkülöző családokban a gyermekük étkeztetése érdekében felmerül a kockázat, hogy valamilyen extra juttatásért cserébe megtesznek egy „semmiségnek tűnő” (pl. pendrive számítógépbe történő behelyezése) cselekedetet. Főleg akkor, ha nincs megfelelő tudásuk arról, hogy mi lehet a tettük következménye. Azonban, ha valaki megfelelő képzést kapott, akkor a büntetőjogi következmények tudatában ez visszatartó erő is lehet. Feltételezhetően a szülő nem szeretné sorsára hagyni gyermekét, amíg ő a börtönben van.

A tagsági függvényeknél egy relatív értéket határoztam meg. Azt vizsgálom, hogy az adott család jövedelméhez képest mennyi a **gyerekek száma**:

- Kevés: [0 0 0.1 0.4];
- Normál: [0.1 0.4 0.6 0.9];
- Sok: [0.6 0.9 1 1].

A családi környezet tehát sok szempontból fontos. De a fenti két felelősségvállalás tekintetében meghatározó tényező mellett szükséges vizsgálni a minőségét is az adott **családi környezet**nek. Egy szeretetteljes környezetben élő személy feltehetően stabilabb személyiséggel rendelkezik, míg azok, akiket szélsőséges esetben akár bántalmaznak is. Ezt elemezve a következő három állapotot különböztetem meg:

- Támogató: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];

- Ellenséges: [0.6 0.9 1 1].

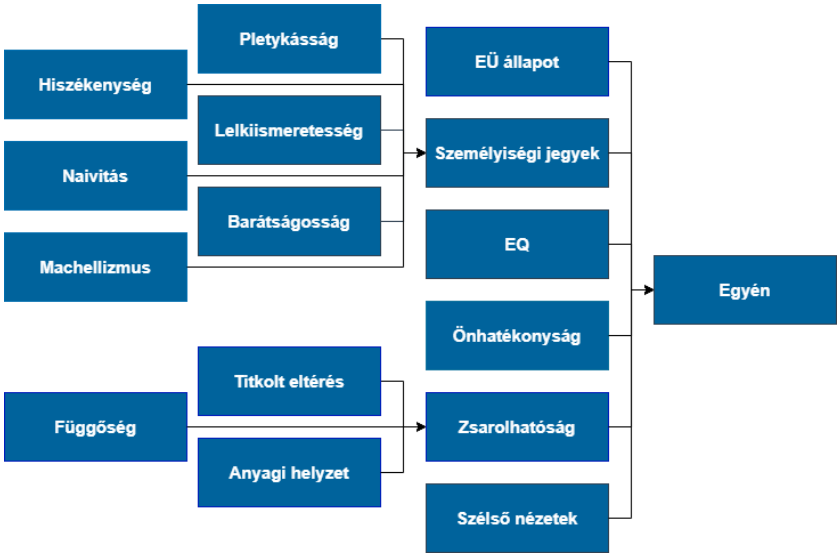
3.2.3 Az egyén más jellemző tulajdonságai

Az ábrán és a fuzzy rendszerben (Egyén).

Ebbe a csoportba olyan kockázati tényezők kerültek, amelyek kifejezetten az adott személyre vonatkoznak, de nem konkrétan a sikerességet befolyásolják. A tagsági függvények a következők:

- Stabil: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Instabil: [0.6 0.9 1 1].

Az egyéni stabilitást befolyásoló tényezőket a következő ábra mutatja be részletesen:



30. ábra - Egyéni stabilitást befolyásoló tényezők (saját szerkesztés)

Egészségügyi állapot

Az ábrán és a fuzzy rendszerben (EÜ állapot).

Feltételeztem, hogy a rossz egészségügyi állapot hatással lehet arra, hogy valaki végül elkövet-e egy adott cselekedetet, mivel az egészségesség a legalapvetőbb fiziológiai szükségleteinkhez tartozik. Ennek véleményem szerint több oka is lehet. Egy súlyosan beteg ember, amennyiben van családja, „úgy is mindegy” alapon könnyebben hajthat végre olyan cselekedetet, mint aki ereje teljében van, és egy esetleges felelősségre vonás az egész életére hatással lehet. A beteg emberek általában igyekeznek megragadni minden lehetőséget, főleg, ha egy drága kezelés kifizetése a tét. Erre releváns forrást nem találtam, ezért a kérdőívemben tértem ki rá.

Itt 3 karakternél építettem be a betegséget. Kifejezetten arra voltam kíváncsi, hogy ha súlyos esetről van szó, többen választják-e kockázati tényezőként. Ezt úgy alakítottam ki, hogy 2 esetben simán „betegeskedő”-ként jellemeztem, míg egy esetben a „súlyos betegsége van” kifejezés szerepelt a leírásban. Ez utóbbira 38 jelölés érkezett, míg a másik kettőre összesen 17. A kapott adatok alapján az feltételezhető, hogy minél betegebb valaki, annál nagyobb kockázatot jelent.

További fontos dolog azon munkavállalók kockázatának a megismerése, akik valamilyen testi, adott esetben szellemi fogyatékossággal, betegséggel rendelkeznek. Ezt az egyszerűség kedvéért szintén az egészségügyi állapotba sorolom, de ha ennek jelentős relevanciája van, akkor érdemes külön foglalkozni vele és a kockázatok kezelésére speciális informatikai eszközöket alkalmazni.

A következő skálával jellemezhető ez a tényező:

- Egészséges: [0 0 0.1 0.4];
- Beteg: [0.1 0.4 0.6 0.9];
- Súlyos beteg: [0.6 0.9 1 1].

Személyiségi jegyek

A SZEM modellben javasolt módon a személyiségi jegyek bevezetését én is fontosnak tartom. Az, hogy milyen belső tulajdonságai vannak egy adott személynek, azt is befolyásolhatják, hogy önmagától követne-e el egy titoksértést valaki, de bizonyos esetekben azt is, hogy mennyire fizethető le egy külsős fél által valamekkora pénzért cserébe. Ezt a tényezőt a személyiségi tényezők kockázatosságával jellemeztem:

- Nem kockázatos: [0 0 0.1 0.4];
- Kezelhető: [0.1 0.4 0.6 0.9];
- Kockázatos: [0.6 0.9 1 1].

Fontosnak tartom kiemelni ismét, hogy a modell nem alkalmas kezelni a klinikai személyiségzavarokat. Münnich és Hunyadi megközelítése e területen az általánosan is elfogadott ötfaktoros (Big 5) modell [152] bevezetése, és azon belül is a lelkiismeretesség (beszabályozottság, felelősség, kötelességtudat stb.) és a barátságosság (szeretetreméltóság, bizalom, őszinteség stb.) vizsgálata, hiszen ezek negatív kapcsolata a becstelenséggel empirikus módon bizonyított [153].

A Teljesítményértékelési Rendszerben (TÉR) található kompetenciák közül a lelkiismeretesség dimenziójához a „*Figyelem a feladatok végrehajtására*” „*Határidők betartása*” „*Munkatempó és feladatvállalás*”, míg a barátságosságéhoz a „*Csapatmunka, együttműködés*” és a „*Problémamegoldás*” kapcsolható [113]. Ezeket figyelembe véve bármely munkahelyen mérhetőek ezek a tényezők.

Számos negatív tulajdonság is beilleszthető ide, amit a támadók előszeretettel használnak ki [53]. Ilyen a hiszékenység, a naivitás és a figyelmetlenség is. Ez utóbbi azonban külön szerepel, mivel különösen nagy szerepe van abban, hogy valaki gondatlanságból követ-e el egy konkrét tettet. Szorosan kötődik ezekhez a tényezőkhöz a pletykás személyiségi jegy, mely a kérdőívet kitöltők válaszai alapján nem hagyható ki a kockázatos tulajdonságok közül.

Mivel egy adott ember személyiségi jegyei, privát élete ennél a tényezőnél mutatkozik meg, így feltételezhetően egy valós felmérésnél ebben az esetben lesznek a legnagyabb bizonytalanságok, adott esetben ezeknél a pontoknál áll a legkevesebb információ a munkáltató rendelkezésére. Ez a fuzzy logikának köszönhetően azonban jól kezelhető, mint ahogy az is, ha egy vizsgáló nem ért egyet az általam meghatározott tényezőkkel, azok osztályozásával. Ezekben az esetekben egyszerűen csak változtatni szükséges a modell szabályrendszerén, illetve a bemeneteken és azok tagsági függvényein.

A fent említett öt személyiségi jegynek (lelkiismeretesség, barátságosság, hiszékenység, naivitás és pletykásság) a tagsági függvényei leírhatók azzal, hogy jellemző-e egy egyénre vagy sem. Az első kettő pozitív tulajdonság, ezért a tagsági függvényeik:

- Igen: [0 0 0.1 0.4];
- Talán: [0.1 0.4 0.6 0.9];
- Nem: [0.6 0.9 1 1].

A három negatív tulajdonságnak pedig a fordítottja:

- Nem: [0 0 0.1 0.4];
- Talán: [0.1 0.4 0.6 0.9];
- Igen: [0.6 0.9 1 1].

Fontos megvizsgálni azonban a manipulációra alkalmas személyiségi jegyeket is. Ezt a viselkedési stílust nevezzük machiavellizmusnak. Az alacsony machok olyan személyek, akik ennek mérsékelt szintjével rendelkeznek. Számukra fontos a

csoportokhoz való tartozás, és nekik fontos elvekkel, emberekkel könnyen tudnak azonosulni. A magas mach személyeknél ennek az ellenkezője igaz. Nekik az önérdek (bizonyos esetben mások érdekének) érvényesítése a prioritás. Ez a viselkedés nem egyenlő a másoknak történő ártással, de ha azzal párosul, akkor nagy kockázatot jelenthet [154]. Fontosnak tartom megjegyezni, hogy a machiavellizmus nem egyenlő a nárcizmussal vagy a (szubklinikai) pszichopátiával, noha sok esetben van átfedés [155].

A tagsági függvények ez esetben a következőek:

- Alacsony: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Magas: [0.6 0.9 1 1].

Érzelmi intelligencia

Az ábrán és a fuzzy rendszerben (EQ).

A magas érzelmi intelligenciával rendelkező személyek képesek tisztán látni az érzelmi állapotuk, a gondolataik és a tetteik közötti kapcsolatot, valamint kontrollt tudnak gyakorolni saját érzelmeik felett. Mivel képesek mások állapotát is megfelelően észlelni, ezért sok esetben befolyásolni tudnak másokat. A magas EQ-val rendelkező egyének a kapcsolatépítés és fenntartás területén is sikeresek tudnak lenni [156].

Ez a képesség tudatosan használva kockázatos is lehet, azonban ennek hiányában egy illetőt sajnos könnyen befolyásolni, így manipulálni is lehet. Az EQ tagsági függvényeit a következő képen határoztam meg:

- Magas: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Alacsony: [0.6 0.9 1 1].

Önhatékonyság

Az önhatékonyság egy nagyon egyszerű, de fontos kockázati tényező. Alapvetően jól mérhető tapasztalati úton. Ez a kockázati tényező azt takarja, hogy amit akar egy egyén, azt véghez is viszi. Ha valakiben ez a tulajdonság erős és ki szeretne csempészni valamilyen szenzitív információt, akkor az meg is teszi. Ellenkező esetben, ha valaki általában hamar feladja a dolgokat, akkor egy-két komolyabb akadály, néhány sikertelen próbálkozás után lehetséges, hogy fel is adja a próbálkozást. A tagsági függvények a következőképpen alakulnak ebben az esetben:

- Nem önhatékony: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Önhatékony: [0.6 0.9 1 1].

Zsarolhatóság

Egy ember alapvetően számos ok miatt zsarolható, azonban véleményem szerint van három nagyon meghatározó tényező, amely az átlagembereket érintheti, és nem minősül elhanyagolhatóan ritkán előforduló extrém esetnek (pl. elrabolják egy családtagját vagy barátját). Egyik, talán legjellemzőbb, ha valaki a társadalmi normától eltér és nem szeretné, ha az kitudódna. Másik eset, ha az illető személy valamilyen erős függőségben szenved, aminek kielégítésével kecsegtet egy harmadik fél. Ez lehet az olcsó, nagymennyiségű dohányáru, a gyógyszer, vagy drogfüggő számára biztosított szer is. A harmadik pedig azoknak az esete, akik anyagilag kiszolgáltatottak, vagy egyszerűen kevesebb a mindennapi betevőjük másoknál.

Ezt a kockázati tényezőt a zsarolhatóság nehézsége alapján értelmezem:

- Nehezen: [0 0 0.1 0.4];
- Átlagosan: [0.1 0.4 0.6 0.9];
- Könnyen: [0.6 0.9 1 1].

Számos olyan ***eltitkolt eltérés*** lehet, amely eltér a társadalmilag elfogadott normától, ráadásul ezek nagyon különbözőek lehetnek konkrét országtól, régiótól függően. Az, hogy valaki nem meri felvállalni például vallását, politikai nézeteit vagy szexuális orientációját, lehet csupán azért, mert fél a közvetlen környezet reakciójától, a kiközösítés lehetőségétől, de bizonyos helyeken előfordulhat, hogy ezek miatt komolyabb szankciók is várhatnak rá. A történelem és sajnos a jelenkor is tele van hasonló példákkal. Egy másik példa az ilyen esetekre, ha valakinek például házasságon kívüli szeretője van, és fél, hogy ez kitudódik. Az ábrán és a fuzzy rendszerben *Titkolt eltérés* néven található meg.

A tagsági függvények az eltérés mértékében a következőek:

- Kicsit: [0 0 0.1 0.4];
- Jobban: [0.1 0.4 0.6 0.9];
- Nagyon: [0.6 0.9 1 1].

A ***függőség*** egy nagyon komplex jelenség. Genetikai hajlamok, neuroanatómiai sajátosságok, pszichológiai jelenségek, a kultúrában gyökerező addiktogén klíma mind hatást gyakorol rá [157]. A kémiai szerek (pl. kábítószer, nikotin, alkohol) által okozott függőség mellett beszélhetünk viselkedési addikciókról is. Ilyen lehet a kleptománia, szex-addikciók, kapcsolatfüggőség, a szerencsejáték-függőség is, de az információs társadalom robbanásszerű fejlődésével párhuzamosan új típusú függőségek is kialakultak. Noha nem a technológia, hanem a vele párhuzamosan kialakuló szocializáció hordozza a veszélyt [158], mégis fontos felismerni azt. Az IT-hoz köthető függőségi forma például az internetfüggőség [159] a cyberszex vagy a cyber-kapcsolatok iránti függőség, a kényszeres netezés, információ túltöltés, számítógép-függőség [160], de az okostelefonok és a közösségi média elterjedésével további típusok is kialakultak.

A függés mértéke alapján a következő kategóriákat határoztam meg:

- Nem függő: [0 0 0 0.1];
- Enyhén függő: [0 0.1 0.35 0.45];
- Függő: [0.35 0.45 0.7 0.8];
- Szenvedélyszerűen függő: [0.7 0.8 1 1].

Természetesen más és más hatással vannak az ember életére, azonban a függőségek a támadói oldalról kihasználhatóak, hiszen egy adott ember életéhez tartozik az adott cselekvés vagy kémiai vegyület. Ezek meghatároznak szokásokat, amelyeket egy social engineering támadás során nagyon könnyen fel lehet használni. A függőségekre tehát kockázati tényezőként kell tekinteni azok súlyosságától függően. Természetesen egy alkalmankénti alkoholfogyasztó személyt más módon kell kezelni, mint egy olyat, aki rendszeresen szintetikus drogokat fogyaszt.

Az ***anyagi helyzet*** jelentőségét véleményem szerint sokan túlmisztifikálják. Egy stabil önképpel rendelkező személy anyagi helyzetétől függetlenül nem fog szándékosan információt szivárogtatni. Azonban két ugyanolyan személyiségű embert feltételezve, akik csak anyagi helyzetükben térnek el, a szegényebb egyén nagyobb kockázatot jelent. Ennek csupán az az oka, hogy a támadók célja is a profitmaximalizálás. Ezért feltételezhetően egy rosszabb anyagi helyzetben lévő embernek kevesebb értékű ellenszolgáltatás (kenőpénz, juttatás stb.) elegendő, mint annak, aki jobb anyagi körülmények között él. Azonban minden esetben kockázatnövelő hatást jelent a

hiteltartozás. Ennek mértéke, jellege (banki, uzsora stb.) határozhatja meg a kockázat növekedését.

Anyagi helyzet szerint négy csoportba sorolhatók az emberek [161]. Ez az érték tipikus fuzzy halmaz. Nem eldönthető, hogy akinek X forintja van, az még szegény, de X+1 forinttól már a középosztályba tartozik. A mélyszegény kategóriába az a háztartás tartozik, ahol a havi bevétel még a szükséges minimum kiadásokat sem fedezi; azaz nincs egészséges lakókörnyezet, nem telik egészséges ételre vagy az alapvető orvosi ellátás fedezésére. Itt a kiberbiztonsági kockázat akkor értelmezhető, ha egy rosszindulatú személy felbérel egy mélyszegénységben élőt, hogy hajtson végre valami tettet.

A szegénységi spektrum egyik végén azok a társadalmi minimum alatt élők találhatók, akik tudnak vásárolni az életben maradáshoz elegendő ételt, fedél van a fejük felett és alap egészségügyi kiadásaikat is fedezni tudják. A skála másik vége pedig, ahol nem okoz gondot egy olcsóbb lakás, gépjármű fenntartása. Az itt lévő háztartások pénzüket beosztva néhány 10 ezer forintot félre tudnak tenni havonta, így akár jól megfontolva nyaralni is el tudnak menni időnként. A gyerek egyetemét a szülők azonban csak lemondással tudják kigazdálkodni és ugyan egy hirtelen jött nagyobb orvosi kiadást ki tudnak fizetni, de egy hosszabb betegség komoly anyagi problémát jelent. A szegény családokban élők számára például a gyermek iskoláztatásának, vagy valamely családtag komolyabb betegsége gyógykezelésének fedezésére tett ígéret lehet megfelelő motiváció egy bizalmasabb információ kiszivárogtatására.

A középosztályba tartozó háztartások számára nem a pénz megléte vagy annak hiánya dönti el, hogy megvesznek-e egy drágább eszközt vagy elmennek-e nyaralni egy nívósabb helyre, hanem az, hogy van-e hozzá kedvük. Ennek a skálának az alján helyezkednek el azok a jól kereső alkalmazottak (pl. fejlesztők), akik egy fizetésből el tudják/tudnák tartani az egész háztartást. Nem költekezhetnek ugyan kényük-kedvük szerint, de nincs gondjuk a hétköznapokban, és tartalékukból egy-két évig is kihúznák munka nélkül. A középosztály tetején vannak azok, akik tulajdonképpen nagyon jól élnek, akár luxusnak tekinthető vagyonuk is van, azonban költekezéseik fedezése érdekében dolgozniuk kell. Ennek a rétegnek a kiberbiztonsági kockázata önmagában nem igazán értelmezhető. Itt általában valamilyen sértettséggel, jellemvonással, kétes

bevételforrás leleplezésének megszellőztetésével lehet őket szándékos információsziváro gtatásra ösztönözni.

Az utolsó kategóriába pedig azok a gazdagok tartoznak, akiknek soha nem kellene már dolgozni, és mégis olyan életszínvonalat tudnak maguknak és családjuknak fenntartani, amit egy átlagos középosztálybeli nem. Ennek a társadalmi kategóriának olyan jelentős vagyona van, hogy inkább csak kedvtelésből keres újabb pénzszerzési lehetőséget. Az ebbe a kategóriába sorolható személyeket anyagi javakkal motiválni önmagában nem érdemes. Számára az adrenalin, a kihívás, az izgalom lehet mozgatóerő.

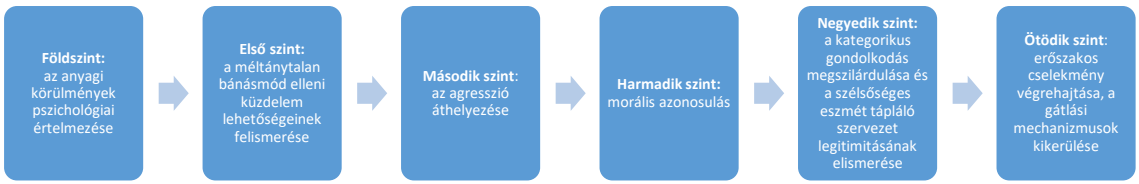
A tagsági függvények az anyagi helyzetet figyelembe véve a következőek:

- Gazdag [0 0 0.1 0.2];
- Középosztálybeli [0.1 0.2 0.45 0.55];
- Szegény [0.45 0.55 0.8 0.9];
- Mélyszegény [0.8 0.9 1 1].

Szélső nézetek

Az adott társadalomhoz képest szélsőségesen eltérő, radikális vallási, politikai, eszmei vagy más típusú nézetek kockázatot jelentenek. Természetesen itt nem arról van szó, hogy egy egyén ne gyakorolhatná alapvető jogait. Csupán egy radikalizálódott személyt könnyebb egy eszme mentén rábírni olyan tettekre, melyeket egy kevésbé szélsőséges társa nem tenne meg. Egy külsős támadónak ráadásul nem is kell egyetértenie vagy azonos eszméket vallania egy célszeméllyel, elég csupán eljátszania azt. Ez növeli az összetartozás élményét, így könnyebben hajt végre bizonyos tetteket.

A kockázat aszerint nő ebben az értelemben, hogy az illető a radikalizálódás folyamatában hol tart. Moghamddamnak a terrorizmusra létrehozott modelljét [162] Nógrádi György és Pákozdi Nóra fordította le [163]. Általánosan értelmezve egy jól definiálható skálát kapunk, legyen szó vallásról, politikáról vagy bármilyen eszméről:



31. ábra - A radikalizálódás modellje Moghamddam, illetve Nógrádi-Pákozdi munkássága alapján (saját szerkesztés)

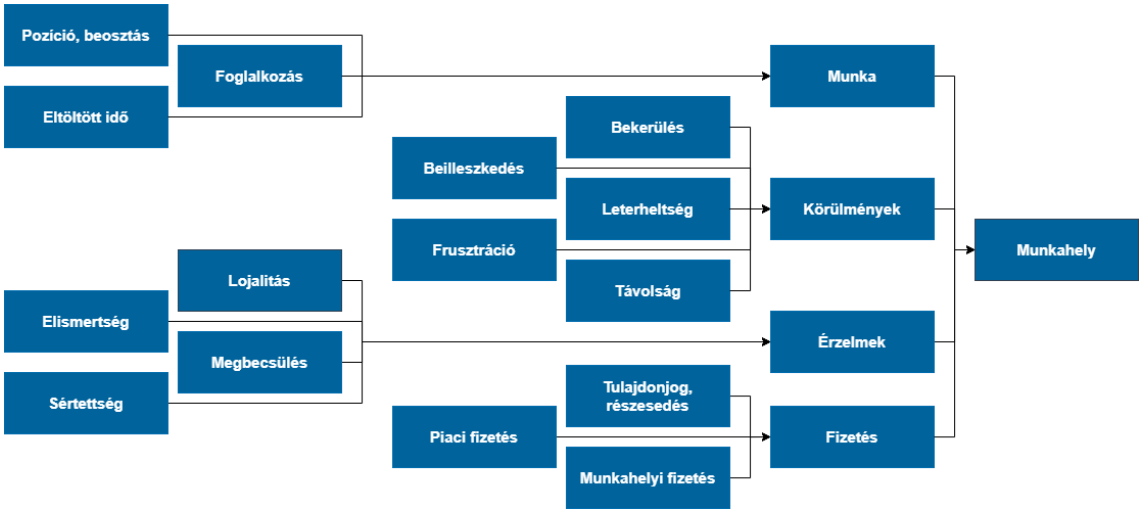
A tagsági függvények ezek alapján a radikalizálódás mértékét alapul véve a következőképpen alakulnak:

- Nem radikális: [0 0 0 0.1];
- Enyhén radikális: [0 0.1 0.35 0.45];
- Radikális: [0.35 0.45 0.7 0.8];
- Nagyon radikális: [0.7 0.8 1 1].

