BÁNKI KÖZLEMÉNYEK
4. ÉVFOLYAM 1. SZÁM

Az emberi tényező fuzzy alapú kiberbiztonsági kockázatelemzése a minősített információszivárgás szempontjából

Váczi Dániel*, Tóth-Laufer Edit**, Szádeczky Tamás***
* Biztonságtudományi Doktori Iskola, Óbudai Egyetem, Budapest, Magyarország
** Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem, Budapest, Magyarország
*** Kandó Kálmán Villamosmérnöki Kar, Óbudai Egyetem, Budapest, Magyarország

***Összefoglalás* — A COVID19 világjárvány miatt gyakorlatilag az egész világ otthonról dolgozott, így a szervezetek digitális átalakítása megkerülhetetlenné vált, ami sok kihívást jelentett a kiberbiztonság területén is. A cikk elkészítésekor még nem állnak rendelkezésre pontos adatok konkrét incidensekről, azok hatásairól, illetve az okozott károk mértékéről. Ennek ellenére valószínűsíthető, hogy a pandémiás káoszban sok vállalat követett el hibát a digitális adaptációs folyamat során, melynek forrása sok esetben az emberi tényező. Az ilyen típusú kockázat kezelése alapvető fontosságú, ennek ellenére kiberbiztonsági területen nincs széles körben elterjedt módszertan az emberi kockázat kezelésére annak nehéz számszerűsíthetősége okán. Ebben a cikkben a szerzők egy olyan fuzzy modellt javasolnak, amely alkalmas az említett kockázatok felmérésére, amennyiben elegendő információ áll rendelkezésükre a munkaerőről. A modell könnyebb érthetősége miatt a szerzők, egy konkrét fenyegetés, a minősített digitális információk kritikus infrastruktúrából történő szivárgását veszik alapul.**

***Kulcsszavak*:** kiberbiztonság, humánfaktor, fuzzy modell, minősített információ szivárgás, kritikus infrastruktúra

1 BEVEZETÉS

A szervezetek védelmi rendszerét kockázat alapúan kell kiépíteni kis- vagy közepes méretű vállalkozás, multinacionális vállalat, nonprofit vagy fórprofit társaság, állam vagy piaci szereplő esetén egyaránt. A gyakorlat sok esetben mégis azt mutatja, hogy ez a folyamat még mindig ad-hoc módon valósul meg.

A kiberbiztonság kiépítése három pillér mentén történik, melyek a technológia, a folyamatok és az emberek [1]. A piacon manapság több jó technológiai megoldás is elérhető, melyek használatáról az adott szervezet elhatározásától és költségvetésétől függően dönthetnek. A technikai jellegű fejlesztések mellett sok szervezet megkezdte a kiberbiztonsági folyamatok kiépítését is. Habár minden szervezet eltérő érettségi szintű, napjainkban már a nagyvállalatok és az állami szereplők többsége rendelkezik egy, a témával foglalkozó szabályzattal. Megállapítható, hogy a technológiák és folyamatok javultak ezen a területen, ám sok esetben ezeket a fejlesztéseket valamilyen törvénynek vagy szabványnak történő megfelelés kényszerítette ki. A fenti két tényezővel szemben aránytalanul kis figyelmet fordítanak azonban az emberi tényezőre a sok gyakorlati eset ellenére, amelyek azt bizonyítják, hogy a szervezetek megfelelő technológiai megoldásai vagy szabályzata nem elegendő, hiszen egy komoly kár okozásához vezethet egy személy szándékos vagy gondatlan tette. Kiváló példa erre a Stuxnet esete, ahol egy munkavállaló hibája öt évvel vetette vissza az ország nukleáris programját [2].

Valószínűleg az emberi tényező a legbonyolultabb és legnehezebben mérhető kockázati tényező, hiszen tele van bizonytalansággal és szubjektivitással, de a fentiek alapján nyilvánvaló, hogy szükség lenne egy hatékony modellre e kockázat értékeléséhez, kezeléséhez. A fuzzy-alapú modellek megfelelő megoldást kínálnak az ilyen típusú problémákra. A fuzzy logikát több helyen alkalmazzák a kockázatok kezelésére, mivel alkalmas a bemeneti adatok és az értékelési folyamat bizonytalanságának, szubjektivitásának, pontatlanságának korrigálására, valamint képes értelmezni a nehezen számszerűsíthető bemeneti értékeket [3], [4].

