

36. Országos Tudományos Diákköri Konferencia

Had- és Rendészettudományi Szekció

Budapest, 2023. április 18-20.

Nemzeti Közszolgálati Egyetem

Rendészettudományi Kar

HIERARCHIKUS FUZZY ALAPÚ KIBERBIZTONSÁGI KOCKÁZATÉRTÉKELŐ MODELL

Jelige: KiberFuzzy

Pályamunka lezárásának időpontja: 2022. április

2023.

Tartalom

1.	Előszó	4
2.	Bevezetés.....	5
3.	Kiberbiztonság és Social Engineering	7
4.	Lágy számítási módszerek – fuzzy logika	11
5.	A fuzzy modell felépítése	17
5.1	Modell felépítése	17
5.2	Szabályozottság alrendszer.....	18
5.2.1	Bemenetek és tagsági függvényeik	18
5.2.2	A kimenet tagsági függvényi	21
5.2.3	Alkalmazott szabály rendszer	21
5.3	Biztonság kontroll alrendszer	23
5.3.1	Bemenetek és tagsági függvényeik	23
5.3.2	A kimenet tagsági függvényi	27
5.3.3	Alkalmazott szabály rendszer	27
5.4	Munkatársak alrendszer.....	29
5.4.1	Bemenetek és tagsági függvényeik	29
5.4.2	A kimenet tagsági függvényi	34
5.4.3	Alkalmazott szabály rendszer	34
5.5	Kockázat besoroló alrendszer.....	36
5.5.1	Bemenetek és tagsági függvényeik	36
5.5.2	A kimenet tagsági függvényi	40
5.5.3	Alkalmazott szabály rendszer	41
5.6	Simulink modell	43
6.	Összegzés	44

7. Irodalomjegyzék	45
--------------------------	----

1. ELŐSZÓ

Az utóbbi évtizedekben a világon és a céges kultúrában is egyre fontosabb szerepet kap a technológia, ezen már nem lepődik meg senki, hiszen a különböző számítástechnikai eszközök több évtizede a mindennapjaink részét képezik. A hordozható és okoseszközök térnyerésének köszönhetően a trend az, hogy egyre több és több okos eszközt használunk. Ezek komplexitása és tudása rohamosan fejlődik, ezzel együtt az ezeket a területeket és eszközöket kihasználni akaró támadók és a kiberbiztonsági szakemberek folyamatos fegyverkezési versenyt vívnak. Mindkét tábor folyamatosan fejlődő módszereket és eszközöket alkalmaz.

A fentiek miatt napjainkban egyre fontosabbá válik eszközeink védelme és a saját informatikai vagy kiberbiztonsági tudatosságunk fejlesztése, például az egyre gyarapodó távmunkalehetőségek miatt. A szervezetek és munkahelyek egyre nagyobb kockázatot vállalnak, ha nem foglalkoznak eléggé munkatársaik és rendszereik kiberbiztonsági szempontból való naprakészen tartásával, folyamatos fejlesztésével.

A dolgozatom témája egy hierarchikus fuzzy modell, ami speciális, bemenetként megadott adatokkal egy cég magasszintű kiberbiztonsági kockázati szintjét méri. A modell egy lágyszámítási módszert használ, az úgynevezett fuzzy logikát, ugyanis ez a módszer az emberi gondolkodás elmosódott határait, a szubjektivitást és a bizonytalanságot nagyon jól tudja kezelni, ami a kiberbiztonság területén, főleg az emberi tényező kezeléséhez szinte elengedhetetlen.

2. BEVEZETÉS

Az informatikai rendszerek napjaink szerves részét képezik – az Eurostat 2021-es felmérése szerint az Európai Unióban a háztartásokban még a legalacsonyabb internethasználati arány is eléri a 84%-ot (Bulgária), az uniós átlag 2020-ban pedig 92% volt. [1] Az egy főre jutó eszközök száma Amerikában 2021-re átlagban 25-re nőtt a pandémia alatt a Deloitte felmérése alapján. [2] 2020 elején a covid-19 vírus sok helyen a munkahelyünket, iskolánkat költöztette otthonunkba, ami meglehetősen új helyzetet teremtett a munkáltatóknak és a munkavállalóknak is. A hirtelen távmunkára váltásra általában nem voltak felkészülve a munkáltatók, így a kiberincidensek is gyarapodtak a nagyvállalatok körében a McAfee és FireEye jelentése szerint. [3] A vállalatok kiberbiztonsági intézkedései a covid-19 vírus miatti változásokkal nem frissültek vagy eleve nem voltak megfelelőek és a pandémia változásai erre erősítettek rá. A kiberbiztonsági incidensek megelőzése és az incidensekre való felkészültség a mai világban meglehetősen fontos a vállalatok számára, legyenek azok kicsi, lokális vagy nagyobb, multinacionális cégek. Ha megfelelően védik az adataikat és érdekeltségeiket, akkor sem biztos, hogy a munkavállalóikat képzik a megfelelő biztonságtudatosságra, pedig napjainkban az emberi tényezőt kihasználó támadások virágkorukat élik, a technológia intenzív fejlődése miatt, amit emberek tömegei nem tudnak vagy nem akarnak követni így egyre átverhetőbbek. A kiberbiztonságban általános nézete, hogy az emberi tényező a leggyengébb láncszem, Bruce Schneier [4] és Kevin Mitnick [5] is referál erre a nézetre könyveikben. Bruce Schneier egyenesen azt taglalja, hogy egy tökéletesen megalkotott biztonságos számítógép hibája az emberekkel való interakcióban rejlik, az hordozza magában legnagyobb veszélyt az emberi hibára alapozva. Bruce Schneier a következőket írta *Secrets and Lies* című könyvében „*People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems*”, ami magyarul annyit jelent, hogy „*Az emberek gyakran a leggyengébb láncszemet képviselik a biztonsági láncban, és nagymértékben felelősek a biztonsági rendszerek meghibásodásáért*”

Az emberi hiba alapvető része a működésünknek, nem tudunk mindig 100%-ban oda figyelni mindenre, viszont egy jól oktatott és képzett munkaerő átlátható technológiákkal kevesebb hibát okoz. Ciarán Mc Mahon díjnyertes pszichológus és kiberbiztonsági tanácsadó cikkében az emberi tényező degradálásáról beszél, hogy az embereket hívjuk a leggyengébb láncszemnek a biztonsági láncban míg ez a hozzáállás, ha csak erre koncentrálunk nem vezet előre, sőt egyenesen káros is a végfelhasználók mentalitására. [6] Mint ahogy az általánosan

használt leggyengébb láncszem is arra utal és Mc Mahon is rámutat, a kiberbiztonság minden esetben több tényezős, bármelyik tényező elhanyagolása hosszútávon kihasználható gyengeséget jelent egy vállalatban. Ennek a gyengeségnek a magasszintű detektálási módjára készítettem egy hierarchikus fuzzy modellt.

Kutatásom célja egy hierarchikus fuzzy modell elkészítése Matlabban a Fuzzy Toolbox és a Simulink segítségével, aminek a funkciója megadott bemenetek alapján egy vállalat kiberbiztonsági kitettségének magasszinten való értékelése az emberi tényezőt kihasználó támadásokra fókuszálva.

A modell létrehozásának előkészítése előtt először a kiberbiztonságnak és a humán tényezőnek kutattam utána tanulmányokban, könyveknek és cikkekben. A dolgozatomban először végig megyek a kiberbiztonság és a fuzzy logika alapjain, ahogy a kutatásomban is tettem, ezután az elkészült modellt ismertetem és végül a modell validálásáról és annak nehézségeiről fogok beszélni.

3. KIBERBIZTONSÁG ÉS SOCIAL ENGINEERING

A Magyarország Kiberbiztonsági Stratégiája a kibertérrel „*A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.*” A kiberbiztonságot a következő képpen definiálja „*A kiberbiztonság 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 kibertérrel megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.*” [23] A kibertérben érkezett támadások megelőzésére és elhárítására szolgál kiberbiztonság. Ezen támadások célja a szenzitív információk elérése, megváltoztatása vagy elpusztítása, pénzszerzés a felhasználóktól, vagy a normális munkamenet akadályozása. A fentiek alapján minden olyan cselekvést és támadási módszert, aminek ez a célja dolgozatomban a kiberbiztonság fogalomkörébe tartozónak vettem.

A vállalati kiberbiztonság tényezőit a támadási fajták általános felosztásával a legkönnyebben jellemezni: A szoftverrel és a hardverrel elkövetett visszaélések; a fizikai támadások; és az emberi tényező kihasználására alapuló támadások [7]. Ezek közül az emberi tényező fejlesztését hanyagolják el leginkább a vállalatok, ugyanis annak sebezhetőségének mérésére általános, könnyen elérhető módszer nem létezik még a piacon. Lehetőségekben gazdag tanulmányok és modellek egyre érkeznek, mint Dr. Váczi Dániel doktori disszertációja egy matematikai modellről, ami szenzitív digitális információszivárgás mérésére alkalmas a humán kockázati tényezőket mérve [8], de még egyik sem annyira elterjedt, mint például a specifikus IT környezeteket értékelő CVSS (Common Vulnerability Scoring System) pontozó rendszer.

A szoftverrel elkövetett visszaélések fogalomkörébe többek között a számítógéppel elkövetett támadások és a vállalat által használt programok sebezhetőségeinek és hiányosságainak kihasználása tartoznak, amiket a támadók ismerve vagy felfedezve kompromittálhatják a céget. A megszámlálhatatlan mennyiségű szoftveres támadási formából csak párat emelek ki most a dolgozat limitációi miatt. Mint például a nulladik napi sérülékenység (zero day vulnerability) olyan kihasználható problémák, amiket még nem

patcheltek¹, avagy javítottak, vagy ha a rendszer nincs rendesen frissítve, nincsen letöltve az a frissítés, amiben a szoftver fejlesztői javították a hibát.

Jelszótörést többféleképpen is végezhetnek a támadók. Olyan szoftverrel, ami próbálgatással igyekszik feltörni a jelszót ez az úgy nevezett brute-force módszer², ami karaktereket fűzve egymáshoz próbálja szoftveresen végig futtatni az összes lehetőséget a belépőfelületen. A jelszó listás módszer, ahol gyakran használt jelszavakat tárolnak és futtatnak végig a szoftverrel hasonlóan, mint a brute-force módszerben. A szivárvány táblás jelszótörés az, amikor jelszavakhoz a hash³ értékeiket kapcsolják hozzá egy nagy táblázatban, ami több terabájt adat is lehet, cserébe a hashelés metódusa miatt nem kell az eredeti jelszót megtalálnia a támadót csak egy olyat, ami ugyan azt a hasht dobja vissza, mint a keresett jelszóhoz tartozik.

Az sql⁴ befecskendezés módszere weboldalak ellen használatos módszer, az oldal beviteli mezőjébe rosszindulatú kód juttatását jelenti, amivel információkat szerezhet, vagy többek között az oldal funkcióiba nyúlhatnak ezzel bele. A túlterheléses vagy szolgáltatásmegtagadásos (DDOS⁵) támadások a hardveri vagy szoftveres limitációkat támadják, a szerverre érkező kérések számának megnövelésével, míg a szerver nem bírja, tovább.

A hardverrel elkövetett visszaélések a vállalat hardveres alapú sérülékenységek kihasználása, vagy azzal való visszaélés, csalás eseteit foglalja magában. Például az alaplap, vagy más eszköz tervezésekor véletlenül vagy direkt benne hagyott sérülékenység kihasználása. Eszközök kicserélése azonosan kinézőre, vagy legalább hasonlóra cseréli a támadó, routernél az adatforgalom megfigyelésére. Figyelemkeltően elhagyott pendriveokkal is előszeretettel támadnak, ezeken kártékony kódot juttathatnak a számítógépre annak csatlakoztatásával. De ide sorolható az is mikor a router és a számítógép közé férkőzik egy eszközzel a támadó Man-In-The-Middle módszerrel és az adatfolyam rajta keresztül továbbítók a két eszköz között.

¹ Patch az informatikai javító csomag, ami a szoftverben kiadás után felfedezett programhibákat.

² Brute-force módszer jelentése nyers erő, ami szisztematikusan próbálgatja a jelszavakat amíg meg nem találja ezzel a kellőt.

³ Hashelés olyan informatikai eljárás amelyikkel bármilyen hosszúságú adatot a megadott hosszúságra képezünk le.

⁴ Struktúrált lekérdező nyelv

⁵ Elosztott túlterheléses támadás

A fizikai támadások, adott helyszín kompromittálásával történik, oda bejutás és ott fizikai tulajdon eltulajdonítás vagy tönkretétel is járhat. Ide tartozik az, ha a vállalatba fizikálisan betörnek, bejutnak a fizikai biztonsági réseket kihasználva. Nem zárt mellékajton, vagy nem megfelelően ellenőrzött bejáraton bejutni.

Az emberi tényező kihasználása a Social Engineering (továbbiakban SE) tudománya, aminek az eszközei emberi természetet manipulálja és használja ki. Ezeket a technikákat kihasználó személy, az ún. Social Engineer, akinek a fő célpontja az információ, egyéb jogosultság és pénzügyi vagy tárgyi javak megszerzése emberek pszichológiai manipulálásával. Sokszor a támadók nem az informatikai környezetet támadják, hanem az ott dolgozó embereket veszik célba. Munkatársnak, esetleg hivatalos személynek adják ki magukat, vagy valakinek, akinek joga van az adott információhoz. Nevezhetjük a meggyőzés tudományának is, hiszen a támadó ráveszi az áldozatot arra, hogy olyan információt osszon meg vele, amihez nincsen jogosultsága. Az ilyen támadások a jóhiszeműsége, a konfliktus kerülésre és a megszokásokra alapoznak [9]. A felkészültebb támadások során megfelelő munkatársakra, vagy személyekre hivatkoznak és a belső szlenget használhatják, ez a támadás legfőbb fegyvere, amely nagyobb sikerességgel is rendelkezik [10].

Az épületbe való bejutásra több módszer is létezik, ami az emberi tényezőt támadja, vagy használja ki. A tail gateing tipikus módszere a Social Engineereknek. Lényege az, hogy úgy jutnak be a támadók egy objektumba, hogy egy csoporthoz csatlakoznak ismeretlenül és velük együtt sétálnak be, vagy egy munkatárs után, aki megtartja nekik a bejáratot. Másik módszer, mikor a beengedő személyzetet veszi rá a támadó, hogy beengedje késést, otthon hagyott beengedő kártyát és kétségbeesést színlelve. Ezek a támadások a megszokásokra, az empátiára, jóhiszeműsége és a segítség nyújtásra való hajlamainkra apellálnak, és ezzel használják ki őket. A Tail gateing a megszokásokra és arra alapoznak, hogy a munkatársainkat beengedik gyakran az emberek maguk után kérdés nélkül is akár. A beengedő személyzethez való fordulással a segítség nyújtásra való hajlamra apellálnak a támadók.

