HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 1. szám 117–137.
DOI: 10.32567/hm.2022.1.8

Gózon Fanni Zsuzsanna,[1] Váczi Dániel,[2] Laufer Edit[3]

Hierarchikus fuzzy alapú kiberbiztonsági kockázatértékelő modell

Hierarchical Fuzzy-based Cybersecurity Risk Assessment Model

Az informatikai rendszerek térnyerésével a kibertámadások egyre kifinomultabbá válnak, ami egyre intenzívebb és összetettebb támadásokat tesz lehetővé. A fenyegetettségek forrása szerint megkülönböztethetünk hardver-, szoftver-, fizikai és emberi tényező alapú támadásokat. Tanulmányunkban elsősorban az emberi tényezővel foglalkozunk, hiszen általában a leggyengébb láncszem az ember, de az egyéb cégbiztonságra ható tényezőket is figyelembe vettük. Egy olyan kockázatértékelési modellt dolgoztunk ki, amely képes megjósolni a vállalat kiberbiztonsági kockázati szintjét. A javasolt hierarchikus modellben fuzzy alapú alrendszereket alkalmazunk, hiszen kiberbiztonsági területen az adatokban és a kiértékelési folyamatban gyakran felmerülő bizonytalanságot és szubjektivitást is kezelni kell.

Kulcsszavak: **fuzzy következtető rendszer, kiberbiztonság, humán sebezhetőség, social engineering**

With the rise of IT systems, cyberattacks are becoming more sophisticated, allowing for more intense and complex attacks. According to the source of the threats, we can distinguish between attacks based on hardware, software, physical and human factors. In this study the human factor is in the focus, because humans are the weakest link; however, other factors affecting company security are also taken into account. The authors propose a risk assessment model that can predict the level of cybersecurity risk in a company. In this hierarchical model, fuzzy-based subsystems

[1] Hallgató, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: fanni.zsuzsanna.gozon@stud.uni-obuda.hu
[2] Doktori hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: vaczi.daniel@phd.uni-obuda.hu
[3] Egyetemi docens, Óbudai Egyetem Mechatronikai és Járműtechnikai Intézet Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: laufer.edit@bgk.uni-obuda.hu

are applied, as in the field of cybersecurity, the uncertainties and subjectivity that often arise in the data and evaluation process, must also be addressed.

Keywords: **fuzzy inference system, cybersecurity, human vulnerability, social engineering**

1. Bevezetés

A cégeknek az üzleti kockázat mellett a biztonsági kockázattal is számolniuk kell. Egy érett szervezetnél utóbbi fontossága és kezelésének prioritása megközelíti az üzleti kockázatokét, mivel közvetlen kölcsönhatásban állnak. Egy minél teljesebb körű információbiztonsági szabályzat készítése, annak betartása és betartatása a cég legfontosabb teendői közé kell hogy tartozzon. Nincs százszázalékos biztonság, de az erre való törekvés a cég méretéhez és más, ebben a tanulmányban nem tárgyalt tényezőkhöz mérten szükséges.[4]

A biztonsági kockázatok a támadás vektorát tekintve négy csoportba oszthatók: a hardveres támadások, a szoftveres támadások, a fizikai támadások és az emberi tényezőt kihasználó támadások, más néven a social engineering.[5]

Tanulmányunk tárgya egy egyszerű, nagymértékben a kiberbiztonságra koncentráló fuzzy modell létrehozása volt, amelyben az emberi tényezőre és az ahhoz szorosabban kapcsolható céges biztonsági szempontokra helyeződött a nagyobb hangsúly. Az emberi tényezőt kihasználó támadások már régóta hatékony eszközei a kiberteret használó különböző támadó csoportoknak. Ennek köszönhetően napjainkban a social engineeringet használó támadások súlyossága egyre nyilvánvalóbbá válik az üzleti és állami szférákban egyaránt. Egyre több kutatás foglalkozik ezzel a területtel. Két nagy kategóriába sorolhatjuk a social engineering támadásokat, az emberi és a technológiai alapúakra.[6] E támadások működését nem célunk kifejteni, de pár példát említünk rájuk, ugyanis a modell felépítését a humán alapú támadások és gyengeségek inspirálták.

A social engineering – emberi alapú – támadási módszereknél általában közvetlen kapcsolat van a célszemély és a támadó között, legyen szó akár telefonos, akár személyes esetről. A másik fő csoportba azok a támadások sorolhatók, ahol a különböző technológiák alapvető működési metódusait kihasználva közvetett módon használják ki a támadók az emberek figyelmetlenségét, naivitását vagy éppen technológiai ismereteinek hiányát. A személyes támadások kevesebb emberre tudnak egyszerre hatni, cserébe, ha megfelelő mennyiségű és minőségű információ áll rendelkezésre, hatásosabbak. A technológiai alapú támadások viszont adatgyűjtésre (például phishing levelekkel) ideálisak, általában több emberre képesek egyszerre hatni, és egyes esetekben, ha csak egy áldozatot sikerül átverni, akkor is hasznos információkhoz juttathatja a támadót.

[4] Tamás Szádeczky: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *AARMS,* 19. (2020), 1. 83–93.

[5] William Steingartner – Darko Galine: Cyber Threats and Cyber Deception in HybridWarfare. *Acta Polytechnica Hungarica,* 18. (2021), 3. 25–45.

[6] Fatima Salahdine – Naima Kaabouch: Social Engineering Attacks: A Survey. *Future Internet,* 11. (2019), 89. 1–17.

Fontos megjegyezni azonban, hogy a social engineeringet nem csak rossz szándékkal használják. Christopher Hadnagy a *The Art of Human Hacking* című könyvében kiemeli, hogy mindenki használja ezeket a módszereket, csak a mögöttes szándék más és más.[7]

Az általunk alkotott modell a fuzzy logikára épül. Ez a megközelítés ilyen területen rendkívül előnyös annak köszönhetően, hogy megfelelően tudja kezelni az éles határokkal nem rendelkező, nehezen számszerűsíthető értékeket.[8] Mind az emberi gondolkodás, mind a kiberbiztonságban a fenyegetettségek kérdése jól modellezhető ilyen módon, hiszen a vizsgált tényezők esetén nincs egy általánosan elfogadott vagy törvényszerű határ, ami a fuzzy megközelítésben alkalmazott tagsági függvények segítségével jól kezelhető, így a kiértékelés megfelelő eredménnyel szolgál.

A cikk további felépítése a következő: A 2. fejezetben a modell felépítését mutatjuk be a hierarchikus rendszer modellből kiindulva, ábrázolva az egyes alrendszerek kapcsolódását, valamint a főbb bemeneti tényezőket. Ezt követően az egyes alrendszerek részletezése következik az alkalmazott fuzzy halmazok, valamint szabályrendszer illusztrálásával. A 3. fejezetben a modell alkalmazhatóságát mutatjuk be egy fiktív cég elemzése által. Végezetül a 4. fejezetben foglaljuk össze az elért eredményeket, valamint a továbbfejlesztésre teszünk javaslatot.

2. A modell felépítése

A javasolt modell négy Mamdani-típusú alrendszerből épül fel, a *Szabályozottság,* a *Biztonsági kontroll* és a *Munkatársak* alrendszerek alkotják, amelyeket a hierarchia utolsó szintjén a *Kockázat besoroló* fog össze és adja meg az eredményt. A rendszer komplexitását és egyszerű bővíthetőséget az 1. ábrán szemléltetett hierarchikus felépítés segíti elő.