3.2.4 Belső munkahelyi tényezők

Az ábrán és a fuzzy rendszerben (Munkahely).

A belső munkahelyi tényezők közé azokat a kockázatokat sorolom, amelyek forrása maga az egyén és nem a külső tényezők. Azonosításuk után további négy kategóriába soroltam a következő ábrán ismertetett módon:



32. ábra - Megállapított belső munkahelyi tényezők (saját szerkesztés)

Összességében kedvezőtlen körülményeknek tekintem azt az állapotot, amikor a munkahelyen található körülmények erősítenek a tett elkövetésében. Amikor inkább gátló hatást eredményeznek, akkor számít kedvezőnek ez a kockázat. Eszerint a következő tagsági függvényeket határoztam meg:

- Kedvező: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Kedvezőtlen: [0.6 0.9 1 1].

Munkával kapcsolatos tényezők

Az ábrán és a fuzzy rendszerben (Munka).

Az üzletmenet szempontjából kiemelt munkát végző személy kockázatosabb, a digitális információszivárgás szempontjából, hiszen nagy valószínűséggel fontosabb információkhoz fér hozzá, mint akik ilyen szempontból jelentéktelenebb munkát végeznek. Ez a státusz eredhet az adott személy **pozíciójából, beosztásából**, a munkahelyen **eltöltött idejéből** és a konkrét munkaköréből, azaz a **foglalkozásából**. Három kategóriába soroltam ezt a tényezőt:

- Jelentéktelen: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Kiemelt: [0.6 0.9 1 1].

Egy adott személy pozíciója fontos adat a kiberbiztonsági kockázatának meghatározásában. Minél magasabb szinten helyezkedik el valaki a szervezeti hierarchiában, feltételezhetően annál több értékes információ birtokában van a szervezettel kapcsolatban.

Noha a felsővezetői beosztásban lévő személyek valószínűleg információs aranybányák lennének egy támadó számára, az ő megközelítésük általában nehezebb. Néha csupán olyan egyszerű oknál fogva, hogy nagyon nehezen lehet őket elérni. Sok esetben nem is ők kezelik a céges levelezésük nagy részét és a telefonon is sokkal nehezebb őket utolérni. Ez azonban nem azt jelenti, hogy lehetetlen ellenük sikeres támadást eszközölni, csupán azt, hogy más fenyegetettségek és támadási vektorok vonatkoznak rájuk, mint az alsóbb lévő szinteken.

Egy célzott social engineering támadássorozat jellemzője, hogy nem egy embertől szeretnének a támadók megismerni mindent, hiszen az feltűnő lehet. Éppen ezért különböző forrásokból szeretnének információmorzsákat begyűjteni, amelyeket együtt kezelve tudnak felhasználni egy technikai támadáshoz. Ha nem további hackelés a cél, hanem a konkrét információk megszerzése, akkor is jó technika lehet ez, hiszen kisebb eséllyel merül fel a gyanú a támadóval szemben.

Az elmúlt 10 évben általam elvégzett social engineering auditok során szerzett tapasztalatok azt mutatják, hogy a középvezetői szint támadása is nagyon jó eredményhez vezet. Ennek a munkavállalói rétegnek a birtokában vannak már kellően értékes információk, és tapasztalataim szerint sok esetben lehet az egójukra hatni. Vezetői attitűdjüktől függ, hogy a hízelgés, a gyengeség és a tudatlanság tettetése vezet

eredményre, vagy pedig a felkészült szakember szerepe. Sokat számít az is a támadások eredményességénél, hogy az adott személy mióta van a cégnél és az adott pozícióban.

A munkahelyi hierarchiát azért van értelme fuzzy értékekkel jellemezni, mert egy helyettes, tanácsadó, esetleg az adott pillanatban még ki nem nevezett vezető ugyanazokkal az információkkal rendelkezhet:

- Beosztott: [0 0 0.1 0.3];
- Alsó vezető: [0.1 0.3 0.4 0.6];
- Középvezető: [0.4 0.6 0.7 0.9];
- Felső vezető: [0.7 0.9 1 1].

Könnyen belátható, hogy a különböző munkakörben dolgozó személyek más és más információkhoz férnek hozzá a munkájuk során. Ez szintén lehet egy kockázati megközelítés. Ahogy a 2.2. fejezetben is említettem, erre külön kitértem a kérdőívemben. Az eredményeit az 2**Hiba! A hivatkozási forrás nem található.**. táblázat tartalmazza.

Kockázatot jelent a kérdőívet kitöltők válaszai alapján az is, hogy ha egy személy olyan unikális tudással rendelkezik a cégen belül, ami csak az ő birtokában van. Ez különösen akkor lehet problémás, ha egyáltalán nincs ledokumentálva a tevékenysége. Egy ilyen forráskód, hálózati architektúra vagy bármilyen más releváns tudás meg nem osztása kockázati tényező. Nem véletlenül foglalkozik a helyettesíthetőséggel és a dokumentálással a legtöbb kiberbiztonsági szakmai ajánlás.

A foglalkozások kockázatosságának tagsági függvényei a következőek:

- Alacsony: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];
- Magas: [0.6 0.9 1 1].

Azt, hogy egy illető milyen régóta dolgozik egy adott szervezetnél, leginkább a többi körülmény figyelembe vételével van értelme vizsgálni. Amennyiben alapvetően inkább pozitív az összkép, akkor egy régóta a csapatban dolgozó személy valószínűleg valóban szeret ott dolgozni, és lojálisabb lesz a céghez. Azonban, ha a negatív hatások az erősebbek, akkor ez komoly kockázatot is jelent. Vizsgálatom során az információkhoz történő hozzáférést, a folyamatok és üzleti titkok potenciális mélyebb ismeretét állítottam a középpontba. Így a régóta ott dolgozó személyeket kockázatosabbnak

tekintem, mint a frissen érkezetteket. Mindenhol más és más az átlagosan eltöltött idő, ezért ezt a tényezőt relatívan, az adott szervezethez képest kell értelmezni:

- Kevés ideje: [0 0 0.1 0.4];
- Átlagos ideje: [0.1 0.4 0.6 0.9];
- Régóta: [0.6 0.9 1 1].

Az egyén munkakörülményei

Az ábrán és a fuzzy rendszerben (Körülmények).

A kontrollok kialakulásában meghatározó tényezők lehetnek a körülmények, melyeket az egyszerűség kedvéért összefoglalóan az alábbiak szerint osztályoztam:

- Kedvező: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Kedvezőtlen: [0.6 0.9 1 1].

Az általam folytatott mélyinterjúból az derült ki, hogy a szervezethez történő **bekerülés** nehézségének leginkább kockázatcsökkentő szerepe van. Ennek oka, hogy ha valaki nagyon nehezen kerül be egy adott szervezethez, mert elsőre elutasították és ennek ellenére többször próbálkozik, akkor feltételezhetően nagyon szereti vagy szüksége van az állására. Ezt igazolja, hogy a kérdőív kitöltői közül is mindösszesen 5-en jelölték meg ezt a tényezőt, mint potenciális veszélyforrást. Ez az arány gyakorlatilag elhanyagolható.

- Nehéz: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Könnyű: [0.6 0.9 1 1].

Egy adott munkaközösségbe történő **beilleszkedés** mértéke nagyban befolyásolhatja az egyént. Amennyiben kirekesztik és nem sikerül megtalálnia a közös hangot a kollégákkal és elfogadtatni önmagát velük, akkor nincs meg a közösségvállalás élménye és még negatívan is hathat ez a tényező. Ellenkező esetben, amennyiben megbecsülik az adott illetőt, ez kockázatcsökkentő hatású, hiszen az emberek általában nem kívánnak rosszat azoknak, akikkel jóban vannak, vagy elismerik a munkájukat.

Ez a tényező az alábbi tagsági függvényekkel jellemezhető:

- Beilleszkedett: [0 0 0.1 0.4];

- Elfogadott: [0.1 0.4 0.6 0.9];
- Kirekesztett: [0.6 0.9 1 1].

Képességeihez viszonyított **leterheltség** esetén akár az alul-, akár a túlterheltség kockázatot jelenthet, ahogy a kérdőívre adott válaszok is mutatják. Az első esetben egyrészt sok ideje lehet valakinek kitervelni valamilyen károkozást, de ennél sokkal fontosabb, hogy középtávon az emberek többsége nem szeret unatkozni. A közegtől függően ez akár azt az érzetet is keltheti az illetőben, hogy nincs megbecsülve. Ha azonban valakit robotnak néznek és képességeihez képest jelentősen túlterhelik, az szintén negatív folyamatokat indíthat el benne.

A skála itt a terhelés mértéktől számítva:

- Megfelelő: [0 0 0.1 0.4];
- Eltérő: [0.1 0.4 0.6 0.9];
- Jelentősen eltérő: [0.6 0.9 1 1].

Munkavégzés közben az embereket számos tényező frusztrálhatja. A kérdőív kiértékelése után egyértelműen látszik, hogy ez magas kockázatot rejt magában. A frusztrációval járó magas stressz komoly pszichés és testi megbetegedések forrása lehet. Megelőzése elsődleges (primer) mentálhigiénés prevencióval lehetséges, mely a kóros folyamatok kialakulását okozza meg. Ez a túl- vagy alulterheltséggel, anyagi-, családi problémákkal együtt komoly kockázatot jelenthet [164].

A **frusztráció** szintjei a következően alakulnak:

- Alacsony: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];
- Magas: [0.6 0.9 1 1].

Főként nemzetközi vállalatoknál okozhat különbséget a lakóhely és a munkavégzés helye közötti **távolság**. E tényező vizsgálatakor érdemes lehet egy nagyobb ország esetén akár regionálisan is különbséget tenni. Amikor egy munkavállaló nem a vállalat székhelyén vagy telephelyén kezd el dolgozni, hanem egy másik országban vagy régióban, akkor a személyiségétől és a közvetlen, illetve közvetett kollégáitól függ, hogy mennyire tud beilleszkedni a munkahelyi közegbe. Ez ráhatással lehet a lojalitásra, ellenkező esetben annak hiányára. Ha ez a második helyzet áll elő, akkor sokkal könnyebben vehető rá valaki egy olyan tettre, mely kárt okozhat az adott vállalatnak.

Ez a helyzet több ok miatt is előállhat. Az is lehet, hogy az illető egy egész régióért felel, így értelemszerűen nem tud egyszerre több országban, de még akár városban sem ott lenni, vagy pedig azért, mert egyszerűen távmunkában dolgozik egy másik országból.

A COVID-19-es pandémia okozta helyzet sok munkáltató figyelmét felhívta arra, hogy a távmunka egy működő modell, és ezért még elfogadottabbá vált. Ettől még az otthoni munkavégzés jelenthet kockázatot a munkáltató számára. Ugyan minden ilyen személy elméletben felelősségre vonható egy általa okozott incidens kapcsán, de előállhat egy olyan szituáció, amikor ezt a távolság vagy az adott ország jogi környezete (pl. kiadatás hiánya) nem teszi lehetővé.

A tagsági függvények egyszerűen a következő képen határozhatóak meg:

- Közel: [0 0 0.3 0.7];
- Távol: [0.3 0.7 1 1].

Munkahellyel kapcsolatos érzelmek

Az ábrán és a fuzzy rendszerben (Érzelmek).

Az embereket nagyon sokszor befolyásolják az érzelmeik, így azokat a tényezőket is figyelembe kell venni, amelyek elősegíthetik vagy gátolhatják egy rosszindulatú tett végrehajtását. Ezeket összegezve a hatásuk szerint a következőek lehetnek:

- Pozitív: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Negatív: [0.6 0.9 1 1].

A szervezethez való **lojalitás** nagyban hozzájárul a cselekedet elkövetésének elutasításához. Amennyiben sikerül az adott munkavállaló számára olyan környezetet teremteni, amelyben egyet tud érteni a megfogalmazott és képviselt értékekkel, akkor kisebb valószínűséggel fog a szervezet számára negatív hatást eredményező tettet elkövetni. Ezen a skála a lojálistól az illojálisig terjed:

- Lojális: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Illojális: [0.6 0.9 1 1].

Az emberek alapvetően szeretik megbecsülve érezni magukat egy olyan közegben, ahol a mindennapjaikat töltik. Azok a személyek, akiknek véleményét elismerik a

munkahelyükön, általában jobban kötődnek a szervezethez. Akit azonban nem becsülnek meg, és nevetség tárgyaként kezelnek, az menekülni szeretne ebből a közegből, extrém esetben akár úgy is, hogy dacból kárt okozzon az őt kinevetőknek.

A következő szinteket határoztam meg az **elismertség** tagsági függvényeit:

- Elismerik: [0 0 0.1 0.4];
- Meghallgatják: [0.1 0.4 0.6 0.9];
- Elutasítják: [0.6 0.9 1 1].

Az előző pontban az emberek véleménye került a vizsgálat középpontjába, vagyis annak ténye, hogy mennyire tekinti hasznosnak az adott személyt a közösség. Fontos kockázati tényezőnek tartották a kérdőívet kitöltők azonban azt is, hogy egy illető munkáját becsülik-e vagy sem. Ugyan önmagában a **megbecsülés** hiánya még nem feltétlen váltja ki azt, hogy valaki kárt okozzon egy szervezetnek, azonban erősíti a szándékot, és más munkahelyi tényezőkre is hatással van. Ezzel ellentétben, ha valakinek megbecsülik a munkáját, akkor az segíthet az elköteleződésben. Ezek alapján három kategóriába soroltam ezt a tényezőt:

- Megbecsült: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Lekicsinyelt: [0.6 0.9 1 1].

A sértett munkavállaló kifejezetten nagy kockázatot jelenthet. Egy több éve húzódó előléptetés vagy meg nem adott fizetésemelés, egy elmaradt bónusz vagy jutalom kifizetése mind okozhatja egy személy sértettségét. Ez például nem megbecsült munkával vagy túlzott leterheltséggel, egy kevésbé befogadó közegben könnyen eredményezheti, hogy az illető megpróbál minél több adatot kilopni saját magának vagy egy konkurens szervezetnek.

A **sértettség** mértékét a frusztráltságéhoz hasonlóan jellemeztem:

- Alacsony: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];
- Magas: [0.6 0.9 1 1].

Az adott személy megfizetettsége

Az ábrán és a fuzzy rendszerben (Fizetés).

Szerencsés eset, ha valakinek a munkája a hobbija, vagy szakmáját élethivatás-szerűen űzi, de jellemzően az emberek azért dolgoznak, hogy cserébe ellentételezést kapjanak. A fizetés önmagában azonban egy szám, és szükséges ismerni a kontextus. Egy személy tehát a következő mértékben lehet megfizetve:

- Nagyon megfizetett: [0 0 0.1 0.4];
- Átlagosan fizetett: [0.1 0.4 0.6 0.9];
- Alulfizetett: [0.6 0.9 1 1].

A fizetés szempontjából egyik meghatározó viszonyítási pont a kollégák átlagfizetése és kapott juttatásai. Könnyen előfordulhat, hogy egy munkavállaló 5 évvel hamarabb érkezett az adott szervezethez, mint a frissen érkező kolléga, mégis, utóbbi akár jelentősen több fizetést kap, így nagy eltérés lehet hasonló munkakörök esetében is.

A relatív **munkahelyi fizetés** tagsági függvényeit a következőképpen határoztam meg:

- Magas: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Alacsony: [0.6 0.9 1 1].

Az előző ponthoz hasonlóan érdemes lehet megvizsgálni nem csak a mikro-, hanem a makrokörnyezetet is. Az adott szervezetnek tisztában kell lennie azzal, hogy a piachoz képest milyen juttatásokat biztosít az adott személynek. Ha ez jelentősen alacsonyabb, mint a konkurenciánál, akkor ez szintén kockázatként jelenik meg.

A skála jellemző **piaci fizetéshez** képes az előző kockázati tényezőhöz hasonlóan alakul:

- Magas: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Alacsony: [0.6 0.9 1 1].

Kockázatcsökkentő tényező lehet, ha az adott személy a fizetésén kívül más módon is érdekelt egy szervezet minél jobb működésében. Hacsak valamilyen más üzleti érdeke ezt nem írja felül, akinek többségi tulajdona van egy szervezetben, azt nagyon nehéz rávenni, hogy önmaga ellen forduljon.

A következő szint, amikor ugyan nincs többségi tulajdona egy személynek, de benne van abban a szűk körben, akik közösen alapították a céget, vagy jelentős részesedést szereztek idő közben. Ezeknek a személyeknek komoly ráhatásuk van a szervezet

működésére, ezért hacsak nincs valamilyen súlyos érdekellentét, akkor nehezen vehetőek rá olyan tettre, ami negatívan befolyásolná a szervezet működését.

A harmadik kategóriában azok a kulcsmunkavállalók vannak, akik valamilyen juttatási csomag mentén olyan részesedéssel rendelkeznek a cégben, aminek az elvesztése befolyásolná a vagyonukat. Ez is enyhítő kockázati tényező lehet, de itt már nincs olyan szoros kötődés az adott céghez. A következő szintbe tartoznak azok a részvényesek, akik tulajdonjoga csekély, így a részesedésükből fakadó haszon vagy annak elvesztéséből keletkező veszteség nincs hatással a hétköznapjaikra. Természetesen azoknak a személyeknek az esetében nem beszélhetünk kockázatcsökkentő tényezőről, akik egyáltalán nem érdekeltek ilyen módon a szervezet működésének megfelelő fenntartásában, hiszen ez számukra „csak egy munkahely”.

Kockázatnövelő tényező lehet, ha valakinek van más szervezetben olyan jelentős érdekeltsége, ami fenn tudja tartani az életszínvonalát ennek a cégnek a kiesése esetén is. Tovább növeli a kockázatot, ha a másik cég valamilyen formában konkurense a szóban forgó szervezetnek.

A tulajdonrészt illetően a következő szinteket határoztam meg:

- Sok: [0 0 0.1 0.4];
- Kevés: [0.1 0.4 0.6 0.9];
- Apró: [0.6 0.9 1 1];

3.3 Külső szubjektív kontrollok

Az ábrán és a fuzzy rendszerben (Külső).

A külső kontrollok tulajdonképpen azok a kockázati tényezők, amelyek nem a vizsgált személy lényéből, egyedi személyiségéből, helyzetéből fakadnak, hanem valamilyen külső tényezőből. Ide tartozik, hogy egyáltalán van-e lehetősége a titoksértésre, de különböző munkahelyi körülmények és állapotok is befolyásolhatják a tett elkövetését. Nagymértékben befolyásoló tényezőt jelent az is, hogy egyedül kivitelezhető-e egy cselekedet, vagy valamilyen mértékben másoktól is függ a siker.

A kontrollok a következők nagyságukat figyelembe véve:

- Nagy: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];

- Kicsi: [0.6 0.9 1 1].

Külső munkahelyi tényezők

Az ábrán és a fuzzy rendszerben (K. munkahelyi t.).

A külső munkahelyi tényezőkhöz olyan körülmények tartoznak, amelyek nem befolyásolhatók az egyén által, de hatásuk van a kockázatra. Vonatkoztatható az egész szervezetre, de bizonyos esetekben lehet értelme egy szervezeti egységre is értelmezni. Ez a kiértékelésnél a gyakorlatban azt jelenti, hogy a négy különálló, általam meghatározott részegység egy vizsgált csoport minden tagjánál többnyire állandó.

A belső munkahelyi tényezőkhöz hasonlóan a következő tagsági függvényeket határoztam meg:

- Kedvezőtlen: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Kedvező: [0.6 0.9 1 1].

Az első munkahelyi tényező a ***kompetens vezetői kontroll***. Ebben az esetben nem a vezetői stílust vagy a főnökök szaktudását kell értelmezni. A kockázatok oldaláról sokkal fontosabb az emberségesség, illetve az, hogy a munkavállaló ne érezze magát egyedül hagyva, elismerje a felettesét. Ez még akkor is igaz, ha az adott beosztott személyisége és kvalitásai nem igényelnek napi szintű ellenőrzést. Az ábrán és a fuzzy rendszerben *Vezetői kontroll* néven található meg.

A vezetők kompetenciája a következő tagsági függvényekkel jellemezhető:

- Kedvező: [0 0 0.1 0.4];
- Értékelhető: [0.1 0.4 0.6 0.9];
- Alacsony: [0.6 0.9 1 1].

Azt, hogy milyen a hangulat egy munkahelyen, a ***közösségi morál*** tényezőjével jellemeztem. Ez alatt azt a körülményt vizsgálom, hogy a munkavállalók általánosan hogyan vélekednek az adott szervezetről. Ha szeretnek ott dolgozni, akkor általánosságban előremutató szervezetként vélekednek róla, s akkor egy stabilabb környezetnek tekinthető. Ha azonban nem szeretnek ott dolgozni, sokan gondolkodnak azon, hogy távozzanak, és akkor ez kockázatként jelenik meg. Ez a tényező is értelmezhető akár szervezeti egységre is bizonyos létszám felett:

- Pozitív: [0 0 0.1 0.4];

- Semleges: [0.1 0.4 0.6 0.9];
- Negatív: [0.6 0.9 1 1].

Hiába pozitív a hangulat egy szervezeten belül, ha alapvetően nem képesek a szervezet fejlődésével új folyamatokat, informatikai megoldásokat bevezetni és alkalmazkodni hozzájuk. Ezt a tényezőt a ***közösség nyitottságával*** jellemeztem, melynél a következő tagsági függvényeket határoztam meg:

- Nyitott: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Zárkózott: [0.6 0.9 1 1].

Végül pedig nagyon fontos munkahelyi körülmény, hogy maga a szervezet ***kiberbiztonsági érettsége*** milyen szinten van saját fejlettségi szintjéhez képest. Ebbe a tényezőbe beleérhetjük, hogy mennyi és milyen kontrollokat vezettek be, vannak-e szabályzatok, és azok mennyire vannak betartva, betartatva. Értem ezalatt azt is, hogy milyen, a kiberbiztonságot érintő folyamatokat vezettek be (pl. incidenskezelés), van-e valamilyen, témához kapcsolódó tanúsítása a szervezetnek (pl. ISO 27000) vagy éppen, hogy milyen a kiberbiztonsági problémákról folytatott belső kommunikáció.

Ezt a tényezőt a következő tagsági függvények írják le:

- Érett: [0 0 0.1 0.4];
- Közepesen érett: [0.1 0.4 0.6 0.9];
- Éretlen: [0.6 0.9 1 1].

Függés mértéke

Ez a tényező leginkább a konkrét támadástól függ. Ha egy külsős személy valamilyen módon rávesz egy munkavállalót, hogy egy információszivárgási csatorna nyitását elősegítő malware-t tartalmazó adathordozót csatlakoztasson egy olyan szerverbe, amihez alapvetően nincs hozzáférése, akkor a függés többszörös, és így jelentős. Egyrészt szükség van a külsős félre, akinek megvan a szaktudása (vagy pénze) a rosszindulatú kód előkészítéséhez, illetve a támadást kivitelező munkavállalónak még hozzáférést is kell szereznie a szerverszobához. Lehetséges, hogy ehhez egy tettestársat is be kell szerveznie. Ráadásul, ha nincs megfelelő informatikai tudása, még fel is kell őt készíteni, hogy sikeres tudjon lenni. Ennek ellentéte, amikor csak egy könnyen hozzáférhető, de szenzitív dokumentumot szeretne valaki befényképezni a telefonjával. Itt a függés mértéke alacsony, szinte elhanyagolható.