A shoulder surfing az a tevékenység, amikor a támadó az áldozat válla fölött a képernyőről olvas le információkat, vagy a billentyűzetről az éppen gépelt jelszót olvassa le. Ez nyilvános helyen használt számítógépnél, de ATM automataknál is előfordulhat, de ha a támadó már valamilyen módon bejutott az épületbe, akkor a munkahelyen is megtörténhet.

Az SE-re jellemző támadások közé tartozik a phishing, spearphishing és a whaleing támadások. A phishing adathalász támadásokat jelent magyarul és e-mailes, sms-es vagy

chates üzeneteket jelentenek, amik arra irányulnak, hogy a támadó többek között kiadhatja magát információra jogosult személynek, vagy szervezetnek, hogy információt szerezzenek az áldozattól vagy rosszindulatú linkek megnyitására vegye rá, malware fájlt töltsen le az áldozattal, ami lehet vírus (virus), zsarolóvírus (ransomware) vagy billentyűleütést monitorozó program (keylogger) is. Ezek az üzenetek a jóhiszeműségekre alapoznak, és azokat támadják sikeresebben, akik napi szinten e-mailekkel dolgoznak és a monotonitás miatt hamarabb bedőlhetnek egy-egy akár valósnak tűnő támadásnak is. A spearphishing hasonló metodikát használ, mint az adathalász támadás, csak itt a támadó nem nagy tételben általános e-maileket alkalmaz, hanem egy áldozatra specializálja a tartalmat és azt az egy személyt, vagy kislétszámú csoportot akarja valamire rávenni. A célzott adathalász üzenetek előkészítése több időt igényel a támadótól, de nagyobb eséllyel is érhet célba. A whaleing annyiban különbözik az eddigiektől, hogy itt magasabb rangú személyeket próbálnak kihasználni a támadók. Ezeknek a telefonos verzióját vishingnek hívják, de a lényegük mindennek ugyanaz, az áldozatot akarják rávenni információk megadására, vagy egyéb dologra, amik csak a támadó céljainak kedveznek.

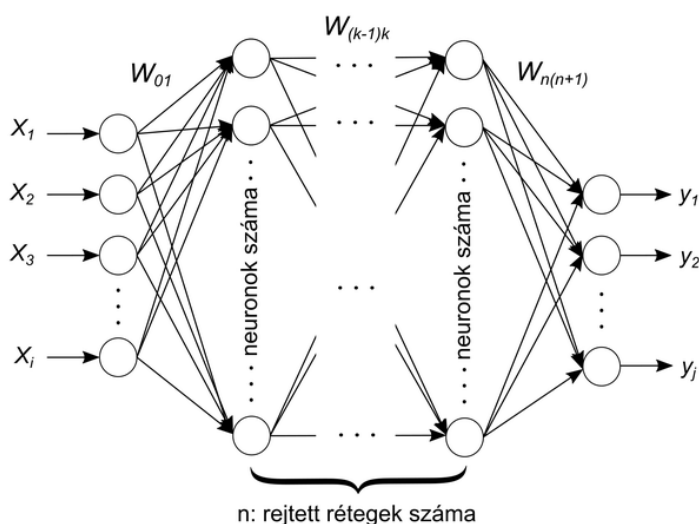
A kuka búvárkodás (dumpster diving) technika a szemét átkutatása az információ szerzése érdekében egy régóta használt és még mindig működőképes SE módszer. Az emberek nagyrésze nem törődik azzal mit is dob ki, és eszébe sem jut, hogy valaki a hulladékba került dolgokat kihasználhatja. Bele sem gondolnak sokan, hogy egy számlából milyen információkat tudnak megszerezni esetleges támadók, pedig rossz kezekben a legkisebb információ is fegyver lehet, akár csak az áldozat bankjának nevéből is szép kis SE támadásokat képezhetnek a támadók. Akár phishingben, akár vishingben kiadhatja magát a támadó, az áldozat bankjának és még ha csak minimális plusz infókat, de plusz infókat szerezhetnek vele. A törölt adathordozókat is kihasználhatják és visszaállíthatják az adatokat megfelelő háttérrel [11].

Az eddig leírt SE támadásokkal szerzett információkkal akár jelszavakat is megpróbálhatnak kitalálni a támadók, sokan alkalmaznak olyan jelszavakat, amiket megfelelő tudással az illetőről kitalálhatók, ilyen információk partner neve, kisállat neve, fontos dátumok és akár fontos hobbik az áldozat életében.

4. LÁGY SZÁMÍTÁSI MÓDSZEREK – FUZZY LOGIKA

A lágy számítási módszerek olyankor kerülnek a képbe, ha kemény számítási módszerek már nem megfelelőek az adott feladatra. A kemény számítási módszerek, amikre jellemző tradicionális rugalmatlanság, egyértelműség és pontosság, míg a lágyszámítási módszerek lehetővé teszik a bizonytalanság, szubjektivitás, pontatlanság és információhiány kezelését, komplex feladatok megoldását [12].

A három leggyakrabban alkalmazott lágy számítási módszer a fuzzy logika, a genetikus algoritmusok és a neurális hálózatok. A genetikus algoritmusok a Darwini evolúciós elmélet inspirálódtak, lehetséges megoldásokhoz jósági függvényeket rendel hozzá, majd ez alapján viszi tovább az egyedeket a következő populációba, a minél magasabb jósági érték elérésére törekedve. A populációk, azaz eredmények a szaporodáson kívül reprodukálódhatnak, kereszteződhetnek és mutálódhatnak. A főcél a legmagasabb jósági függvény elérése, a legjobb megoldás megtalálása érdekében. A másik lágyszámítási módszer a neurális hálózatok, amik egyre nagyobb érdeklődésnek örvendenek a tudományos világban. Az emberi agy kapcsolataira, azaz a neuron kapcsolatokra épül, ebben az esetben egy-egy neuron egyszerű számítási egységek, amikből azonos feladatokat végzők párhuzamosan rétegekbe rendeződnek és a következő szintnek adja tovább az eredményét.



1. ábra: Neurális hálózat kinézete [13]

A dolgozatban tárgyalt modell fuzzy logikával készült a kiberbiztonságban nehezen számszerűsíthető tényezők miatt, hiszen a fuzzy logika tökéletes a szubjektivitás és a pontatlanság kezelésére. Ahogy a neve is mutatja a fuzzy az elmosódott határok kezelésére tökéletes, ami az emberi gondolkodás alapvető jellegzetessége. Egy szemléletes példa a

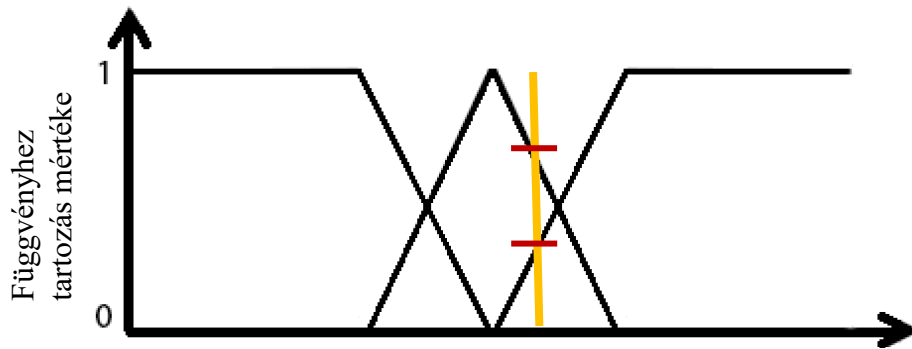
homokkupac probléma, vagyis, hogy mikor lesz homokkupac a homokkupac? Hol a határa, amikor már csak pár szem homokot látunk és nem egy homokkupacot. Vagy mi az az életkor, amitől már valaki öregnek számít? Az emberi gondolkodás nem rendelkezik éles határokkal. Képesek vagyunk egy dolgot több csoportba is bekategorizálni úgy, hogy mindkettőbe tartozik az adott dolog, mégsem tartozik teljesen egyikben sem. A fuzzy logika ennek a szimulálására tökéletes ugyanis a bináris, azaz kétértékű logikát terjeszti ki a keményszámításokban használatos halmazhoz tartozás helyett, a halmazhoz tartozás mértékét definiálva. A halmazhoz tartozást a tagsági függvényekkel reprezentálja és kezeli a bemeneteken egy fuzzy logikát használó modell.

A fuzzy logikai modell bemeneteit fuzzifikálni kell a tagsági függvények segítségével, majd a kiértékelés a szakértői tudást tartalmazó szabályrendszer segítségével történik. Két fő típusa a Mamdani és a Takagi-Sugeno, az első rendszer kimenete a bemenetekhez hasonlóan tagsági függvényeken adja meg a szabálykimeneteket, míg a második rendszer szabálykimenetei ennél változatosabb és kevesebb számítási igényű konstans vagy a bemeneteket tartalmazó függvény lehetnek. A dolgozatomban Mamdani típusú következtetési rendszert készítettem, így annak a felépítését fogom ismertetni.

Mamdani típusú következtetési rendszer lépései [14]:

1. Fuzzifikálás
2. Tüzelési szint meghatározása
3. Implikáció
4. Aggregáció
5. Defuzzifikáció

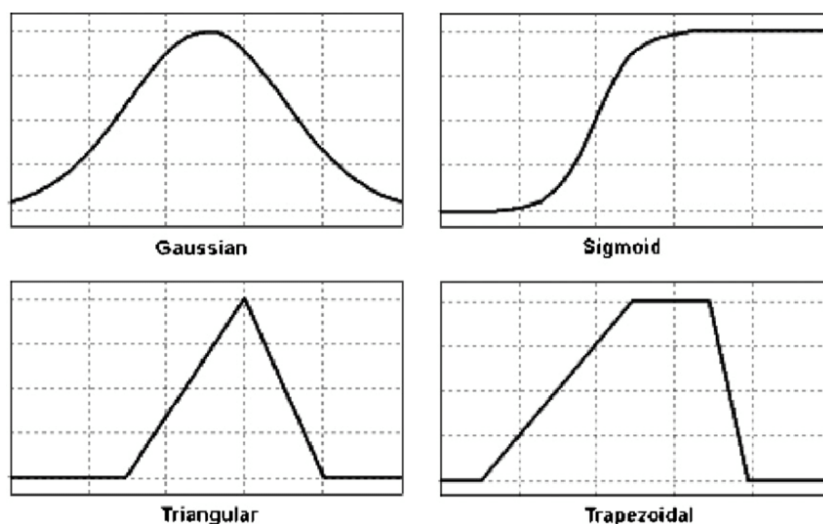
A bemenetekhez, több egymást átfedő tagságifüggvényt rendelünk, ez a 2. ábrán látható. Ahol az egyik tagsági függvény halmazhoz tartozás értéke 1 ott a többinek 0, viszont a 0 és 1 közötti átmeneteken két tagsági függvény fedheti egymást.



2. ábra: Lehetséges fuzzy tagsági függvények sebességre vonatkozóan

A fuzzifikálás az első lépése a fuzzy logikában, amikor a bemeneten kapott értéket a tagsági függvényekre képezzük le és megadjuk annak a halmazhoz tartozás értékét. Például a 2. ábrán látható bemenetek a sárga értéket kapjuk az „x” tengelyen, ami két tagsági függvényt metsz egy-egy pontban a piros vonalaknál. A metszéspontoknak az „y” tengelyen való értéke a tengelyhez tartozás mértéke. Az az ábrán látható bemeneti értékhez a háromszög alakú tagságifüggvényen 0,7 és a jobb szélső trapéz alakún 0,3 halmazhoz tartozási értéket rendelünk.

A 3. ábrán a tipikusan használatos tagsági függvények fajtáit láthatjuk, a gauss függvényt, a szigmoid függvényt, a háromszög és a trapéz függvényt. Míg a gauss és a szigmoid függvények az emberi gondolkodáshoz közelebb állnak a számítási igények miatt a trapéz és a háromszög függvények megfelelő közelítést adnak.



3. ábra: Tagsági függvények fajtái⁶ [15]

⁶ https://www.researchgate.net/figure/Four-types-of-fuzzy-membership-functions-Gaussian-sigmoid-triangular-and-trapezoidal_fig3_230905093

A tüzelési szintben találjuk a szabályokat, amikkel a szakértői tudást tudjuk belevinni a modellünkbe. A szabályok a halmazelmélet általános műveleteit használják, az AND-t (konjunkció), a OR-ot (diszjunkció) és a NOT-et (negáció). Ezek mellett a szabályok, HA [bemenet tagságfüggvénye] AKKOR [kimenet tagságfüggvénye] alapfelépítéssel vannak definiálva. A tüzelési szint a szabályok feltétel részének kiértékelése után kapott érték a bemenetek fuzzifikált értékeinek a megfelelő operátor általi összekapcsolásával.

Az AND kapcsolat modellezésére a fuzzy metszeteket használjuk, melyeket t-normáknak nevezzük, de az egyszerűbb érthetőség kedvéért metszeteknek nevezzük őket továbbiakban a dolgozatban.

Zadeh-féle metszet [16]:

$$t(a, b) = \min(a, b) \quad (2)$$

Algebrai szorzat metszet:

$$t(a, b) = ab \quad (3)$$

Korlátos különbség metszet:

$$t(a, b) = \max(0, a + b - 1) \quad (4)$$

Drasztikus metszet:

$$t_{min}(a, b) = \begin{cases} a & \text{ha } b = 1 \\ b & \text{ha } a = 1 \\ 0 & \text{különben} \end{cases} \quad (5)$$

Az OR kapcsolatot fuzzy uniókkal, az úgynevezett t-konormáknak értékeljük ki, de az egyszerűbb érthetőség érdekében unióknak nevezzük őket a dolgozat folyamán.