A szakértői tudást a szabálybázison keresztül vittük be a rendszerbe, ahol az egyes szabályok felépítése a következő:

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

ahol $A_{j,ij}$ a j-edik bemenethez tartozó i_j-edik fuzzy halmaz, $i_j = 1, \ldots, n_j$, n_j a j-edik bemenethez tartozó fuzzy halmazok száma.

A szabályok kiértékelése során az aggregációt a sum (1), a defuzzifikációt pedig a bisector (2) módszerrel végeztük.

[7] Christopher Hadnagy*: Social Engineering: The Art of Human Hacking.* Hoboken, Wiley, 2011. 22–27.

[8] László Pokorádi: Fuzzy Techniques in the Aircraft Engineering. In Zobory I. (szerk.): *Proceedings of the 7th Mini Conference on Vehicle System Dynamics, Identification and Anomalies.* Budapest, BME Vasúti Járművek Tanszék, 2001. 443–448.

$$y = \frac{\sum_{i=1}^{n} w_i y_{B_i}}{\sum_{i=1}^{n} w_i} \tag{1}$$

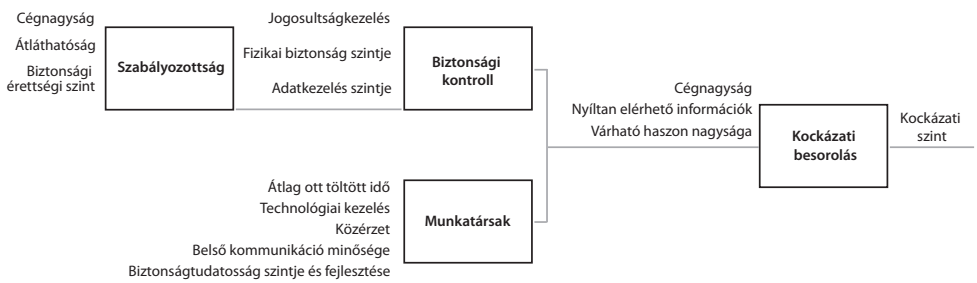
ahol n a szabályok száma, w_i az i-edik szabály tüzelési szintje, Y_{B_i} annak mértéke, hogy az adott szabálykimenet milyen mértékben játszik szerepet a végső döntésben.

A bisector módszer a görbe alatti területet két egyenlő részre osztja:

$$D = P_k \cdot K_{gy} \cdot \frac{s}{v} \tag{2}$$

ahol $\alpha = min\{y;\ y \in \mu_A\}$, $\beta = max\{y;\ y \in \mu_A\}$. A két egyenlő részt képező függőleges vonal $y = BOA$ az $y = \alpha, y = \beta, z = 0$ z $= \mu_A$(y) esetén.

A fuzzy alrendszereket Matlab Fuzzy Logic Toolbox környezetben építettük fel, és az egyes alrendszereket Matlab Simulink segítségével kötöttük össze.



1. ábra: A rendszer felépítése
Forrás: a szerzők szerkesztése

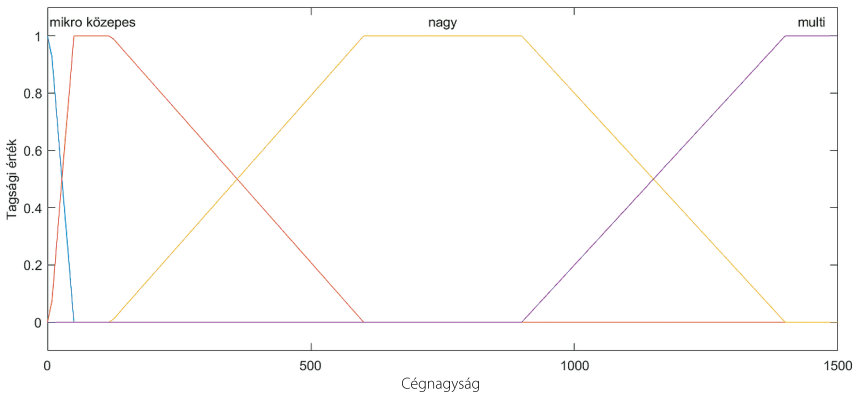
2.1. Szabályozottság alrendszer

A *Szabályozottság* alrendszer a cég szabályozottságát és annak alaptényezőit vizsgálja, értékeli, a cég nagyságát figyelembe véve.

2.1.1. Bemenetek

Az első bemenet a *Cégnagyságot* veszi figyelembe. Ez a tényező azért fontos, mert a különböző méretű cégeknél más körülmények és szabályok/szabályozások eltérő mértékben lehetnek megfelelők. Például egy kisebb méretű szervezetnél mindenki ismer mindenkit, így egyes támadási technikákat nehezebb hatékonyan alkalmazni esetükben, akár kisebb biztonsági érettség mellett is.

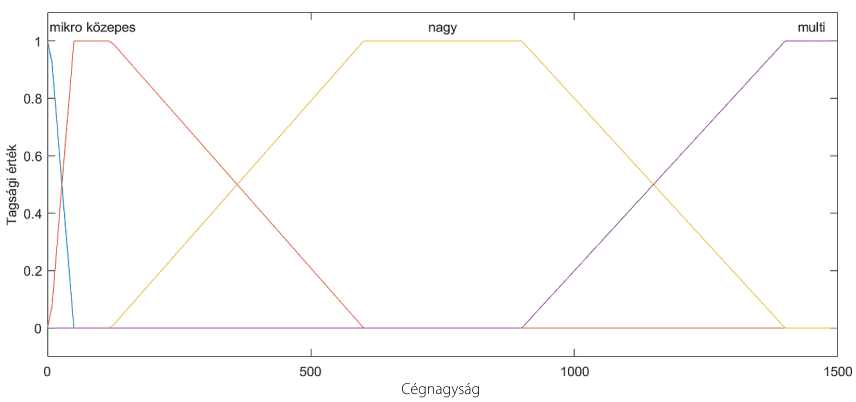
A 2. ábrán látható *Cégnagyság* bemenet tagsági függvényei trapéz alakúak, a bemenet mértékegysége [fő]. A négy tagsági függvény a *mikro,* amely 1 és 5 között veszi fel a maximális értéket, míg a *közepes* értéke 50 és 130 között, a *nagy* értéke 600 és 900 között, a multié pedig 1300 fölött a tartomány végéig, 1500-ig maximális. Ha ennél többen dolgoznak a cégnél, az a modell esetében nem okoz változást, hiszen ez is a multi kategóriába sorolható 1 tagsági értékkel.



2. ábra: Cégnagyság bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

Az *Átláthatóság* bemenet a cég folyamatainak és működésének átláthatóságát vizsgálja belső szemszögből. Ugyanis hiába vannak meg a szabályok és az elvárások, ha nem átláthatók, esetlegesen ebből következően nem betarthatók.

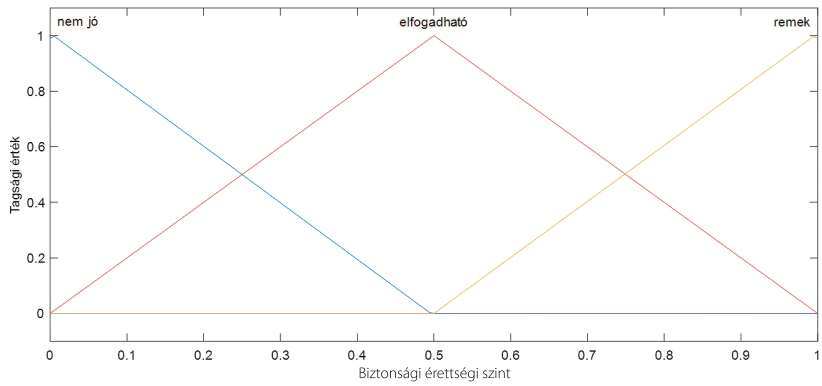
A bemenetet lefedő tagsági függvények a 3. ábrán láthatók, három háromszög függvény formájában, ahol a bemenet értéke a [0,1] intervallumbeli értékkel adott. A függvényekhez rendelt nyelvi jellemzők a *nem jó,* az *elfogadható,* és a *remek.* Az érték növekedésével növekszik a cég szabályozottsága, mint az ábrán is látható.