A tagsági függvények a függés mértéke alapján a következőek:

- Magas: [0 0 0.3 0.7];
- Alacsony: [0.3 0.7 1 1].

Lehetőség

Fontos tényező, ahogyan a függés mértékében is részben kitértem rá, hogy mennyire van lehetősége egy illetőnek hozzáférni szenzitív adatokhoz. A kérdőívet kitöltők messze kimagaslóan az ilyen típusú kockázatokat emelték ki a legjobban, mint kockázati tényező. Egy szervezet életében az nem kivitelezhető, hogy senki ne férjen hozzá érzékeny adatokhoz, hiszen a napi működés válna lehetetlenné így. Egy megfelelően, a „need-to-know”[72] elv mentén kialakított és karbantartott jogosultságkezelés azonban nagy mértékben hozzásegíthet a kockázatok csökkentéséhez.

Ezt figyelembe véve a lehetőségek alapján a következő szinteket határoztam meg az adatok elérésének nehézségével kapcsolatban:

- Nehéz: [0 0 0.1 0.4];
- Közepesen nehéz: [0.1 0.4 0.6 0.9];
- Könnyű: [0.6 0.9 1 1].

Kétféle hozzáférést lehet ebben az esetben megkülönböztetni. Egyrészt az ***adatokhoz történő hozzáférés mértékét***, mely az informatikai, illetve a fizikai terekbe történő ***területi bejárási jogosultság*** kezelését jelenti. Az ábrán és a fuzzy rendszerben *Hozzáférés mértéke*, illetve *Bejárási jogosultság* néven találhatóak meg. Mindkét esetben a szabályozottságot tekintettem alapnak a tagsági függvények kialakításánál:

- Nagyon szabályozott: [0 0 0.1 0.4];
- Alapszintű: [0.1 0.4 0.6 0.9];
- Szabályozatlan: [0.6 0.9 1 1].

3.4 Tett elkövetésének megítélése

Az ábrán és a fuzzy rendszerben (Megítélés).

[72] A need-to-know elvet a legkisebb jogosultság (least privilege) elvének is nevezik. Lényege, hogy csak annyi és olyan minőségű adathoz, információhoz férhessen hozzá egy munkavállaló, amennyihez a munkája elvégzése érdekében feltétlen szüksége van.

Érdemes figyelembe venni, hogy az illető hogyan ítéli meg a saját tettét, illetve önmagát egy esetleges titoksértés után. Itt érdemes figyelembe venni, hogy milyen környezetből érkezik, milyen a morális felfogása, vagy éppen azt, hogy vajon arányban van-e a várt nyereség az esetleges büntetés mértékével.

Szubjektív norma

A szubjektív norma alatt azt a tényezőt értjük, amikor az egyén érzékeli a környezetéből fakadó nyomást az információszivárogtatás meg nem tételét illetően. Ilyen szempontból a szervezeti kultúra, azaz a menedzsment, a biztonsági szakemberek, a közvetlen kollégák hozzáállása (elutasító vagy nemtörődöm hozzáállása) nagyon fontos lehet. Az általuk használt kommunikáció fontos kockázatnövelő vagy -csökkentő tényező lehet. A szubjektív norma magában foglalja annak a motivációját is, hogy mennyire kíván eleget tenni az adott személy ennek a nyomásnak. A munkakörnyezet mellett azonban a közvetlen családi, baráti környezet hozzáállása (a „rossz társaság") is fontos lehet.

Ezt a tényezőt a környezet hozzáállása alapján a következőkkel jellemeztem:

- Elítélő: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Támogató: [0.6 0.9 1 1].

Nyereség-veszteség aránya

Az ábrán és a fuzzy rendszerben (Nyereség-veszteség).

Egy titoksértés elkövetésekor az egyén a felelősségre vonás elmaradásában bizakodik. Ez főleg természetesen abban az esetben igaz, ha tudatosan követi el. Ha úgy ítéli meg, hogy az elkövetés utáni nyereség jóval kedvezőbb, mint a lebukás esetén rá váró szankciók, akkor könnyebben követi el az adott tettet. Valószínűleg nem sokan vállalnák fel azt a kockázatot, amit Edvard Snowden a tettével felvállalt. Ahogy a történelem több példája is mutatja, vannak, akik megteszik. Természetesen igaz ez kisebb léptékben is. Ilyenkor egy jól végiggondolt támadásnál a szervezeti kockázatok mellett a jogi következményeket is megvizsgálják. Egy titoksértés kiderülése után akár a kémkedés vádjával is gyanúsíthatnak valakit.

Ha a nyereség-veszteség aránya alacsony, akkor feltételezhetően könnyebben elkövetik a tettet, mint ha magas. Eszerint a következő tagsági függvényeket határoztam meg:

- Magas: [0 0 0.1 0.4];
- Közepes: [0.1 0.4 0.6 0.9];
- Alacsony: [0.6 0.9 1 1].

Morális felfogás

Minden személy mást és mást tekint helyesnek. Van, aki szerint egy virág letépése is bűn, mások kipusztulás szélén álló állatfajok egyedeit ölik meg szórakozásból. Ebben az esetben nem az a kérdés, hogy mi a legális és mi nem, hanem hogy az adott embernek milyen az értékítélete. A stabil értékrenddel rendelkező személyek kevésbé kockázatosak, mint az instabil társaik. Létezik olyan ideológiai, politikai értékrendszer, ahol nem feltétlen egyértelmű, hogy hol húzódik a határ. A szó hétköznapi értelmében vett egészséges morális felfogás szerint azonban a lopás, így gyakorlatilag a titoksértés is elítélendő.

Ezt a tényezőt aszerint határoztam meg, hogy ki mennyire ítéli el az adott tettet:

- Nagyon: [0 0 0.1 0.4];
- Kicsit: [0.1 0.4 0.6 0.9];
- Egyáltalán: [0.6 0.9 1 1].

Önértékelés

Az önértékelés egy nagyon egyszerű tényező. Azt mutatja meg, hogy a tett elkövetése után az illető hogyan tekint magára: jó vagy rossz emberként. Azonban amennyire egyértelmű a meghatározás, ennek mérése annál nehezebb. Egyértelműen csak pszichológus bevonásával vagy valamilyen mélyebb beszélgetés után lehet megsejteni ezt egy munkavállalóról.

A tagsági függvények ebben az esetben a következőek:

- Rossz: [0 0 0.1 0.4];
- Semleges: [0.1 0.4 0.6 0.9];
- Jó: [0.6 0.9 1 1].

Tapasztalat

Amennyiben a társadalmi normák megsértése nem áll távol egy illetőtől vagy a vele egy háztartásban élőtől, kockázatot jelent kiberbiztonsági szempontból is. Természetesen a tiltott adatszerzés és az információs rendszer elleni bűncselekmények súlyosabb kockázati értéket képviselnek, mint egy gyorshajtási szabálysértés. A kutatás során

összegyűjtöttem azokat a Büntető Törvénykönyv [165] által megfogalmazott bűncselekményeket, melyek elkövetői potenciális bűnismétlés elkövetése miatt kiemelten kockázatosak a információszivárogtatás szempontjából. A 7. függelékben található lista összeállítása dr. Simon Béla r. őrnagy rendőrségi tanácsossal folytatott interjú alapján készült.

Fontosnak tartom megemlíteni a rendőrségi tanácsos úrral folytatott interjú alapján, hogy a felsorolt bűncselekmények a bűnügyi statisztikai rendszerben regisztrált bűncselekmények között sok esetben nem jelennek meg. Ennek oka, hogy látszólagos alaki halmazatot képeznek, illetve a gyakorlatban kvázi elnyelődnek a nagyobb súlyú bűncselekményben. Ilyen esetre példa az, amikor egy elkövető kilesi a barátnője jelkódját a telefonjáról, majd, miután megnézte az üzenetváltásokat, akkor féltékenységből emberölést követ el. Az ilyen esetek valós halmazati büntetést érdemelnének, de a gyakorlat nem ezt mutatja. Ráadásul egy erkölcsi bizonyítványban a szabálysértések nem is szerepelnek.

Ezeket figyelembe véve a tagsági függvények nem a konkrét tettet minősítik, hanem azt, hogy bűnismétlőnek tekinthető-e az illető a függelékben szereplő tettek esetén vagy nem:

- Nem: [0 0 0.1 0.4];
- Talán: [0.1 0.4 0.6 0.9];
- Igen: [0.6 0.9 1 1].

3.5 Digitális kompetencia

Az ábrán és a fuzzy rendszerben (Kompetencia).

Ahogy korábban írtam, a digitális kompetencia vizsgálata alapvetően a kiberbiztonsági kockázatok elemzésénél arra enged következtetni, hogy van-e esély arra, hogy egy elkövető gondatlanságból kövessen el egy titoksértést, és szivárogtasson ki minősített adatokat. Ha erre kicsi esély van, akkor felmerülhet a gyanú a szándékos elkövetésre. A digitális kompetencia azonban eléggé összetett. Függ egy egyén életvitelétől, hátterétől és a munkáltatótól is.

Online jelenlét

Mint sok mindenben az életben, az online csalások felismerésében is fontos a tapasztalat. Ha valaki otthonosan mozog az online térben, akkor számára az ottani

szokások, mechanizmusok jó alapot képezhetnek arra, hogy könnyebben felismerjenek egy furcsa megkeresést, vagy észleljék, ha valami „túl jó, ahhoz, hogy igaz legyen”. Ez természetesen így sem garancia, de nagyobb esély van rá.

Az online jelenlétet a gyakorisággal a következő tagsági függvényekkel jellemeztem:

- Tudatos aktív jelenlét: [0 0 0.1 0.4];
- Aktív jelenlét: [0.1 0.4 0.6 0.9];
- Passzív jelenlét: [0.6 0.9 1 1].

Digitális eszközök használatának gyakorisága

Az ábrán és a fuzzy rendszerben (Használat).

Nem csak az online tér ismerete, de a különböző eszközök használata is fontos tényező. Manapság a társadalom egy részé számára teljesen természetszerű, hogy különböző okos eszközök vannak a lakásában, és sokak esetében már egyfajta függőség is létre jött a telefonjukkal. Azonban Magyarországon is, de szegényebb országokban még inkább, vannak olyan személyek, csoportok, akiket vagy nem érdekelnek a „digitális kütyük” vagy nincs is lehetőségük ezek otthoni használatára.

A gyakoriságot a következő módon jellemeztem:

- Sokat használja: [0 0 0.1 0.4];
- Átlagosan használja: [0.1 0.4 0.6 0.9];
- Alig használja: [0.6 0.9 1 1].

Körülvevő digitális eszközök száma

Az ábrán és a fuzzy rendszerben (Eszközszám).

Azt is érdemes megvizsgálni, hogy egy személy csak egy-két eszközt használ, vagy esetleg sokfélét. Ez azért fontos, mert nagy a különbség aközött, hogy valaki egy típusú eszközt (pl. okostelefont) megtanult jól kezelni, illetve aközött, hogy bátran hozzá mer nyúlni bármilyen rendszerhez. Ezt az őt körülvevő digitális eszközök számával lehet jellemezni. Ennek oka, hogy minél többféle eszközt használ, annál jobban megvan az esély a működés logikájának megértésére. Így legyen szó bármilyen új szervezeti eszközről, azt magabiztosan használja, és valószínűleg nem fog véletlenül valamilyen műveletet elvégezni.

Ezt a tényezőt a következő tagsági függvényekkel jellemeztem:

- Sok: [0 0 0.1 0.4];
- Átlagos: [0.1 0.4 0.6 0.9];
- Kevés: [0.6 0.9 1 1].

Felhasználói ismeretek

Míg a digitális eszközök használatának gyakorisága és száma között is van összefüggés, addig az online jelenlét és a felhasználói ismeretek között is van hasonlóság, de mégis különböznek. Az, hogy valaki a közösségi médiában jelen van és ismeri az online tér mechanizmusait, nem jelenti azt, hogy érti a számítógép vagy okostelefon működését. Lehetséges, hogy valaki könnyen vásárol az interneten, de ugyanaz a személy nem biztos, hogy érti az eszköz fájlstruktúráját, vagy a másolás, kivágás és beillesztés funkciókat.

Ez utóbbit jellemeztem a felhasználói ismeretekkel, mely tagsági függvényei a következőek:

- Profi: [0 0 0.1 0.4];
- Felhasználói szintű: [0.1 0.4 0.6 0.9];
- Alapszintű: [0.6 0.9 1 1].

Nyelvismeret (angol)

Továbbá fontos kockázatcsökkentő tényező az idegennyelv-tudás. Mivel az angol vált az üzleti kommunikáció és az informatika alapjává, ezért ennek ismerete különösen hasznos lehet egy véletlen károkozás megelőzésére. Ha a célszemély nem érti a képernyő tartalmát, akkor könnyen előfordulhatnak véletlen kattintások, esetleg egy phishing kampány is hatékonyabb lehet ellene.

Az angol nyelvtudás a következőképpen jellemezhető:

- Anyanyelvi szintű: [0 0 0 0.1];
- Felső szintű: [0 0.1 0.25 0.35];
- Középszintű: [0.25 0.35 0.65 0.75];
- Alapszintű: [0.65 0.75 0.9 1];
- Nincs: [0.9 1 1 1].

Digitális szocializáció

A digitális szocializáció egy koralapú meghatározás. Az, hogy valaki élete melyik szakaszában ismerkedett meg az információs technológiával, általában összefüggésben van a digitális írástudásával. Természetesen önmagában nem jelenthető ki, hogy egy idősebb generációba tartozó személy biztosan kevésbé jártas a technológiában, mint egy fiatal társa. Azonban a különböző generációk képviselői a digitalizáció dinamikus fejlődését nem egyforma mértékben képesek követni, ezért más és más kockázatot rejtenek. Sajnos a hétköznapok azt mutatják, hogy nincsen olyan korosztály, ahol általánosan kielégítő lenne a biztonságtudatosság. Természetesen egy általánosfelhasználó-szintű személyt kell jelen esetben vizsgálni. Érdemes külön kezelni a mérnököket és biztonsági szakembereket, akikre munkájukból fakadóan más fenyegetettségek vonatkoznak.

A 2010 után született alfa („digitális bébi") generáció szülötteiről még nincsenek tapasztalataink a munkahelyi kiberbiztonság terén, hiszen jelenleg még nem munkaképes gyermekekről van szó. Ettől függetlenül jelentenek kockázatot, de csak közvetett módon, amennyiben a szülő eszközéhez hozzáférnek és ott valamilyen gondatlan letöltéssel, kattintással vagy más módon elősegítik a támadókat. A veterán generáció szintén kiesik az aktív munkavállalók közül, hiszen e csoportba tartozó személyek a 70-es éveik második felén is túl vannak, így már biztosan elérték a nyugdíjkorhatárt. Természetesen vannak ilyen idős korban is aktív emberek, azonban olyan kevesen, hogy velük érdemes külön foglalkozni. Korukból fakadóan nem mozognak nagyon otthonosan a digitalizációban, és mivel jellemzően nincs rendszerszintű ismeretük a technológiában, így egy támadó akár ki is használhatja tudatlanságukat, tájékozatlanságukat.

Egy átlagos Baby-boomer (született 1946-1964) élete derekán – 30-40 éves korában – találkozott először a mai technológia alapjaival és leginkább alapszinten ért az újabb szoftverekhez és hardverekhez. Munkájából adódóan szükséges kezelnie a számítógépet, de tudása és biztonságtudatossága jellemzően alacsony, így sokszor könnyű támadási felületet biztosít egy támadónak. Viszonylag hamar megvezethető különböző phishing támadással, de a telefonos hívás alapú jelszó és adatkérő technikáknak is gyakran bedől.

Az X generáció (született 1965-1979) jóval komfortosabban mozog a technológiai világban. Napi szinten használják a különböző eszközöket, és mivel nem beleszülettek, hanem tanulták a digitalizációt, általában van egyfajta óvatos távolságtartásuk. Ez egyfajta elővigyázatosságot is jelent, hiszen a már megszerzett tapasztalatok miatt jobban értik, hogy nem árt óvatosnak lenni. Ellenük többször lehet szükség összetettebb támadások kivitelezésére, azonban az emberi hiszékenységet, naivitást kihasználó social engineering támadások ellenük is sokszor hatékonyak. Ettől függetlenül manapság biztonsági szempontból kiemelten fontos korosztály. Sokszor nem tudják, hogyan viszonyuljanak gyermekeik által használt újabb és újabb platformokhoz [166], ráadásul ők teszik ki a munkaerőpiac jelentős hányadát, és jellemzően a vezetők is közülük kerülnek ki.

A munkaerőpiac másik nagy hányadát az Y generáció (született 1980-1995) alkotja. Ezen személyek szocializációjának fontos részét képezte a technológia, hiszen a számítógépek, telefonok, szórakoztató elektronikai eszközök az ő fiatalkorukban kezdtek elterjedni szélesebb körben. Viszonyuk a közösségi médiához, a különböző webes platformokhoz, szoftverekhez sem idegen. Megtanulták használni azokat munkavégzésre, és a magánéletükben is aktív felhasználók. Az átlag Y generációs személy hajlamos az életét erősen az Internethez kötni és sok személyes információt megosztani magáról publikusan. Ez aranybánya lehet a támadók számára. Noha ennek a korosztálynak a tagjai jellemzően (főleg a multinacionális cégeknél) fogékonyabbak a biztonsági kockázatok megértésére, általánosságban nem jelenthető ki, hogy egy előkészített célzott támadást nehéz lenne ellenük véghezvinni.

A social engineerek előszeretettel személyesítenek meg gyakornokokat, friss munkavállalókat. Ennek oka, hogy könnyű a nevükben segítséget és információt kérni. Ezekben a pozíciókban jelenleg a Z generáció (született 1996-2010) tagjai ülnek. Ezek a fiatalok beleszülettek a technológiába. Nem okoz nehézséget számukra az újabb eszközök, alkalmazások megismerése és alkalmazása, hiszen gyermekkoruktól fogva veszi őket körül ez a dinamikusan fejlődő környezet. Támadói oldalról kihasználható, hogy a munka világában kevés időt töltöttek, de már teljesen más megközelítést kell ellenük alkalmazni. A régi csalások számukra nem mindig működnek. De mivel szociális kapcsolataik jelentős részét a közösségi médiában, chat alkalmazásokon keresztül ápolják, ráadásul természetszerű számukra az online párkapcsolat-keresés, az

ismeretlenek általi kommentek, megkeresések kezelése, ezért nagyon hihető támadások építhetőek fel ellenük.

A fentiek alapján azt, hogy milyen idős korában találkozott először a digitális technológiával, a következő szintek határozhatóak meg:

- Gyermekként: [0 0 0.1 0.3];
- Fiatalként: [0.1 0.3 0.4 0.6];
- Középkorúként: [0.4 0.6 0.7 0.9];
- Időskén: [0.7 0.9 1 1].

Kiberbiztonsági tudatosság

Ez az a tényező, ami a munkáltatók által a leginkább befolyásolható, és egyben a legfontosabb is a kockázatok csökkentése érdekében. Ha megfelelő minőségű és mennyiségű kiberbiztonsági tudatossági kampányban kell részt vennie a felhasználóknak, akkor sok esély van arra, hogy felismerjenek egy zsarolóvírus-támadást [167] vagy más rosszindulatú kibertevékenységet. A hatékonyság elérésére azonban nem elegendő évente egyszer egy általános ismereteket tartalmazó tantermi prezentáció, vagy egy semmitmondó, elavult e-learning oktatóanyag elérhetővé tétele. Mivel folyamatosan újabb és újabb típusú támadásokat használnak a támadók, és minden szervezetnek más a fenyegetettségi profilja, ezért a szervezetre szabott, rendszeres, releváns tartalmakkal kell képezni a felhasználókat.

Szerencsére a tudatosságnövelő megoldások piaca bővül, és a videós tartalmaktól kezdve, a játékos phishing e-mail küldő kampányok szervezésére alkalmas megoldástól a virtuálisvalóság-alapú szimulációs platformokig [168] bővült a skála. Ráadásul a tudatosság szintjének a mérése sem csak hasraütés-szerűen történik már, hanem matematikai és informatikai módszerekkel mérhető megoldások is léteznek [169] [170].

A kiberbiztonsági tudatosság skálája a felhasználót vizsgálva a következő:

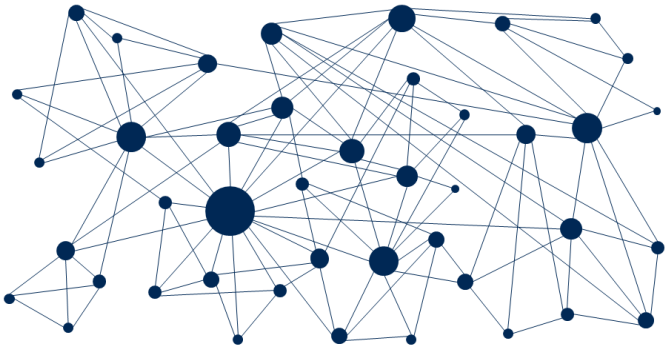
- Tudatos: [0 0 0.1 0.3];
- Jellemzően_felismerő: [0.1 0.3 0.4 0.6];
- Szituáció függő: [0.4 0.6 0.7 0.9];
- Meggondolatlan: [0.7 0.9 1 1].

A 3. fejezet összefoglalása

Ebben a fejezetben meghatároztam és strukturáltam azokat a kockázati tényezőket, amelyek a digitális információszivárgás szempontjából fontosak. Ezeket, megfeleltetve a fuzzy modell bemeneteiként, meghatároztam a tagsági függvényeket, melyeket MatLab Fuzzy Toolbox segítségével el is készítettem külön rendszerekként. Ezeket a *1. függelékben* ismertetett módon letölthető .zip fájl tartalmazza.

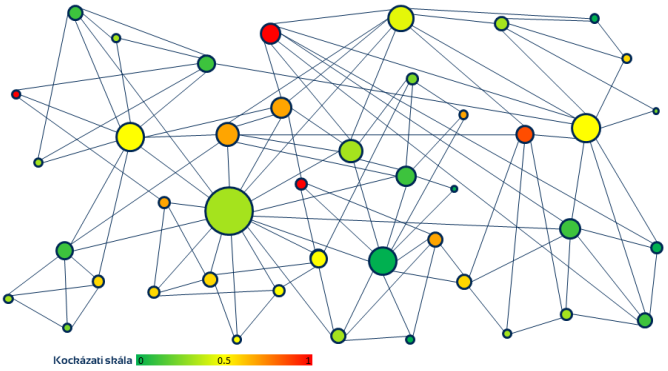
4 KIBERBIZTONSÁGI HUMÁNKOCKÁZATI MODELL

A kiberbiztonsági humánkockázati modellnek, mely a minősített digitális információk szivárgásának humán kockázatát vizsgálja, két fő összetevője van. Az alapját a szervezet informális és formális kapcsolatainak feltérképezéséből létrehozott szociális és informatikai hálózat alkotja. Itt a kapcsolatok száma jelenti a pontok fokszámát. Ezeket az ábrázolásnál a pontok nagyságának arányos növelésével javaslom jelölni. Szemléltetésre a *2.5. fejezetben* korábban ismertetett, vállalatnál készített *21. ábrát* módosítottam. A *33. ábrán* tehát az látható, hogy az adott munkavállaló (a hálózat egy pontja) mekkora kapcsolati tőkével rendelkezik. Minél nagyobb egy pont, annál nagyobb a fokszáma, azaz a formális és informális kapcsolatainak száma.