Zadeh-féle unió:

$$s(a, b) = \max(a, b) \quad (6)$$

Algebrai összeg unió:

$$s(a, b) = a + b - ab \quad (7)$$

Korlátos összeg unió:

$$s(a, b) = \min(1, a + b) \quad (8)$$

Drasztikus unió:

$$t_{min}(a, b) \begin{cases} a \text{ ha } b = 0 \\ b \text{ ha } a = 0 \\ 1 \text{ különben} \end{cases} \quad (9)$$

Az implikáció a tüzelési szint után képez fuzzy halmazt az adott szabálykimeneten az implikációs operátorokkal részkövetkeztetésképpen. Ha a szabály úgymond tüzelt, akkor az alapján kapjuk meg a szabályba befutó bemenetek alapján a szabálykimenethez tartozó fuzzy halmazt. A kapott részkövetkeztetéseket az aggregációval összegzünk. Több operátorral is végezhetjük ezt a folyamatot, a leggyakrabban használt a minimum és a szorzat operátor.

Minimum implikációs operátor:

$$t(a, b) = \min(a, b) \quad (10)$$

Szorzat implikációs operátor:

$$t(a, b) = ab \quad (11)$$

Az aggregáció az az individuális szabályokból kapott halmaz eredményeket egyesíti, összesíti a kimenetre az aggregációs operátorok segítségével egy halmazzá. [17]. Tekintheünk úgy az aggregációra, ami létrehozza a teljes rendszerkimenetet képviselő komplex eredmény halmazt, amiből, majd az eredményt a defuzzifikáció adja majd meg crisp értékkel az eredményt.

Maximum aggregációs operátor:

$$h(a_1, \dots, a_n) = \max(a_1, \dots, a_n) \quad (12)$$

Korlátos összeg aggregációs operátor:

$$h(a_1, \dots, a_n) = \min(1, \sum_{i=1}^n a_i) \quad (13)$$

Algebrai összeg aggregációs operátor:

$$h(a, b) = a + b - ab \quad (14)$$

A fuzzy logika utolsó lépése a defuzzifikáció, bár a nevéből logikus lenne, de nem inverze a fuzzifikációnak, hanem az aggregáció eredmény halmazából csinál számszerű értéket [14]. Több számítási módszer létezik, amivel az adott problémából kiindulva az aggregáció után kapott halmazt a legjobban tudjuk reprezentálni, mint eredmény. Többek között a Largest Of

Maxima (LOM) a halmaz maximumához tartozó legnagyobb értéket, a Mean Of Maximam (MOM) a maximumhoz tartozó középső értéket és a Smallest Of Maxima (SOM) pedig a legkisebbet adja meg eredménynek. Létezik még a Centre of Area (COA) módszer, ami a halmaz geometriai középpontját adja eredménynek [18]. Ennek a képlete:

$$y_{COA} = \frac{\int_{y \in B^*} y B^*(y) dy}{\int_{y \in B^*} B^*(y) dy} \quad (15)$$

A Bisector (BOA) módszer eredménye a halmazt két egyenlő részre osztja, Ennek a képlete:

$$\int_{\alpha}^{y^{BOA}} B^*(y) dy = \int_{y^{BOA}}^{\beta} B^*(y) dy \quad (16)$$

ahol $\alpha = \min\{y; y \in \text{supp} B^*\}$, $\beta = \max\{y; y \in \text{supp} B^*\}$, és B^* a következtetés.

Említésre méltó még a Centre Of Gravity (COG) metódus, ami a halmaz súlypontját adja meg.

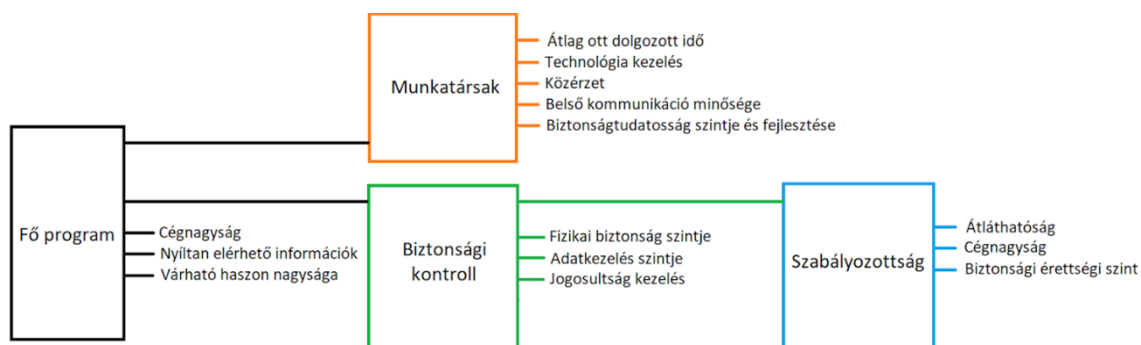
5. A FUZZY MODELL FELÉPÍTÉSE

5.1 Modell felépítése

Az általam javasolt modell hierarchikus felépítésű, ami a könnyű bővíthetőség mellett a szabályrendszer komplexitását is csökkenti. A modell egyes alrendszerei a Matlab Fuzzy Logic Toolbox környezetben készültek, melyeket a Simulink segítségével kötöttem össze. Erről mélyebben a 5.6-os fejezettrészben lesz szó. A különböző szinteken értékelődnek ki a részrendszerek. A modell felépítését a 4. ábra szemlélteti. A rendszer négy értékelő, Mamdani típusú alrendszerből, részrendszerből áll. Ahhoz, hogy a fő kockázati besoroló alrendszer eredményt adhasson, szükség van az alatta lévő szinten elhelyezkedő két rendszer eredményére. A második szinten elhelyezkedő részrendszerek közül a biztonsági kontroll alrendszerének lefutásához pedig a harmadik szinten elhelyezkedő szabályozottsági alrendszerének eredménye is be kell, hogy fusson. Az alrendszerek a következők:

- Kockázati besoroló (fő) rendszer
- Biztonsági kontroll mértéke
- Emberi tényezőkön alapuló kockázat meghatározás
- Szabályozottság meghatározása

Mint előbb olvasható volt, a Szabályozottság alrendszer kimenete befut a Biztonsági kontroll alrendszerbe, majd a Biztonsági kontroll és az Emberi tényezők alrendszer eredménye befut a végső eredményt előállító Kockázat értékelő alrendszerbe, ami figyelembe veszi az előzőek eredményét is.



4. ábra: Egyszerűsített rendszer nézet, a bemenetekkel együtt

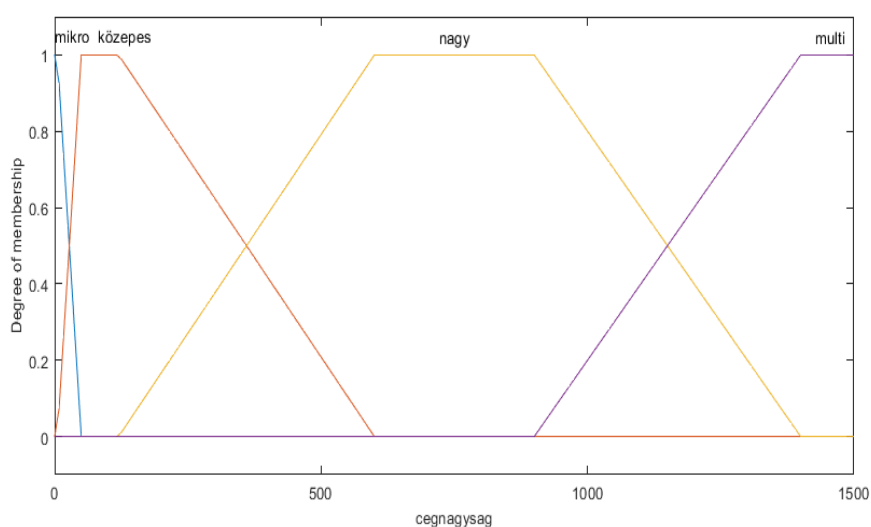
5.2 Szabályozottság alrendszer

A szabályozottság alrendszer vizsgálja azt, hogy adott cégen belül a nagyságához képest mekkora a szervezettség. Figyelembe veszi az átláthatóságot, a cég nagyságát, valamint a biztonságtudatosságot, hogy az alkalmazottak általánosságban mennyire nyitottak az új intézkedések elfogadására, szükségességük megértésére. Ha ezek bármelyik-e hibádzik a szabályozottság egyensúlya sérül.

5.2.1 Bemenetek és tagsági függvényeik

1) Cégnagyság:

A cégnagyság a szabályozottság alprogramba azért került bele, mert ha egy cég nagyobb, akkor ugyanazok a szabályok és munkakörülmények nem ugyanolyan hatással vannak a biztonsági tényezőkre, mint egy 4 fős cégnél, egy 100 vagy akár egy 1000 fős cégnél. Egy kisebb cégnél könnyebben ismerik egymást az alkalmazottak és kevesebb probléma adódhat ebből, mint egy nagyobb cégnél lehetséges.



5. ábra: Cégnagyság tagsági függvényei

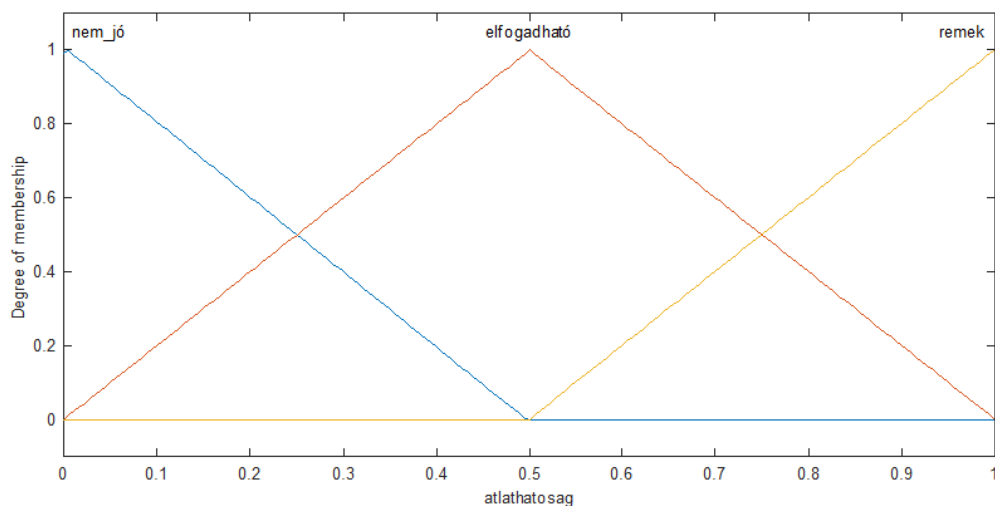
A szabályozottság program második bemenete a cégnagyság, főben megadva az [1, 1500] tartományban, melyet a trapéz alakú tagsági függvények osztanak fel. A *mikro* tagsági

függvény 1 és 5 fő között van, a *közepes* tagsági függvény maximuma 5 és 130 között, a *nagy* függvény maximuma 550 és 900 fő között és a *multi* függvényé pedig 1000 fölött.

2) Átláthatóság:

Az Átláthatóság bemenetben a szervezet működésének és folyamatainak egyértelműséget vizsgálja a modell. A zavaros, nem áttekinthető struktúra minden esetben potenciális veszélyforrás. Ha nem egyértelmű, hogy kinek, mire van jogosultsága, mihez fér hozzá, hol és mikor tartózkodhat, vagy milyen folyamatot hogyan és mikor kell végrehajtani, az zűrzavarhoz vezethet. A zűrzavarban pedig nagyon könnyű elrejtőzni és azt kihasználni.

Ha egyértelműen meg van szabva, hogy ki mihez fér hozzá, és milyen folyamatot, hogyan kell végrehajtani, egy esetleges lopás vagy biztonsági incidens során vissza lehet követni, vagy leszűkíteni a gyanúsítottak számát, hogy ki lehetett az elkövető, vagy kit használtak ki a hozzáférésért. Ennek elavult kezelése súlyos problémát jelenthet egy esetleges támadó megjelenése esetén. [19]



6. ábra: átláthatóság tagsági függvényei

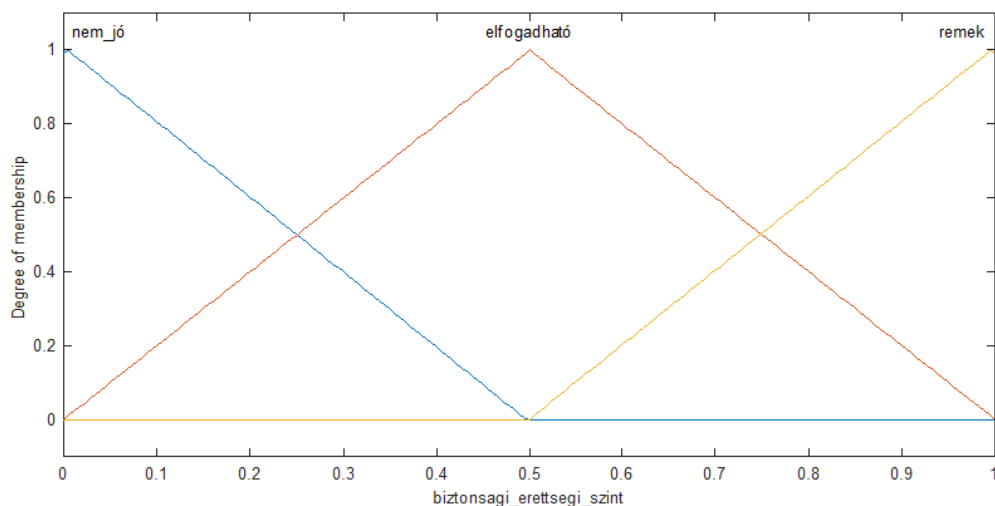
A szabályozottság alrendszer első bemenete az átláthatóság szintjét veszi bele a következtetési rendszerbe. Felépítését három háromszög alakú tagsági függvény alkotja arányosan a nulla és egy közötti tartományban elosztva. A tagsági függvények a *nem_jó*, az *elfogadható* és a *remek* neveket kapták.

3) Biztonsági érettségi szint:

A Biztonsági érettségi szint a Szabályozottság alrendszer harmadik bemenete, a szervezet és a biztonság viszonyát vizsgálja. A munkatársak az újonnan bevezetett biztonsági óvintézkedésekkel szemben gyakran nem túl befogadóak, nehézségként, vagy akár kellemetlen plusz feladatnak élik meg. Emiatt a cég megfelelő hozzáállása nélkül, nem lesznek kifejezetten motiváltak ezen intézkedések betartására,

A csallók mindig új és kreatív módszerekkel próbálkoznak, ezért a cégeknek is javát szolgálja, ha a munkavállalót felkészítik időszakosan ezekre. Például lehet tesztelni a munkatársakat automatikusan generált adathalász emailekkel, amiket, ha nem jelentenek és akár még bele is esnek a csapdába, akkor a cég megfelelő oktatásra küldheti őket.