3. ábra: Átláthatóság bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *Szabályozottság* alrendszer utolsó bemenete a cég *Biztonsági érettségi szintjét* vizsgálja, ami a cég biztonsághoz való hozzáállását méri fel, mennyire tartja azt fontosnak, mennyire ügyel rá és tartja frissen az ilyen irányú ismereteit.

A *biztonsági érettségi szint* három tagsági függvénye háromszög alakú, az értelmezési tartomány [0,1] között van, ahol a nagyobb értékek magasabb érettségi szintet jelölnek. A nyelvi jellemzők: *nem jó, elfogadható, remek,* ahogy az a 4. ábrán is látható.

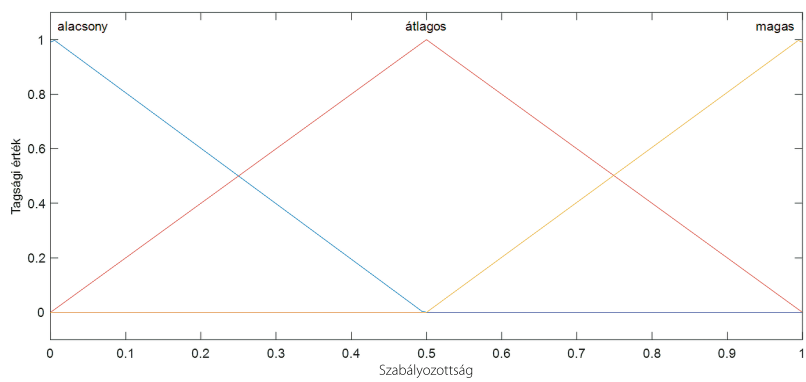


4. ábra: Biztonsági érettség szint bemenet tagsági függvénye
Forrás: a szerzők szerkesztése

2.1.2. Kimenet és szabályok

A cég szabályozottságának meghatározása súlyozott szabályok alapján történik. Az így előállított érték a *Biztonsági kontroll* alrendszerbe fog befutni, ugyanezeket a tagsági függvényeket alkalmazva.

A *Szabályozottság* értéke [0,1] tartománybeli értéket vesz fel, amelyet háromszög alakú függvények fednek le: *alacsony, átlagos, magas.* Ebben az esetben is az érték növekedésével növekszik a szabályozottság megfelelősége.



5. ábra: Szabályozottság kimenet tagsági függvényei
Forrás: a szerzők szerkesztése

A kimenetet 33 súlyozott szabály segítségével határozzuk meg. A súlyozás a rosszabb kimeneteket eredményező szabályokat nagyobb súllyal veszi figyelembe, mint a magas kimeneti értéket. Ezt a súlyozást alkalmaztuk a többi alrendszerben is.

Az alkalmazott szabályok páronkénti vizuális reprezentációja a 6. ábrán látható. Az oszlopok és a sorok találkozásában található a kimeneten kapott tagsági függvény jelölése. A piros szín az alacsony, a sárga az átlagos, a zöld pedig a magas kimeneti értéket jelöli, az egyes négyzetekbe írt számok pedig az adott szabály súlyát jelölik a kiértékelés során.

		Cégnagyság				Biztonsági érettségi szint (nyitottság, befogadó-készség)		
		multi	nagy	közepes	mikro	remek	elfogad-ható	nem jó
Áthatóság	remek	0,8	0,8	0,8	0,8	0,8	0,8	0,8
	elfogad-ható	0,8	0,8	0,8	0,8	0,8	0,8	1
	nem jó	1	1	1	0,8	0,8	1	1
Cégnagyság	multi					0,8	0,8	1
	nagy					0,8	0,8	1
	közepes					0,8	0,8	1
	mikro					0,8	0,8	0,8

6. ábra: Szabályozottság szabályai
Forrás: a szerzők szerkesztése

2.2. Biztonsági kontroll alrendszer

A *Biztonsági kontroll* alrendszer a cég biztonsági szabályozottságát vizsgálja, amelybe beleértjük a jogosultságkezelést, a fizikai biztonságot és az adatkezelést, valamint ezek mellé fut be a szabályozottság alrendszer kimenete is.

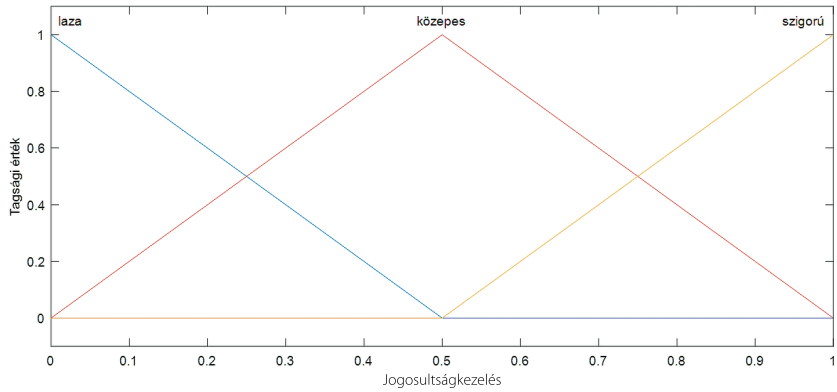
Az alrendszer szerepe a cég meglévő biztonsági szabályozottságának és értelmezhetőségének vizsgálata.

2.2.1. Bemenetek

A *Jogosultságkezelés* bemenet a cégen belül a munkatársak jogosultságainak frissen tartását és annak általános kezelését veszi figyelembe. Nagy sebezhetőséget nyújthat egy cégen belül, ha a jogosultságok nem megfelelően vannak kezelve. Például egy

már nem ott dolgozó fiókját és jogosultságait nem törlik, ami kihasználhatóvá teszi a céget akár az eltávozó dolgozó, akár mások támadása ellen.

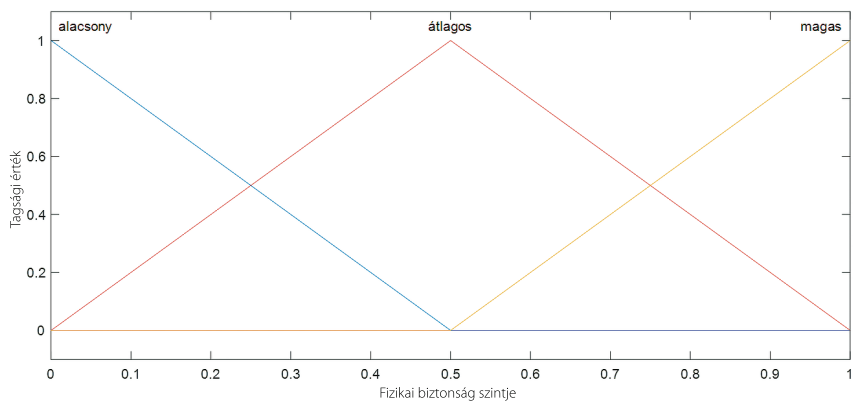
A bemenet három háromszög tagsági függvénnyel rendelkezik, nevük a *laza, közepes, szigorú,* ezek egyenletesen osztják fel a [0,1] közötti értelmezési tartományt.