Ebben a cikkben a kiberbiztonsági területen fellépő emberi kockázatok vizsgálatára alkalmas fuzzy modellünket mutatunk be. A javasolt modellt alkalmazva a szervezetek sokkal reálisabb képet kaphatnak erről, a nehezen mérhető kockázatról úgy, hogy véletlenszerű számok helyett könnyen értelmezhető nyelvi jellemzőket kell megadniuk, mint például: kicsi, nagy, alacsony, magas stb. E módszer segítségével az eredmény könnyen érthetővé válik a laikusok számára is.

2 AZ EMBERI TÉNYEZŐ A KIBERBIZTONSÁGBAN

Számos kiberbiztonsági incidens köthető valamilyen módon emberi tévedéshez, annak ellenére, hogy a szervezetek sok energiát fektetnek ennek csökkentésére. Ezeknek az eseményeknek különböző okai lehetnek. Egy külső vagy belső támadó célpontja lehet egy adott szervezet, vagy akár egy ott dolgozó konkrét személy is, azonban sok esetben a támadásnak nincs kiszemelt célpontja, csak az a célja, hogy valakinek – bárki is legyen az – kárt okozzon. A kiber-történelem tele van sikeres támadásokkal, amelyek az emberi tényező miatt lehettek eredményesek. Néha a siker kulcsa nem más, mint a megfelelő oktatás hiánya, de előfordulnak azok az esetek, amikor a támadók alapvető emberi viselkedéseket használtak ki. Sokan könnyen becsaphatóak, zsarolhatóak, mások szeretnek segíteni embertársaikon, vagy akadnak esetek, ahol egyszerűen csak figyelmetlenek, nemtörődömök. Külön szakirodalom található arról,

hogyan lehet az embereket kihasználni az informatikai rendszerek elleni támadások során [5].

Azokban a szervezetekben, ahol odafigyelnek a minél teljesebb körű kiberbiztonság építésére, ott a munkaerő képzése mellett, általában megpróbálják social engineering tesztekkel, vagy különböző játékos kampányokkal felhívni a figyelmet ezekre a veszélyekre. Sajnos ezek a módszerek azonban nem elegendőek a célzott, kifinomult támadások ellen, ugyanis ezekben az esetekben nagymértékben előkészített támadásokkal állunk szemben. A támadók előzetesen megvizsgálják, hogy ki lehet a gyenge láncszem a munkavállalók között [6], információkat gyűjtenek a célpont életmódjáról, illetve az őt körülvevő digitális környezet sérülékenységeiről. Ezen információmorzsák megszerzésére manapság számos lehetőség kínálkozik. A speciális „hacker eszközök" mellett a különböző nyílt forrású információszerzésre irányuló (OSINT - Open Source Intelligence) technikák is rendelkezésükre állnak [7], illetve az úgynevezett deep és dark web is számos lehetőséget kínál a kárt okozni kívánók számára.

3 Digitális minősített információ szivárgás, mint vizsgált kockázat

Annak bizonyítására, hogy a fuzzy logika alkalmas a kockázatok felmérésére, a minősített digitális információk szándékos vagy gondatlan szivárgását vizsgáltuk. Azért ezt a fenyegetést választottuk, mert könnyen elképzelhető és megérthető; nem ágazat specifikus; a különböző embertípusok a változó környezeti körülmények hatására jól differenciálható kockázati szinttel rendelkeznek.

A minősített információknak több különböző típusa van. Léteznek állami és szövetségi rendszereken belüli (például NATO, EU) titkok, de ide sorolhatók az üzleti, banki, orvosi, jogi vagy egyéb titkokat is. A vizsgálat során nem tettünk különbséget a minősített információk típusai között. Fontos azonban meghatározni, hogy milyen adathordozón jelennek meg ezek. Mivel a tanulmány a kiberbiztonsági kockázatokat vizsgálja, ezért úgy döntöttünk, hogy csak a digitális formában előforduló minősített információkat vizsgáljuk. A tanulmány tehát figyelmen kívül hagyja azokat az eseteket, amikor az információk szóbeli, vagy papír alapú formában szivárognak. A továbbiakban a minősített információ kifejezés alatt minden esetben annak digitális formáját értjük.