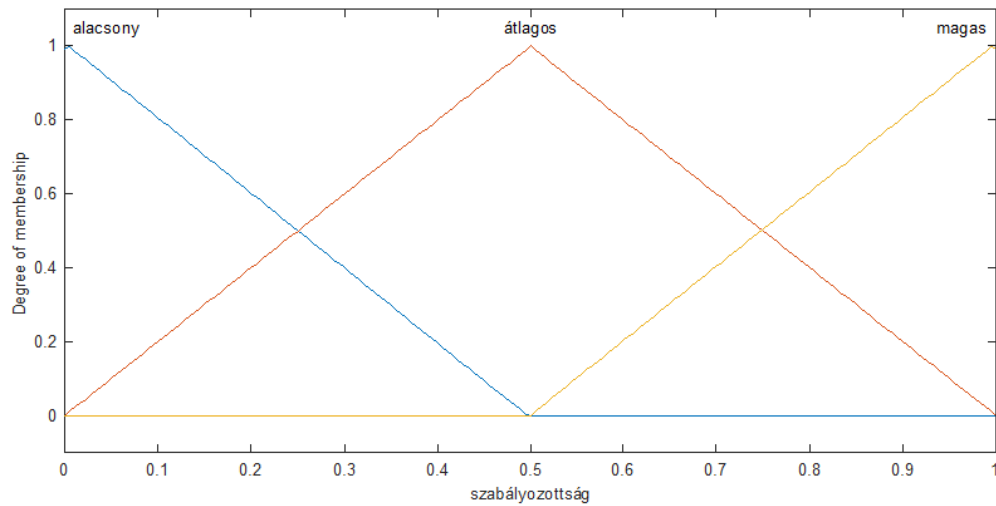
Alapvetően a biztonság viszonylatában elterjedt az a felfogás, hogyha a biztonságot feláldozzuk a kényelem oltárán, az adott vállalat (adott esetben a munkahelyünk) kerülhet veszélybe, vagy szűnhet meg. Ez a hozzáállás hosszútávon javítható, fejleszthető, ebben elvitathatatlan szerepe van a cégnek. Tanfolyamokkal, megfelelő légkör biztosításával, vagy ha más nem segít, megfelelő munkaerő alkalmazásával javítani lehet az érettségi szinten.



7. ábra: Biztonsági érettségi szint tagsági függvényei

A szabályozottság harmadik bemenete a biztonsági érettségi szintet veszi bele a következtetési rendszerbe. Három háromszög alakú tagsági függvény arányosan oszlik meg a nulla és egy közötti tartományban. A tagsági függvények itt is a *nem_jo*, az *elfogadható* és a *remek* neveket kapták.

5.2.2 A kimenet tagsági függvényei



8. ábra: Szabályozottság tagsági függvényei

A szabályozottság alrendszer kimenete a szabályozottság mértéke, amit majd a Simulink segítségével továbbad a Biztonsági kontroll alrendszernek. A kimenet három tagsági függvényen adhat eredményt nulla és egy közötti tartományban, az alacsony, az átlagos és a magas háromszögalakú tagsági függvényeken.

5.2.3 Alkalmazott szabály rendszer

A szabályozottság alrendszer kimenetén a 8. ábrán látható három háromszög alakú tagsági függvényre ad eredményt a SOM típusú defuzzifikáció a 33 súlyozott szabály alapján. A SOM annyit jelent, hogy az eredmény függvény maximumának legkisebb értékét adja meg.

		cégnagyság				Biztonsági érettségi szint		
		multi	nagy	közepes	mikro	remek	elfogadható	nem jó
átláthatóság	remek							
	elfogadható							
	nem jó							
cégnagyság	multi							
	nagy							
	közepes							
	mikro							

9. ábra: A szabályozottság alrendszerhez tartozó szabályrendszer felépítése

Ez a szabályrendszer hivatott arra, hogy reprezentálja a folyamatok szabályozottságának kiértékelését, ezzel megmutatva, hogy *magas*, *átlagos* vagy *alacsony* a mértékük. A szabályok felépítése vizuálisan a 9. ábrán láthatjuk, a vízszintes sorok és a függőleges sorok a bemenetek tagságifüggvényeit reprezentálják, a sorok és oszlopok metszés pontjaiban a tagságifüggvények ÉS (AND) kapcsolata mellett a szabályhoz rendelt kimeneti tagsági függvényt jelenít meg a szín kóddal. A zöld területek jelentik a magas szabályozottságot, a sárgák az átlagosat, míg a piros területek a kedvezőtlen kombinációkat, ilyen esetekben javasolt az átfogóbb vizsgálat a bemeneteken mi is okozza az állapotot.

A szabályok súlyozva lettek, mert a rendszer megfelelőbb eredményeket ad vissza, ha erősebb súllyal vesszük számításba a rosszabb értékeket. Tesztjeim szerint hamarabb és

eredményesebben sorolja a veszélyt a rosszabb kategóriába ilyen szabályrendszer mellett, ami a bemenetek alapján indokolt is. A szabályok súlyozásának alapja, hogy amelyik szabály az alacsony kimenetet adná értéknek, azt 1-es súllyal veszi számításba a fuzzy alrendszer. Ami az átlagos és magas kimenetet adja eredménynek, azok 0,8 súllyal szerepelnek.

5.3 Biztonság kontroll alrendszer

A biztonsági kontroll a szabályozottság alprogram eredményét felhasználva azt vizsgálja, hogy a cég területén mennyire szigorú a különböző adat- és jogosultságkezelési protokollok és a fizikai biztonság szintje. Itt a tényleges szintet vizsgálom, hiszen hiába vannak meg a szabályok, ha nincsenek számon kérve, betartatva. Minden cégnek fontos a biztonsági szint felmérése, tudni kell mi a jelenlegi szintje a munkatársaknak és a szabályoknak, hogy a javítás és felkészülésre legyen lehetőség.

5.3.1 Bemenetek és tagsági függvényeik

1) Fizikai biztonság szintje:

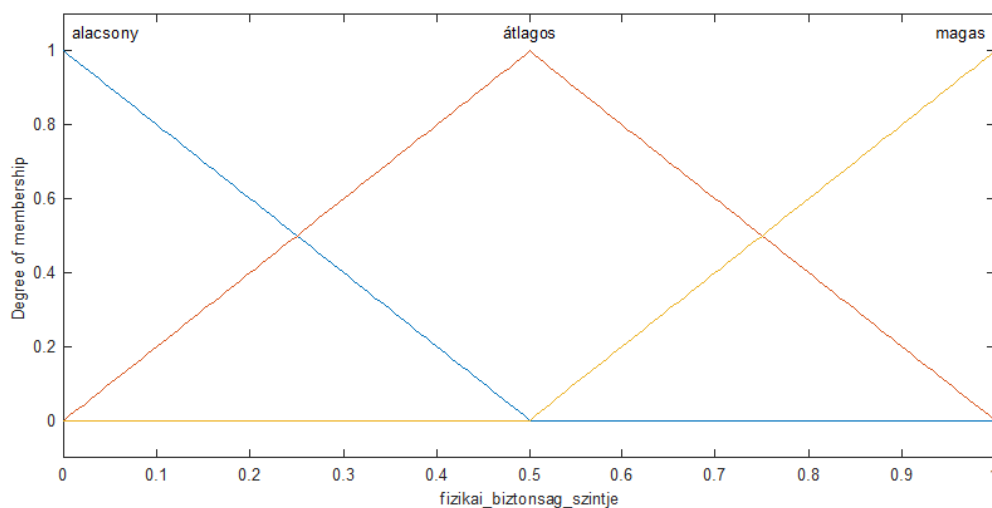
A fizikai biztonság szintje a Biztonsági kontroll első bemenete a cég fizikai védelmi intézkedéseit veszi figyelembe. Van-e jó be- és kiléptetési rendszer, ami segítségével nyomon lehet követni, hogy ki mikor tartózkodott az épületben vagy akár komplex rendszer esetén értékes adatok vagy fizikális értékek közelében. Megnehezítheti a csálók fizikai bejutását. nem számolva a SE módszerekkel való bejutás lehetőségét ebben a bemenetben. Ezen kívül számon lehet tartani, hogy a cég területéről való távozás során potenciálisan ki mit vihet haza, így módon a fizikai adatlopást (pl. hardveres adattárolók eltulajdonítása) meg lehet akadályozni.

Van-e kamerarendszer kiépítve, aminek segítségével lehet rögzíteni és nyomon követni az épületben tartózkodók mozgását. Ellenőrizni lehet vele az épület olyan pontjait, ahol esetleg egy betörő be tudna jutni és a rendszeres személyes ellenőrzése nehezen kivitelezhető lenne (pl. szerelőaknáknak, tetőablakok, tűzlétrák).

Van-e biztonsági személyzet, akik be tudnak avatkozni, ha gyanús személyt és/vagy tevékenységet észlelnek. Jelenlétük elrettentheti a kis stílusú csálókat, a komolyabb támadások ellen persze nem véd a pusztán jelenlétük.

Ezek mellett lehetséges megoldás lehet riasztók beépítése. Segítséget nyújthatnak az illetéktelen behatolás esetén, ráadásul a biztonsági személyzetnek nem is kell közvetlenül jelen lenni (legalábbis nagy létszámban), ha a riasztórendszer élesítve van.

A bemenetet úgy kell megadni, hogy közben figyelembe vesszük, mennyire van rá szükség, mekkora a telephely.



10. ábra: Fizikai biztonság szintje tagsági függvényei

A biztonsági kontroll alrendszer első bemenete a fizikai biztonság szintje, nullától egyig megadva, melyet a háromszög alakú tagsági függvények osztanak fel három részre. A tagsági függvények az *alacsony*, az *átlagos* és a *magas* megnevezéseket kapták.

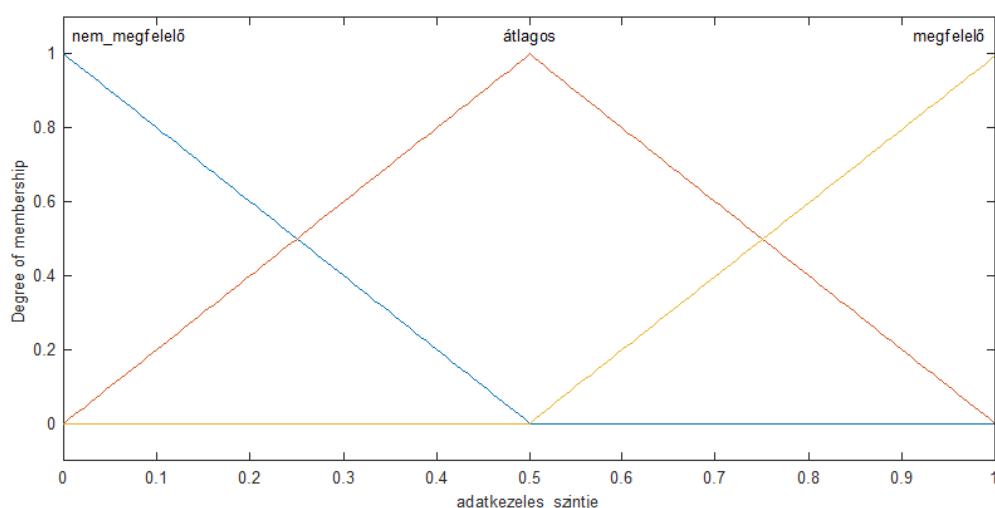
2) Adatkezelés szintje:

Az adatkezelés a Biztonsági kontroll alrendszer második bemenete, amiben azt vizsgálom, hogy a szervezetben a számítástechnikai és fizikai szinten az adatkezelés mennyire megfelelően van kezelve.

Az adatok és az adathordozók védeltségére és megfelelő kezelésére folyamatosan figyelnie kell a dolgozóknak. Még olyan, elsőre talán triviálisnak tűnő dolgokra is, mint a hulladékkezelés érdemes jobban oda figyelni, hiszen a vállalati hulladékokra specializáltan is történtek és történnek SE támadások. A kidobott papírhulladék információt tartalmazhat, így megsemmisítéséről gondoskodni kell, jó ötletnek tűnhet az iratmegsemmisítő használata, de a megfelelő motivációval a támadó azt is helyre állíthatja. Az elektronikus adathordozók semlegesítéséről is gondoskodni kell, ha már nincsenek használatban. Az, hogy törölve lettek a

fileok az adattárolóról nem akadályozza meg, hogy megfelelő szoftverekkel visszaállíthassák azokat illetéktelen kezekben [20].

Az adathordozók munkahelyről elvitele szintén hatalmas kockázatot rejt magában, elvesztés vagy elrablás esetén. Sok esetben még a meghibásodott adathordozóból is lehet adatokat kinyerni, így azok semlegesítéséről is a munkahelyről gondoskodni kell. Mindezek mellett nem csak a munkahelyen kívülre jutott adatok vannak veszélyben; a munkatérben a közvetlen dolgozókon kívül például a takarító személyzet, a karbantartás, vagy akár eltévedt vendég is hozzáférhet a kint felejtett dokumentumokhoz, lezáratlan számítógépekhez, megfelelő szabályozások vagy munkavállalói magatartás hiányában.



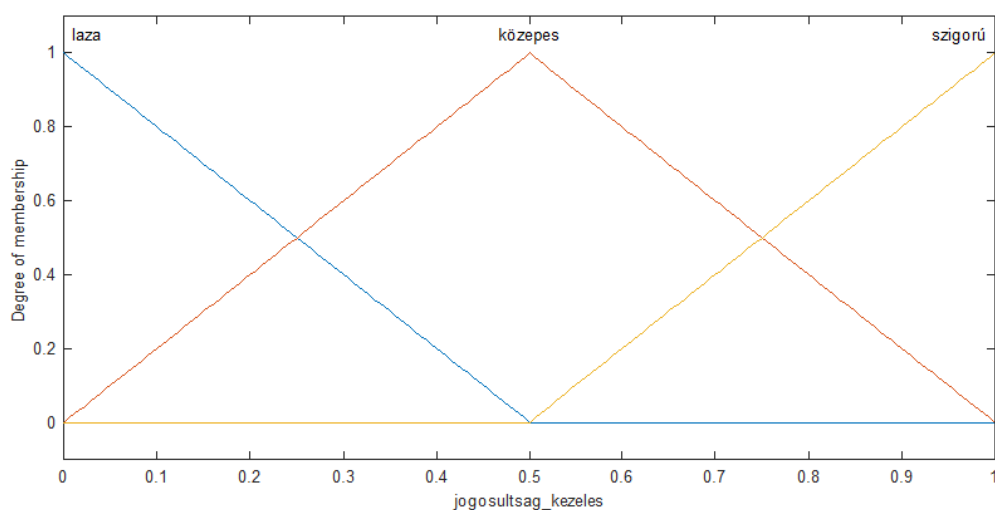
11. ábra: Adatkezelés szintjének tagsági függvényei

A bemenet háromszög alakú tagsági függvényei az *alacsony*, az *átlagos* és a *magas* a nulla és az egy közötti tartományban.