7. ábra: Jogosultságkezelés bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *fizikai biztonság szintje* bemenet, mint a neve is mutatja, a kézzel fogható védelmi intézkedéseket vizsgálja. Ebbe beleértendő a beléptető rendszer és az őrzés-védés szintje, illetve a szükséges fizikai protokollok milyensége.

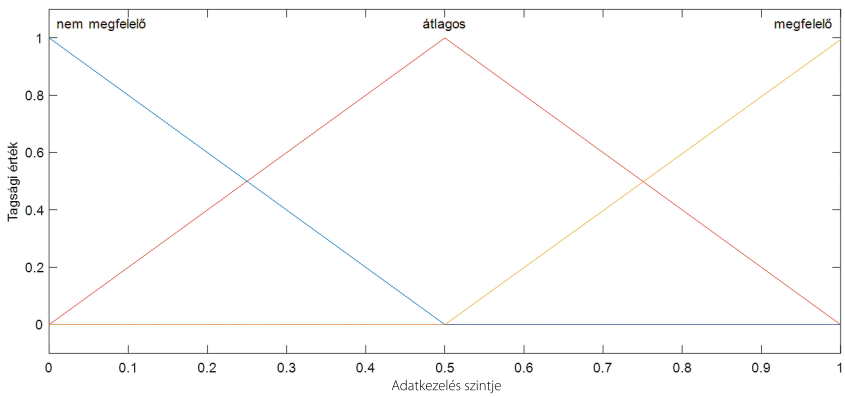
A tagsági függvények itt is [0,1] között vannak, *alacsony, átlagos* és *magas* néven. A nagyobb érték magasabb biztonsági szintet jelöl.



8. ábra: Fizikai biztonság szintje bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

Az *adatkezelés szintje* a fizikai és számítástechnikai szinten egyaránt itt kerül kiértékelésre. Ideértjük a fizikai információt hordozó papírok kezelésének és megsemmisítésének szabályozottságát, a leselejtezett adathordozók kezelését és a dolgozók által tudott információk kiadásának szabályozottságát.

Mint eddig az alrendszerben mindenhol, itt is három háromszög alakú tagsági függvénye van a kimenetnek. Ezek elhelyezkedése a 9. ábrán látható, neveik pedig *nulla, nem megfelelő, átlagos* és *megfelelő.*



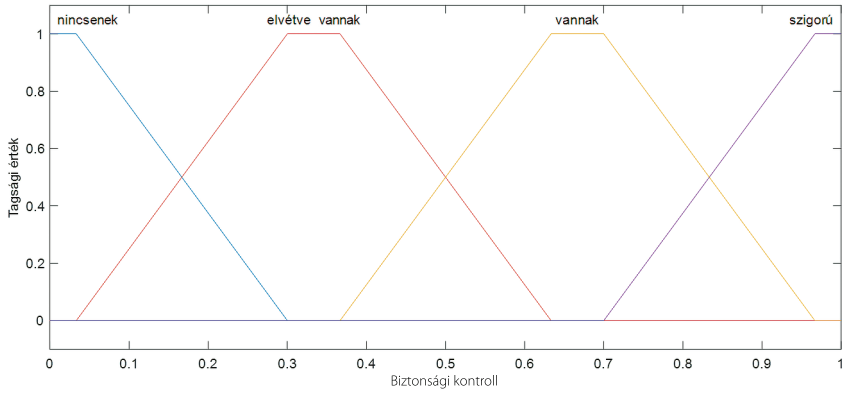
9. ábra: Adatkezelés szintje bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *Szabályozottság* alrendszer kimenete itt bemenetként kapott helyet. A bemeneti tartomány lefedésére alkalmazott tagsági függvényeket az 5. ábrán látható módon határoztuk meg.

2.2.2. Kimenet és szabályok

A *Biztonsági kontroll* alrendszer kimenete a cég biztonsági szabályozottságának mértékét mutatja. Ez a kimenet fog a Simulink segítségével befutni bemenetként a végső kockázatot értékelő alrendszerbe.

A kimenetet négy trapéz alakú tagsági függvény reprezentálja a következő elnevezésekkel: *nincsen, elvétve van, van* és *szigorúak.* Ezek arányosan oszlanak el a [0,1] tartományban. Ebben az esetben is a nagyobb érték a jobb biztonsági szempontból.



10. ábra: Biztonsági kontroll kimenet tagsági függvényei
Forrás: a szerzők szerkesztése

A szabályrendszer 57 súlyozott szabályt tartalmaz. A szabályok az egyes bemenetek tagsági függvényeit párosítják össze, és ehhez határozzák meg a kapcsolódó kimeneti tagsági függvényt a 11. ábrán látható módon, ahol a zöld szín a *szigorú,* a sárga a *van,* a narancssárga az *elvétve van,* és a piros a *nincsen* tagsági függvényt jelképezi, az egyes négyzetekbe írt számok pedig az adott szabály súlyát jelölik a kiértékelés során. Ezeket kiegészítve további erősítő szabályokat vezettünk be a *Szabályozottság* kimenetének erősítésére, vagyis a *Szabályozottság* bemenethez azonnali kimeneti értékeket rendeltünk, ezzel kicsit ráerősítve annak fontosságára és az erejére az alrendszerben.

		Fizikai biztonság szintje			Adatkezelés szintje (digitális, papíralapú...)			Szabályozottsága (folyamatok)		
		magas	átlagos	alacsony	megfelelő	átlagos	nem megfelelő	magas	átlagos	alacsony
Jogosultságkezelés	szigorú	0,8	0,8	0,9	0,8	0,8	0,9	0,8	0,8	0,9
	közepes	0,8	0,8	0,8	0,8	0,8	0,9	0,8	0,8	0,8
	laza	0,8	0,8	1	0,9	0,9	1	0,8	0,9	1
Fizikai biztonság szintje	magas				0,8	0,8	0,9	0,8	0,8	0,9
	átlagos				0,8	0,8	0,9	0,8	0,8	0,8
	alacsony				0,8	0,8	1	0,8	0,9	1
Adatkezelés szintje (digitális, papíralapú...)	megfelelő							0,8	0,8	0,9
	átlagos							0,8	0,8	0,9
	nem megfelelő							0,9	0,9	1

11. ábra: A biztonsági kontroll szabályai
Forrás: a szerzők szerkesztése

2.3. Munkatársak alrendszer

A *Munkatársak* alrendszer a munkatársak átverhetőségét és kihasználhatóságát vizsgálja a humán tényezős támadások alapján, egyszerűsített bemenetekkel. Figyelembe veszi a munkavállalók átlagosan eltöltött idejét az adott szervezetben, a technológia kezelésének szintjét, a belső kommunikáció minőségét és a biztonságtudatosság szintjét.