A szivárgás különböző csatornákon keresztül történhet. Előfordulhat online vagy hálózati kapcsolat nélküli, úgynevezett offline szivárgás. Ez utóbbira jó példa a számítógép képernyőképének okostelefon kamerájával történő rögzítése. Meg kell különböztetni azokat az eseteket, amikor a szivárogtató személy továbbítja magukat az információkat, illetve amikor hozzáférést biztosít mások számára egy rendszerekhez [8]. Az elkövető személyek különböző motivációk mentén követhetik el ezeket a tetteket. A teljesség igénye nélkül lehetséges ok a pénzügyi nyereszkedés, a tudás fitogtatása, a ranglétrán történő előbbre jutás elősegítése, a hatalom fitogtatása, de szexuális motiváció is vezetheti az elkövetőt a tette végrehajtásakor.

4 A humán kockázat azonosítása

A kiberbiztonsági kockázatkezelés a szervezetek számára célszerű, átlátható, és nem ad-hoc módon elvégzett. A különféle nemzetközi szabványokban és jogszabályokban (pl.: NIST SP 800-53 R4 [9], az Általános Adatvédelmi Rendelet - GDPR [10], ISO / IEC 27001: 2013 [11]) történő kiemelés is alátámasztja ezt. Az emberi kockázatok kezelésének fontossága ezek alapján is látszik, azonban jelenleg nincs egy megbízható, elterjedt, pontos módszer ennek felmérésére.

A kiberbiztonsági kockázatkezelés általános folyamata i) a kockázat azonosítása, ii) elemzése, iii) a megelőző intézkedések tervezése és iv) azok végrehajtása [12]. A folyamat egyszerűnek tűnik, azonban az emberi kockázatok azonosítása sok szervezet számára nagy kihívást jelenthet, hiszen nem áll rendelkezésükre könnyen alkalmazható módszertan. Ebben a cikkben a szerzők a kockázatkezelés azonosítási szakaszát vizsgálják, mely az egyik legnagyobb kihívást jelenti, hiszen az emberi lény nagyon összetett, a vizsgálandó tényezők nehezen számszerűsíthetők. A különböző személyek eltérő személyiséggel rendelkeznek, eltérő az életcéljuk, a motivációjuk és az életkörülményei. Ahhoz, hogy a szervezetek megfelelő hatékonysággal tudják azonosítani ezt a kockázatot megfelelő információkra, és egy olyan modellre van szükségük, amely képes kezelni az emberi tényezőből fakadó sokféleséget és bizonytalanságot.

A kritikus infrastruktúrákban a megfelelő munkaerő kiválasztására nagyobb figyelmet fordítanak, mint általában máshol. Sok esetben mind a lehetséges jövőbeli, mind az aktuális alkalmazottakat különböző szintű biztonsági ellenőrzéseknek vetik alá. Ebből fakadóan ezek a munkáltatók az átlagnál több információval rendelkeznek a munkavállalóikról, így könnyebben tudják azonosítani a kiberbiztonság szempontjából kockázatosabb alkalmazottakat is. Ezekben az esetekben sem elegendőek azonban az általánosan használt módszerek és modellek, hiszen azok nem képesek a valósághoz közelítő eredményt adni. A megfelelőbb eredmények elérése érdekében a fuzzy megközelítés alkalmazása indokolt a módszertan javítása érdekében.

5 Fuzzy logika a kiberbiztonsági kockázatkezelésben

A fuzzy logika célja a nehezen számszerűsíthető, így matematikailag nehezen leírható problémák kezelése [13]. Mivel a kiberbiztonságban az emberi tényező általában szubjektív és bizonytalan, ezért van szükség egy ilyen típusú megközelítésre. A szakértői ismeretek az alkalmazott szabályalapon keresztül beépülnek a fuzzy rendszerbe, ahol egy Mamdani típusú következtetési rendszerben a *HA állapot*, *AKKOR következtetés* típusú szabályokat alkalmazzák a szerzők, az alábbiak szerint:

$$HA\ x_1\ A_{1,i_1}\ és \dots és\ x_n\ A_{n,i_n}\ AKKOR\ y\ B_{i_1,\dots,i_n} \quad (1)$$

ahol $x_1, \dots, x_n$ a bemeneti paraméterek, A_{k,i_k} a k-ik bemenethez tartozó i_k fuzzy halmaz , $B_{i_1,\dots,i_n}$ az i_j szabály konzekvens része, $i_j = 1, \dots, n_j$ és n_j a *j-edik* bemenethez tartozó halmazok száma [14].