3) Jogosultság kezelés

Az alrendszer harmadik bemenete a jogosultság kezelést veszi számításba, itt főleg az információkhoz való hozzáférések és a számítástechnikai hozzáférések frissen tartását vizsgáljuk. Nem megfelelően kezelt jogosultság kezelésnél, olyan alkalmazottak is hozzáférhetnek bizalmas adatokhoz, akiknek nem lenne szabad, akár a hanyagul kezelt e-mail továbbítások miatt, akár a nem frissen tartott szerver hozzáférések révén. A fölösleges hozzáférések adatokhoz, biztonsági szempontból mindig rizikósok.

Azon kívül, hogy kinek van jogosultsága az egyes meghajtókhoz való hozzáféréshez, vagy fájlok eléréséhez, a kilépett munkavállalók hozzáférési jogosultságaira is különös figyelmet kell fordítani. Inaktivált, de nem törölt fiókon keresztül egy támadó akár a távozott munkatárs segítségével, akár a támadó által a rendszerben felfedezett inaktív, de nem törölt hozzáférésű fiók jogainak kihasználásával is bejuthat a belső rendszerbe. Így a jogosultság kezelés igen fontos probléma, amire külön munkaerőt alkalmazhat a vállalat, vagy nagyobb kiterjedtségnél opció lehet külső szolgáltatás igénybevétele, amit számos cég kínál automatizált megoldást.



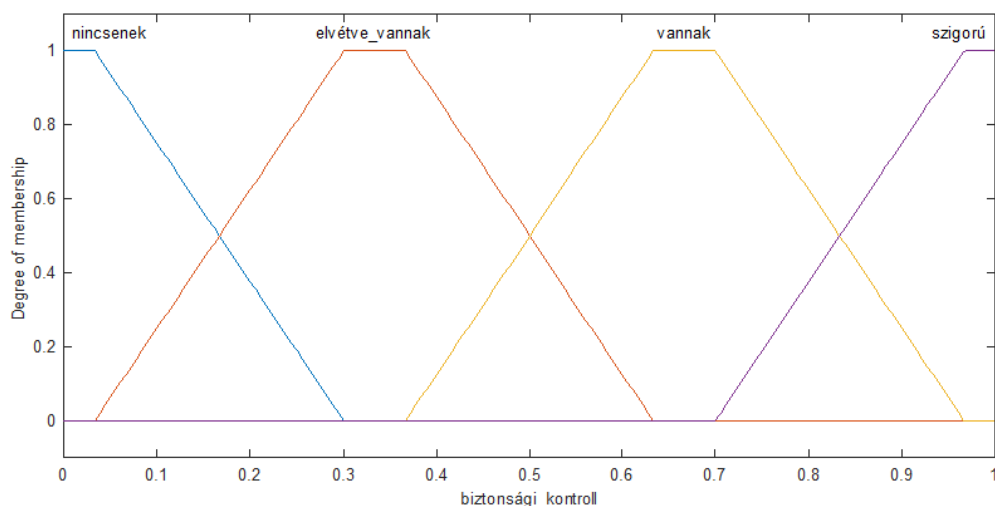
12. ábra: Jogosultságok kezelésének tagsági függvényei

A biztonsági kontroll harmadik bemenete a jogosultság kezelést veszi bele a következtetési rendszerbe. A tagsági függvények háromszög alakúak a *laza*, a *közepes* és a *szigorú* megnevezéseket kapták a nulla és egy közötti intervallumon.

4) Szabályozottság

Az alrendszer negyedik bemenete a szabályozottság alrendszer fentebb leírt kimenetét használja bementként a biztonsági kontroll alrendszerben. Az ott megkapott crisp értéket a Simulink adja tovább itt bemenetnek a Szabályozottság kimenetével azonos tagsági függvényekre.

5.3.2 A kimenet tagsági függvényei



13. ábra: A biztonsági kontroll tagsági függvényei.

A biztonsági kontroll alrendszer kimenete a biztonsági kontroll megállapított szintje, amit majd a Simulink segítségével tovább ad a fő kockázatértékelő rendszernek. A négy trapéz alakú tagsági függvény szintén $[0,1]$ tartományban értelmezhető. A *nincsenek*-től az *elvétve vannak*-on át a *vannak*-on keresztül egészen a *szigorú*-ig adhat vissza értéket a MOM módszer segítségével, ami a defuzzifikációt úgy végzi el, hogy a függvény maximumához tartozó középértéket adja vissza.

5.3.3 Alkalmazott szabály rendszer

A biztonsági kontroll program kimenete a cég biztonsági szabályozottságának mértékét adja meg nullától egyig terjedő skálán, a defuzzifikáció segítségével adja meg a végső crisp értéket az 57 darab súlyozott szabály alapján.

		fizikai biztonság szintje			Adatkezelés szintje			Szabályozottsága		
		magas	átlagos	alacsony	megfelelő	átlagos	nem megfelelő	magas	átlagos	alacsony
jogosultság kezelés	szigorú									
	közepes									
	laza									
fizikai biztonság szintje	magas									
	átlagos									
	alacsony									
Adatkezelés szintje	megfelelő									
	átlagos									
	nem megfelelő									

14. ábra: A biztonsági kontroll alrendszerhez tartozó szabályrendszer

A szabályrendszer itt is hasonlóan épül fel, mint az előző alrendszerben és majd fog a többi alrendszerénél is. Minden tagságifüggvényt összekapcsoltam ÉS (AND) kapcsolattal a többi bemenet tagságifüggvényeivel és a kimeneten a megfelelőt rendeltem hozzá. Ez látszik a 14. ábrán, a sorok és oszlopok metszetében színnel reprezentálva a kimeneten kapott értéket.

Ezen alrendszer esetében 4 féle kimenet fordulhat elő. Zöld akkor, ha a biztonsági kontroll szigorú, citromsárga, ha a cégnek vannak protokolljai, az általam vizsgált bemenetek egy részénél azonban hiányosságok előfordulnak, és további szigorítások lehetnek szükségesek. Narancssárga, ha a cég elvétele rendelkezik elégséges biztonsági szinttel, de sebezhetőségeket könnyű megtalálni egy rosszindulatú behatolás esetén, piros pedig, ha gyakorlatilag nem megfelelőek a biztonsági intézkedések, ha egyáltalán vannak.

A biztonsági kontroll szabályok súlyozása úgy történt, hogy amelyik szabály a *nincsenek* kimenetet adná értéknek, azt 1-es súllyal veszi számításba, ami az *elvétve vannak* kimenetet adja eredménynek azok 0,9 súllyal szerepelnek és ami a *vannak* és a *szigorú* kimenetet adja vissza eredményképpen az 0,8 súlyú.

5.4 Munkatársak alrendszere

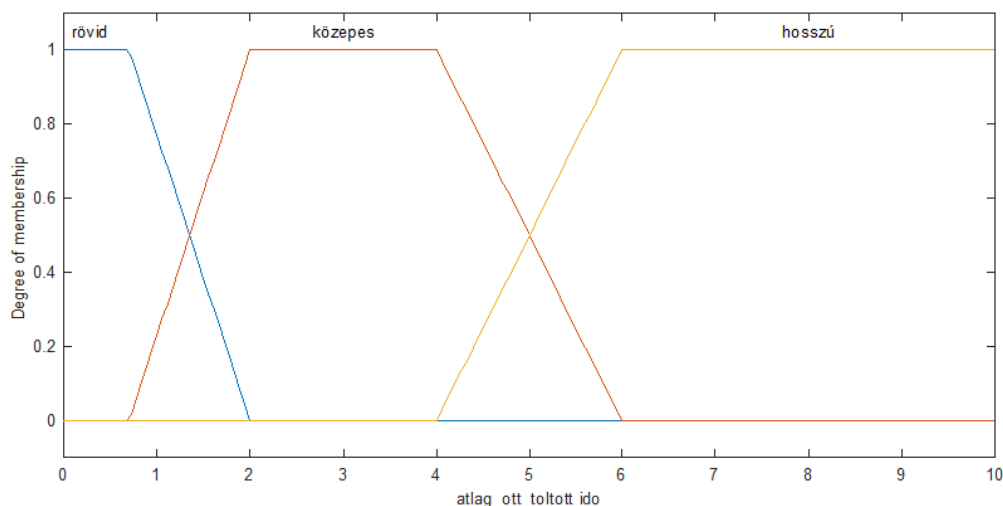
A kiberbiztonságban a legnehezebben kontrollálható és megjósolható elem az emberi tényező. Tulajdonságaink, érzelmeink, amelyek emberré tesznek minket, könnyen kihasználhatók, ha valaki megfelelően él SE módszerekkel, vagy a manipulálás tudományával. A támadók legkönnyebben a naivitást, a lustaságot, a hiszékenységet, a sértettség érzést és a mohóságot használják ki.

A munkavállalóknak képeseknek kell lenniük a fenyegetéseket felismerni, a támadásokat megakadályozni, megelőzni. Mindez azonban nem elég, kellő motiváció híján a munkatársak nem fognak törődni ezekkel a feladataikkal, sőt, ők maguk is potenciális fenyegetéssé válhatnak. Többek között ezeket a szempontokat veszi figyelembe a munkatársak alrendszere, ami a munkatársak biztonságosságát veszi figyelembe átlagban.

5.4.1 Bemenetek és tagsági függvényeik

1) Átlag ott töltött idő:

Az átlag ott töltött idő a munkavállalók átlagos munkahelyen eltöltött idejét veszi figyelembe és vonja be az értékelő rendszerbe. Ha ez az idő kevés, akkor sok a cégen kívüli ember, aki ismerheti a belső információkat/felépítést, illetve az ott dolgozó embereknek több az “ismeretlen arc”, így egy jogosulatlanul a munkahelyen tartózkodó idegent nehezebben vesznek észre. Ezek mellett egy gyorsan változó környezetben kevésbé van meg a csoporthoz tartozás érzése és az emberek kevésbé érznek felelősséget a munkahelyük és munkatársaik jóléte iránt.

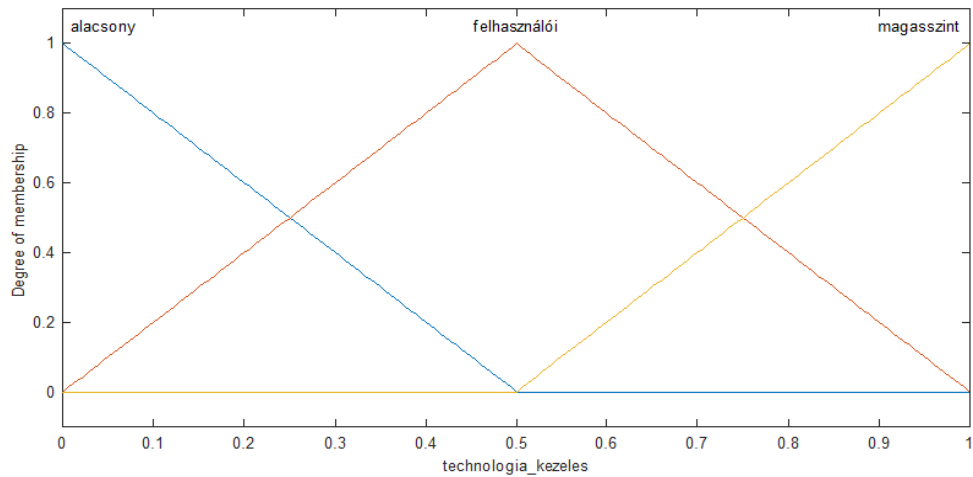


15. ábra: Átlag eltöltött idő tagsági függvényei

A munkatársak alprogram első bemenete a munkatársak átlag cégnél töltött idejét veszi be számszerűen években mérve, a rövid tagsági függvény maximum része 0,8 évig (~10 hónapig) tart, míg a közepes maximum része 2 évtől 4 évig tart, a hosszú idő függvény 6 évtől kezdődik és egészen 10-ig és azon túl tart. A kimeneti eredményen nem változtat, ha a hosszú tagsági függvény maximum részét megnövelnénk 10 fölé, így, ha az érték a fölötte van bőven elég a 10 évet jelölni, ugyanaz lesz az eredmény.

2) Technológia kezelés:

Minden munkavállalónak biztos tudással kell rendelkeznie az általa használt technológiákat és eszközöket illetően. Ha bizonytalanságok lépnek fel felhasználói szinten, hogy egyes technológiákat hogyan kell rendeltetésszerűen kezelni, akkor egy Social Engineer egy rosszindulatú megkörményezés esetén, az adott munkatársat könnyen ráveheti olyan dologokra, amik megkárosíthatják a céget. (pl.: szándékon kívüli szivárogtatás, érzékeny információk kiadása, anyagi kár okozása a munkáltatónak, stb). Egy munkáltatónak mindig prioritás kell, hogy legyen a dolgozók képzése minimum a munkájuk során használt technológiákkal kapcsolatban, így nehezebb lesz őket megtéveszteni.