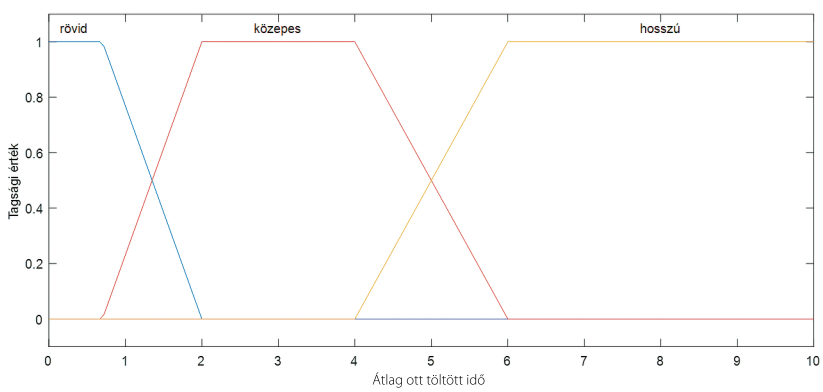
A *Munkatársak* alrendszer teljes mértékben az emberi tényezőre koncentrál, az általános hozzáállást és tudatosságot veszi figyelembe az összes dolgozó átlagában, nem személyenkénti leosztásban.

A *Munkatársak* kimenete a végső kockázatértékelőbe fog befutni a Simulinknek köszönhetően.

2.4. Bemenetek

Az *átlagosan ott töltött idő* bemenet a munkatársak átlagolt cserélődését veszi figyelembe éves szinten. Ha a fluktuáció nagy, az a cég szempontjából nem szerencsés. Ennek oka, hogy kisebb valószínűséggel alakul ki lojalitás a munkavállalókban, így nagyobb a szervezeten belülről érkező támadások elkövetésének potenciálja. Minél nagyobb az átlagos munkaviszony hossza, annál kisebb az esélye az ilyen esetek bekövetkezésének.

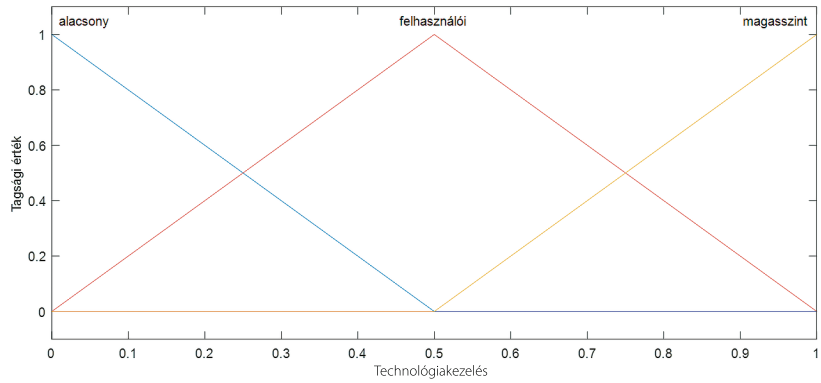
Az alkalmazott tagsági függvények a 12. ábrán láthatók, a *rövid* maximuma 0 és 0,8 év között, a *közepes* maximuma 2 és 4 év között, a *hosszú* pedig 6 és 10 között ábrázolódik. A tíz fölötti érték nem adható meg, de természetesen minden magasabb érték a *hosszú* halmazhoz tartozna, 1 tagsági értékkel.



12. ábra: Átlagosan ott töltött idő bemeneti tagsági függvényei
Forrás: a szerzők szerkesztése

A *technológiakezelés* bemenet a pandémia idején kifejezetten fontos, ugyanis egy technológiailag kevésbé potens munkatárs nagyobb veszélyforrás lehet. Igaz ez a munkahely által biztosított informatikai infrastruktúra ismeretének hiányára, de potenciális veszélyforrás lehet a magánéletben használt eszközök óvatlan kezelése is, ha hatással lehet a szervezetre.

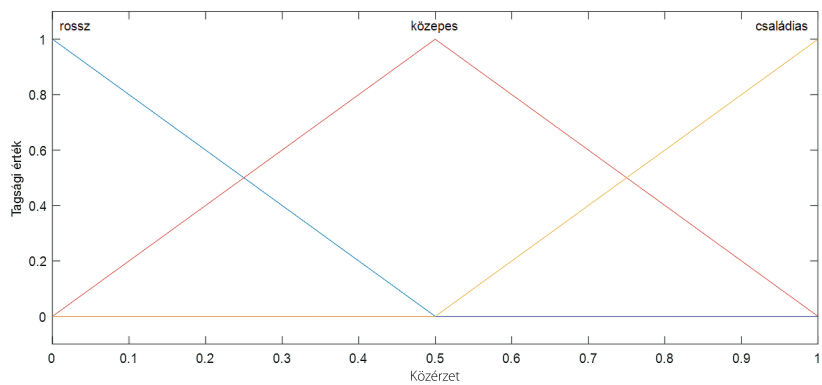
A bemenet [0,1] intervallumban adható meg, a hozzárendelt háromszög alakú tagsági függvények az *alacsony,* a *felhasználói* és a *magas szint*.



13. ábra: Technológiakezelés bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *közérzet* bemenet a munkatársak céghez és a munkájukhoz való viszonyulását vizsgálja. Minél jobban érzi magát egy dolgozó a munkahelyén, annál inkább érdeke, hogy megpróbálja védeni azt, akár direkt, akár indirekt módon.

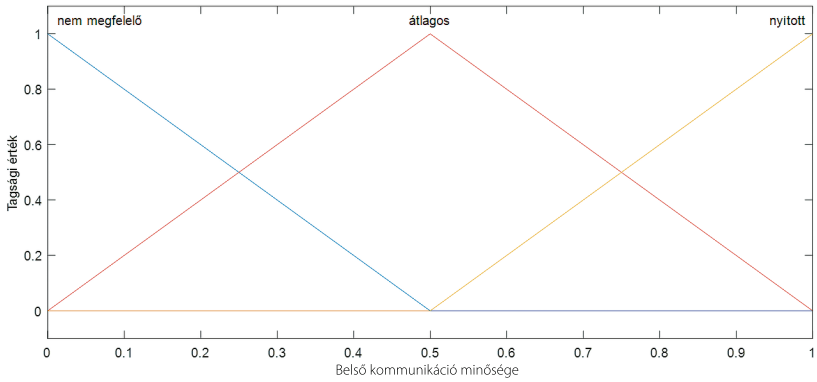
A közérzet tagsági függvényei az eddig használt hármas osztást követik, *rossz, közepes, családias* kategóriákkal.



14. ábra: Közérzet bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *belső kommunikáció minősége* egy cégben azt veszi figyelembe, hogy mennyire jó a munkatársak között és a cég felé irányuló kommunikáció. A nem megfelelő, utolsó pillanatra hagyott változtatások stresszt okozhatnak és ronthatják a munkamorált.

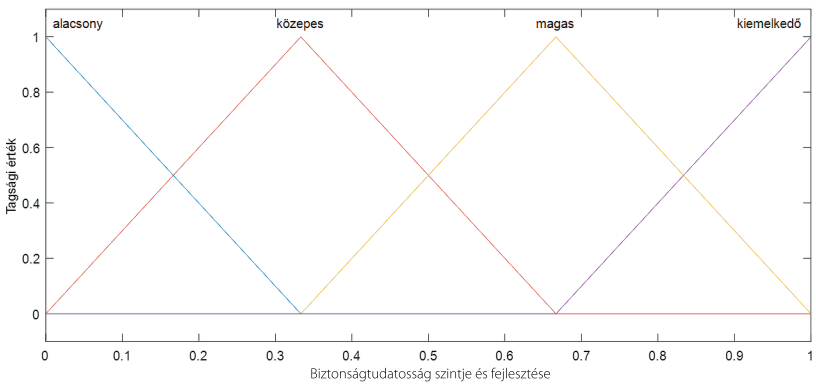
A bemenet a *nem megfelelő,* az *átlagos,* a *nyitott* tagsági függvényeken vehet fel értéket. Ezek a 15. ábrán láthatók.