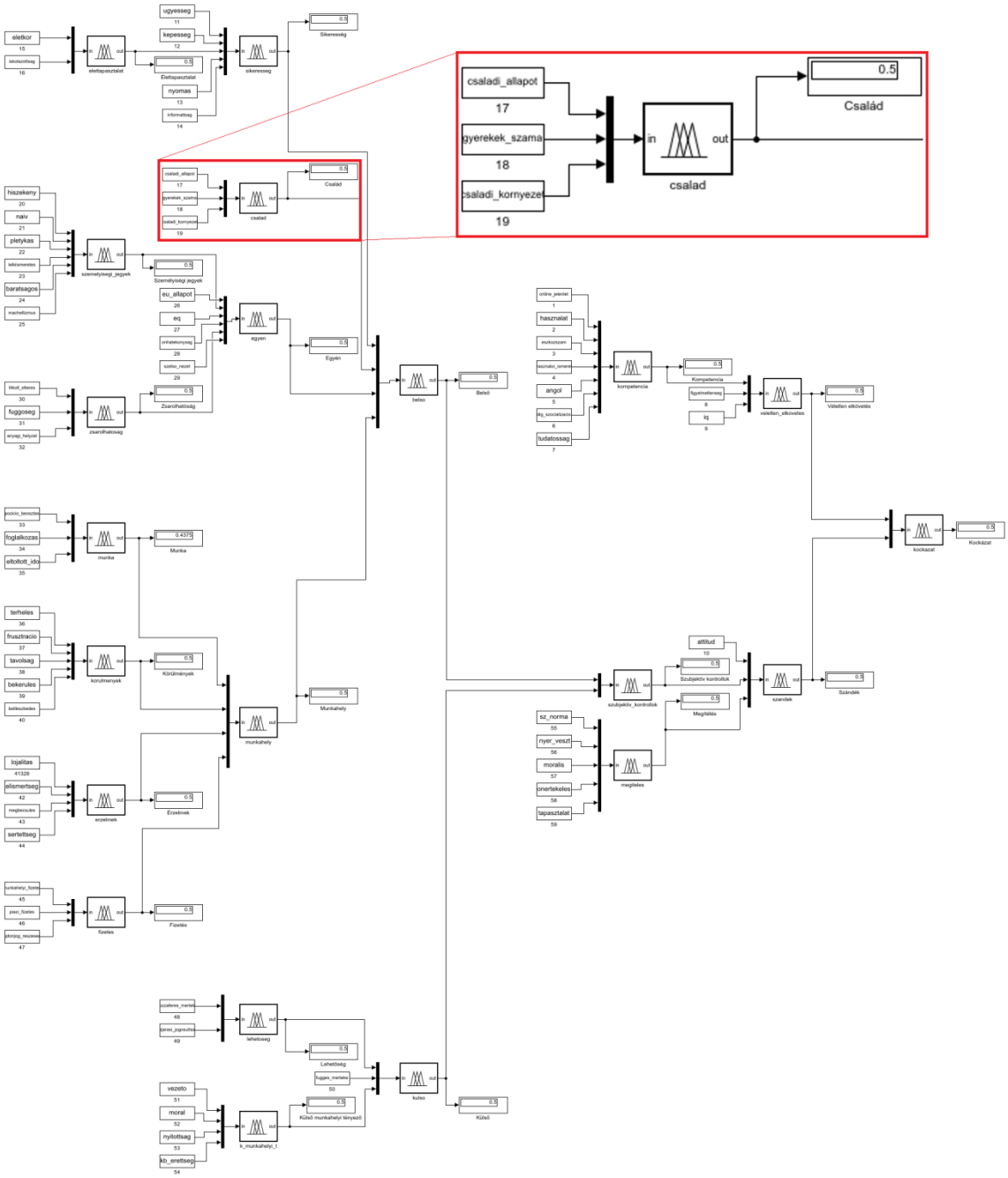
33. ábra - A fokszámmal súlyozott pontok alkotta szervezeti hálózat (saját szerkesztés)

Ezeket a pontokat azonban a kockázati fuzzy modell alapján kapott értékekkel szükséges kiegészíteni. A pontos kockázati értékek megadása mellett érdemes egy színskálával is szemléltetni a nagyobb vizualizáció kedvéért, a *34. ábrán* szemléltetett módon.



34. ábra - A fokszámmal súlyozott pontok alkotta, kockázati értékkel színnel jelölt szervezeti hálózat (saját szerkesztés)

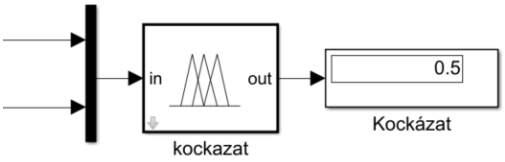
A kockázati értékek meghatározásához létrehoztam a MatLab program Fuzzy Toolboxa segítségével összesen 21 fuzzy rendszert, melyeket egymásba ágyaztam a Simulink modullal. Az egymásba kapcsolt rendszer a bemenetekkel együtt a következő ábrán (valamint nagyítható .png formátumban az 1. függelékben leírtak alapján a Google Drive-ban található mappában) látható:



35. ábra - A kiberbiztonsági kockázatok mérésére alkalmas egymásba ágyazott fuzzy modellek Simulink blokkvázlata (saját szerkesztés)

A rendszer minden bemenete 0 és 1 közötti érték, illetve a tagsági függvények trapéz alakúak, a fentiekben ismertetett paramétereket alkalmazva (*3.1-3.5 fejezetek*). A

kiértékelés minden esetben Mamdani módszerrel történt minimum operátorokkal a *HA állapot, AKKOR következtetés* szabályok (*10. függelék*) mentén úgy, hogy minden szabály súlya 1-es (100%-os) értéket vett fel. A MatLabban mindenhol középértéket (0.5-öt) adva a deffuzifikált végeredmény is 0.5-öt ad:



36. ábra - A modell kimenete 0.5-ös értékekkel (saját szerkesztés)

A modell validálását a kérdőívem utolsó kérdésének segítségével végeztem el. A 16 karakternél az ott megadott leíráshoz rendeltem kockázati értékeket. Azoknál a bemeneteknél, ahol hiányzott adat, ott az értékeket a karakterhez igazítva adtam meg, és úgy futtattam le a szimulációt. Ez kicsit torzítja ugyan az eredményt, azonban megfigyelhető, hogy egymáshoz képest hogyan változnak a különböző karakterek részeredményei és a végső kockázati érték. Ennek megfelelően hol kisebb, hol nagyobb mértékben volt eltérés a modell által adott és a várt kimenet között, de minden esetben változtak egymáshoz viszonyítva az eredmények.

A rendszer működését a következőkben fiktív karakterekkel, három esettanulmány segítségével szemléltetem. Az első egy általam véletlenszerűen kialakított referenciaszemély, akinek feltételezésem szerint közepes kockázatot kell hordoznia. A másik kettő pedig a kérdőívben a kiberbiztonsági szakemberek által a 16-ból a leginkább és a legkevésbé kockázatos karaktert mutatja be kiegészített jellemzőkkel.

Első esettanulmány

Az első esettanulmányban egy átlagos keresetű fiatal nagyvállalati munkavállaló adatait adtam meg, aki BSc diplomával rendelkezik. Alapvetően ügyes és rátermett. Rendezett családi háttere van és nincs gyermeke. Egészséges, nincsenek függőségei. Kicsit hiszékeny és naiv, ugyanakkor képes manipulatív lenni. Munkahelyi körülményei rendezettek. Az apró tett, amit el szeretne követni, ugyan nem függ nagyon másoktól és nem is érezné magát rosszul, ha elkövetné azt, de a szervezetnél jól kialakítottak a különböző hozzáférési folyamatok, és a kiberbiztonsági érettség is relatív magas. Ugyan elég precíz, de digitális kompetenciája, illetve intelligenciája is csak átlagos. A

megadott értékek a MatLabban szereplő elnevezések szerint abc sorrendben a következőek:

Angol=0.3; *anyagi helyzet*=0.6; *attitud*=0.2; *baratsagos*=0.5; *beilleszkedes*=0.5; *bejarasi jogosultsag*=0.3; *bekerules*=0.8; *csaladi allapot*=0.3; *csaladi kornyezet*=0.3; *dig szocializacio*=0.3; *eletkor*= 0.4; *elismertseg*=0.4; *eltoltott ido*=0.3; *eq*=0.4; *eszkozszam*=0.7; *eu allapot*=0.2; *felhasznaloi ismeretek*=0.5; *figyelmetlenseg*=0.2; *foglalkozas*=0.5; *frusztracio*=0.4; *fugges merteke*=0.8; *fuggoseg*=0.2; *gyerekek szama*=0.0; *hasznalat*=0.9; *hiszekeny*=0.7; *hozzaferes merteke*=0.2; *informaltsag*=0.6; *iq*=0.5; *iskolazottsag*=0.7; *kb erettseg*=0.3; *kepesseg*=0.6; *lelkiismeretes*=0.3; *lojalitas*=0.2; *machellizmus*=0.7; *megbecsules*=0.4; *moral*=0.4; *moralis*=0.8; *munkahelyi fizetes*=0.5; *naiv*=0.7; *nyer veszt*=0.5; *nyitottsag*=0.5; *nyomas*=0.9; *onertekeles*=0.7; *onhatekonysag*=0.7; *online jelenlet*=0.6; *piaci fizetes*=0.3; *pletykas*=0.2; *pozicio beosztas*=0.0; *sertettseg*=0.3; *sz norma*=0.7; *szelso nezet*=0.8; *tapasztalat*=0.3; *tavolsag*=0.2; *terheles*=0.5; *titkolt elteres*=0.7; *tudatossag*=0.3; *tulajdonjog reszesedes*=1.0; *ugyesseg*=0.8; *vezeto*=0.5.

Az értékek áttekintő táblázatot a 7. függelék első táblázata tartalmazza, ahol a sorok utolsó értékeit én adtam meg, míg az előttük lévő számok a modell által számított eredmények. A karakter bemeneteit az *1. függelékben* ismertetettek alapján az *esettanulmany_bemenetek.xlsx* első (*Első esettanulmány)* munkalapja is tartalmazza.

A várt módon a kockázat 0,5 értéket vett fel, és a szintén fontos két részeredmény is ekörül alakult (a szándék 0,4175, míg a véletlen elkövetés 0,4175). Ugyanennek a karakternek a bemeneti értékei közül a véletlen elkövetés tényezőinek negatív irányba történő módosítása esetén egyértelműen nő a kockázat, ahogy a *3. táblázat* is mutatja:

Tényező		
Név	**Eredeti érték**	**Módosított érték**
Figyelmetlenség	0,2	1
IQ	0,5	0,8
Online jelenlét	0,6	0,7
Nyelvismeret (angol)	0,3	0,5
Kiberbiztonsági tudatosság	0,3	0,8
Megváltozott eredmények		
Név	**Eredeti érték**	**Megváltozott érték**
Kompetencia	0,5	0,5272
Véletlen elkövetés	0,4175	0,6799
Kockázat	0,5	0,5358

3. táblázat - Megváltozott eredmények a módosított bemeneti értékek alapján (saját szerkesztés)

Jól látszik, hogy már ilyen kis változtatásokkal is hatást gyakorolhatunk a rendszerre. Ennek a karakternek a módosított bemeneteit az *esettanulmany_bemenetek.xlsx* második (*Első esettanulmány_mod)* munkalapja tartalmazza.

Második esettanulmány

A második esettanulmányban a kérdőív alapján legkisebb kockázatot kapó karaktert határoztam meg a kockázati értékekkel. Ebben az esetben azokat a tényezőket, amelyek nem voltak ismertek az eredeti jellemzés alapján, inkább kedvező irányba módosítottam, hogy megvizsgáljam, hogy a viszonylag kevés rossz tulajdonság okoz-e eltérést a kockázati értékben.

Ez a karakter egy külsős hosztesz munkatárs, akinek az a munkája, hogy minél több új ügyfelet szerezzen. Kicsit butácska, kevés érzékeny információnak van a tudatában, azonban az új termékekről sokat tud. Egyedülálló, bulizós típus. Erős a közösségimédia-jelenléte, de nem igazán ért azon kívül a kütyükhöz. Szülei gazdagok, akik sokat segítenek neki. Az anyacégnél van néhány kolléga, akivel sokat beszél, de rajtuk kívül nem igazán tisztelik, fogadják el a többiek. A megadott értékek, melyeket a *esettanulmany_bemenetek.xlsx* 3. munkafüle is tartalmaz, a következők:

Angol=0.2; *anyagi helyzet*=0.3; *attitud*=0.0; *baratsagos*=0.0; *beilleszkedes*=0.9; *bejarasi jogosultsag*=0.0; *bekerules*=1.0; *csaladi allapot*=0.0; *csaladi kornyezet*=0.0; *dig szocializacio*=0.2; *eletkor*= 0.8; *elismertseg*=0.9; *eltoltott ido*=0.1; *eq*=0.3; *eszkozszam*=0.3; *eu allapot*=0.0; *felhasznaloi ismeretek*=0.6; *figyelmetlenseg*=0.0; *foglalkozas*=0.0; *frusztracio*=0.7; *fugges merteke*=0.1; *fuggoseg*=0.1; *gyerekek szama*=0.0; *hasznalat*=0.0; *hiszekeny*=0.6; *hozzaferes merteke*=0.0; *informaltsag*=0.2; *iq*=0.7; *iskolazottsag*=0.4; *kb erettseg*=0.1; *kepesseg*=0.2; *lelkiismeretes*=0.0; *lojalitas*=0.8; *machellizmus*=0.4; *megbecsules*=0.9; *moral*=0.2; *moralis*=0.2; *munkahelyi fizetes*=0.5; *naiv*=0.7; *nyer veszt*=0.2; *nyitottsag*=0.3; *nyomas*=0.0; *onertekeles*=0.0; *onhatekonysag*=0.7; *online jelenlet*=0.0; *piaci fizetes*=0.2; *pletykas*=0.6; *pozicio beosztas*=0.0; *sertettseg*=0.2; *sz norma*=0.1; *szelso nezet*=0.0; *tapasztalat*=0.0; *tavolsag*=0.0; *terheles*=0.3; *titkolt elteres*=0.0; *tudatossag*=0.2; *tulajdonjog reszesedes*=1.0; *ugyesseg*=0.1; *vezeto*=0.7.

A várt módon a kockázati érték az előző 0,5 értéktől ugyan nem sokkal, de alacsonyabb lett (0,4927), mint ahogy az alatta lévő szinten lévő részeredmény is (szándék 0,3792, véletlen elkövetés 0,4198). Az alsóbb szinten lévő fuzzy rendszerek részeredményeiben

több esetben jelentős eltérés van az első esettanulmányhoz képest, mint ahogy az előzőhöz hasonlóan a *7. függelék* második táblázata tartalmazza.

Harmadik esettanulmány

A harmadik esetben arra voltam kíváncsi, hogy egy kifejezetten rossz kockázati értékekkel rendelkező karakter végső eredménye nagyobb mértékben tér-e el a középértéktől, mint a második esettanulmányban lévő. Igyekeztem itt is a realitás talaján maradni a bemenetek megadásakor, de néhol szándékosan rossz körülményeket adtam meg.

Az itt vizsgált vezetői asszisztens a kérdőív alapján a munkájából fakadóan vezetői és más fontos megbeszéléseken ül bent a főnökével, ahol mindig jegyzetel. Sok rendszerhez van hozzáférése, hiszen sok esetben a felettesének a nevében is dolgozik. Kedves, kommunikatív, ezért sok információ eljut hozzá. Alapvetően jól meg van fizetve, de két éve várja a fizetésemelést vagy előléptetést, amit sajnos idén sem kapott meg. Családos, középkorú nő. Több nagyvállalatnál dolgozott már, ismeri a folyamatokat, nagyon precíz az élet minden területén.

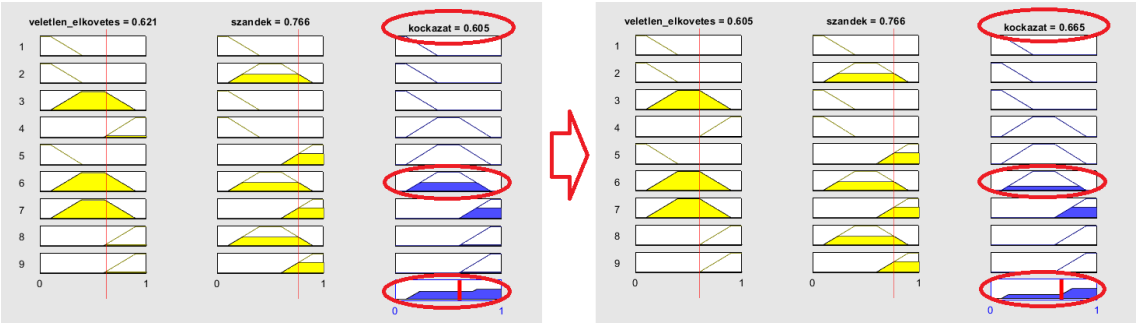
A negatív körülmények vizsgálata érdekében olyan további bemeneteket adtam, amelyek gyengébb céges biztonsági kontrollokat, negatív munkaköri hangulatot és rossz magánéleti körülményeket reprezentál. Ezek alapján a következő kockázati tényezőket határoztam meg, melyeket az *esettanulmany_bemenetek.xlsx* 4. munkafüle is tartalmaz:

Angol=1.0; *anyagi helyzet*=0.8; *attitud*=1.0; *baratsagos*=0.8; *beilleszkedes*=1.0; *bejarasi jogosultsag*=1.0; *bekerules*=1.0; *csaladi allapot*=1.0; *csaladi kornyezet*=1.0; *dig szocializacio*=0.7; *eletkor*= 0.4; *elismertseg*=1.0; *eltoltott ido*=1.0; *eq*=1.0; *eszkozszam*=1.0; *eu allapot*=0.9; *felhasznaloi ismeretek*=0.7; *figyelmetlenseg*=1.0; *foglalkozas*=1.0; *frusztracio*=1.0; *fugges merteke*=1.0; *fuggoseg*=0.8; *gyerekek szama*=1.0; *hasznalat*=1.0; *hiszekeny*=0.6; *hozzaferes merteke*=1.0; *informaltsag*=1.0; *iq*=0.7; *iskolazottsag*=0.7; *kb erettseg*=1.0; *kepesseg*=0.8; *lelkiismeretes*=0.7; *lojalitas*=1.0; *machellizmus*=1.0; *megbecsules*=0.8; *moral*=1.0; *moralis*=0.9; *munkahelyi fizetes*=0.3; *naiv*=1.0; *nyer veszt*=1.0; *nyitottsag*=1.0; *nyomas*=1.0; *onertekeles*=1.0; *onhatekonysag*=1.0; *online jelenlet*=1.0; *piaci fizetes*=0.3; *pletykas*=1.0; *pozicio beosztas*=0.3; *sertettseg*=1.0; *sz norma*=0.1; *szelso nezet*=1.0; *tapasztalat*=1.0; *tavolsag*=0.6; *terheles*=1.0; *titkolt elteres*=1.0; *tudatossag*=1.0; *tulajdonjog reszesedes*=1.0; *ugyesseg*=0.8; *vezeto*=1.0.

A harmadik karakter kockázati értéke 0,6048, a szándék mértéke 0,7659, míg a véletlen elkövetés 0,6212.

A *7. függelékben* található táblázat megmutatja, hogy az egybe ágyazott fuzzy rendszerek kimenetei milyen eredményt vesznek fel akkor, ha minden bemenet 0, 0,5 vagy 1, illetve milyet a három esettanulmány és az első módosított esetében. Az oszlopokat a végső kockázat szerinti emelkedő sorrendben rendeztem.

Ennél az esetnél megvizsgáltam, hogy egy szabály súlyának csökkentése mennyire változtatja meg a végeredményt. A *kockazat* rendszerben az *If (veletlen_elkovetes is magas) and (szandek is atlagos) then (kockazat is kockazatos)* szabály figyelembevételi súlyát a felére csökkentettem. Ez a *37. ábrán* látható módon azt eredményezte, hogy ugyan minden bemeneti érték változatlan maradt, de a kockázat végül 0,6045-ről 0,6647-re nőtt. Az így módosított fuzzy rendszer a 1. függelékben leírtak alapján letölthető anyagok közül *kockazat2.fis* néven található meg.



37. ábra - Kockázat változása a szabály súlyának módosításával (saját szerkesztés)

Továbbfejlesztési lehetőségek

Ismerve a fuzzy logikát és hálózatelemzést egyesítő modell által adott kockázati értéket és részeredményeket, egy szervezet meg tudja határozni a számára információszivárgás szempontjából kritikus személyeket. Az eredmények ismeretében a döntéshozó eldöntheti, hogy milyen megoldással kezeli az adott személy nyújtotta kockázatot. Az általam létrehozott általános moduláris modellt egy szervezet igényei, szabályzatai, rendelkezésére álló információk alapján a saját képére formálhatja a bemenetek és a szabályok módosításával, törlésével, vagy esetleg újak hozzáadásával. Ily módon más kiberbiztonsági fenyegetettségek vizsgálatára is alkalmas a modell.

Fontos hangsúlyozni, hogy a Simulink nem kezeli a hiányzó bemeneteket. Ilyen esetekben hibára fut a számítás. Ennek értelmében, ha az általam összeállított komplex

rendszerben található bemenetek munkajogi vagy gyakorlati szempontból nem megadhatóak, mindenképpen szükséges a módosított fuzzy modell megalkotása.

A MatLab Fuzzy Toolbox és a Simulink rendelkezik olyan funkcionális korlátokkal, melyek hiányában pontatlanabb számítás végezhető el, mint véleményem szerint szükséges lenne. Az így elkészített modell például nem képes kezelni, ha egy bemenet hiányzik. Ezt egy célszoftver lefejlesztésével orvosolni lehetne.

Másik hiányosság, hogy ugyan egy rendszeren belül a szabályok súlyozása állítható, azonban ez nehezen átlátható módon tehető meg. Egy egyszerűbb állíthatóságnak azért lenne jelentősége, mert egy szervezet átláthatóbb módon állíthatná be, hogy melyik bemenet vagy alrendszerből származó érték számára a hangsúlyosabb. Ez látszik a harmadik esettanulmány végén látható példán keresztül. Az általam készített modellben a szabályok egyenkénti súlyozását nem végeztem el, mivel az túlmutat az értekezésen a szervezeti specifikációk miatt.

A súlyozás megvalósítására megoldást nyújthat egy hierarchikus, többszintű kockázatkezelési modell (AHP[73]) fuzzy környezetben történő alkalmazása. Ezzel a megoldással a döntés minőségi és mennyiségi szempontjait tovább lehet bővíteni a célkitűzéseknek, kritériumoknak megfelelően [171].

A célszoftvert érdemes lehet olyan tudással felruházni, mely a megfelelő szervezeti háló ismeretében elkészíti a fejezet elején ismertetett hálózati ábrát is. Ebben az esetben érdemesnek tartom olyan irányba is elvinni a fejlesztést, mely képes kezelni a szervezetnél már nem dolgozó kollégák kockázatát is.

A modellnek számos más felhasználási lehetősége lehet. Érdemesnek tartok további kutatásokat folytatni nem csak nagyobb létszámú szervezetek esetén, de akár a kis- és középvállalatok fenyegetettségeinek kezelésére is. Ebben az esetben a hálózati dimenzió feltételezhetően elveszítené funkcionalitását, azonban rá tudna világítani olyan hiányosságokra, melyek ismeretén akár az adott vállalat üzleti sikeressége is múlhat.