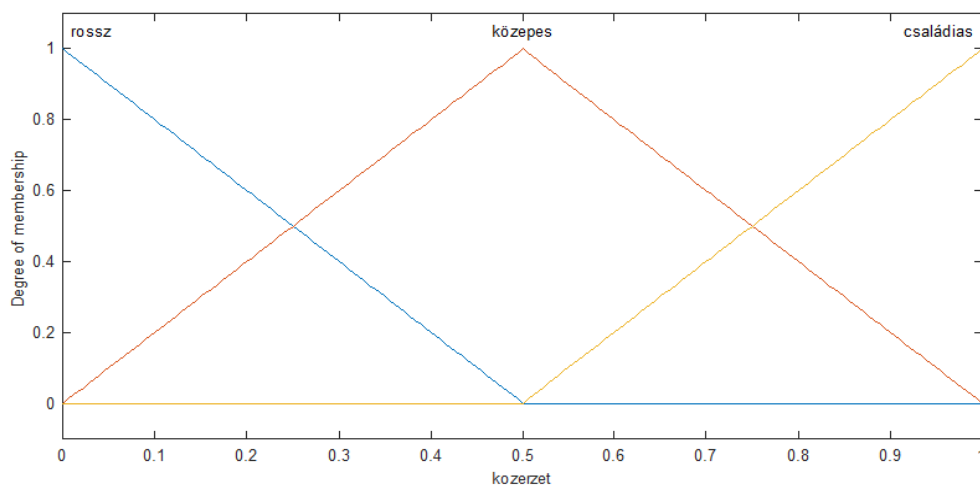


16. ábra: Technológia kezelésének tagsági függvényei

A második bemenet a technológia kezelésének szintjét veszi figyelembe. Az *alacsony*, a *felhasználói*, a *magasszint* tagságifüggvények háromszög alakúak és a nulla és egy közötti tartományban.

3) Közérzet:

A rossz/demotiváló munkakörnyezet nem teszi érdekeltté a munkavállalókat abban, hogy a cég értékeit megvédjék. Extrém esetben a munkavállaló bosszúvágyból járul hozzá a cég pénzének és adatainak ellopásához. A kiközösítés, ami alapvetően negatív irányba befolyásolja a munkavállaló közérzetét, míg a felszabadult, pozitív hangulat, illetve a támogató környezet pozitív irányba tolja ugyanezt.

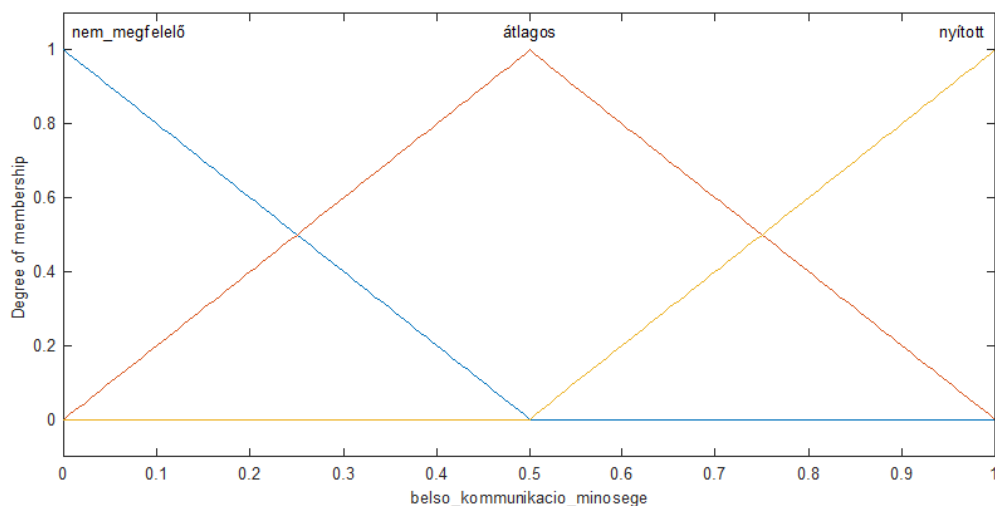


17. ábra: Közérzet tagsági függvényei

A munkatársak alrendszer harmadik bemenete az emberek közérzetét veszi bele a következtetési rendszerbe. Három háromszög alakú tagsági függvény arányosan a nulla és egy közötti tartományban arányosan elosztva a 17. ábrán látható módon.

4) Belső kommunikáció minősége:

A Munkatársak alrendszer negyedik bemenete a belső kommunikáció minőségét veszi bele a következtetési rendszerbe, például egy alacsonyabb rangú személy felé hogyan vannak közölve az információk a felettesei által. Főleg a nyitottságot és a lehetőséget a visszakerdezésre az, amit fontosnak tartok, hiszen, ha a munkavállaló nem kérdezhet vissza a feljebbvalója utasításaira, kéréseire (ebből adódóan a feljebbvalója tényleges kilétére), a feljebbvaló adataival esetleg visszaélő csalo esetlegesen furcsa utasításait is teljesíteni fogja kérdés nélkül. Emellett, ha jó a kommunikáció, családias a légkör, az a munkamorált és a munkahelyhez való tartozás érzését is erősíti, ami elősegíti, hogy a munkavállaló a saját és a cég/vállalat érdekeit is fontosnak tartva jobban odafigyeljen az esetleges támadásokra/támadási kísérletekre és jelentse is azokat.



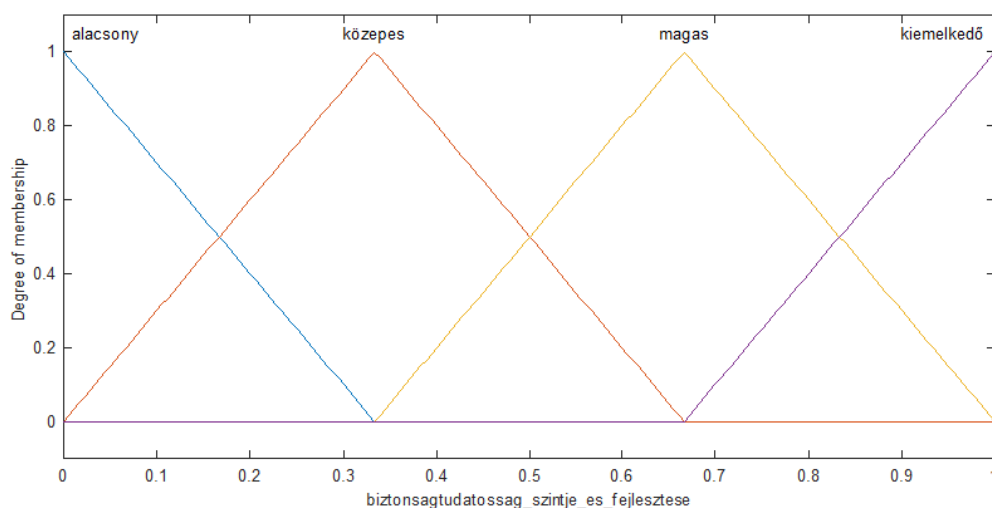
18. ábra: Belső kommunikáció minőségének tagsági függvényei

A *nem_megfelelo*, az *atlagos* és a *nyitott* tagsági függvények háromszögűek és arányosan a nulla és egy közötti tartományban arányosan elosztva a 18. ábrán látható módon.

5) Biztonságtudatosság szintje és fejlesztése:

A munkatársak persze nem csak szándékosan segíthetik a csalókat. Lehetnek felelőtlenek, naivak, vagy csak nincsenek tisztában azzal, hogy a csalók malmára hajtják a vizet. Ha a munkahelyen kívül is összejárnak nyilvános helyen, alacsonyabb biztonságtudatossági szinttel rendelkező munkavállalói körök, szóba kerülhetnek üzleti titkok, belső jellegzetességek. A kényes információkat kihallgatva és kihasználva a csaló észrevétlenül lehet jelen akár fizikailag, akár virtuálisan a cégben, de minimum olyan információkhoz juthat hozzá, amikhez nem lenne jogosultsága. Ilyen összejárások rendszeressége és állandósága a kulcs, ha nincs megfelelő biztonsági tudatosság a munkavállalók körében. Az ebédszüneti közeli gyors éttermes gyülekezés megfelelő alkalom lehet a folyamatos információ kihallgatásra.

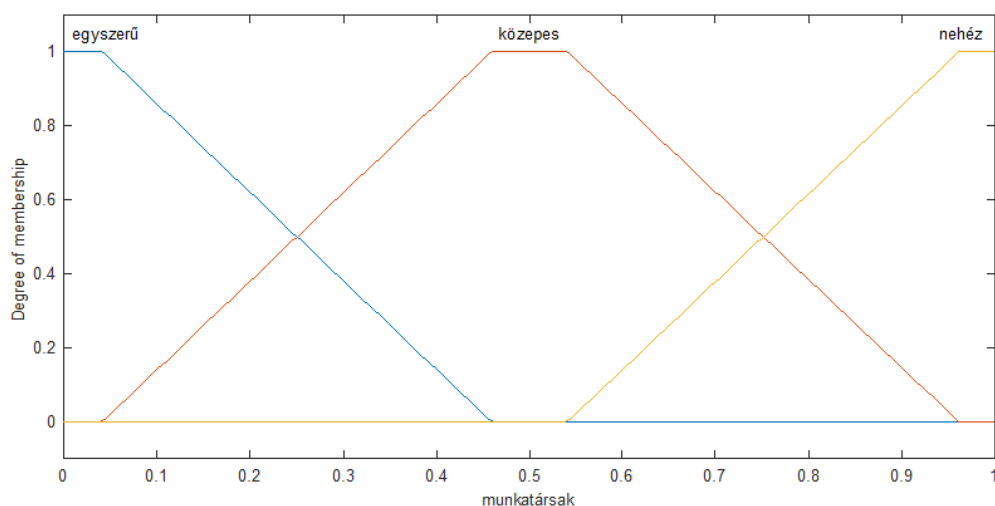
Éppen ezért tájékoztatni kell a munkavállalókat a veszélyekről, és világossá kell tenni, milyen információkat nem szabad kívülállók birtokába juttatni. E célból sok cég titoktartási szerződést írat alá munkavállalóival, amely meghatározza a bizalmas információk körét. A veszélyekről való tájékoztatással munkavállalók megtudják, milyen következményekkel járnak a hibáik, ennek hatására és megfelelő hozzáállással felelősségteljesebben több rálátással tarthatják be a biztonsági intézkedéseket.



19. ábra: Biztonságtudatosság szintjének tagsági függvényei

A biztonság szintje és fejlesztése bemenetet négy háromszög alakú tagsági függvény alkotja a 19. ábrán látható módon, nevezik a nullától az egyig haladva *alacsony*, *közepes*, *magas* és *kiemelkedő*.

5.4.2 A kimenet tagsági függvényei



20. ábra: Munkatársak tagsági függvényei

A munkatársak alrendszer kimenete a munkatársak kihasználtságával kapcsolatban ad vissza eredményt *egyszerű*, *közepes* és *nehéz* trapéz alakú tagsági függvényeken. Ezt az eredményt a Simulink adja tovább a fő kockázat értékelő azonos nevű és kinézetű bemenetének.

A kimeneten a három trapéz alakú tagsági függvény $[0,1]$ tartományban értelmezhető. A MOM defuzzifikációs módszert használtam az alrendszer eredményének kialakításához, ami úgy végzi el a defuzzifikációt, hogy a függvény maximumához tartozó középső értéket adja vissza crisp értéként.

5.4.3 Alkalmazott szabály rendszer

A Munkatársak alrendszer kimenete a munkatársak átverhetőségét adja meg, a 102 darab súlyozott szabály alapján.

		technológia kezelés			közérzet			belső kommunikáció minősége			biztonságtudatosság szintje és fejlesztése			
		magasszint	felhasználói	alacsony	családias	közepes	rossz	nyitott	átlagos	nem megfelelő	kiemelkedő	magas	közepes	alacsony
átlag ott töltött idő	hosszú (5-10 év)	zöld	zöld	sárga	zöld	zöld	piros	zöld	zöld	sárga	zöld	zöld	sárga	piros
	közepes (2-5 év)	zöld	sárga	piros	zöld	sárga	piros	zöld	sárga	piros	zöld	zöld	sárga	piros
	rövid (0,5-1 év)	sárga	piros	piros	zöld	sárga	piros	sárga	piros	piros	zöld	sárga	piros	piros
technológia kezelés	magasszint	fekete			zöld	zöld	sárga	zöld	zöld	sárga	zöld	zöld	sárga	piros
	felhasználói				zöld	sárga	piros	zöld	sárga	piros	zöld	zöld	sárga	piros
	alacsony				sárga	piros	piros	sárga	piros	piros	zöld	sárga	piros	piros
közérzet	családias	fekete			fekete			zöld	sárga	piros	zöld	zöld	sárga	piros
	közepes							sárga	piros	piros	zöld	zöld	sárga	piros
	rossz							piros	piros	piros	sárga	piros	piros	piros
belső kommunikáció minősége	nyitott	fekete			fekete			fekete			zöld	zöld	sárga	piros
	átlagos										zöld	sárga	piros	piros
	nem megfelelő										sárga	sárga	piros	piros

21. ábra: Munkatársak alrendszerhez tartozó szabályrendszer felépítése

Ezen szabályrendszer arra hivatott, hogy megadja, mennyire nehéz a munkatársak átejtése, átverése, kihasználása. Ha a 21. ábrán a bemenetek tagsági függvényeinek találkozásában az érték zöld, az azt jelöli, hogy nehéz kihasználni a munkavállalókat egy esetleges Social Engineer támadással, felkészültek és nehéz őket becsapni. A nehezen kihasználható kategóriába eső munkatársak nagy valószínűséggel nem hajlanak önszántukból a cég megkárosítására, valamint a veszélyekkel és azok formájával is tisztában vannak. A sárga szín a közepes jelzőt kapta, ami közepesre értékeli a munkatársak felkészültségét és átverhetőségét. Míg ahol piros színt látunk, az azt jelenti, hogy relatíve könnyű dolga van a behatolónak. Olyan lehetőségeket “biztosít” többek között a munkavállalók tudatossága, hozzáállása vállalatban, amely nagyban növeli a fenyegetések számát, és nagy valószínűséggel megkárosítja majd a céget, és vagy esetleges ügyfeleit egy SE támadás alkalmával.

A szabályok súlyozása a megfelelő eredmények előállítása érdekében történt, még hozzá úgy, hogy az egyszerű kimenetet értéknek adó szabályt 1-es súllyal veszi számításba, míg ami a közepes és nehéz kimenetet adja eredménynek azok 0,9 súllyal szerepelnek.