15. ábra: Belső kommunikáció minősége bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *biztonságtudatosság* szintje és fejlesztése a *Szabályozottságban* felvett *biztonsági érettségi szint* párjának is nevezhető. Itt azonban a cég által megtett biztonsági óvintézkedések szintje helyett a munkatársak hozzáállását vizsgáljuk meg. Ez a bemenet az egyénnel szemben támasztott biztonsági elvárások és a rá vonatkozó szabályozások betartását jellemzi. Fontos megvizsgálni, hiszen hiába vannak meg a szabályok, ha senki sem tartja be azokat.[9]

Itt az általános hármas felosztású tagsági függvények helyett négyes felosztást alkalmaztunk: *alacsony, közepes, magas, kiemelkedő.*



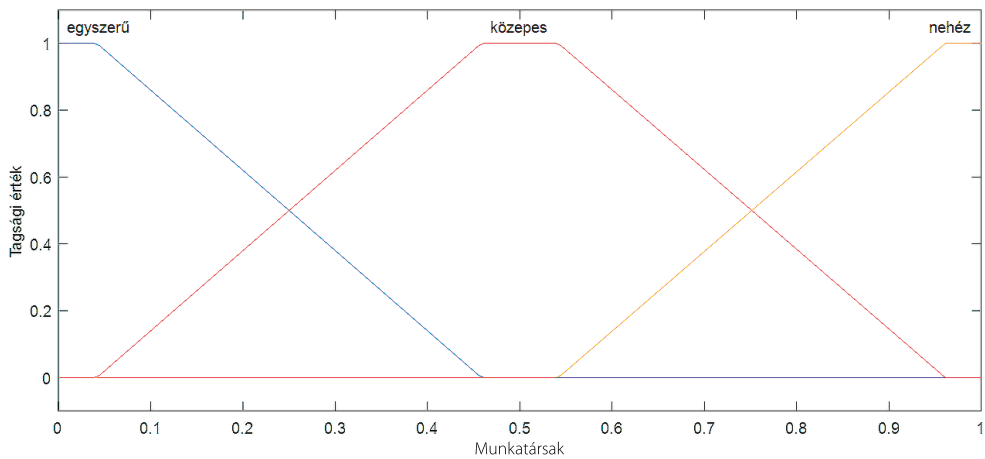
16. ábra: Biztonságtudatosság szintje és fejlesztése
Forrás: a szerzők szerkesztése

[9] Jakus Attila – Tick Andrea: IT biztonsági kockázatok és kockázatkezelés. *Hadmérnök,* 12. (2017), 1. 182–202.

A *Munkatársak* kimenetén egy átlagos értéket kapunk, ahol az összes munkatársat figyelembe véve határozzuk meg a szintet, nem pedig egy-egy személy értékét becsüljük meg. Szükség esetén az alrendszer ilyen módon tovább fejleszthető.

2.5. Kimenet és szabályok

A kimeneten az *egyszerű,* a *közepes* és a *nehéz* tagsági függvényre futhat ki végül a kimenet, ami a végső kockázatértékelőbe továbbítja majd az értékét.



17. ábra: Munkatársak kimeneti tagsági függvényei
Forrás: a szerzők szerkesztése

A szabályrendszer 102 bemenetpáronkénti szabályra épül, hasonlóan súlyozva, mint az előző alrendszerek. A 18. ábrán látható a szabályrendszer grafikus váza, a sorok és oszlopok találkozásában található szín jelzi a két tagsági függvény *ÉS* kapcsolatára válaszként kapott kimeneti tagsági függvényt. A zöld szín a *nehéz,* a sárga a *közepes,* a piros az *egyszerű* tagsági függvényt hivatott reprezentálni.

		Technológiai kezelés			Közérzet			Belső kommunikáció minősége			Biztonságtudatosság szintje és fejlesztése			
		magas	felhasz-nálói	alacsony	családias	közepes	rossz	nyitott	átlagos	nem megfelelő	kiemel-kedő	magas	közepes	alacsony
Átlag ott töltött idő	hosszú	0,9	0,9	0,9	0,9	0,9	1	0,9	0,9	0,9	0,9	0,9	0,9	1
	közepes	0,9	0,9	1	0,9	0,9	1	0,9	0,9	1	0,9	0,9	0,9	1
	rövid	0,9	0,9	1	0,9	0,9	1	0,9	1	1	0,9	0,9	1	1
Technológiai kezelés	magas				0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	1
	felhasz-nálói				0,9	0,9	1	0,9	0,9	1	0,9	0,9	0,9	1
	alacsony				0,9	1	1	0,9	1	1	0,9	0,9	1	1
Közérzet	családias							0,9	0,9	1	0,9	0,9	0,9	1
	közepes							0,9	1	1	0,9	0,9	0,9	1
	rossz							1	1	1	0,9	1	1	1
Belső kommunikáció minősége	nyitott										0,9	0,9	0,9	1
	átlagos										0,9	0,9	1	1
	nem megfelelő										0,9	0,9	1	1

18. ábra: Munkatársak szabályrendszer
Forrás: a szerzők szerkesztése

3. Kockázatbesoroló alrendszer

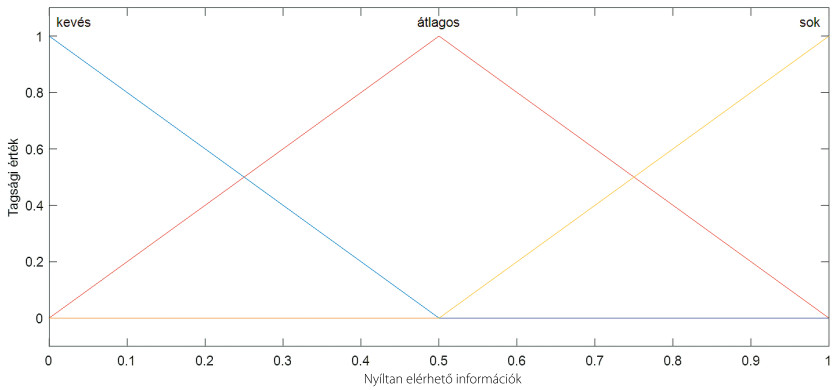
A *Kockázatbesoroló* alrendszer valójában a fő fuzzy rendszer, amely a cég kiberbiztonsági kockázatát mutatja, alapvetően a humán tényezős támadások esetén. Két új bemenetet vesz figyelembe a már használt cégnagyság mellett: a nyíltan elérhető információkat és a várható haszon nagyságát. Ezek mellé futnak be a *Biztonsági kontroll* és a *Munkatársak* alrendszerek kimenetei, itt már bemenetként.

3.1. Bemenetek

A *Cégnagyság* már a *Szabályozottságból* ismert bemenet tagsági függvényeit a 2. ábra szemlélteti.

A második bemenet, a *Nyíltan elérhető információk,* a cég ismertségét és a róla nyilvánosan elérhető információk mennyiségét veszi figyelembe. Minél ismertebb egy cég, annál jobb lehet az elérése, cserébe biztonsági szempontból kockázatosabb is. Az adott cégről kint lévő információk mennyisége is kulcsfontosságú. Minél több az elérési lehetőség és egyszerűbb az információszerzés a cégről, annál sebezhetőbb lesz az egyes támadásokkal szemben.

A többi eddig használt bemenetekkel ellentétben, ez esetben a kisebb érték a jobb biztonsági szempontból.