Rejtett információk és összefüggések megismerését segítheti a modell átalakítása a 2.1 fejezetben forrásként megjelölt nemzetbiztonsági átvilágítási kérdőív specifikus feldolgozásában. Ezen túl segítséget nyújthat az ellenőrzés nem publikus folyamatában, mint ahogy a titkosszolgálatok látókörébe került célszemélyek profilozásában is.

[73] Analytical Hierarchy Process, azaz analítikus hierarchikus eljárás.

A 4. fejezet összefoglalása

Ebben a fejezetben bemutattam a hálózatelméleten és a fuzzy logikán alapuló modellemet, valamint 3 esettanulmányon keresztül alátámasztottam annak működését. Bemutattam a rendszer korlátait és továbbfejlesztési lehetőségeit.

5 ÖSSZEGZETT KÖVETKEZTETÉSEK

Új tudományos eredmények

Az értekezésem új tudományos eredményeit az alábbi tézisek tartalmazzák:

1. Meghatároztam azokat a kockázati tényezőket, amelyek nagy valószínűséggel befolyásolják azt, hogy digitális minősített információt szivárogtasson ki egy személy.

A 2.1. fejezetben ismertetett különböző kiberbiztonsági, szociológiai, pszichológiai irodalmak és a lefolytatott mélyinterjúk, valamint a 2.2. fejezetben elemzett kérdőív alapján megállapítottam, hogy jól körülírható azoknak a különböző kockázati tényezőknek a köre, amelyek befolyásolják azt, hogy egy személy gondatlanságból vagy szándékosan szenzitív információt szivárogtat ki egy szervezetből. Ezeket a 3. fejezetben rendszereztem, illetve indokoltam fontosságukat. Mivel ezek nem egyszerű crisp (szám) értékek, hanem a köznyelvben használatos szavakkal jellemezhető értékek, ezért mindegyik tényezőhöz fuzzy tagsági függvényeket rendeltem.

Kapcsolódó publikációim: [23] [27] [172] [173] [174] [175].

2. Megalkottam egy olyan fuzzy modellt, amelyet alkalmazva a megfelelő információk (bemenetek) ismeretében megsejthető, hogy mely személyek jelentenek kockázatot a szervezeten belül az információszivárogtatást, mint fenyegetettséget figyelembe véve egy célzott támadás esetén.

A MatLabban létrehoztam egy olyan specifikus különböző fuzzy rendszereket egymásba ágyazott rendszert, amely bemeneti értékeit a 3. fejezetben leírtak szerint alkalmazva valóságot megközelítő eredményt ad. A 4 fejezetben ismertetett modell kimenete a kérdőíves kutatásom során megadott válaszokkal összhangban vannak, melyet három esettanulmánnyal alátámasztottam. A modell kezeli az esetleges bizonytalanságokat. A bemenetek és a szabályok módosításával bármely szervezet alkalmazni tudja a saját kockázatvállalása és szabályzata alapján.

Kapcsolódó publikációim: [106] [117] [118] [172].

3. Megállapítom, hogy a hálózatelemzési módszerek és a fuzzy logika külön-külön is alkalmas a kockázatok mérésére, de együtt pontosabb eredményt adnak.

Együttes alkalmazásukra létrehoztam egy modellt a kiberbiztonsági szempontból kockázatos személyek beazonosítását figyelembe véve.

A szakirodalom feldolgozása alapján megvizsgáltam a hálózatelemzési módszerek és a fuzzy logika szabályszerűségeit és azok együttes használatának lehetséges módját. A fuzzy logika alkalmazhatóságát a 2.4. fejezetben ismertettem, míg a hálózatelméletét a 2.5. fejezetben. Együttes alkalmazásukat a 4. fejezetben fejtettem ki.

Kapcsolódó publikációim: [23] [25] [106] [117] [118] [142] [172].

Ajánlások

Kutatásaim elsősorban olyan szervezetek, kritikus infrastruktúrák kiberbiztonsági, azon belüli is a digitális információszivárgás fenyegetettségének humán kockázatainak kezelésére alkalmazhatók, ahol megfelelő mennyiségű és minőségű információ áll a munkáltató részére, és kellően nagy a munkavállalók köre.

A rendszert általánosan azonban minden magán- és állami intézmény profiltól függetlenül használhatja a kockázatai kezelésének csökkentése, hiszen a fuzzy logika képes kezelni a rendelkezésre nem álló információkat. Amennyiben az adott szervezet létszáma nem éri el a kritikus tömeget, ahol van értelme a hálózati összefüggések elemzésének, ott csak a fuzzy értékek meghatározása is segíthet a döntéshozóknak.

IRODALOMJEGYZÉK

[1] K. Fehér, *Digitalizáció és új média*. Budapest: Akadémiai Kiadó, 2016.

[2] „CYBERCRIME: COVID-19 IMPACT”. INTERPOL General Secretariat, 0 2020.

[3] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról - Hatályos Jogszabályok Gyűjteménye*. Elérés: aug. 16, 2020. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

[4] *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról*. 2013. Elérés: aug. 16, 2020. [Online]. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845

[5] *A hálózati és információs rendszerek biztonságára vonatkozó Stratégia*. 2018. [Online]. Elérhető: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf?fbclid=IwAR1kVfAyc8Ro6kYyKaQbBS6wY_mgE-Iq6bqhtAKk8zjsZZjPwlZoP8PbxA8#!DocumentBrowse

[6] ISACA, „The Business Model for Information Security”. ISACA, 2010.

[7] Y. K. Dwivedi *és mtsai.*, „Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life”, *International Journal of Information Management*, o. 102211, júl. 2020, doi: 10.1016/j.ijinfomgt.2020.102211.

[8] „A National Cybersecurity Agenda for Resilient Digital Infrastructure”. Aspen Cybersecurity Group, 2020. Elérés: jan. 05, 2021. [Online]. Elérhető: https://www.aspeninstitute.org/wp-content/uploads/2020/12/FINAL-Aspen-Natl-Cybersecurity-Agenda-Dec-2020.pdf

[9] P. Fehér-Polgár és P. Michelberger, „The Information Security Risks of the BYOD, From Theoretical Point of View”, in *2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2019, o. 83–88. doi: 10.1109/SISY47553.2019.9111514.

[10] A. Keszthelyi, „Paradigmaváltás - biztonság - emberi tényező”, *TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI*, köt. 7, o. 406–412, 2015.

[11] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, 1. Cambridge: Techlology Press, 1948.

[12] C. E. Shannon, „A mathematical theory of communication”, *The Bell System Technical Journal*, köt. 27, sz. 3, o. 379–423, júl. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[13] G. Fülöp, *Az információ*, 2. bővített és Átdolgozott kiadás. Budapest: Eötvös Loránd TudományegyetemKönyvtártudományi - Informatikai Tanszék, 1996. Elérés: jan. 20, 2021. [Online]. Elérhető: https://mek.oszk.hu/03100/03118/03118.pdf

[14] J. De Vriendt, P. Laine, C. Lerouge, és Xiaofeng Xu, „Mobile network evolution: a revolution on the move”, *IEEE Commun. Mag.*, köt. 40, sz. 4, o. 104–111, ápr. 2002, doi: 10.1109/35.995858.

[15] A. Tóth, „A felhőinformatika alapjai”, *HÍRVILLÁM = SIGNAL BADGE*, köt. 2, o. 85–90, 2011.

[16] Gottdank T., *Szolgáltatásalapú világ*. Bicske: SZAK Kiadó, 2013.

[17] Mayer-Schönberger V. és Kenneth Cukier, *Big Data*. Budapest: HVG Kiadó Zrt., 2014.

[18] M. Klausz, *Megosztok, tehát vagyok*. Budapest: Antheneum Kiadó, 2017.

[19] D. Z. H. Marquardt Madeline, „Cognitive Ability and Vulnerability to Fake News”, *Scientific American*. https://www.scientificamerican.com/article/cognitive-ability-and-vulnerability-to-fake-news/ (elérés szept. 28, 2020).
[20] K. Fehér és O. Király, „Álhíresülés – a hamis hírek dinamikája a médiában”, *Századvég*, sz. 2017/2., o. 39–50, 2017.
[21] P. Bányász, L. Dobos, G. Palla, és P. Pollner, „Lélektani műveletek a közösségi médiában”, in *Hálózatok a közszolgálatban*, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 111–133. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
[22] „Russia-backed Facebook posts »reached 126m Americans« during US election”, *the Guardian*, okt. 31, 2017. http://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million (elérés jan. 08, 2021).
[23] D. Váczi, Z. Bederna, V. Szalánczi-Orbán, és T. Szádeczky, „Az incidenskezelés szervezeti háttere”, in *Hálózatok a közszolgálatban*, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 205–222. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
[24] A. Tóth és P. Török, „IoT attacks and recommendation for protection solutions”, *AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT*, köt. 2019, o. 15–26, 2019.
[25] Z. Bederna, D. Váczi, T. Szádeczky, és P. Pollner, „Támadás hálózatba szervezve”, in *Hálózatok a közszolgálatban*, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 223–247. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
[26] Z. Bederna és T. Szádeczky, „Effects of botnets – a human-organisational approach”, *Security and Defence Quarterly*, júl. 2021, doi: 10.35467/sdq/138588.
[27] D. Váczi, „Célzott támadások módszertana”, in *Célzott kibertámadások*, 2018, o. 52–75.
[28] E. H. Spafford, „The internet worm program: an analysis”, *SIGCOMM Comput. Commun. Rev.*, köt. 19, sz. 1, o. 17–57, jan. 1989, doi: 10.1145/66093.66095.
[29] P. Szőr, *A vírusvédelem művészete*. Bicske: SZAK Kiadó, 2010.
[30] Z. Haig és I. Várhegyi, „A cybertér és a cyberhadviselés értelmezése”, *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, sz. Eleektronikus szám, 2008, Elérés: jan. 10, 2021. [Online]. Elérhető: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf
[31] Európai Tanács, „Convension on Cybercime”, *Treaty Office*. https://www.coe.int/en/web/conventions/full-list (elérés jan. 10, 2021).
[32] P. Tálas, „A varsói NATO-csúcs legfontosabb döntéseiről”, *NEMZET ÉS BIZTONSÁG: BIZTONSÁGPOLITIKAI SZEMLE*, sz. 2, o. 97–101, 2016.
[33] C. Fekete és Z. Sipos, „A kibertér megjelenése az orosz katonai műveletekben a 2008-as orosz–grúz háború tükrében”, *HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA*, sz. 145, o. 59–71, 2017.
[34] L. Kovács és M. Sipos, „A Stuxnet és ami mögötte van”, *HADMÉRNÖK*, köt. 5, o. 163–172, 2010.
[35] L. Kovács és M. Sipos, „A Stuxnet és ami mögötte van II.”, *HADMÉRNÖK*, köt. VI, o. 222–231, 2011.
[36] „ENISA Threat Landscape - The year in review”. https://www.enisa.europa.eu/publications/year-in-review (elérés dec. 28, 2020).
[37] K. Fehér, *Kezdő hackerek kézikönyve*. Budapest: BBS-INFO Kiadó, 2016.

[38] K. Finklea, „Dark Web”, Congressional Research Service, 10 2017. [Online]. Elérhető: https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf
[39] P. Warren és M. Streeter, *Az internet sötét oldala*. Budapest: HVG Kiadó Zrt., 2005.
[40] C. Krasznay, „A polgárok védelme egy kiberkonfliktusban”, *HADMÉRNÖK*, köt. 7, o. 142–151, 2012.
[41] C. Vida, „A hírszerzés szerepe, jelentősége, az információgyűjtés fajtái és formái”, in *Nemzetbiztonsági alapismeretek*, Budapest: Nemzeti Közszolgálati Egyetem, 2013, o. 102–105.
[42] H. Modderkolk, „Dutch agencies provide crucial intel about Russia’s interference in US-elections”, *de Volkskrant*, jan. 25, 2018. https://www.volkskrant.nl/gs-b4f8111b (elérés jan. 11, 2021).
[43] T. Szádeczky, „Terrorism in cyberspace”, 2008.
[44] P. Bányász, „Kiberbűnözés és közösségi média”, *NEMZETBIZT SZLE*, köt. 4, sz. 4, o. 55–74, 2017.
[45] M. Zerzri, „The Threat of Cyber Terrorism and Recommen-da-tions for Countermeasures”, *Cyber Terrorism*, sz. 04–2017, o. 6, 2017.
[46] Z. Haig, *Információs műveletek a kibertérben*. Dialóg Campus Kiadó, 2018.
[47] G. Berki, „Kiberháborúk, kiberkonfliktusok”, in *Műhelymunkák*, 2016, o. 245–284.
[48] H. Dalziel, „Cyber Kill Chain (Chapter 2)”, in *Securing Social Media in the Enterprise*, H. Dalziel, Szerk. Boston: Syngress, 2015, o. 7–15. doi: 10.1016/B978-0-12-804180-2.00002-6.
[49] C. Krasznay, „Kiberbiztonsági kihívások az ICS/SCADA világban”, *VÍZMŰ PANORÁMA: VÍZ- ÉS CSATORNAMŰVEK ORSZÁGOS SZAKMAI SZÖVETSÉGE LAPJA*, köt. XXVIII/2020., o. 2–5, 2020.
[50] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, és W. Zhang, „Kill Chain for Industrial Control System”, *MATEC Web of Conferences*, köt. 173, o. 01013, 0 2018, doi: 10.1051/matecconf/201817301013.
[51] R. Messier, *CEH v10 Certified Ethical Hacker Study Guide*. New York: John Wiley & Sons Inc, 2019.
[52] D. P. Twitchell, „Social engineering in information assurance curricula”, in *Proceedings of the 3rd annual conference on Information security curriculum development*, New York, NY, USA, szept. 2006, o. 191–193. doi: 10.1145/1231047.1231062.
[53] H. Cristopher, *Social Engineering - The scinece of Human Hacking*. Indianapolis: John Wiley & Sons, Inc., 2018.
[54] K. D. Mitnick, *A legendás hacker - A rábeszélés művészete*. Budapest: Perfact-Pro Kft., 2003.
[55] F. Schulz Von Thun, *A kommunikáció zavarai és feloldásuk*. Budapest: Háttér Kiadó, 2012.
[56] C. S. Carver és M. F. Scheir, *Személyiségpszichológia*. Budapest: Osiris Kiadó Kft., 2011.
[57] G. Csepeli, *Szociálpszichológia*. Budapest: Osiris Kiadó Kft., 2006.
[58] S. Klein, *Munkapszichológia - a 21. században*. Budapest: Edge 2000 Kft., 2018.
[59] „Pretexting: Your Personal Information Revealed”. Federal Trade Commission, Bureau of Consumer Protection, Office of Consumer and Business Education, 2001. [Online]. Elérhető: https://books.google.hu/books?id=fhETbHbsmKUC
[60] A. Demarais és V. White, *Első benyomás*. Budapest: HVG Kiadó Zrt., 2008.

[61] M. J. Horowitz, „Modes of Representation of Thought”, *J Am Psychoanal Assoc*, köt. 20, sz. 4, o. 793–819, okt. 1972, doi: 10.1177/000306517202000405.
[62] P. Ekman és W. V. Friesen, *Unmasking the Face: A Guide to Recognizing Emotions from Facial Clues*. ISHK, 2003.
[63] W. Glasser, *Choice Theory: A New Psychology Of Personal Freedom*. New York: HarperCollins Publishers, 1999.
[64] R. B. Cialdini, *Influence: The Psychology of Persuasion, Revised Edition*, Revised edition. New York: Harper Business, 2006.
[65] B. Annis és J. Gray, *Nemek intelligenciája*. Budapest: Trivium Kiadó, 2013.
[66] A. Keszthelyi, „Jelszavakról – iparági legrosszabb gyakorlatok”, *TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI*, köt. 7, o. 261–268, 2015.
[67] A. Keszthelyi, „About passwords”, *ACTA POLYTECHNICA HUNGARICA*, köt. 10, o. 99–118, 2013, doi: 10.12700/APH.10.06.2013.6.6.
[68] K. Fehér, *Hackertechnikák*. Budapest: BBS-INFO Kiadó, 2018.
[69] P. J. Varga, „Az okos otthonok vezeték nélküli alkotóelemeinek biztonsága”, *KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI*, köt. 9, o. 83–87, 2017.
[70] Z. Rajnai, „A kritikus információs infrastrukturák összetétele, biztonsági kérdései”, in *Nemzetközi Gépész és Biztonságtechnikai Szimpózium*, 2012, o. 15–22.
[71] „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)”, o. 88.
[72] Horváth A., „A kritikus infrastruktúra védelem komplex értelmezésének szükségessége”, in *Fejezetek a kritikus infrastruktúra védelemből*, Budapest: Magyar Hadtudományi Társaság, 2013, o. 18–37. [Online]. Elérhető: http://mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf
[73] *UNITING AND STRENGTHENING AMERICA BYPROVIDING APPROPRIATE TOOLS REQUIREDTO INTERCEPT AND OBSTRUCT TERRORISM(USA PATRIOT ACT) ACT OF 2001*. Elérés: jan. 11, 2021. [Online]. Elérhető: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[74] *Critical Infrastructure Protection (PDD 63)*. Elérés: jan. 11, 2021. [Online]. Elérhető: https://fas.org/irp/offdocs/pdd/pdd-63.htm
[75] T. Szádeczky, „Information Security Law and Strategy in Hungary”, *Academic and Applied Research in Military and Public Management Science (AARMS) HU ISSN 2498-5392*, köt. 14, o. 281–289, 0 2015.
[76] *A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (EGT-vonatkozású szöveg)*, köt. OJ L. 2008. Elérés: jan. 11, 2021. [Online]. Elérhető: http://data.europa.eu/eli/dir/2008/114/oj/hun
[77] Z. Haig, B. Hajnal, L. Kovács, L. Muha, és Z. N. Sik, *A kritikus információs infrastruktúrák meghatározásának módszertana*. ENO Advisory Kft., 2009.
[78] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról,kijelöléséről és védelméről*. Elérés: jan. 11, 2021. [Online]. Elérhető: https://net.jogtar.hu/getpdf?docid=a1200166.tv&targetdate=20180101&printTitle=2012.+%C3%A9vi+CLXVI.+t%C3%B6rv%C3%A9ny

[79] W. K. H. Kft, *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról - Hatályos Jogszabályok Gyűjteménye*. Elérés: jan. 24, 2021. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300065.kor

[80] M. Lajos, *A kritikus információs infrastruktúrák védelme*. Budapest: RelNet Technológia Kft., 2015. [Online]. Elérhető: http://real.mtak.hu/78935/1/A_kritikus_informacios_infrastrukturak_vedelme_u.pdf

[81] International Telecommunication Union, „Measuring digital developmentFacts and figures 2020". 2020. Elérés: jan. 17, 2021. [Online]. Elérhető: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

[82] K. M. Stine, K. Quill, és G. A. Witte, „Framework for Improving Critical Infrastructure Cybersecurity". febr. 19, 2014. Elérés: jan. 24, 2021. [Online]. Elérhető: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity

[83] C. Krasznay, „Kiberbizonytalanság – A NATO szerepe a kibervédelemben", *FÓKUSZBAN*, köt. 2019, o. 54–59, 2019.

[84] S. Tamás, „Governmental Regulation of Cybersecurity in the EU and Hungary after 2000", *AARMS – Academic and Applied Research in Military and Public Management Science*, köt. 19, sz. 1, Art. sz. 1, okt. 2020, doi: 10.32565/aarms.2020.1.7.

[85] „1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról". http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (elérés jan. 18, 2021).

[86] W. K. H. Kft, *271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól - Hatályos Jogszabályok Gyűjteménye*. Elérés: jan. 18, 2021. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1800271.KOR

[87] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, köt. OJ L. 2016. Elérés: jan. 18, 2021. [Online]. Elérhető: http://data.europa.eu/eli/dir/2016/1148/oj/eng

[88] Anita T., „A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései", in *Kritikus Információs Infrastruktúrák Védelme*, Deák V., Szerk. Budapest: Nemzeti Közszolgálati EgyetemKözigazgatási Továbbképzési Intézet, 2019, o. 8–34. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13803/Kritikus%20informacios%20infrastrukturak%20vedelme_Eves%20tovabbkepzes_felelos%20szemely.pdf;jsessionid=8F44F5B1C47A4BD15D3EAB06068234DC?sequence=3&fbclid=IwAR0QR_CVd0l9pB3rRLcwVnhIkiZajGJH3vyciCBvtEWi9sZSHlnhCJPB7lM

[89] ENISA, „Részletes leírás a CSIRT-csoportok létrehozásáról". 2006. [Online]. Elérhető: file:///C:/Users/User/AppData/Local/Temp/CSIRT_setting_up_guide_ENISA-HU.pdf

[90] L. Kovács, *A kibertér védelme*. Dialóg Campus Kiadó; Nordex Kft., 2018.

[91] Z. Haig, *Információ - Társadalom - Biztonság*. Budapest: NKE Szolgál-tató Kft., 2015.

[92] C. Krasznay, „A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban", *NEMZET ÉS BIZTONSÁG: BIZTONSÁGPOLITIKAI SZEMLE*, köt. 10, o. 38–53, 2017.

[93] J. Dykstra és C. L. Paul, „Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations”, előadás 11th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 18), 2018. Elérés: jan. 24, 2021. [Online]. Elérhető: https://www.usenix.org/conference/cset18/presentation/dykstra

[94] W. K. H. Kft, „2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról - Hatályos Jogszabályok Gyűjteménye”. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (elérés jan. 24, 2021).

[95] K. D. Mitnick és W. L. Simon, *A legendás hacker - A megtévesztés művészete*. Budapest: Perfact-Pro Kft., 2003.

[96] J. Beinschróth, „Informatikai biztonsági szabványok”, 2007.

[97] T. Dezső és I. Kertész, „Információszerzés az ókorban”, in *A hírszerzés története az ókortól napjainkig*, J. Boda és K. Regényi, Szerk. Budapest: Dialóg Campus Kiadó, 2019. Elérés: jan. 20, 2021. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12692/web_PDF_Hirszerzes_tortenete_okortol_napjainkig.pdf?sequence=1

[98] J. Boda és K. Regényi, „Középkor – A klasszikus hírszerzés hajnala”, in *A hírszerzés története az ókortól napjainkig*, J. Boda és K. Regényi, Szerk. Budapest: Dialóg Campus Kiadó, 2019. Elérés: jan. 20, 2021. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12692/web_PDF_Hirszerzes_tortenete_okortol_napjainkig.pdf?sequence=1

[99] C. Vida, P. Balogh, és J. Kis-Benedek, „A hírszerzés önálló ágai”, in *Nemzetbiztonsagi alapismeretek*, I. Kobolka, Szerk. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó, 2013. Elérés: jan. 20, 2021. [Online]. Elérhető: https://cmsadmin-pub.uni-nke.hu/document/nbi-uni-nke-hu/nemzetbiztonsagi-alapismeretek.original.pdf

[100] J. Beinschróth, *Kriptográfiai alkalmazások, rejtjelezések, digitális aláírás, digitális pénz*. 2016.

[101] P. Hudoba, „Public key cryptography based on the clique and learning parity with noise problems for post-quantum cryptography”, *Proceedings of the 11th Joint Conference on Mathematics and Computer Science*, o. 102–112, 2018.