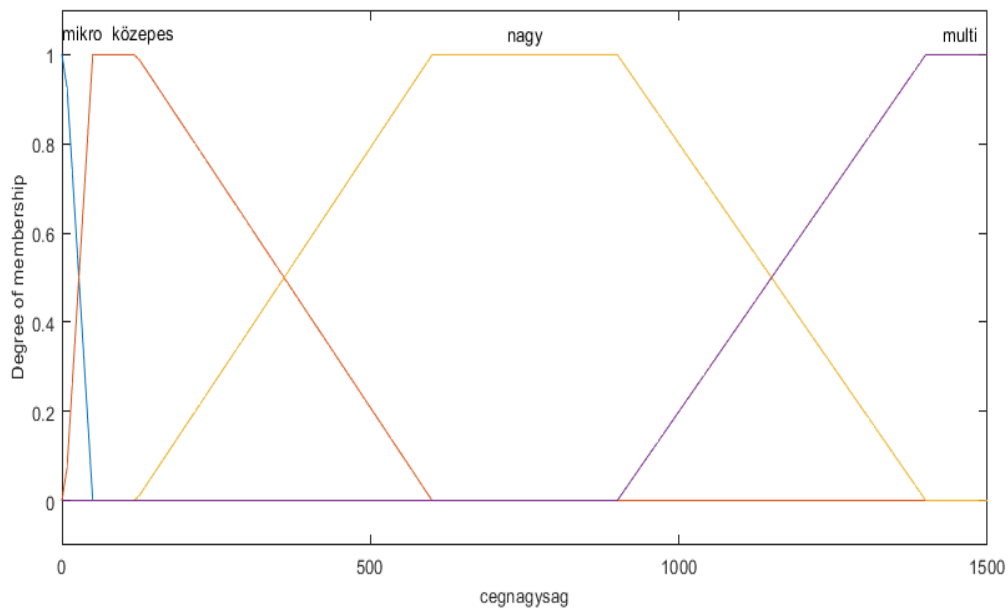
5.5 Kockázat besoroló alrendszer

A vállalatok kiberbiztonsági kockázatának felmérése szakmai munka és az ehhez szükséges a szakmai tapasztalati tudást a szabályrendszerrel integráltam a modellbe. A kockázat besoroló alrendszer a vállalat kockázati szintjét méri és ad eredményt a bemenetei alapján. Ennek az alrendszernek a feladata az eddig kiértékelt alrendszerek és mellette másik két új, valamint egy már használt bemenettel együtt a vállalat kockázati szintjének automatizált meghatározása a Simulink segítségével. Itt már csak két bemenetnek kell értéket adni, az első bemenet értékét már definiáltuk, míg az utolsó kettő bemenet két alrendszer kimenete és azon kapja meg azok értékét. Az eredményből és a bemenetek áttanulmányozásából következtetni lehet arra, hogy min is kell sürgősen javítani a munkatárs fókuszú kiberbiztonsági kockázati szint javításához.

5.5.1 Bemenetek és tagsági függvényeik

1) Cégnagyság:

Korábban a cég nagyságát a szabályozottság programban látható első bemenetnél is vizsgáltam. A tanulmányozott esetek alapján arra jutottam, hogy a nagyobb cégek gyakrabban válnak célponttá. Ha sokan dolgoznak a cégnél, akkor nehezebb észrevenni egy behatolást és a behatolni igyekvő személynek könnyebb kiadni magát egy munkatársnak, mert nem ismer mindenki mindenkit egy bizonyos nagyság után. Valamint nagyobb cég nagyobb potenciális haszonnal is kecsegtet, ezért elsősorban a multinacionális cégeket tartom a legveszélyeztetettebbeknek [21].

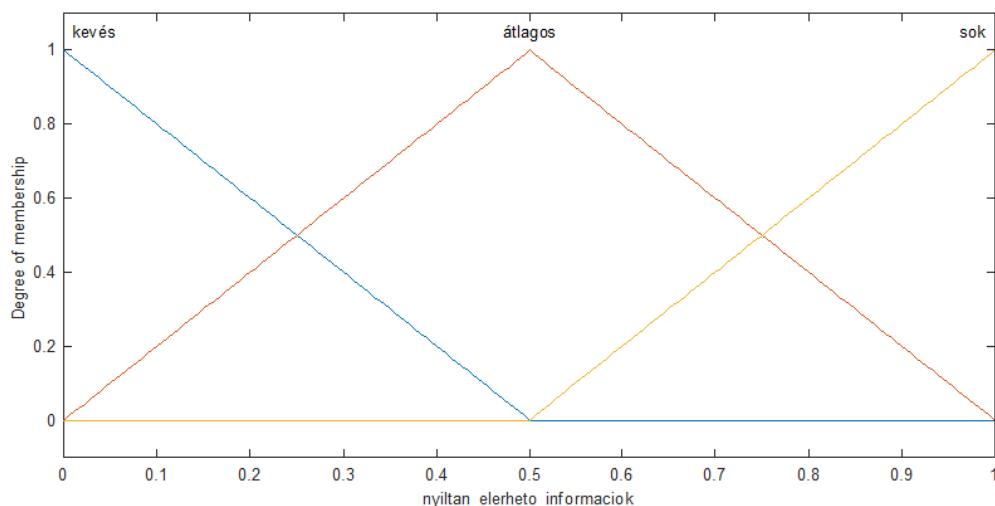


22. ábra: Cégnagyság tagsági függvényei

A hierarchia utolsó szintjén szereplő, végső eredményt előállító alrendszer első bemenete a Cégnagyság, főben megadva az $[1, 1500]$ tartományban, melyben négy trapéz alakú tagsági függvény oszlik el, mint a Szabályozottság alrendszer bemenetén is. A *mikro* tagsági függvény maximuma, ahol a halmazhoz tartozás értéke 1 az 1 és 5 fő között van, a *közepes* tagsági függvény 5 és 130 között, a *nagy* függvény maximuma 550 és 900 fő között és a *multi* függvényé pedig 1000 fölött. Nem indokolt a *multi* tagságifüggvény maximumának 1000 fölé növelése

2) Nyíltan elérhető információk:

Egy nagyobb vállalat több reklámot engedhet meg magának a nagyobb bevétele miatt és érdekében. Ha a cég gyakrabban és több információt oszt meg magáról és termékeikről, jobban kihasználható, hiszen egy jól ismert cég hamarabb kerülhet csálók látókörébe, mint egy kevésbé ismert, és magasabb biztonsági védelmi szintre van szüksége, mint egy ismeretlen vállalatnak. Ha egyszerűbb információt gyűjteni a cégről, működéséről és felépítéséről, az egyben azt is elősegíti, hogy azt egy támadásban felhasználják. Márpedig üzleti érdek a minél több elérhető reklám és információ is, hogy a potenciális ügyfelek/vásárlók minél könnyebben rájuk találjanak.



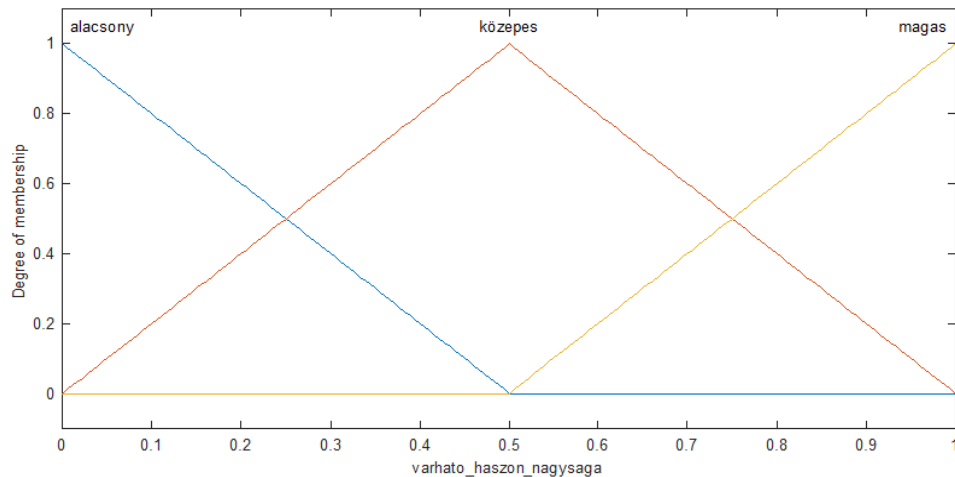
23. ábra: Nyíltan elérhető információk tagsági függvényei

A Kockázati besoroló alrendszer második bemenete a nyíltan elérhető információk mennyiségét veszi bele a modellbe. Három háromszög alakú tagsági függvény a nulla és egy közötti tartományban, nullától egyig a *kevés*, az *átlagos* és a *sok* tagsági függvényen kaphatjuk a bemeneti értékeket.

3) Várható haszon nagysága:

Ugyan a kicsi védtelen cégeket is könnyű támadni, de mivel ezek nagy többségében nem rendelkeznek akkora bevétellel vagy befolyással, hogy megérje egy csalónak a fáradozást. Ezért úgy láttam, hogy a pénzügyi haszon nagyban összefügg a vállalat vagy cég bevételeivel, illetve sikerességével. Ezek alapján egy magas nyereséggel kecsegtető vállalat hamarabb válhat célponttá. Viszont a magas nyereség nem csak a pusztán pénzügyi haszonra értendő, hanem üzleti titkokra, emberek személyes adataira, új találmányokra és technológiákra, dokumentumokra is érthetjük a lehetséges haszon értékét. Ezeket pedig zsarolásra, későbbi támadásokra használhatják, vagy pénzzé is tehetik eladva azokat.

A kapcsolati haszon is motiválhatja a csalókat. A vizsgált esetben a cég-cég, illetve a személyes kapcsolatok használhatóságát vettem figyelembe. A vállalat védelmi rendszerét meg lehet kerülni, akár egy vele kapcsolatban álló, kisebb cégen keresztül is. Csupán információ szerzés miatt is behatolhatnak a cégbe, hogy egy másik, vele kapcsolatban álló céget nagyobb eséllyel tudjanak megtámadni. Ha ez sikerült, akkor a beszállító vagy megrendelő cég nevében is tud kikérni bizalmas információkat.

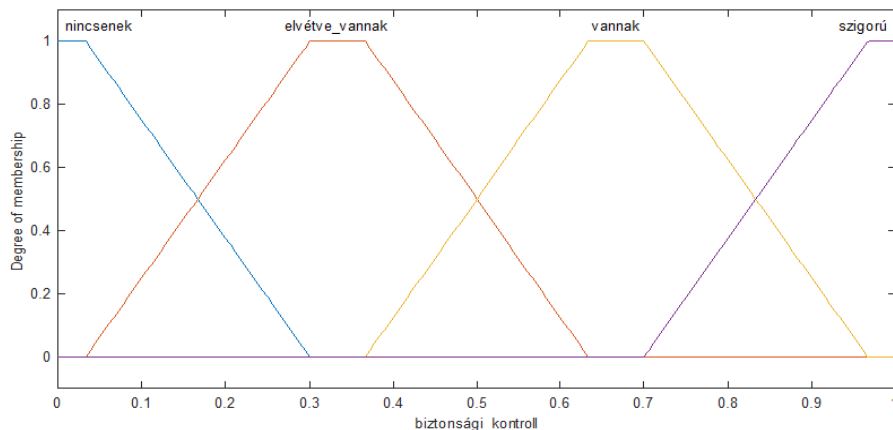


24. ábra: Várható haszon nagysága tagsági függvényei

A főprogram harmadik bemenete a potenciálisan haszonszerzés nagyságát veszi bele a következtetési rendszerbe. Az *alacsony*, *közepes* és *magas* tagságifüggvények háromszög alakúak és arányosan oszlanak meg a nulla és egy közötti tartományban. A tagságifüggvények nevei magától értetődően szubjektív fogalmak világviszonylathoz viszonyítva.

4) Biztonsági kontroll:

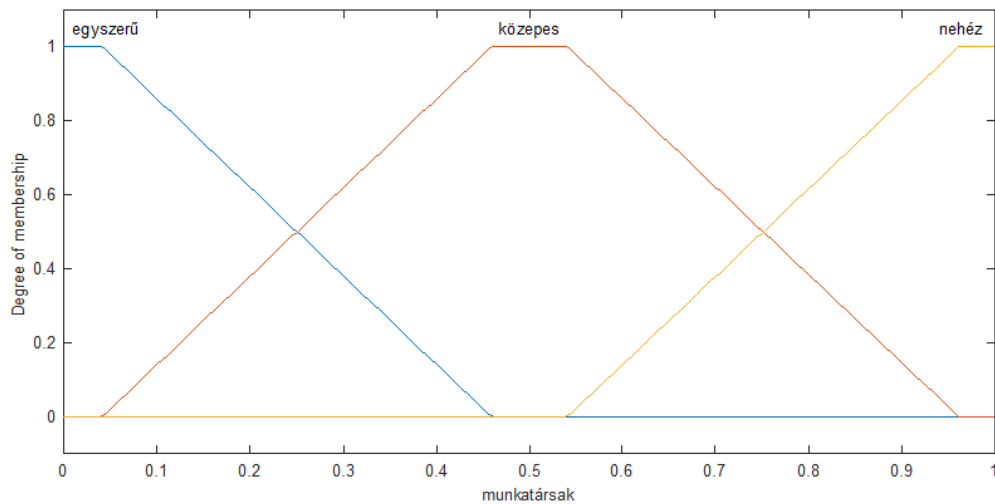
A Biztonsági kontroll bemenet az azonos nevű alrendszer kimenetével egyező tagsági függvényeket használ. Az alrendszer kiementének eredményét a Simulink modell összeköttetése juttatja el a bementre így ez nem egy kézileg megadható érték, hanem az alrendszer bemenetei alapján a szabályok szerint kiértékelt eredmény fut be ide, az azonos tagságifüggvényekkel rendelkező biztonsági kontroll bemenetre.



25. ábra: A biztonsági kontroll tagsági függvényei.

5) Munkatársak:

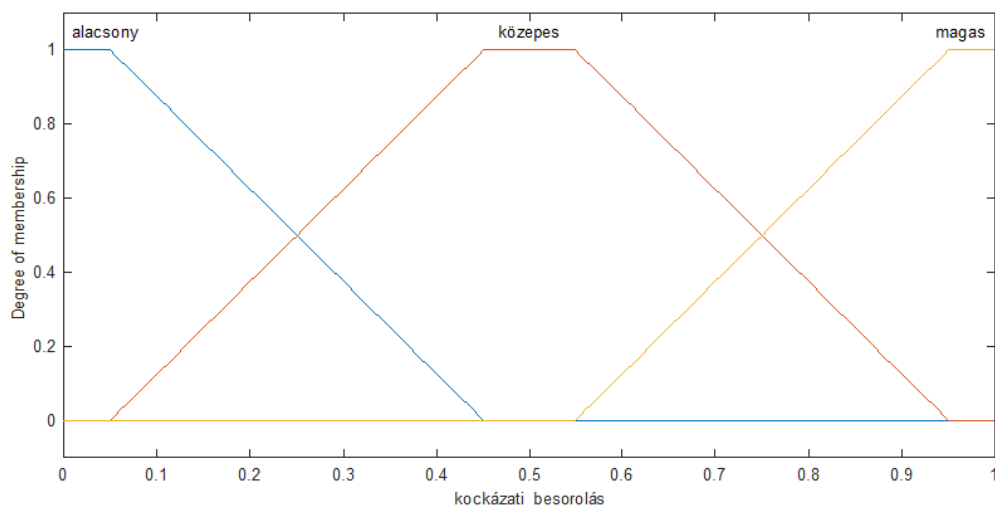
A Kockázati besorolás ötödik bemenete a Munkatársak alrendszer kimenete. A tagsági függvények megegyeznek az ottani kimenettel, és mint az előző bemenet, ennek az eredménye is a Simulink segítségével fut be és ez által kerül a végső értékelő bementére.