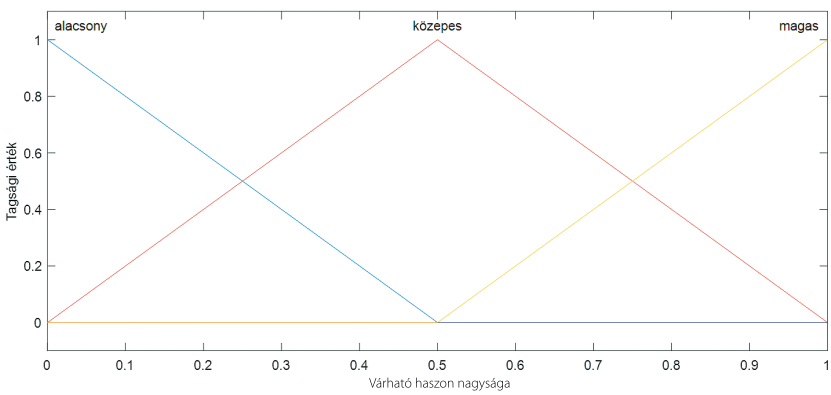


19. ábra: Nyíltan elérhető információk bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

A *Várható haszon* nagysága a cég által birtokolt és eltulajdonítható információs, pénzügyi hasznot veszi figyelembe. Minél nagyobb a haszon, annál jobban megéri a támadóknak foglalkoznia vele. Emellett fontos tényező az is, hogy mennyire nehezen érhető el a kívánt információ. Ennek meghatározására általánosan az alábbi képlet használatos:[10]

$$Kockázat = Fenyegetettség\ x\ Sebezhetőség\ x\ Nyereség \qquad (3)$$

A bemenet értékelése az előzőhöz hasonlóan alakul, azaz a kisebb a cég szempontjából kedvezőbb érték. Az *alacsony, közepes* és a *magas* tagsági függvényeket rendeljük hozzá a [0,1] intervallumbeli értékhez.



20. ábra: Várható haszon nagysága bemenet tagsági függvényei
Forrás: a szerzők szerkesztése

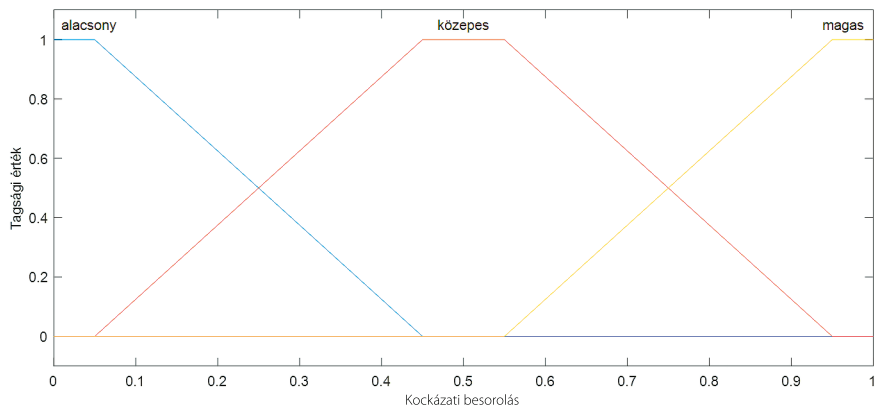
[10] John R. Vacca (szerk.): *Computer and Information Security Handbook.* Burlington, Morgan Kaufmann, 2009. 225–231.

Bemenetként fut be a *Biztonsági kontroll* kimenete is a 10. ábrán illusztrált tagsági függvényekkel, valamint a *Munkatársak* kimenete a 17. ábrán szemléltetett módon.

3.2. Kimenet és szabályok

A *kockázati besoroló* kimenetén kapjuk meg a modell utolsó és egyben legfontosabb eredményét, a cég összesített kiberbiztonsági kockázatát. A *Várható haszon* és a *Nyilvánosan elérhető információk* elnevezésű bemenetek viszik bele a rendszerbe azokat a tényezőket, amelyek megmutatják, hogy mennyire könnyen elérhetők az információk a támadók számára és mennyire tűnik kifizetődőnek számukra.

A kimenet trapéz alakú tagsági függvényei a *Várható haszon nagyságához* hasonlóan a magasabb értékhez társítanak rosszabb kimenetet. A függvényekhez rendelt nyelvi változók: *alacsony, közepes* és *magas.*



21. ábra: Kockázatbesoroló kimenet tagsági függvényei
Forrás: a szerzők szerkesztése

A kockázati besoroló alrendszer kimenetét meghatározó 122 szabályt az eddigiekben ismertetett módszerrel súlyoztuk. Erősítő szabályok a *Biztonsági kontrollhoz* hasonlóan itt is jelen vannak, mind a *Munkatársak* mind a *Biztonsági kontroll* bemenetén kapott értékeket azonnali kimenetre kapcsolják, ezáltal erősebb a hatásuk. A szabályokat az erősítőkön kívül a 22. ábrán láthatjuk, a zöld szín a kimeneten az alacsony tagsági függvényt jelenti, a sárga a közepeset és a piros a magasat. Ez a rendszer szolgáltatja a teljes rendszerkimenetet.

		Nyiltan elérhető információk			Várható haszon nagysága			Biztonsági kontroll				Munkatársak		
		kevés	átlagos	sok	alacsony	közepes	magas	szigorú	vannak	elvétve vannak	nincsenek	nehéz	közepes	egyszerű
Cégnagyság	multi	0,9	0,9	1	0,9	0,9	1	0,9	0,9	1	1	0,9	0,9	1
	nagy	0,9	0,9	1	0,9	0,9	1	0,9	0,9	1	0,9	0,9	0,9	1
	közepes	0,9	0,9	1	0,9	0,9	1	0,9	0,9	1	1	0,9	0,9	1
	mikro	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	0,9	1	0,9	0,9	1
Nyiltan elérhető információk	kevés				0,9	0,9	0,9	0,9	0,9	0,9	1	0,9	0,9	1
	átlagos				0,9	0,9	1	0,9	0,9	1	1	0,9	0,9	1
	sok				0,9	1	1	0,9	1	1	1	0,9	1	1
Várható haszon nagysága	alacsony							0,9	0,9	0,9	1	0,9	0,9	0,9
	közepes							0,9	0,9	1	1	0,9	0,9	0,9
	magas							0,9	1	1	1	0,9	1	1
Biztonsági kontroll	szigorú											0,9	0,9	0,9
	vannak											0,9	0,9	1
	elvétve vannak											0,9	1	1
	nincsenek											1	1	1

22. ábra: Kockázati besoroló szabályai
Forrás: a szerzők szerkesztése

4. Esettanulmány

A modell működésének szemléltetése érdekében egy fiktív cég elemzését mutatjuk be.

Egy fiktív nagyobb céget vizsgáltunk, egészen jó átláthatósággal és biztonsági érettségi szinttel. A foglalkoztatott munkatársainak számát 1110-re vettük fel. Az átláthatóságát nem a remek értékre, de nem is csak elfogadhatóra értékeltük, a biztonsági érettségi szintnek hasonló értéket adtunk meg.

Adatok:

cégnagyság (fő, [0,1500]): *1110*
átláthatóság [0,1]: *0,7*
biztonsági érettségi szint [0,1]: *0,7*

A kiértékelés után a *Szabályozottság* kimenete ebben az esetben 0,64 lett, ami a tagsági függvényeken az átlagos és a magas közé esik, inkább az átlagos irányába. A cég nagysága bemenet a kimeneten lefelé húzta a szabályozottságot.