A bizonytalanságot és a szubjektivitást a megfelelő tagsági függvényekkel lehet kezelni, amelyek felosztják a bemeneti univerzumot. A modellben teljes bemeneti készlet lefedésére a Ruspini-partíciót alkalmaztuk, azaz $\sum_{i=1}^{n} \mu_i(x) = 1$ és $\mu_i(x) \geq 0$, ahol $\mu_i(x)$ a tagsági függvény [15], amely meghatározza, hogy egy adott érték milyen mértékben tartozik egy halmazhoz. A függvény alakja a feladattól függ, a modellben a Gauss-alakú tagsági függvényeket (2) alkalmaztuk a bemeneti értékek fuzzifikálása céljából.

$$\mu_{A_i}(x) = e^{-\frac{(x-c_i)^2}{2\sigma_i{}^2}} \quad (2)$$

ahol c_i az A_i fuzzy halmaz középértéke, σ_i pedig a szórása. A bemeneti tényezőket és azok tagsági függvényeit a következő szakasz ismerteti.

A fuzzifikációt követően a Zadeh t-normával (minimum operátor) történik a kiértékelés.

$$w_i = \min_j \mu_{A_{j,i_j}}(x) \quad (3)$$

ahol $\mu_{A_{j,i_j}}(x)$ a j bemenet az i_j antecedenshez tartozó fuzzifikált érték.

A rendszerkimenet eléréséhez először azt határozzuk meg, hogy egy adott szabály milyen mértékben vesz részt a végső eredményben. Ezt a műveletet a maximum operátor (4) segítségével végezzük el a Gauss alakú konzekvensre, majd az eredményül kapott halmazok összesítése ismét a maximum operátor segítségével történik.

$$y_{B_i} = \max_i(w_i, \mu_{B_i}) \quad (4)$$

ahol w_i az i-ik szabály erőssége és μ_{B_i} annak következménye.

Ez az aggregálás komplex alakú fuzzy halmazt hoz létre, amelyet végül defuzzifikálni szükséges, hogy egy egzakt értéket kapjunk, amely a legjobban reprezentálja az eredménykészletet. Az optimális módszer kiválasztása alkalmazástól függ. Ebben a modellben a COG (Center of Gravity) módszert használtuk (5).

$$y_R = \frac{\int_{y\in\mu_B} \mu_B(y) y dy}{\int_{y\in\mu_B} \mu_B(y) dy} \quad (5)$$

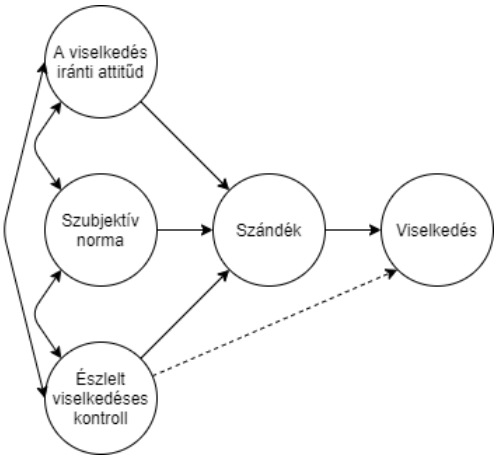
ahol $\mu_B(y)$ a komplex alakú következménykészlet.

6 Az emberi tényező kockázatainak azonosítása, azaz a fuzzy alapú kiberbiztonsági modell ki- és bemenetei

Jelen kutatás célja egy fuzzy modell alkalmazása a dolgozók kiberbiztonsági kockázatának azonosítása érdekében a digitális minősített információ szivárgását alapul véve. A bemenetek ennek megfelelően úgy kell megválasztani, hogy tartalmazzák azokat a tényezőket, amelyek befolyásolják a személyeket az adott cselekedet végrehajtására. Annak érdekében, hogy a bizonytalanság és a szubjektivitás megfelelően kezelhető legyen, elengedhetetlen a bemeneti tartomány megfelelő partíciójának meghatározása, azaz a tagsági függvények definiálása. Ez a fejezet bemutatja a vizsgált tényezőket, és a hozzájuk rendelt tagsági függvényeket. Az egyes bemenetek tartományait egységesen, a [0 10] intervallumon határoztuk meg.