26. ábra: Munkatársak tagsági függvényei

5.5.2 A kimenet tagsági függvényi

A kockázati besoroló kimenetén kapjuk meg az eredményt, ami megmondja a vállalat kiberbiztonsági kockázatát a hierarchikus fuzzy modellbe érkező bemenetek kiértékelésével. A kimenet három trapéz alakú tagsági függvény az *alacsony*, a *közepes* és a *magas* kockázatot jelezhetnek előre. A kimeneten kapott értékből lehet következtetni, mennyire kockázatos az adott vállalat. Ha a bemeneteket áttanulmányozzuk, akkor mérlegelni lehet, melyik bemeneti tényező húzza le vagy fel az értéket, a modell bemeneteinek változtatásával.



27. ábra: Kockázati besorolás tagsági függvényei

5.5.3 Alkalmazott szabály rendszer

A cégnagyság, a nyíltan elérhető információk, a várható haszon nagysága, a biztonsági kontroll és munkatársak bemenet értékei alapján a szabályrendszer az aggregáció és a defuzzifikáció alapján kapjuk meg a kimenet értékét. A szabályrendszer megalkotásában figyelembe vettem a kockázat általános képletét [22]

$$\text{Kockázat} = \text{Fenyegetettség} \times \text{Sebezhetőség} \times \text{Nyereség} \quad (17)$$

A *Nyereség* a várható haszon nagysága feleltethető meg, a *Sebezhetőség* a munkatársak és a biztonsági kontroll bemenetekhez hasonlítható, a *Fenyegetettség* meg a cégnagyság és a nyíltan elérhető információkhoz köthetők. Nem pontosan implementáltam az egyenletet, de figyelembe vettem a szabályrendszer elkészítésekor.

A defuzzifikáció a SOM módszer szerint adja meg a végső szám értéket a 115 darab súlyozott szabály alapján. A SOM a defuzzifikáció előtti maximumhoz tartozó értékek legkisebb értékét adja meg.

A három szín jelöli, hogy a megadott bementek tagsági függvényei ÉS (AND) kereszteződésében látható színek jelzik, hogy milyen eredményt ad a konkrét szabály a kimeneten. A zöld szín a táblázatban az alacsony tagságfüggvényt jelenti a kimeneten, azaz relatív biztonságos, a sárga a közepes és a piros meg a magas tagságfüggvényt hívja meg.

Magas érték esetén a vállalat potenciálisan több ponton sebezhető, ki van téve az esetlegesen öt érő támadásoknak, ami ellen nehezen vagy egyáltalán nem tud védekezni jelenlegi állapotában.

A modell pontosságának megőrzése érdekében erősítő szabályt alkalmaztam, amely a biztonsági protokoll alrendszer súlyozását változtatja az adott alrendszer kimenete alapján. “Nincsenek” és “elvétve vannak” kimenetek esetén a súlyozás magas, “elvétve vannak” esetén közepes, és “szigorú” esetén alacsony.

		nyíltan elérhető információk			várható haszon nagysága			biztonsági kontroll				Munkatársak		
		kevés	átlagos	sok	alacsony	közepes	magas	szigorú	vannak	elvétve vannak	nincsenek	nehéz	közepes	egyszerű
cégnagyság	multi													
	nagy													
	közepes													
	mikro													
nyíltan elérhető információk	kevés													
	átlagos													
	sok													
várható haszon nagysága	alacsony													
	közepes													
	magas													
biztonsági kontroll	szigorú													
	vannak													
	elvétve vannak													
	nincsenek													

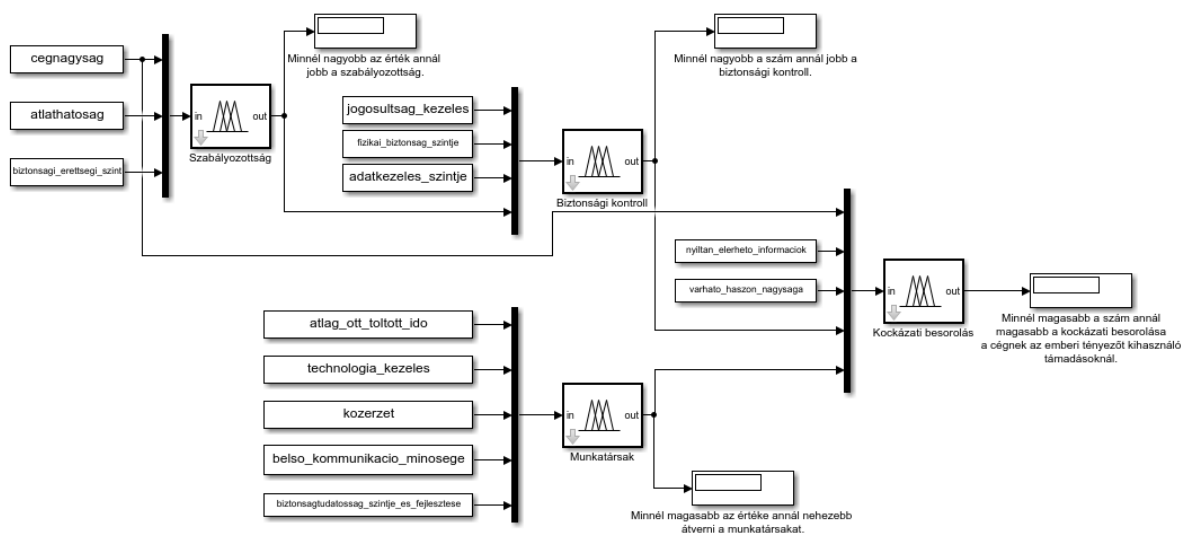
28. ábra: A főprogramhoz alkalmazott szabályrendszer az alábbi ábrán látható.

A szabályok súlyozása úgy történt, hogy amelyik szabály a *magas* kimenetet adná értéknek, azt 1-es súllyal veszi számításba, a *közepes* és *alacsony* kimenetet eredménynek adó szabályok 0,8 súllyal szerepelnek.

5.6 Simulink modell

A Simulink modell négy fajta modullal készült, amik közül a legfontosabb a Fuzzy Logic Controller, ami a fájlnev megadása után a Fuzzy Logic Toolbox-ban felépített modellt implementálja be a rendszerünkbe. A bemeneteket a From Workspace elemekkel tudtam megfelelően a modellbe venni, amik egy bizonyos Mux nevű elemmel tudtam bevezetni a fuzzy logikai egységekbe. Végül az eredményeket és részeredményeket a Display elemet kötöttem a fuzzy logikai egységek kimenetére, amik a végeredményt crisp értékét jelenítik meg.

A 29. ábrán látható módon épül fel a Simulink modell, azon látható a modell hierarchikus rendszer felépítése. A három alrendszer kimenetének a megfelelő bemeneti helyre adását és a negyedik kockázati besoroló alrendszer kimenetének megjelenítését láthatjuk.



29. ábra: Simulinkban a modell gyakorlati felépítése

A bemeneteknek a From Workspace elemekkel adhatunk értéket, amiket, mint a neve is mutatja a Matlab fő munkafelületén adhatunk értéket, ahonnan a Fuzzy Toolbox-ot is meg tudjuk nyitni. Ha minden bemenetnek értéket adtunk, akkor már csak futtatni kell a szimulációt és ki is dobja nekünk a Display elemeken a rész eredményeket és a végeredményt a modell.

6. ÖSSZEGZÉS

A XXI. században a cégeket rengeteg “irányból” érheti támadás. Mind fizikailag, mind virtuálisan fenyegetettségnek vannak kitéve, sőt, a cég munkavállalói is fenyegetést jelenthetnek akár szándékosan, akár akaratlanul. A támadóknak a cég pénzére, adataira, és ügyfeleire fáj a foguk. Ezekre a problémákra léteznek univerzális, minden területre kiterjedő megoldások, azonban a cégek pénzügyei keretei nem végtelenek. Emiatt alaposan átgondolt stratégiát kell alkalmazniuk, és azon területekre kell nagyobb erőforrásokat csoportosítaniuk, ahol a legveszélyeztetettebbek. Ennek a stratégiának a kialakításában segíthet az általam megalkotott magasszintű modell. A fuzzy logika segítségével az egyes kimenetek kétértékű igen-nem logikájánál összetettebb függvényekkel dolgozhatunk, hiszen tagsági függvények segítségével a halmazhoz tartozás mértékét is ki lehet fejezni.

Amellett, hogy a modell jelen formájában jól képes értékelni a megadott bemenetek alapján a cég helyzetét, bőven lehetséges a bővítése több bemenettel és a meglévő bemenetek szétszedésével akár új fuzzy alrendszerekre. Több bemenettel az eddigieknél is részletesebb, pontosabb és átfogóbb képet kaphatunk a cég fenyegetettségéről. A modell tanulópéldának és elnagyoltabb értékelésre tökéletes lehet, de mély és átfogó kép készítésére még tovább fejlesztés szükséges.

A modell átfogó validálására több cég megvizsgálásával és bevonásával lett volna lehetséges, ami ennek a dolgozat kereteibe nem fért bele. A modell átfogó tesztelése a vállalatok helyzetével, a bemenetekkel kapcsolatban, és az előforduló incidensek összevetésével lenne lehetséges, amely információk feldolgozása és kiértékelése után lehetne mélyebben finom hangolni a modellt. A validálás és javítások után az egyszerűbb kezelhetőség miatt, szükség van egy felhasználóbarát kezelőfelület létrehozására is, hogy egyszerűbb legyen megadni az információkat.

7. IRODALOMJEGYZÉK

- [1] Eurostat, Households - level of internet access – (elérés 2022.04.04.)
https://ec.europa.eu/eurostat/databrowser/view/isoc_ci_in_h/default/table?lang=en
- [2] Deloitte: How the Pandemic Stress-Tested the Increasingly Crowded Digital Home – (elérés 2022.04.04.) <https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-pandemic-stress-tested-digital-home.html>
- [3] McAfee, Tis The Season for Holiday Cyber Threats Targeting Enterprises in a Pandemic World (elérés 2022.04.04.) <https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/tis-the-season-for-holiday-cyber-threats-targeting-enterprises-in-a-pandemic-world/>
- [4] Schneier, Bruce, Secrets and Lies: Digital Security in a Networked World. New York, John Wiley & Sons (2000)
- [5] Kevin Mitnick, The art of Deception: Controlling the Human Element of Security. Indianapolis, John Wiley & Sons (2002)
- [6] Ciarán Mc Mahon, In Defence of the Human Factor. *frontiers in Psychology – Cognition* szekció (elérés 2022.04.05.)
<https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01390/full>
- [7] Fehér Krisztián, Kezdő hackerek kézikönyve pp. 31. (2016)
- [8] Dr. Váczi Dániel, doktori disszertáció, Kiberbiztonsági humán kockázati matematikai modell szenzitív digitális információszivárgás potenciáljának mérésére (2021)
- [9] Kevin D. Mitnick, A legendás hacker - A rábeszélés művészete. Budapest: Perfect-Pro Kft., 2003.
- [10] Deák Veronika – A social engineering human alapú támadási technikái
- [11] SecurInfo, Ipari létesítmények fizikai biztonsága, biztonsági zónák kialakítási elvei: <https://www.securinfo.hu/termek/biztonsagi-szolgalat-az-eloero-eszkozei/885-ipari-letesitmenyek-fizikai-biztonsaga-biztonsagi-zonak-kialakitasi-elvei.html>
- [12] Stuart Russell et al, Mesterséges intelligencia, Tananyagbővítés 2005.
- [13] Élet és Tudomány ISSN:0013-6077-1418-1665 (elérés 2022.04.06.)
https://www.eletestudomany.hu/neuralis_halozatok (2016)

[14] Tóthné Dr. Laufer Edit, Fuzzy rendszerek mérnöki alkalmazása, Óbudai Egyetem, (2020)

[15] Rezaee, Reza & Kadkhodaie, Ali & Alizadeh, Pooya. (2007). Intelligent approaches for the synthesis of petrophysical logs. Journal of Geophysics and Engineering. 5. 12. 10.1088/1742-2132/5/1/002.

[16] Gózon Fanni Zsuzsanna, TDK, FUZZY ALAPÚ DÖNTÉSTÁMOGATÓ RENDSZER SZEREPJÁTÉKBAN FELLÉPŐ KOCKÁZAT KEZELÉSÉRE (2020)

[17] Kóczy, T. László, Tikk, Domonkos, Botzheim János, Intelligens rendszerek pp.59 (2007)

[18] Oļegs Užga-Rebrovs, Gaļina Kuļešova, Comparative Analysis of Fuzzy Set Defuzzification Methods in the Context of Ecological Risk Assessment, Information Technology and Management Science, vol. 20, no. 1, pp. 25-29, 2018

[19] Jobline, Céges átláthatóság: Barátkozzunk meg a kellemetlennel (2017) (elérés 2022. 02.09.)https://karrierplusz.jobline.hu/allaskeresok/20171211_Ceges_atlathatosag_baratkozzunk_meg_a_kellemetlennel

[20] Robert M. Weaver, Joseph A. Cazier, Dumpster Diving: A study on data recovery and exploitation, (2007) (elérés 2022.04.05.)
https://www.researchgate.net/publication/272831473_DUMPSTER_DIVING_A_STUDY_ON_DATA_RECOVERY_AND_EXPLOITATION

[21] CSO Big-name companies easy target for social engineers (2011) (elérés 2022. 02.09.)
<https://www.csoononline.com/article/2130028/big-name-companies-easy-target-for-social-engineers.html>

[22] John R. Vacca, Computer and Information Security Handbook (2009), Morgan Kaufmann Publications, pp. 225-231

[23] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiája (2013)