A második alrendszer bemeneteihez szinte maximumértékeket adtunk meg, a kitalált cég ugyanis jól kezeli és frissen tartja a jogosultságokat, a fizikai biztonság is jobb az átlagosnál. A fenti bemenetek és a magasnak besorolt adatkezelési szint mellé még befut az előzőkben megkapott szabályozottság kimenete.

Adatok:

jogosultságkezelés [0,1]: *0,9*
fizikai biztonság szintje [0,1]: *0,8*

adatkezelés szintje [0,1]: *0,9*
szabályozottság [0,1]: *0,64*

A biztonsági kontroll eredménye így 0,76 lett, ami annyit tesz, hogy bármennyire is magasnak adtuk meg az önálló bemenetet, mivel a szabályozottság értéke alacsonyabb, mint a többi bemenet, az lenyomta a biztonsági kontroll értékét.

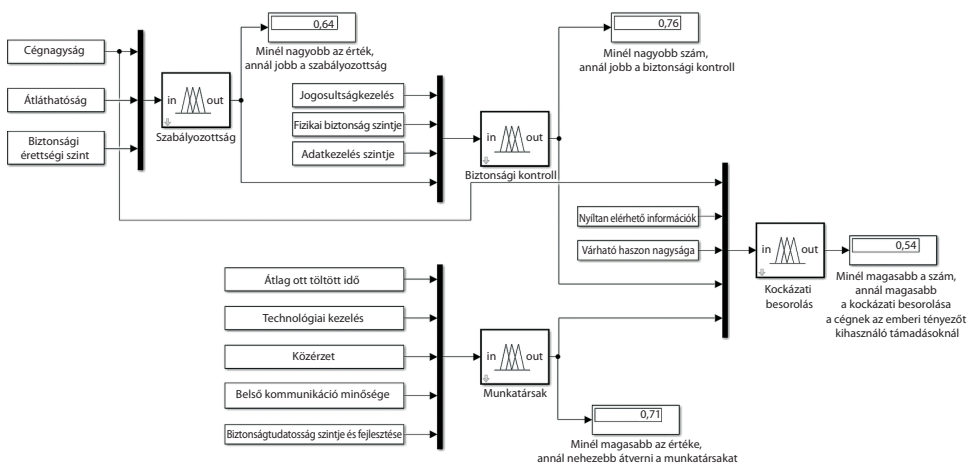
A munkatársak bemeneteihez a projektenként változó cégfelépítés miatt az átlag ott töltött időt 3 évre határoztuk meg. A technológiakezelést kifejezetten magasra értékeltük, míg a közérzet szintje közepesnek mondható, az utolsó pillanatos változtatások és értesítések miatt. A belső kommunikáció minőségének értéke kicsit magasabb a közérzeténél.

Adatok:
átlag ott töltött idő (év, [0,10]): *3*
technológia kezelés [0,1]: *0,9*
közérzet [0,1]: *0,5*
belső kommunikáció minősége [0,1]: *0,6*
biztonságtudatosság szintje és fejlesztése [0,1]: *0,8*

A munkatársak kimenete a megadott bemenetek alapján 0,71 lett, ami a *vannak* tagsági függvényre ad nullától különböző értéket. A közepes bemenetek mellett a technológiakezelés és a biztonságtudatosság szintje és fejlesztése húzta fel az eredményt.

A kockázati besoroló megkapja a *Munkatársak* és a *Biztonsági kontroll* kimenetét, valamint a *Szabályozottságban* már használt *Cégnagyság* bemenet is. A két új információt, amelyet a rendszerbe be tudunk vinni, viszonylag magas értékekkel adtuk meg, ugyanis a cég ismert és viszonylag sok róla az információ, ezért a várható haszon is magas a céges titkok és kapcsolatok, valamint a pénz mozgása miatt.

Adatok:
cégnagyság (fő, [0,1500]): *1110*
nyíltan elérhető információk [0,1]: *0,8*
várható haszon nagysága [0,1]: *0,9*



23. ábra: Simulinkben az esettanulmány eredménye és részeredményei
Forrás: a szerzők szerkesztése

A végső kockázati szint 0,54 lett, amely egy közepes kockázatot jelent. A *Munkatársak* és a *Biztonsági kontroll* alrendszerek viszonylag jó eredménye mellett a magas haszonszerzési lehetőség és a sok nyílt információ miatt a cég kockázata közepesre nőtt egy humán alapú támadás esetén.

5. Összegzés

Manapság az informatikai rendszerek használata átszövi életünket. Számos előnye mellett azonban ez fokozott kockázatot is hordoz magában, különösen a vállalatok és állami szereplők számára. Ennek eredményeként a kiberbiztonsági kérdések egyre fontosabb kutatási területet képeznek. A számos figyelembe veendő tényező közül általában az ember bizonyul a leggyengébb láncszemnek. A probléma kezelésére egy hierarchikus, emberitényező-központú kiberbiztonsági modellt dolgoztunk ki, amelyben a kiértékelést fuzzy következtetési rendszerrel végeztük. A befolyásoló tényezők jellemzői és a közöttük fennálló kapcsolat indokolja a fuzzy megközelítés alkalmazását. Ennek oka, hogy a kiberbiztonsági rendszerek tele vannak bizonytalanságokkal, szubjektivitással, ami ilyen módon jól kezelhető. A javasolt modell négy alrendszerből áll: 1. Szabályozottság, 2. Biztonsági kontroll, 3. Munkatársak, 4. Kockázati besoroló. Ezek mindegyike külön fuzzy rendszernek tekinthető. Segítségükkel a befolyásoló tényezők egyes logikai csoportjainak kockázatát külön értékelhetjük ki. Ennek a szerkezetnek nagy előnye az is, hogy biztosítja az átláthatóságot és a bővíthetőséget, ami megkönnyíti akár új tényezők beépítését is. A fuzzy modell megbízhatóságának bizonyításához további interjúk és esettanulmányok készítése szükséges. A szerzők további tervei között szerepel az emberi tényező pszichológiai vonatkozásainak mélyebb tanulmányozása a későbbi kutatások során.

Köszönetnyilvánítás

Szeretnénk köszönetet mondani Kinczel Tamás Bencének, Gyulai Tamásnak, Lélek Kitti Alexandrának és Hüse Zoltánnak, akik segítségünkre voltak a modell felépítése során.

Felhasznált irodalom

Hadnagy, Christopher: *Social Engineering: The Art of Human Hacking.* Hoboken, Wiley, 2011.

Jakus Attila – Tick Andrea: IT biztonsági kockázatok és kockázatkezelés. *Hadmérnök,* 12. (2017), 1. 182–202. Online: http://hadmernok.hu/171_15_jakus.pdf

Pokorádi László: Fuzzy Techniques in the Aircraft Engineering. In Zobory I. (szerk.): *Proceedings of the 7th Mini Conference on Vehicle System Dynamics, Identification and Anomalies.* Budapest, BME Vasúti Járművek Tanszék, 2001. 443–448.

Salahdine, Fatima – Naima Kaabouch: Social Engineering Attacks: A Survey. *Future Internet,* 11. (2019), 89. 1–17. Online: https://doi.org/10.3390/fi11040089

Steingartner, William – Darko Galinec: Cyber Threats and Cyber Deception in Hybrid Warfare. *Acta Polytechnica Hungarica,* 18. (2021), 3. 25–45. Online: https://doi.org/10.12700/APH.18.3.2021.3.2

Szádeczky Tamás: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *AARMS,* 19. (2020), 1. 83–93. Online: https://doi.org/10.32565/aarms.2020.1.7

Vacca, John R.: *Computer and Information Security Handbook.* Burlington, Morgan Kaufmann, 2009.