6.1 Szándék

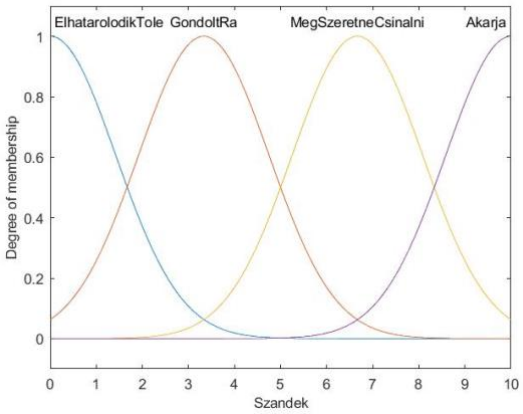
Az első bemenet Ajzen tervezett magatartás elméletének modelljéből származik, ahol meghatározza, hogy a viselkedés szándékból fakad - amint az az 1. ábrán látható [16].



1. ábra: Ajzen: Tervezett magatartás elméletének modellje (1991)

A tervezett viselkedés összetett és nehezen mérhető; szavakkal azonban különbséget lehet tenni a különféle szintek között, mely tökéletes fuzzy bemenetként szolgál. A modellben a következő tagsági függvényeket definiáltuk (2. ábra):

- ElhatárolódikTőle;
- GondoltRá;
- MegSzeretnéCsinálni;
- Akarja.



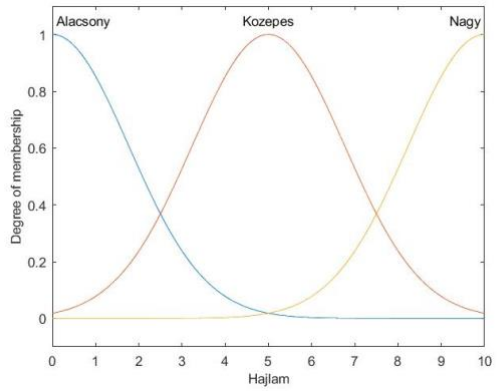
2. ábra: A szándékot leíró tagsági függvények

6.2 Hajlam

A hajlam a különböző személyiségtípusok mögött rejlő kockázatokat határozza meg, hiszen az információszivárgás kockázatát illetően a különböző emberi tulajdonságok különböző kockázatokat rejtenek. Sokféle megközelítés létezik a típusok kategorizáláshoz. Minél stabilabb a személyisége egy illetőnek, annál kevésbé valószínű, hogy szándékosan szivárogtat információt, valamint a reális önkép is nagyban befolyásolja a kockázatot. Noha a fuzzy logika alkalmas a bizonytalanságok kezelésére, a mentális klinikai eseteket (például pszichopatákat) ettől a modelltől külön szükséges

kezelni. A bemenet jellemzésére a következő függvényeket definiáltuk (3. ábra):

- Alacsony;
- Közepes;
- Nagy.



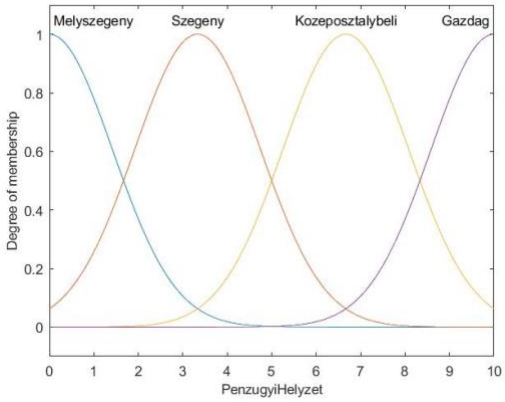
3. ábra: A hajlamot leíró tagsági függvények