[102] *2009. évi CLV. törvény a minősített adat védelméről - Hatályos Jogszabályok Gyűjteménye*. Elérés: jan. 24, 2021. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a0900155.tv

[103] *2011/292/EU A TANÁCS HATÁROZATA (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról*. Elérés: febr. 12, 2021. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32011D0292&from=EN

[104] Z. Kuris és Z. Faggyas, „Minősített adatokat kezelő informatikai rendszerek kockázatértékelése és kockázatmenedzsmentje”, *HADMÉRNÖK*, sz. VI./3., o. 117–130, 2011.

[105] P. Papadimitriou és H. Garcia-Molina, „A Model for Data Leakage Detection”, előadás 25th International Conference on Data Engineering, Shanghai, China, 2009. Elérés: febr. 11, 2021. [Online]. Elérhető: http://ilpubs.stanford.edu:8090/886/

[106] D. Vaczi, E. Toth-Laufer, és T. Szadeczky, „Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage”, in *2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2020, o. 000113–000118. doi: 10.1109/SISY50555.2020.9217053.

[107] B. Schneier, *Schneier a biztonságról*. Budapest: HVG Kiadó Zrt., 2010.
[108] I. Ajzen, „The theory of planned behavior”, *Organizational Behavior and Human Decision Processes*, köt. 50, sz. 2, o. 179–211, 0 1991, doi: 10.1016/0749-5978(91)90020-T.
[109] Hunyadi G. és Münnich Á., „A szilárd erkölcsiség elvárása a rendvédelemben: egy lehetséges pszichológiai modell”, *Belügyi Szemle*, köt. 64, sz. 6, Art. sz. 6, jún. 2016, doi: 10.38146/BSZ.2016.6.2.
[110] M. Walter, *Personality and Assessment*. Wiley, 1968.
[111] A. W. Wicker, „Attitudes versus Actions: The Relationship of Verbal and Overt Behavioral Responses to Attitude Objects”, *Journal of Social Issues*, köt. 25, sz. 4, o. 41–78, 1969, doi: https://doi.org/10.1111/j.1540-4560.1969.tb00619.x.
[112] Hunyadi G., Malét-Szabó E., és Münnich Á., „A rendvédelmi szervek szervezeti normáinak és kultúrájának, mint a szilárd erkölcsiség egyik alapvető háttértényezőjének empirikus próbavizsgálata”, 2016, [Online]. Elérhető: http://www.bm-tt.hu/assets/letolt/kutat/2016/SZEM.kulktura.tanulmany.pdf
[113] P. Csató, G. Hunyadi, E. Malét-Szabó, és Á. Münnich, *Az erkölcsi értékrend és a személyiség közötti kapcsolat vizsgálati szempontjai*. Budapest: Crew Kft, 2015. Elérés: márc. 07, 2021. [Online]. Elérhető: https://bmprojektek.kormany.hu/download/5/0a/51000/Az%20erk%C3%B6lcsi%20%C3%A9rt%C3%A9krend%20%C3%A9s%20a%20szem%C3%A9lyis%C3%A9g%20k%C3%B6z%C3%B6tti%20kapcsolat.pdf?fbclid=IwAR1HlU1A5XVJ3ufU1toGW1tM3sJPM-tD4z8KN__c5T8BoceAgVP7E4wnlPQ
[114] C.-H. S. Lin és C.-F. Chen, „Application of Theory of Planned Behavior on the Study of Workplace Dishonesty”, előadás 2010 International Conference on Economics, Business and Management, Manila, Philippines, 2010. [Online]. Elérhető: http://www.ipedr.com/vol2/14-P00029.pdf
[115] W. K. H. Kft, „1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról - Hatályos Jogszabályok Gyűjteménye”. https://net.jogtar.hu/jogszabaly?docid=99500125.tv (elérés ápr. 04, 2021).
[116] „Nemzetbiztonsági ellenőrzés - NBF”. https://www.nbf.hu/hasznos-informaciok/nemzetbiztonsagi-ellenorzes/ (elérés febr. 28, 2021).
[117] F. Z. Gozon, E. Laufer, és D. Váczi, „Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment”, *Proc. of the IEEE 19th International Symposium on Intelligent Systems and Informatics*, 2021. (Megjelenés alatt.)
[118] E. Laufer, T. Szadeczky, és D. Váczi, „Human risk factors to measure the potential of digital information leakage”, *Biztonságtudományi Szemle*, sz. III. évf. 3. szám, o. 55–65.
[119] J. Beinschróth, *A kockázatok kezelése, védelmi intézkedések*. 2018.
[120] Z. Horváth, „A kockázatmenedzsment információbiztonsági kérdései”, *MINŐSÉG ÉS MEGBÍZHATÓSÁG*, köt. 50, o. 148–156, 2016.
[121] L. Kovács, *Kiberbiztonság és -stratégia*. Dialóg Campus Kiadó - Nordex Kft, 2018.
[122] S. C. Patel, J. H. Graham, és P. A. S. Ralston, „Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements”, *International Journal of Information Management*, köt. 28, sz. 6, o. 483–491, 0 2008, doi: 10.1016/j.ijinfomgt.2008.01.009.
[123] K. Hiromitsu és H. Ernest J., *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2. kiadás. Wiley-IEEE Press, 2000. Elérés: márc. 07, 2021. [Online]. Elérhető: https://ieeexplore.ieee.org/book/5264399

[124] P. A. S. Ralston, J. H. Graham, és J. L. Hieb, „Cyber security risk assessment for SCADA and DCS networks”, *ISA Transactions*, köt. 46, sz. 4, o. 583–594, okt. 2007, doi: 10.1016/j.isatra.2007.04.003.
[125] H. Al-Khateeb, G. Epiphaniou, A. Reviczky, P. Karadimas, és H. Heidari, „Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation”, *IEEE Sensors Journal*, köt. 18, sz. 12, o. 4822–4831, 2018, doi: 10.1109/JSEN.2017.2782751.
[126] M. M. Silva, A. P. H. de Gusmão, T. Poleto, L. C. e Silva, és A. P. C. S. Costa, „A multidimensional approach to information security risk management using FMEA and fuzzy theory”, *International Journal of Information Management*, köt. 34, sz. 6, o. 733–740, 0 2014, doi: 10.1016/j.ijinfomgt.2014.07.005.
[127] V. Jaganathan, P. Cherurveettil, és P. Muthu Sivashanmugam, „Using a Prediction Model to Manage Cyber Security Threats”, *The Scientific World Journal*, máj. 03, 2015. https://www.hindawi.com/journals/tswj/2015/703713/ (elérés márc. 07, 2021).
[128] Z. Zhang, P.-H. Ho, és L. He, „Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach”, *Computers & Security*, köt. 28, sz. 7, o. 605–614, okt. 2009, doi: 10.1016/j.cose.2009.03.005.
[129] A. P. Henriques de Gusmão, M. Mendonça Silva, T. Poleto, L. Camara e Silva, és A. P. Cabral Seixas Costa, „Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory”, *International Journal of Information Management*, köt. 43, o. 248–260, 0 2018, doi: 10.1016/j.ijinfomgt.2018.08.008.
[130] Lotfi. A. Zadeh, „Fuzzy sets”, in *Information and control*, 3. kiad., köt. 8, 1965, o. 338–353.
[131] E. Laufer, „Mamdani-típusú következtetési rendszeren alapuló kockázatkiértékelő módszerek optimalizálása”, PhD Thesis, 2014.
[132] Lotfi. A. Zadeh, „Outline of a New Approach to the Analysis of Complex Systems and Decision Processes”, *IEEE Transactions on Systems, Man, and Cybernetics*, köt. SMC-3, sz. 1, o. 28–44, 0 1973, doi: 10.1109/TSMC.1973.5408575.
[133] E. H. Mamdani és S. Assilian, „An experiment in linguistic synthesis with a fuzzy logic controller”, *International Journal of Man-Machine Studies*, köt. 7, sz. 1, o. 1–13, 0 1975, doi: 10.1016/S0020-7373(75)80002-2.
[134] P. Martin Larsen, „Industrial applications of fuzzy logic control”, *International Journal of Man-Machine Studies*, köt. 12, sz. 1, o. 3–10, 0 1980, doi: 10.1016/S0020-7373(80)80050-2.
[135] T. Takagi és M. Sugeno, „Fuzzy identification of systems and its applications to modeling and control”, *IEEE Transactions on Systems, Man, and Cybernetics*, köt. SMC-15, sz. 1, o. 116–132, 0 1985, doi: 10.1109/TSMC.1985.6313399.
[136] R. Fuller, *Fuzzy Reasoning and Fuzzy Optimization*. Abo: Turku Centre for Computer Science, 1998.
[137] J. Dombi és E. Laufer, „Reducing the Computational Requirementsin the Mamdani-type Fuzzy Control”, *ACTA POLYTECHNICA HUNGARICA*, köt. 17, o. 25–41, 2020, doi: 10.12700/APH.17.3.2020.3.2.
[138] M. Stanley, „The Small-World Problem. Psychology Today”, *PsychologyToday*, sz. 1, o. 61–67, 1967.
[139] A.-L. Barabási - A hálózatok új tudománya, *Behálózva*, 2016. kiad. Budapest: Libri Kiadó.
[140] P. Erdős és A. Rényi, „On The Evolution of Random Graphs”, *Magyar Tudományos Akadémia Matematikai Kutató Intézet Közlöny 5*, o. 17–61, 1960.

[141] H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, és A.-L. Barabási, „The large-scale organization of metabolic networks”, *Nature*, köt. 407, sz. 6804, Art. sz. 6804, okt. 2000, doi: 10.1038/35036627.
[142] D. Kiss és D. Váczi, „A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján”, *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, köt. 28, o. 151–168, 2018, doi: 10.17047/HADTUD.2018.28.1.151.
[143] A.-L. Barabási, *A hálózatok tudománya*. Budapest: Libri Kiadó, 2016.
[144] Birher N., Bertalan P., Kele J., Bertalanné Pályi A., Molnárné Barna K., és Molnár T., *Hálózatokban*, 2014. kiad. Veszprém: Okter-Nobus Kiadó.
[145] H. C. Sözen, N. Basım, és K. Hazır, „Social Network Analysis in Organizational Studies”, *International Journal of Business and Management*, köt. 1, o. 21–35, 0 2009.
[146] R. Cross és K. Ehrlich, „Managing Collaboration at the Point of Execution: Improving Team Effectiveness with a Network Perspective”, 0 2008.
[147] G. R. Maio és G. Haddock, *The Psychology of Attitudes and Attitude Change*, 1st edition. Los Angeles ; London: SAGE Publications Ltd, 2010.
[148] D. Katz, „The Functional Approach to the Study of Attitudes”, *The Public Opinion Quarterly*, köt. 24, sz. 2, o. 163–204, 1960.
[149] E. Snowden, *Permanent Record*, 1st Edition. New York: Metropolitan Books, 2019.
[150] J. Gomes, P. Ahokangas, és K. Atta-Owusu, „Business modeling facilitated cyber preparedness”, *International Journal of Business and Cyber Security*, köt. 1, o. 54–67, 0 2016.
[151] Lazányi K., „A szervezeti biztonság és a munkahelyi stressz kapcsolata”, *TAYLOR*, köt. 8, sz. 5, Art. sz. 5, jan. 2016.
[152] R. R. McCrae és P. T. Costa, „Validation of the five-factor model of personality across instruments and observers”, *Journal of Personality and Social Psychology*, köt. 52, sz. 1, o. 81–90, 1987, doi: 10.1037/0022-3514.52.1.81.
[153] T. L. Giluk és B. E. Postlethwaite, „Big Five personality and academic dishonesty: A meta-analytic review”, *Personality and Individual Differences*, köt. 72, o. 59–67, 0 2015, doi: 10.1016/j.paid.2014.08.027.
[154] Tünde P., „A manipulatív viselkedési evolúció perspektívája”, o. 288.
[155] S. Jakobwitz és V. Egan, „The dark triad and normal personality traits”, *Personality and Individual Differences*, köt. 40, sz. 2, o. 331–339, 0 2006, doi: 10.1016/j.paid.2005.07.006.
[156] Goleman D., *Érzelmi intelligencia a munkahelyen*. Budapest: SHL Hungary Kft., 2002.
[157] B. Pikó, „Függőségek és a mértéktelenség kultúrája”, *Valóság: Társadalomtudmányi Közlöny*, köt. 60, sz. 3, o. 16–23, 2017.
[158] G. John M., „Internet Addiction Guide”, *Psych Central*, máj. 17, 2019. https://psychcentral.com/net-addiction (elérés márc. 15, 2021).
[159] J. Talyigás, *Az internet a kockázatok és mellékhatások tekintetében*. Budapest: Scolar Kiadó, 2010.
[160] I. Hullám és L. Muha, „Új típusú függőségek az információs társadalomban és azok hatása az informatikai biztonságra”, *HADTUDOMÁNYI SZEMLE*, sz. 3/2, o. 70–76, 2010.
[161] „Mi az a középosztály, ki a szegény és hol kezdődik a gazdag? – Kiszámoló – egy blog a pénzügyekről”, júl. 03, 2019. https://kiszamolo.hu/mi-az-a-kozeposztaly-ki-a-szegeny-es-hol-kezdodik-a-gazdag/ (elérés márc. 14, 2021).

[162] M. Fathali M., „The Staircase to Terrorism: A Psychological Exploration.”, *American Psychologist*, köt. 60, o. 161–169, 2005, doi: https://doi.org/10.1037/0003-066X.60.2.161.
[163] G. Nógrádi és N. Pákozdi, „A családi háttér szerepe a radikalizálódás folyamatában”, *HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA*, sz. 4, o. 25–39, 2016.
[164] Barics T., Juhász É., Karamánné Pakai É., és Szabó J., *Munkahelyi lelki egészségvédelem – mentális egészség, stresszkezelés, változások elfogadásának segítése*. Pécs: Pécsi Tudományegyetem, 2014.
[165] W. K. H. Kft, „2012. évi C. törvény a Büntető Törvénykönyvről - Hatályos Jogszabályok Gyűjteménye”. https://net.jogtar.hu/jogszabaly?docid=a1200100.tv (elérés márc. 14, 2021).
[166] M. A. Moreno, *Szex, drogok, Facebook*. Budapest: Móra Könyvkiadó, 2015.
[167] Z. Nyikes és E. Szűcs, „A zsarolóvírus-támadással szembeni védekezés a biztonságtudatosság növelésével”, *Prevention for ransomware attack by security awareness increasing*, 2019, Elérés: szept. 14, 2021. [Online]. Elérhető: https://eda.eme.ro/xmlui/handle/10598/31230
[168] „cyex | Cyber Security Awareness Platform”, *cyex*. https://cyex.io/ (elérés ápr. 23, 2021).
[169] Z. Bederna, „Components of Security Awareness and Their Measurement Part 1”, *ISACA Journal*, sz. 5, 2020, Elérés: ápr. 23, 2021. [Online]. Elérhető: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/components-of-security-awareness-and-their-measurement-part-1
[170] Z. Bederna, „Components of Security Awareness and Their Measurement Part 2”, *ISACA Journal*, sz. 5, 2020, Elérés: ápr. 23, 2021. [Online]. Elérhető: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/components-of-security-awareness-and-their-measurement-part-2
[171] M. Takács és E. Laufer, „The AHP Extended Fuzzy Based Risk Management”, in *10th WSEAS International Conference on Artificial Intelligence, Knowledge Engeneering and Data Bases (AIKED’11)*, 2011, o. 269–272.
[172] D. Váczi, „Az emberi tényező kockázatainak modellezési lehetősége Fuzzy-logikával a vasútnál, mint kritikus infrastruktúrában”, *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, köt. 29, o. 80–91, 2019, doi: 10.17047/HADTUD.2019.29.3.80.
[173] D. Váczi, „Informatikai behatolások és felismerésük”,
[174] D. Váczi és T. Szádeczky, „A Threat for the Trains: Ransomware as a New Risk”, *INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS*, köt. 17, o. 1–6, 2019, doi: 10.7906/indecs.17.1.1.
[175] T. Szádeczky és D. Váczi, „Kiberbiztonsági változások a fizetési szolgáltatásoknál”, *HADMÉRNÖK*, köt. 13, o. 443–452, 2018.

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

Függelék

1. függelék: Google Drive-ba feltöltött fájlok listája

A lenti táblázat összefoglalja a Google Drive-ból letölthető *vd_phd_ertekezes.zip* fájl kicsomagolása után a lenti táblázatban található fájlok találhatóak meg.

Link:https://drive.google.com/drive/folders/13xOboHJm-SpO6Y8Q3HhjiSVcWwF7Dbyy?usp=sharing

QR kód beolvasásával is megtalál:

Fájl neve	**Leírás**
belso.fis	MatLab fuzzy rendszer.
bemenetek.xlsx	A fuzzy rendszer bemeneteinek kipróbálását segítő táblázat.
bemenetlista_simulink.txt	A bemenetek listája tagolva txt változatban 0,5-ös alapértelmezett értékkel.
csalad.fis	MatLab fuzzy rendszer.
egyen.fis	MatLab fuzzy rendszer.
elettapasztalat.fis	MatLab fuzzy rendszer.
erzelmek.fis	MatLab fuzzy rendszer.
esettanulmany_bemenetek.xlsx	A *4. fejezetben* ismertetett esettanulmányokban használt értékek.
fizetes.fis	MatLab fuzzy rendszer.
fuzzymodel.png	Az *5. függelékben* található ábra nagyítható verziója.
k_munkahelyi_t.fis	MatLab fuzzy rendszer.
kockazat.fis	MatLab fuzzy rendszer.
kockazat2.fis	MatLab fuzzy rendszer.

kompetencia.fis	MatLab fuzzy rendszer.
korulmenyek.fis	MatLab fuzzy rendszer.
kulso.fis	MatLab fuzzy rendszer.
lehetoseg.fis	MatLab fuzzy rendszer.
megiteles.fis	MatLab fuzzy rendszer.
munka.fis	MatLab fuzzy rendszer.
munkahely.fis	MatLab fuzzy rendszer.
sikeresseg.fis	MatLab fuzzy rendszer.
simulink_fuzzy_model.slx	A kockázati fuzzy modell szimulációs fájlja. Ennek segítségével tekinthető át az egymásba illesztett fuzzy rendszerek, valamint a szimulációs eredmények is itt generálhatóak.
szabályok.xlsx	A *10. függelékben* található szabályok .xlsx formátumban
szandek.fis	MatLab fuzzy rendszer.
szemelyisegi_jegyek.fis	MatLab fuzzy rendszer.
szubjektiv_kontrollok.fis	MatLab fuzzy rendszer.
veletlen_elkovetes.fis	MatLab fuzzy rendszer.
zsarolhatosag.fis	MatLab fuzzy rendszer.

2. függelék: A fuzzy rendszer kipróbálásának folyamata

Szükséges szoftverek:

- Táblázatkezelő (ajánlott Microsoft Excel újabb verziója);
- MatLab Fuzzy Toolbox és Simulink kiegészítéssel;
- Tömörítő program a .zip állomány kicsomagolására.

Kipróbálás folyamata:

- Töltsd le a tömörített *vd_phd_ertekezes.zip* fájlt a következő linkről, majd csomagold is ki: https://drive.google.com/drive/folders/13xOboHJm-SpO6Y8Q3HhjiSVcWwF7Dbyy?usp=sharing.
- Nyisd meg a MatLab programot és a menüsáv alján navigálj abba a mappába, amit kicsomagoltál.
- Nyisd meg a *bemenetek.xlsx* dokumentumot. Az *E* és *F* oszlopban jelzett skála megmutatja az adott tényezőhöz rendelet leginkább és legkevésbé kockázatos tagsági függvényeket. Ez alapján a *C* oszlop értékének módosításával legenerálódik a *D* oszlopba egy egyszerűen kimásolható bemeneti érték lista. Ezt (az első sor kivételével) jelöld ki és használd a másolás funkciót.
  Megjegyzés: Az *E* és *F* oszlop értékei, önmagukban félrevezetőek lehetnek. Megértésükhöz érdemes a 3.1-3.5 fejezeteket tanulmányozni.
- A MatLab *Command Window* felületére kattintva használd a beillesztés funkciót, majd nyomj egy Entert. Ekkor megtörténik az értékek megadása. (Ha a későbbiek során csak egy-két értéket szeretnél módosítani, nem szükséges mindet újra megadni, hanem elegendő a konkrét sort beírni a szögletes zárójel második értékének módosításával.).
- A kicsomagolt mappában nyisd meg a *simulink_fuzzy_model.slx* fájlt. Ezt követően, ha nem indul el automatikusan a kalkuláció, akkor a *Run* funkció segítségével tudod elindítani a kalkulációt, mely eltarthat akár percekig is. Ennek állapotát a jobb alsó sarokban megjelenő folyamatjelző sáv fogja mutatni.
- A *Command Window* felületen megadott új értékek után, minden esetben szükséges a szimuláció újbóli elindítása a *Run* funkcióval.

3. függelék: A kérdőív kérdései

Ön milyen területen dolgozik? (Feleletválasztós, több megadható válasz)

- Biztonsági auditor
- Biztonsági elemző
- Biztonsági mérnök
- Biztonsági rendszeradminisztrátor
- Biztonsági stratéga
- Biztonsági tanácsadó
- Biztonsági tesztelő/etikus hacker
- CSO/CISO/CIAO/IBF
- CSO/CISO/CIAO/IBF helyettes
- Hálózati adminisztrátor
- Igazságügyi szakértő (forensics)
- Incidenskezelő (szervezeti)
- Információbiztonsági menedzser
- Projektmenedzser
- SOC (felügyelet, biztonsági esemény elemzés)
- Technikai tanácsadó
- Üzemeltetési menedzser
- Egyéb biztonsági
- Egyéb (Utána szabad szavas válaszadási lehetőség)

Mennyi év tapasztalata van IT/kiber-/információbiztonsági területen? (Feleletválasztós, egy megadható válasz)

- Nincs
- Gyakornok vagyok
- 3 év vagy kevesebb
- 4 -6 év
- 7-10 év
- 11-15 év
- 16-25 év
- Több mint 25 év

Milyen biztonsági területeken van munkatapasztalata? (Feleletválasztós, több megadható válasz)

- A végfelhasználók biztonságtudatossága
- Adatvédelem
- Alkalmazás biztonság
- Auditálás

- Biztonsági adminisztráció
- Biztonsági architektúra és modellek
- Biztonsági gyakorlatok tervezése
- Biztonsági menedzsment
- Biztonsági normatív szabályozás (nem adatvédelem)
- Biztonsági tervezés
- BYOD
- Felhő alapú szolgáltatások biztonsága
- Fenyegetettség modellezés
- Incidensreagálás
- Jogosultságkezelés
- Kockázatkezelés
- Kriminalisztika
- Mobileszközök védelme
- Oktatás
- Személyi biztonsági kockázatok kezelése
- Távközlés és hálózatbiztonság
- Üzemeltetés biztonság
- Üzletmenet-folytonosság és katasztrófa utáni helyreállítási tervezés
- Semelyikben

Milyen szektorban dolgozik? (Feleletválasztós, egy megadható válasz)

- Akadémiai szektor
- Állami szektor
- Egészségügy
- Energia szektor
- Építőipar
- Idegenforgalom
- Ipari szektor (nehézipar, könnyűipar stb.)
- IT és technológiai szektor
- Kis- és nagykereskedelem
- Közlekedési szektor
- Mezőgazdaság
- Pénzügyi szektor
- Tanácsadói szektor
- Távközlési és média szektor
- Védelmi szektor
- Egyéb

Melyik országban dolgozik? (Legördülő lista)

Mennyi fő dolgozik a szervezeténél az országban? (Feleletválasztós, egy megadható válasz)

- Kevesebb mint 10
- 10-50
- 50-250
- 250-1000
- Több mint 1000

Milyen a vállalat jellege? (Feleletválasztós, egy megadható válasz)

- Multinacionális
- Lokális jelentőségű

Mennyire tartja önmagát jó emberismerőnek? (Feleletválasztós, egy megadható válasz)

- Egyáltalán nem jó
- Kicsit
- Átlagos
- Átlagosnál jobb
- Nagyon jó

Mennyire tartja általában kockázatosnak az adott munkakörben dolgozó személyeket kiberbiztonsági szempontból? (1-6 skála, ahol az 1-es a "egyáltalán nem kockázatos"-t, a 6-os a "kritikus"-t jelenti)

- Asszisztens (nem vezetői)
- Biztonsági őr a recepción
- Controller
- Gyakornok
- Hosztesz
- HR-es
- Informatikus
- IT biztonsági munkatárs
- Jogász
- Külsős munkavállaló (tanácsadó)
- Kirendeltség vezető (fióktelep)
- Könyvelő (pénzügyes, bérszámfejtő)
- Marketinges
- Takarító/ karbantartó munkatárs
- Ügyfélszolgálati munkatárs
- Vezetői asszisztens

Jelöljön ki a kurzorával (vagy érintőképernyőn dupla koppintással) az alábbi 16 darab karakterleírásban külön-külön minimum 1 maximum 3 szót vagy rövid kifejezést, amely Ön szerint kockázatossá teszi abból a szempontból, hogy külső megkeresésre vagy önszántukból, esetleg gondatlanságból szenzitív információt szivárogtathatnak ki.