6.3 Pénzügyi helyzet

A pénzügyi helyzet hatása túlmutat az anyagi javak birtoklásán. A kevesebb pénzzel rendelkező személyek tudása valószínűleg kevésbé naprakész. Ennek az az oka, hogy pénz hiányában feltehetően nem vagy ritkán vásárolnak digitális eszközöket, így korlátozott lehetőségük van arra, hogy megismerjék a technológiákat. Legyen szó az új fenyegetésekkel kapcsolatos tájékozottságról vagy a digitális eszközök megfelelő felhasználásáról, így ez a tényező lehet kockázatnövelő hatású. Ennek a bemenetnek van egy másik vetülete is. Azokban az esetekben, amikor valaki személyiségéből fakadóan hajlamos a korrupcióra, akkor a szegényebb rétegből érkezők számára egy támadó könnyebben elő tudja teremteni az ingerküszöbnek megfelelő pénzmennyiséget. Tehát kevesebb pénz lehet elegendő egy szegényebb embernél, mint egy másik, ugyanazokkal a személyiségjegyekkel rendelkező, jómódú embertársánál. Ez azt jelenti, hogy minél kevesebb pénz elég ahhoz, hogy egy illetőt valaki rábeszélje az információ kiszivárogtatására, annál nagyobb a valószínűsége, hogy több támadó potenciális célpontjává válik. Egy személy pénzügyi helyzetének vizsgálata során továbbá figyelembe kell azt is venni, hogy kik és hányan élnek vele azonos háztartásban.

A felsorolt tényezők miatt a tagsági függvények meghatározásakor az életminőséget vettük alapul (4. ábra):

- Mélyszegény;
- Szegény;
- Középosztálybeli;
- Gazdag.



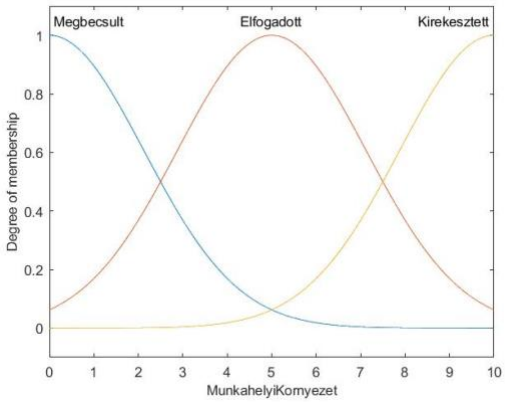
4. ábra: A pénzügyi helyzetet leíró tagsági függvények

6.4 Munkahelyi környezet

A bizalmas információk definíció szerint kapcsolódnak egy szervezethez. Ebből következően a szivárogtatási hajlandóságot nagyban befolyásolja a munkavállaló lojalitási szintje. A közösség összetartó erejének, illetve az adott közösséghez tartozás érzetének hiánya megkönnyíti a károkozási szándék kialakulását.

A kockázatot csökkenteni lehet egy átlátható szervezeti működéssel és vezetéssel, valamint egy olyan vállalati kultúra megteremtése is kockázatcsökkentő hatású lehet, mellyel az alkalmazottak könnyen tudnak azonosulni. Ezt a bemenetet a közösséghez való tartozás mértékével jellemeztük (5. ábra):

- Kirekesztett;
- Elfogadott;
- Megbecsült.



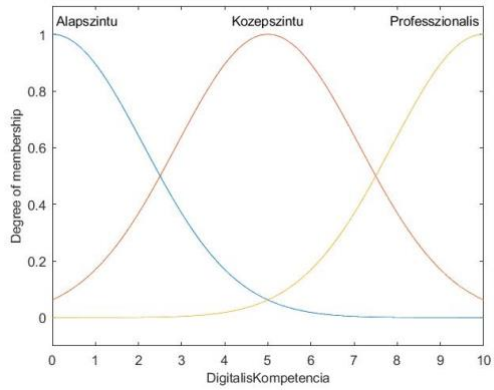
5. ábra: A munkahelyi környezetet leíró tagsági függvények

6.5 Digitális kommpetencia

Szükség van egy olyan bemenetre is, amely segít megkülönböztetni a gondatlanságot és a szándékos károkozást. Ha egy alkalmazottnak nincs elegendő ismerete, amely lehetővé tenné a gyanús esetek megkülönböztetését, akkor a gondatlan adatszivárgás kockázata magasabb. Számos példát láthatunk, ahol egy nagyobb volumenű információbiztonsági incidenst egy informatikai szakember okozott, mivel kiterjedtebb tudással rendelkezett a rendszerről, mint egy kevesebb IT ismerettel rendelkező kollégája. Híres példa erre Edward Snowden, egykori CIA rendszergazda [17]. Ha kevésbé lett volna kompetens, akkor jóval kisebb károkat okozhatott volna.