(A megadott karaktereket, a kiértékeléssel együtt a következő függelék tartalmazza.)

Olvassa végig a felsorolt tényezőket, majd miután mindet elolvasta jelölje be, hogy Ön szerint melyik milyen mértékben növeli annak a kockázatát, hogy egy személy zsarolhatóvá válik, így szenzitív információkat szivárogtathasson ki? (1-6 skála, ahol az 1-es a " egyáltalán nem növeli "-t, a 6-os a " nagyon növeli "-t jelenti)

- A tény, hogy az illető külsős munkatárs
- A tény, hogy az illető párkapcsolatban van, így a párjáért is felel
- Alacsony EQ szint
- Alacsony IQ szint
- Az illető már követett el apróbb szabályszegéseket
- Az illetőnek több gyermeket kell eltartania
- Figyelmetlenség
- Függőség
- Gyenge erkölcs
- Gyenge értékítélet/értékrend
- Kevés élettapasztalat
- Megfelelő, figyelmes vezető hiánya
- Munkahelyi közösségbe történő be nem illeszkedés
- Nagyarányú hozzáférés érzékeny adatokhoz
- Nagy munkatapasztalat az adott helyen és pozícióban
- Negatív véleményt formáló társas közeg
- Önismeret hiánya
- Pszichés terhelhetőség (feszültségtűrés, frusztráció tolerancia)
- Rossz egészségügyi állapot
- Rossz pénzügyi helyzet (vélt vagy valós egzisztenciális problémák)
- Sértettség (fizetésemelés, előléptetés hiánya)
- Szervezet iránti lojalitás hiánya
- Társadalmi normától való titkos eltérés (vallás, szexualitás, politikai nézet stb.)

Mit gondol mekkora a kockázata annak, hogy az itt leírt karakterek külső megkeresésre vagy önszántukból, esetleg gondatlanságból szenzitív információt

szivárogtatnak ki? (1-100 skála, ahol az 1-es a " egyáltalán nem kockázatos "-t, a 6-os a " nagyon kockázatos "-t jelenti)

A következő függelékben található karakterek összerendelése konkrét munkakörökkel.

4. függelék: Kérdőívben vizsgált karakterek:

A zárójelben lévő számok mutatják meg, hogy az előtte lévő aláhúzott szót vagy kifejezetést mennyien jelölték be összesen kockázatnak. Az első szám azt mutatja meg, hogy a 174 kitöltő közül mennyien jelölték be összesen, míg a második, hogy ebből mennyien rendelkeznek releváns kiberbiztonsági tapasztalattal.

Agilis (7;5), egyetemista (6;0), van párja (7;4), de gyakran flörtöl a cégen belül másokkal (45;35). Anyagi háttere gyenge (64;42), szegényebb családból származik (6;4). Korából fakadóan a technológiára fogékonyabb (11;8), átlagos aktív felhasználó (9;7), aki a közösségi médiát is sokat használja (53;41). Monoton munkát végez precízen (13;10), ami nincs megbecsülve (77;53), sokkal több munkát is el tudna végezni (7;5). Nem sikerült teljesen beilleszkednie (26;14), a teljes állású munkavállalók "csak egy gyakornok"-ként kezelik (24;16). Nem alakult még ki teljesen az erkölcsi értékrendje (87;69). Dohányzik (6;5), sokat jár bulizni (11;8).

Általánosabb feladatok lát el (1;0). Kávét főz, vendégeket kísér (17;10). Segít a nyomtatásban, fénymásolásban (37;29), ami során kerülhet hozzá a tudta nélkül (52;40) kifejezetten szenzitív dokumentum (93;66), aminek a fontosságáról ő nem tud (68;51). Nagyon nehezen került be a szervezetbe, a harmadik pozícióira hívják be (7;5), ezért ő nagyon félti az állását (27;20). Nagycsaládos (1;0), otthonülő típus, aki gyakran betegeskedik (7;6). A férje informatikus (19;15), akinek a fizetéséből átlagosan élnek (4;3).

Belépőkártyákon (25;18) kívül hozzáfér dolgozói adatokhoz (107;75). Ismeri a vezetőség és sok más munkatárs rutinját (70;51). Sok rá nem tartozó információt hall (81;55), leginkább pletykák, fél információk (32;23) formájában. Tudja, hogy mi történik az épületben (14;11). Egyedülálló középkorú férfi (11;10). A haverokkal (7;5) átlag heti kétszer (11;7) a törzshelyükön (19;15) iszogatnak (31;22). Szereti a technológiát (5;3), sokat olvas az újdonságokról (2;1).

Főként az ügyfelekkel foglalkozik (10;4). Távol vannak a központból (14;13), ezért sok információ csak közvetve és lassan ér el hozzá (23;22). Ez frusztráló számára (78;55), mivel nincsen érdemi ráhatása a dolgok menetére (15;10). Sok pénzügyi adathoz fér hozzá (126;103). Családos ember (2;2), egy gyerekkel (5;4), átlagfizetéssel (10;8). Munkája során használja csak a különböző technikai eszközöket (10;7). Passzívan van

jelen a közösségi médiában (9;8), ahol időnként megoszt néhány érdekesnek tűnő bejegyzést (20;16). Betegeskedő típus (17;14).

Jól keres, az érzelmi intelligenciája alacsony (20;11), kicsit introvertált (9;4). A többi informatikussal találja meg a közös hangot, akikkel sokat jár kávézni (6;4), ahol legtöbbször szakmai kérdésekről beszélgetnek (115;11). Itt leginkább szakmáznak. Ha kirúgnák, hamar találna másik munkát (10;9). Bizonyos védelmi kontrollokat meg tud kerülni (133;98), akár tudattalanul is (36;26) a kényelmesebb munkavégzés miatt (35;25). Nagyon szenior kolléga (6;5), nem tartozik alá ember (7;6), de sok mindenhez van hozzáférése (82;58). Két gyermekes családapa (7;5), akinek súlyos betegsége van (38;27).

Középvezető (7;6). Van egy kis csapata, de felette több szint van még. Tipikusan olyan főnök típus, aki parancsokat osztogat (21;15). Alapvetően jól helyezkedik (18;11), és ezért jutott feljebb (7;4). Szakmailag sokkal jobbak is vannak a csapatában (30;24), ami őt frusztrálja (90;62). 50-es éveit tapossa (4;3), sajnos férje korán elhunyt (7;6), három gyermeke (2;2) már különél tőle (2;2). Extrovertált (37;26) személyisége miatt sok látszat kapcsolatot (35;24) tart fent, de szoros kötelék egyik kollégájával sem alakult ki (25;17).

Külföldi kolléga (13;8), aki nem rég érkezett (6;5) családjával az országba, kifejezetten a jelenlegi jól fizető munkája (5;3) miatt. Korábban nagyon rosszul keresett (4;4). Nem ismeri a helyi szokásokat (50;31), mivel kicsit más kulturális közegből (14;9) jött, ezért nehéz a beilleszkedése (21;14;). Kedves, szorgalmas (5;3), szakmailag nagyon ügyes (7;4), aki sok pénzügyi adathoz fér hozzá (106;74). Erős dohányos (6;4), és néha egy-két füves cigit (49;32) is elszív. Otthoni barátaival az internetes alkalmazásokon (28;23) keresztül tartja a kapcsolatot. Nagyon szeret online játékokkal játszani (72;49).

Külsős munkatárs (17;12), akinek az a munkája, hogy minél több új ügyfelet szerezzen (7;4). Kicsit butácska (50;35), kevés érzékeny információnak van a tudatában (18;12), azonban az új termékekről sokat tud (85;43). Egyedülálló (12;8), bulizós (23;14) típus. Erős a közösségi média jelenléte (71;53), de nem igazán ért azon kívül a kütyükhöz (32;24). Szülei gazdagok (2;2), akik sokat segítenek neki (2;2). Az anyacégnél van néhány kolléga, akivel sokat beszél (10;7), de rajtuk kívül nem igazán tisztelik, fogadják el a többiek (39;24).

Negyvenes évei (3;3) végén járó felsővezető (7;7). Számos érzékeny adathoz fér hozzá (115;81). Tipikus vezető típus, aki példamutatással vezeti a csapatát (2;2), magas az érzelmi intelligenciája (2;1). Lojális a vállalathoz (4;1), de ha kirúgnák, könnyen találna új munkahelyet (10;6). Nagyon le van terhelve (63;20). Elvált (19;8), egy gyermeke vele él (27;14), aki súlyos egészségügyi problémákkal (55;39) küzd. Ő maga dohányzik (2;2), és esténkét 1-2 whisky-t megiszik (29;24), hogy oldja a feszültségét (10;9).

Ő munkakörét tekintve egy magányos farkas (25;20), aki a régióért felelős(7;6). A csapatának a többi része másik országokban van (8;6), ezét szakmailag egy kicsit egyedül érzi magát (43;29). Van ugyan kijelölt felettese, de ő szakmailag nem ért ehhez a munkához (43;20). Ez frusztrálja (83;53). Biztos a helye, mert nincs más, aki el tudja végezni a komplex munkáját (47;39). Egyedülálló (9;7), intelligens (7;5), kicsit introvertált (11;5) fiatal (4;2)férfi, átlagos anyagi helyzettel (10;6).

Rálát több érzékeny adatra, folyamatra (72;46), de csak magas szinten (8;4). A részleteket nem ismeri (3;2). Jó kapcsolatot ápol a többi csapattal (4;2), de a munkájával sok gond van (24;14), többek között nagyon figyelmetlen (100;69). A főnöke többször figyelmeztette (16;11) már és kitűztek különböző célokat, amik elérése szükséges azért, hogy maradhasson a vállalatnál (14;9). Válás előtt álló nő (26;17). Nagyon szegények (54;39) és jelenlegi munkája nélkül nem tudná eltartani a két gyerekét (24;17). Nem igazán van tisztában az informatikai eszközökkel (59;43).

Sok helyre van bejárása (85;58). Átlagos intelligenciájú (6;2), viszonylag rossz egzisztenciával (54;32). Idősebb korosztályú (9,4), aki a digitális technológiákhoz nem ért (55;41). Kicsit pletykás (96;67), szívesen beszélget ezért az aktuális munkavégzés helyén a többi munkatárssal (19;13). Nyugdíj közelében van (10;8), aki egész életében minimálbért kapott (39;33). Nem iszik (3;2), nem dohányzik (3;2), de napi 1-1 kávé nélkül úgy érzi, nem tud meglenni (1;1).

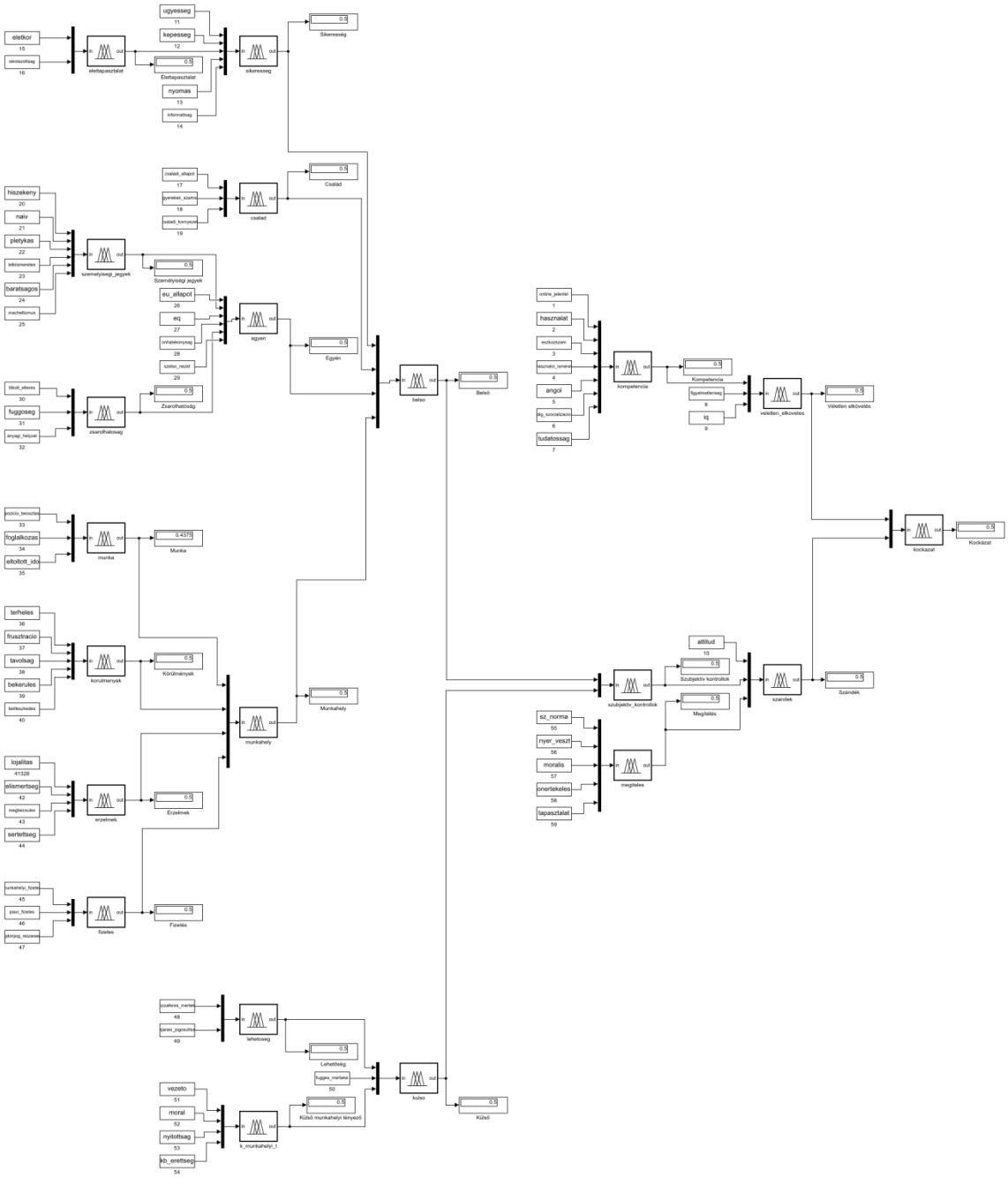
Sok személyes adathoz fér hozzá (141;97). Néhány éve dolgozik a vállalatnál (3;2), ez az első munkahelye (8;4). Jól végzi a munkáját, ezért amikor a főnök szabadságon van, neki delegál bizonyos jogköröket (43;28), és dönthet kisebb ügyletek kapcsán (11;4). Tudatos felhasználó (1;1), munkája során sokat használja a különböző közösségi média felületeket és más internetes platformokat (39;31). Néhány éves párkapcsolata van (2;2), extrovertált (12;8), szereti a társaságot (4;3). Rossz anyagi helyzetű családból származik (13;9), de jelenlegi fizetésére nincs panasza.

Tisztában van a védelmi kontrolokkal (47;36), jól ismeri a technológiát (33;26). Jól megfizetett munkáját (6;3) sokszor csak szükséges rosszként értékelik (37;24), ami csak bosszúságot okoz másoknak (8;4). Erkölcsileg ugyan erős és precíz munkatárs, de ő a mindig elégedetlenkedő típus (107;81). Neki semmi nem elég, rossz a kávé, a fizetés és gyakorlatilag minden (34;23). Egyedülálló (7;5), középkorú nő (8;6), aki a közvetlen kollégáival nem igazán jön ki (24;16), de a cégnél sokakkal ápol jó kapcsolatot (13;9).

Vezetői és más fontos megbeszéléseken bent ül a főnökével, ahol jegyzetel (32;28). Sok rendszerhez van hozzáférése (105;72). Kedves, kommunikatív (15;8) ezért, sok információ eljut hozzá (42;14). Alapvetően jól meg van fizetve (;), de két éve várja a fizetésemelést vagy előléptetést (65;47), amit sajnos idén sem kapott meg (48;31). Családos (3;3), középkorú nő. Több nagyvállalatnál dolgozott már, ismeri a folyamatokat (9;7), nagyon precíz az élet minden területén (2;2).

Vezetői pozíció (6;4). A fióktelepen ő a kiskirály (34;27), de amikor bemegy a központba, ott rájön, hogy nem annyira nagy ász (22;15). Ettől függetlenül felelősségteljes a munkája (5;4), hiszen sok beosztottjának az életére gyakorol hatást (8;6). Sok pénzügyi, treasury adathoz fér hozzá (124;89). Elvált (8;7), két gyermeke van (6;4), akik nem élnek vele együtt (6;3). Biztos anyagi háttere van (;), kicsit harsányabb (22;14), szétszórtabb (68;47) típus. Átlagos informatikai ismeretei vannak (13;9). Az üzleti alkalmazásokat ismeri leginkább (9;8).

5. függelék: A kiberbiztonsági kockázati fuzzy rendszer



6. függelék: Kockázati tényezők és kapcsolataik

Kockázat	Szándék	Attitűd				
		Szubjektív kontrollok	Belső	Sikeresség	Ügyesség	
					Élettapasztalat	Életkor
						Iskolázottság
					Képesség	
					Nyomás	
					Informáltság	
				Család	Családi állapot	
					Gyermekek száma	
					Családi környezet	
				Egyén	EÜ állapot	
					Személyiségi jegyek	Pletykásság
						Hiszékenység
						Lelkiismeretesség
						Naivitás
						Barátságosság
						Machellizmus
					EQ	
					Önhatékonyság	
					Szélső nézetek	
					Zsarolhatóság	Titkolt eltérés
						Függőség
						Anyagi helyzet
				Munkahely	Munka	Pozíció, beosztás
						Foglalkozás
						Eltöltött idő
					Környezet	Leterheltség
						Frusztráció
						Távolság
						Bekerülés
						Beilleszkedés
					Érzelmek	Lojalitás
						Elismertség
						Megbecsülés
						Sértettség
					Fizetés	Tulajdonjog, részesedés
						Piaci fizetés
						Munkahelyi fizetés
			Külső	Lehetőség	Hozzáférés mértéke	
					Bejárási jogosultság	
				Függés mértéke		
				K. munkahelyi t.	Vezetői kontroll	
					Közösségi morál	
					Közösség nyitottsága	
					Kiberbiztonsági érettség	
		Megítélés	Szubjektív norma			
			Önértékelés			
			Tapasztalat			
			Nyereség-veszteség			
			Morális felfogás			
	Véletlen elkövetés	Figyelmetlenség				
		IQ				
		Kompetencia	Online jelenlét			
			Felhasználói ismeretek			
			Eszközszám			
			Használat			
			Nyelvismeret (angol)			
			Digitális szocializáció			
			Kiberbiztonsági tudatosság			

7. függelék: Esettanulmányok értékeit és eredményeit összefoglaló táblázat

Első esettanulmány:

Kockázat **0,5**	Szándék **0,4175**	Attitűd **0,2**				
		Szubjektív kontrollok **0,5**	Belső **0,5028**	Sikeresség **0,6085**	Ügyesség **0,8**	
					Élettapasztalat **0,5486**	Életkor **0,4**
						Iskolázottság **0,7**
					Képesség **0,6**	
					Nyomás **0,9**	
					Informáltság **0,6**	
				Család **0,4019**	Családi állapot **0,3**	
					Gyermekek száma **0**	
					Családi környezet **0,3**	
				Egyén **0,5272**	EÜ állapot **0,2**	
					Személyiségi jegyek **0,4485**	Pletykásság **0,2**
						Hiszékenység **0,7**
						Lelkiismeretesség **0,3**
						Naivitás **0,7**
						Barátságosság **0,5**
						Machellizmus **0,7**
					EQ **0,4**	
					Önhatékonyság **0,7**	
					Szélső nézetek **0,8**	
					Zsarolhatóság **0,5398**	Titkolt eltérés **0,7**
						Függőség **0,2**
						Anyagi helyzet **0,6**
				Munkahely **0,4906**	Munka **0,3728**	Pozíció, beosztás **0**
						Foglalkozás **0,5**
						Eltöltött idő **0,3**
					Környezet **0,5825**	Leterheltség **0,5**
						Frusztráció **0,4**
						Távolság **0,2**
						Bekerülés **0,8**
						Beilleszkedés **0,5**
					Érzelmek **0,4175**	Lojalitás **0,2**
						Megbecsülés **0,4**
						Elismertség **0,4**
						Sértettség **0,3**
					Fizetés **0,582**	Tulajdonjog, részesedés **1**
						Piaci fizetés **0,3**
						Munkahelyi fizetés **0,5**
			Külső **0,5985**	Lehetőség **0,3543**	Hozzáférés mértéke **0,2**	
					Bejárási jogosultság **0,3**	
				Függés mértéke **0,8**		
				K. munkahelyi t. **0,4602**	Vezetői kontroll **0,5**	
					Közösségi morál **0,4**	
					Közösség nyitottsága **0,5**	
					Kiberbiztonsági érettség **0,3**	
		Megítélés **0,5515**	Szubjektív norma **0,7**			
			Önértékelés **0,7**			
			Tapasztalat **0,3**			
			Nyereség-veszteség **0,5**			
			Morális felfogás **0,8**			
	Véletlen elkövetés **0,4175**	Figyelmetlenség **0,2**				
		IQ **0,5**				
		Kompetencia **0,5**	Online jelenlét **0,6**			
			Felhasználói ismeretek **0,5**			
			Eszközszám **0,7**			
			Használat **0,9**			
			Nyelvismeret (angol) **0,3**			

			Digitális szocializáció **0,3**	
			Kiberbiztonsági tudatosság **0,3**	

Második esettanulmány:

Kockázat **0,4927**	Szándék **0,3792**	Attitűd **0**				
		Szubjektív kontrollok **0,3948**	Belső **0,3992**	Sikeresség **0,3475**	Ügyesség **0,1**	
					Élettapasztalat **0,6457**	Életkor **0,8**
						Iskolázottság **0,4**
					Képesség **0,2**	
					Nyomás **0**	
					Informáltság **0,2**	
				Család **0,1372**	Családi állapot **0**	
					Gyermekek száma **0**	
					Családi környezet **0**	
				Egyén **0,418**	EÜ állapot **0**	
					Személyiségi jegyek **0,4292**	Pletykásság **0,6**
						Hiszékenység **0,6**
						Lelkiismeretesség **0**
						Naivitás **0,7**
						Barátságosság **0**
						Machellizmus **0,4**
					EQ **0,3**	
					Önhatékonyság **0,7**	
					Szélső nézetek **0**	
					Zsarolhatóság **0,1372**	Titkolt eltérés **0**
						Függőség **0,1**
						Anyagi helyzet **0,3**
				Munkahely **0,3992**	Munka **0,1372**	Pozíció, beosztás **0**
						Foglalkozás **0**
						Eltöltött idő **0,1**
					Környezet **0,5708**	Leterheltség **0,5**
						Frusztráció **0,7**
						Távolság **0**
						Bekerülés **1**
						Beilleszkedés **0,9**
					Érzelmek **0,582**	Lojalitás **0,8**
						Megbecsülés **0,9**
						Elismertség **0,9**
						Sértettség **0,2**
					Fizetés **0,531**	Tulajdonjog, részesedés **1**
						Piaci fizetés **0,2**
						Munkahelyi fizetés **0,5**
			Külső **0,2338**	Lehetőség **0,1372**	Hozzáférés mértéke **0**	
					Bejárási jogosultság **0**	
				Függés mértéke **0,1**		
				K. munkahelyi t. **0,4485**	Vezetői kontroll **0,7**	
					Közösségi morál **0,2**	
					Közösség nyitottsága **0,3**	
					Kiberbiztonsági érettség **0,1**	
		Megítélés **0,3201**	Szubjektív norma **0,7**			
			Önértékelés **0,7**			
			Tapasztalat **0,3**			
			Nyereség-veszteség **0,5**			
			Morális felfogás **0,8**			
	Véletlen elkövetés **0,4198**	Figyelmetlenség **0**				
		IQ **0,7**				
		Kompetencia **0,3915**	Online jelenlét **0**			
			Felhasználói ismeretek **0,6**			
			Eszközszám **0,3**			
			Használat **0**			
			Nyelvismeret (angol) **0,2**			
			Digitális szocializáció **0,2**			
			Kiberbiztonsági tudatosság **0,2**			

Harmadik esettanulmány:

Kockázat **0,6052**	Szándék **0,7662**	Attitűd **1**				
		Szubjektív kontrollok **0,5948**	Belső **0,6135**	Sikeresség **0,6799**	Ügyesség **1**	
					Élettapasztalat **0,5486**	Életkor **0,4**
						Iskolázottság **0,7**
					Képesség **1**	
					Nyomás **1**	
					Informáltság **1**	
				Család **0,8628**	Családi állapot **1**	
					Gyermekek száma **1**	
					Családi környezet **1**	
				Egyén **0,7662**	EÜ állapot **0,9**	
					Személyiségi jegyek **0,6272**	Pletykásság **1**
						Hiszékenység **0,7**
						Lelkiismeretesség **0,8**
						Naivitás **1**
						Barátságosság **0,8**
						Machellizmus **1**
					EQ **1**	
					Önhatékonyság **1**	
					Szélső nézetek **1**	
					Zsarolhatóság **0,8628**	Titkolt eltérés **1**
						Függőség **0,8**
						Anyagi helyzet **0,8**
				Munkahely **0,6017**	Munka **0,6085**	Pozíció, beosztás **0,3**
						Foglalkozás **1**
						Eltöltött idő **1**
					Környezet **0,7065**	Leterheltség **1**
						Frusztráció **1**
						Távolság **0,6**
						Bekerülés **1**
						Beilleszkedés **1**
					Érzelmek **0,8628**	Lojalitás **1**
						Megbecsülés **0,8**
						Elismertség **1**
						Sértettség **1**
					Fizetés **0,5515**	Tulajdonjog, részesedés **1**
						Piaci fizetés **0,3**
						Munkahelyi fizetés **0,3**
			Külső **0,7572**	Lehetőség **0,8628**	Hozzáférés mértéke **1**	
					Bejárási jogosultság **1**	
				Függés mértéke **1**		
				K. munkahelyi t. **0,8628**	Vezetői kontroll **1**	
					Közösségi morál **1**	
					Közösség nyitottsága **1**	
					Kiberbiztonsági érettség **1**	
		Megítélés **0,8628**	Szubjektív norma **1**			
			Önértékelés **1**			
			Tapasztalat **1**			
			Nyereség-veszteség **1**			
			Morális felfogás **0,9**			
	Véletlen elkövetés **0,6212**	Figyelmetlenség **1.0**				
		IQ **0,7**				
		Kompetencia **0,6272**	Online jelenlét **1**			
			Felhasználói ismeretek **0,7**			
			Eszközszám **1**			
			Használat **1**			
			Nyelvismeret (angol) **1**			
			Digitális szocializáció **0,7**			
			Kiberbiztonsági tudatosság **1**			

8. függelék: Összefoglaló táblázat a fuzzy rendszerek értékeiről

Fuzzy kimenet neve	**Minden 0**	**2. eset**	**1. eset**	**Minden 0,5**	**1. eset mod**	**3. eset**	**Minden 1**
Kockázat	0,2811	0,4927	0,5	0,5	0,5358	0,6052	0,7189
Véletlen elkövetés	0,1372	0,4198	0,4175	0,5	0,6799	0,6212	0,8628
Kompetencia	0,1372	0,3915	0,5	0,5	0,5272	0,6272	0,8628
Szándék	0,2338	0,3792	0,4175	0,5	0,4175	0,7662	0,7662
Szubjektív kontrollok	0,4041	0,3948	0,5	0,5	0,5	0,5948	0,5948
Belső	0,3547	0,3992	0,5028	0,5	0,5028	0,6135	0,6453
Sikeresség	0,1372	0,3475	0,6085	0,5	0,6085	0,6799	0,8628
Élettapasztalat	0,1372	0,6457	0,5486	0,5	0,5486	0,5486	0,8628
Család	0,1372	0,1372	0,4019	0,5	0,4019	0,8628	0,8628
Egyén	0,2338	0,418	0,5272	0,5	0,5272	0,7662	0,7662
Személyiségjegy	0,1372	0,4292	0,4485	0,5	0,4485	0,6272	0,8628
Zsarolhatóság	0,1372	0,1372	0,5398	0,5	0,5398	0,8628	0,8628
Munkahely	0,2428	0,3992	0,4906	0,5	0,4906	0,6017	0,7572
Munka	0,1372	0,1372	0,3728	0,4375	0,3728	0,6085	0,8628
Körülmények	0,1372	0,5708	0,5825	0,5	0,5825	0,7065	0,8628
Érzelmek	0,1372	0,582	0,4175	0,5	0,4175	0,8628	0,8628
Fizetés	0,1372	0,531	0,582	0,5	0,582	0,5515	0,8628
Külső	0,2428	0,2338	0,5985	0,5	0,5985	0,7572	0,7572
Lehetőség	0,1372	0,1372	0,3543	0,5	0,3543	0,8628	0,8628
Külső munkahelyi tényező	0,1372	0,4485	0,4602	0,5	0,4602	0,8628	0,8628
Megítélés	0,1372	0,3201	0,5515	0,5	0,5515	0,8628	0,8628

9. függelék: A potenciális bűnismétlés elkövetése miatt kiemelten kockázatos bűncselekmények listája titoksértés esetén

- Az emberi méltóság és egyes alapvető jogok elleni bűncselekmények
    - Személyes adattal visszaélés,
    - Közérdekű adattal visszaélés,
    - Magántitok megsértése,
    - Levéltitok megsértése,
- Az állam elleni bűncselekmények
    - Kémkedés,
    - Kémkedés az Európai Unió intézményei ellen,
    - A szövetséges fegyveres erő ellen elkövetett kémkedés,
- A minősített adat és a nemzeti adatvagyon elleni bűncselekmények
    - Minősített adattal visszaélés,
    - A nemzeti adatvagyon körébe tartozó állami nyilvántartás elleni bűncselekmény,
- Az igazságszolgáltatás elleni bűncselekmények
    - Igazságszolgáltatással összefüggő titoksértés,
- A korrupciós bűncselekmények
    - Vesztegetés,
    - Vesztegetés elfogadása,
    - Hivatali vesztegetés,
    - Hivatali vesztegetés elfogadása,
    - Vesztegetés bírósági vagy hatósági eljárásban,
    - Vesztegetés elfogadása bírósági vagy hatósági eljárásban,
    - Befolyás vásárlása,
    - Befolyással üzérkedés,
    - Korrupciós bűncselekmény feljelentésének elmulasztása,
- A hivatali bűncselekmények
    - Jogosulatlan titkos információgyűjtés vagy leplezett eszköz jogosulatlan alkalmazása,
- A közbizalom elleni bűncselekmények
    - Közokirat-hamisítás,
    - Biztonsági okmány hamisítása,

    - Hamis magánokirat felhasználása,
    - Okirattal visszaélés,
    - Egyedi azonosító jellel visszaélés,
- A vagyon elleni erőszakos bűncselekmények
    - Zsarolás,
- A vagyon elleni bűncselekmények
    - Lopás
    - Jogtalan elsajátítás,
- A szellemi tulajdonjog elleni bűncselekmények
    - Bitorlás,
    - Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése,
    - Védelmet biztosító műszaki intézkedés kijátszása,
    - Jogkezelési adat meghamisítása,
    - Iparjogvédelmi jogok megsértése,
- A gazdálkodás rendjét sértő bűncselekmények
    - Gazdasági titok megsértése,
- A fogyasztók érdekeit és a gazdasági verseny tisztaságát sértő bűncselekmények
    - Üzleti titok megsértése,
- Tiltott adatszerzés és az információs rendszer elleni bűncselekmények
    - Tiltott adatszerzés,
    - Információs rendszer vagy adat megsértése,
    - Információs rendszer védelmét biztosító technikai intézkedés kijátszása.

10.függelék: Fuzzy rendszerek szabályai

A fuzzy rendszerek szabályait a mind egyesével nem listázom ki, azonban az áttekintő táblázatokat ide illesztem. Minden szabály HA (IF) ÉS (AND) AKKOR (THAN) alapú és 1-es súllyal került beszámításra. Az értelmezés elősegítése érdekében a kockázatok fuzzy rendszernél használt szabályok listájával együtt jelenítem meg az áttekintő táblázatot. A szabályok a következőek:

1. If (veletlen_elkovetes is alacsony) and (elkovetes_hajlandosaga is alacsony) then (kockazat is nem_kockazatos) (1)
2. If (veletlen_elkovetes is alacsony) and (elkovetes_hajlandosaga is atlagos) then (kockazat is nem_kockazatos) (1)
3. If (veletlen_elkovetes is atlagos) and (elkovetes_hajlandosaga is alacsony) then (kockazat is nem_kockazatos) (1)
4. If (veletlen_elkovetes is magas) and (elkovetes_hajlandosaga is alacsony) then (kockazat is kezelheto) (1)
5. If (veletlen_elkovetes is alacsony) and (elkovetes_hajlandosaga is magas) then (kockazat is kezelheto) (1)
6. If (veletlen_elkovetes is atlagos) and (elkovetes_hajlandosaga is atlagos) then (kockazat is kezelheto) (1)
7. If (veletlen_elkovetes is atlagos) and (elkovetes_hajlandosaga is magas) then (kockazat is kockazatos) (1)
8. If (veletlen_elkovetes is magas) and (elkovetes_hajlandosaga is atlagos) then (kockazat is kockazatos) (1)
9. If (veletlen_elkovetes is magas) and (elkovetes_hajlandosaga is magas) then (kockazat is kockazatos) (1)

A hozzá tartozó táblázat pedig a következőképpen néz ki:

kockazat		veletlen_elkovetes				
		alacsony	atlagos	magas		
szandek	alacsony					Nem kockázatos
	atlagos					Kezelhető
	magas					Kockázatos

A többi fuzzy rendszernél a következő szabályokat alkalmaztam:

veletlen_elkovetes		kompetencia			iq			
		professzionalis	kozepszintu	alapszintu	magas	atlagos	gyenge	
figyelmetlenseg	preciz							Alacsony
	atlagos							Átlagos
	figyelmetlen							Magas
kompetencia	professzionalis							
	kozepszintu							
	alapszintu							

szandek		attitud			megiteles			
		jo	semleges	rossz	elitelendo	semleges	helyeslo	
szubjektiv_kontroll	nehez							Alacsony
	atlagos							Átlagos
	konnyu							Magas
megitelese	elitelendo							
	semleges							
	helyeslo							

kompetencia		online_jelenlet			hasznalat			eszkozszam			
		tudatos_aktiv_jelenlet	aktiv_jelenlet	passziv_jelenlet	sokat_hasznalja	atlagosan_hasznalja	alig_hasznalja	sok	atlagos	keves	
hasznalat	sokat_hasznalja										Professzionalis
	atlagosan_hasznalja										Középszintű
	alig_hasznalja										Alapszintű
eszkozszam	sok										
	atlagos										
	keves										
felhasznaloi_ismeretek	profi										
	felhasznaloi_szintu										
	alapszintu										
angol	anyanyelvi_szintu										
	felso_szintu										
	kozepszintu										
	alapszintu										
	nincs										
dig_szocializacio	gyerekkent										
	fiatalkent										
	kozepkorukent										
	idoskent										
tudatossag	tudatos										
	jellemzoen_felismero										
	szituacio_fuggo										
	meggondolatlan										

kompetencia		felhasznaloi_ismeretek			angol					dig_szocializacio				
		profi	felhasznaloi_szintu	alapszintu	anyanyelvi_szintu	felso_szintu	kozepszintu	alapszintu	nincs	gyerekkent	fiatalkent	kozepkorukent	idoskent	
angol	anyanyelvi_szintu													Professzionalis
	felso_szintu													Középszintű
	kozepszintu													Alapszintű
	alapszintu													
	nincs													
dig_szocializacio	gyerekkent													
	fiatalkent													
	kozepkorukent													
	idoskent													
tudatossag	tudatos													
	jellemzoen_felismero													
	szituacio_fuggo													
	meggondolatlan													

szubjektiv_kontrollok		belso			
		nagy	kozepes	kicsi	
kulso	nagy				Nehéz
	kozepes				Átlagos
	kicsi				Könnyű

megiteles		sz_norma			nyer-veszt			moralis			onertekeles				
		elitelo	semleges	tamogato	magas	kozepes	alacsony	nagyon	kicsit	egyaltalan	rossz	semleges	jo		
nyer-veszt	magas														Elítélendő
	kozepes														Semleges
	alacsony														Helyeslő
moralis	nagyon														
	kicsit														
	egyaltalan														
onertekeles	rossz														
	semleges														
	jo														
tapasztalat	nem														
	talan														
	igen														

kulso		lehetoseg			fugges_merteke			
		nehez	kozepesen_nehez	konnyu	magas	alacsony		
fugges_merteke	magas							Kicsi
	alacsony							Közepes
k_munkahelyi_t	kedvezotlen							Nagy
	semleges							
	kedvezo							

k_munkahely_t		vezeto			moral			nyitottsag				
		kedvezo	ertekelheto	alacsony	pozitiv	semleges	negativ	nyitott	semleges	zarkozott		
moral	pozitiv											Kedvezőtlen
	semleges											Semleges
	negativ											Kedvező
nyitottsag	nyitott											
	semleges											
	zarkozott											
kb_ erettseg	erett											
	kozepesen_erett											
	eretlen											

lehetoseg		hozzaferes_merteke				
		nagyon_szabalyozott	alapszintu	szabalyozatlan		
bejrasi_ jogosultsag	nagyon_szabalyozott					Nehéz
	alapszintu					Közepesen nehéz
	szabalyozatlan					Könnyű

belso		sikeresseg			csalad			egyen				
		eselytelen	atlagos	eselyes	pozitiv	semleges	negativ	stabil	atlagos	instabil		
csalad	pozitiv											Kicsi
	semleges											Közepes
	negativ											Nagy
egyen	stabil											
	atlagos											
	instabil											
munkahely	kedvezo											
	semleges											
	kedvezotlen											

csalad		csaladi_allapot			gyerekek_szama				
		eros	köztes	gyenge	keves	normal	sok		
gyerekek_szama	keves								Pozitív
	normal								Semleges
	sok								Negatív
csaladi_kornyezet	tamogato								
	semleges								
	ellenseges								

sikeresseg		ugyesseg			elettapasztalat			kepesseg			nyomas		
		ugyetlen	atlagos	ugyes	tapasztalt	atlagos	tapasztalatlan	keptelen	attol_fugg	kepes	alulteljesit	atlagosan_teljesit	tulteljesit
elettapasztalat	tapasztalt												
	atlagos												
	tapasztalatlan												
kepesseg	keptelen												
	attol_fugg												
	kepes												
nyomas	alulteljesit												
	atlagosan_teljesit												
	tulteljesit												
informaltsag	informalatlan												
	atlagos												
	informalt												

Esélytelen
Átlagos
Esélyes

elettapasztalat		iskolazottsag		
		magas	kozepes	alacsony
eletkor	idos			
	kozepkoru			
	fiatal			

Tapasztalt
Átlagos
Tapasztalatlan

egyen		eu_allapot			szemelyesegi_jegyek			eq			onhatekonysag			szelsonezetek			
		egeszseges	beteg	sulyos_beteg	nem_kockazatos	kezelheto	kockazatos	magas	atlagos	alacsony	nem_onhatekony	atlagos	onhatekony	nem_radikalis	enyhen_radikalis	radikalis	nagyon_radikalis
szemelyesegi_jegyek	nem_kockazatos																
	kezelheto																
	kockazatos																
eq	magas																
	atlagos																
	alacsony																
onhatekonysag	nem_onhatekony																
	atlagos																
	onhatekony																
szelsonezetek	nem_radikalis																
	enyhen_radikalis																
	radikalis																
	nagyon_radikalis																
zsarolhatosag	nehezen																
	atlagosan																
	konnyen																

Stabil
Átlagos
Instabil

szemelyisegi_jegyek		hiszekeny			naiv			pletykas			lelkiismeretes			baratsagos		
		nem	talan	igen	nem	talan	igen	nem	talan	igen	igen	talan	nem	igen	talan	nem
naiv	nem															
	talan															
	igen															
pletykas	nem															
	talan															
	igen															
lelkiismeretes	igen															
	talan															
	nem															
baratsagos	igen															
	talan															
	nem															
machellizmus	alacsony															
	atlagos															
	magas															

Nem kockázatos
Kezelhető
Kockázatos

zsarolhatosag		titkolt_elteres			fuggoseg			
		kicsit	jobban	nagyon	nem_fuggo	enyhen_fuggo	fuggo	szenvedelyszeruen_fuggo
fuggoseg	nem_fuggo							
	enyhen_fuggo							
	fuggo							
	szenvedelyszeruen_fuggo							
anyagi_helyzet	gazdag							
	kozeposztalybeli							
	szegeny							
	melyszegeny							

Nehezen
Átlagosan
Könnyen

munkahely		munka			korulmenyek			erzelmek			
		jelentektelen	atlagos	kiemelt	kedvezo	semleges	kedvezotlen	pozitiv	semleges	negativ	
kornyezet	kedvezo										Kedvező
	semleges										Semleges
	kedvezotlen										Kedvezőtlen
erzelmek	pozitiv										
	semleges										
	negativ										
fizetes	alulfizetett										
	atlagosan_fizetett										
	nagyon_megfizetett										

munka		pozicio_beosztas				foglalkozas			
		beosztott	also_vezeto	kozepvezeto	felso_vezeto	alacsony	kozepes	magas	
foglalkozas	alacsony								Jelentéktelen
	kozepes								Átlagosan
	magas								Kiemelt
eltoltott_ido	keves_ideje								
	atlagos_ideje								
	regota								

korulmenyek		leterheltseg			frusztracio			tavolsag		bekerules			
		megfelelo	eltero	jelentosen_eltero	alacsony	kozepes	magas	kozel	tavol	nehez	atlagos	konnyu	
frusztracio	alacsony												Kedvező
	kozepes												Semleges
	magas												Kedvezőtlen
tavolsag	kozel												
	tavol												
bekerules	nehez												
	atlagos												
	konnyu												
beilleszkedes	beilleszkedett												
	elfogadott												
	kirekesztett												

erzelmek		lojalitas			elismeres			megbecsules			
		lojalis	semleges	illojalis	elismerik	meghallgatjak	elutasitjak	megbecsulik	semleges	lekicsinyelt	
elismeres	elismerik										Pozitív
	meghallgatjak										Semleges
	elutasitjak										Negatív
megbecsules	megbecsulik										
	semleges										
	lekicsinyelt										
sertetseg	alacsony										
	kozepes										
	magas										

csalad		tulajdonjog_reszesedes			piaci_fizetes			
		sok	keves	apro	magas	atlagos	alacsony	
piaci_fizetes	magas							Nagyon megfizetett
	atlagos							Átlagosan fizetett
	alacsony							Alulfizetett
munkahelyi_fizetes	magas							
	atlagos							
	alacsony							

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretnék köszönetet mondani a témavezetőmnek, Dr. Szádeczky Tamásnak a hihetetlen szakmai és emberi támogatásért, amit kaptam tőle. Hálás vagyok a példamutatásáért és a sok áldozatos munkáért, amivel segített eredményeim elérésében, és az értekezésem elkészítésében. Azt hiszem, nála jobb témavezetőt senki nem kívánhat magának. Nagyon köszönök mindent!

Köszönöm a Biztonságtudományi Doktori Iskola tagjainak és tanáraimnak a szakmai támogatást és a publikálási lehetőségek biztosítását. Külön hálás vagyok Prof. Dr. Rajnai Zoltánnak szakmai és emberi hozzáállásáért, melyet felém tanúsított, és amivel elősegítette folyamatos fejlődésemet. Köszönöm az ügyvivő szakértőinek, Farkasné Hronyecz Erikának és Lévay Katalinnak a rengeteg segítséget, amit kaptam tőlük.

Köszönettel tartozom Dr. Laufer Editnek, akit ugyan csak a doktori tanulmányaim legutolsó szakaszában ismertem meg, de magas színvonalú szakmai segítségére, iránymutatására mindig számíthattam.

Köszönöm Hegedűs Juditnak, Fehér Sándornak és Hegyi Krisztiánnak, hogy megosztották velem a mélyinterjúk során szakmai tudásukat. Hálás vagyok Baittrok Borbálának a kérdőíves kutatásom lehetővé tételében, és köszönöm az ISACA Budapest Chapter és a Hétpecsét vezetőségének, hogy segítették a kérdőívem célhoz juttatását, illetve hálás vagyok minden kitöltőnek, aki megtisztelt véleményével és idejével.

Hálás vagyok a Doktoranduszok Országos Szövetségének, hogy lehetővé tette, hogy megismerjem „Magyarország Koronaékszereit”, a doktorandusz társaimat. Különösen köszönöm a Hadtudományi Osztály 2016-2018-as elnökségének, Dr. Kiss Dávidnak, Dr. Bányász Péternek, Orbók Ákosnak, Berki Gábornak és Gyenei Balázsnak, hogy segítették elnöki munkámat, és barátságukkal, szakmai tudásukkal mellettem voltak. Kiemelt köszönet illeti Berzsenyi Dánielt és Bederna Zsoltot is, akikkel vállat vállnak vetve haladtunk előre a tudományos és szakmai pályánkon.

Köszönöm feleségemnek, Révész Fanninak, szüleimnek, Tóth Erikának és Váczi Mihálynak, a családom többi tagjának és a barátaimnak azt az önzetlen áldozatvállalást, végtelen türelmet, kifogyhatatlan bíztatást és odaadó szeretetet, amivel támogattak az utamon.