A skála másik végét vizsgálva megfigyelhető egy pozitív, kockázatcsökkentő hatás. Ezt jól szemlélteti annak a bangladesi banki alkalmazottnak a példája, aki biztonságtudatosságának és felkészültségének köszönhetően 800 millió dollárt tudott megmenteni a munkáltatójának [18]. A digitális kompetencia számos különféle tényezőből áll. Összefoglalva, a következő szinteket azonosítottuk a modellben (6. ábra):

- Alapszintű;
- Középszintű;
- Professzionális.

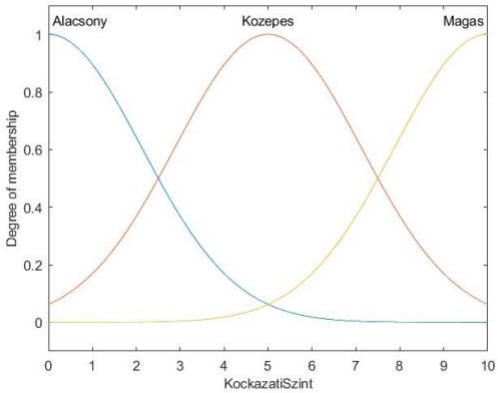


6. ábra: A digitális kompetenciát leíró tagsági függvények

6.6 A munkavállalók kockázati szintje (kimenet)

A rendszer kimenete a munkavállaló-specifikus kockázati érték, amelyet három különböző szintre osztottunk, a 7. ábrán látható módon:

- Alacsony;
- Közepes;
- Magas.



7. ábra: A kockázati szintet leíró tagsági függvények

A rendszert alapvetően az alkalmazott szabályrendszer határozza meg, amely a szakértői ismereteken alapszik. A kockázatértékelési modellben egy teljesen lefedő szabályrendszert alkalmaztunk, azaz a bemenetek bármilyen kombinációjával megfelelő következtetés, kimenet kapható. Az alkalmazott szabályrendszer a következő felépítésű szabályokat tartalmaz:

Szándék == ElhatárolódikTőle és Hajlam == Alacsony => KockázatiSzint = Alacsony (1)

7 MODELL EREDMÉNYEK

A javasolt modellt Matlab Fuzzy Logic Toolbox környezetben valósítottuk meg.

7.1 Potenciális információszivárgás (esettanulmány)

A modell teszteléséhez egy kitalált karaktert határoztunk meg annak érdekében, hogy reprezentálja azt a személyt, aki potenciálisan szivárogtathat bizalmas digitális információkat. Ez a karakter egy agilis irodai dolgozó a vállalat központjában, akit nem motiválnak és állandóan túlterhelnek. Személyisége nem túl stabil és családi problémákkal is küzd. A modellben ezt a karaktert a következő paraméterekkel jellemeztük:

•Szándék (I): MegSzeretnéCsinálni (8);

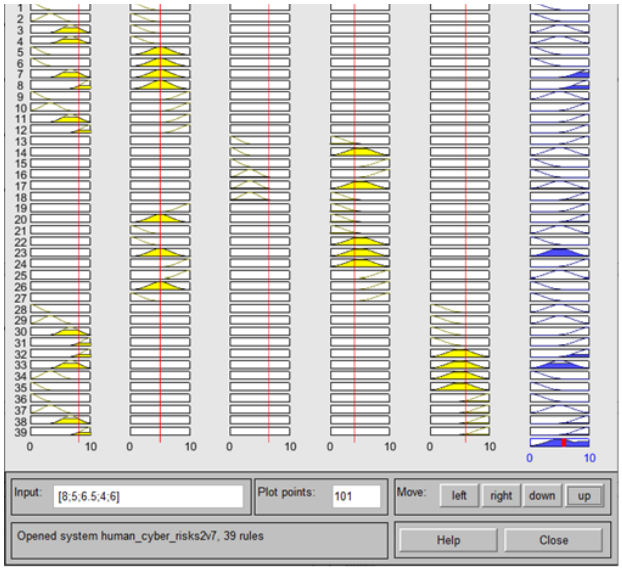
•Hajlam (T): Alacsony (5);

•Pénzügyi helyzet (F): Középosztálybeli (6.5);

•Munkahelyi környezet (O): Elfogadott (4);

•Digitális kompetencia (D): Közepes (6).

A modell 39 szabályból álló rendszerét használva közepes kockázatú (5,67) szintet kaptunk eredményül, amint azt a 8. ábra is szemlélteti.

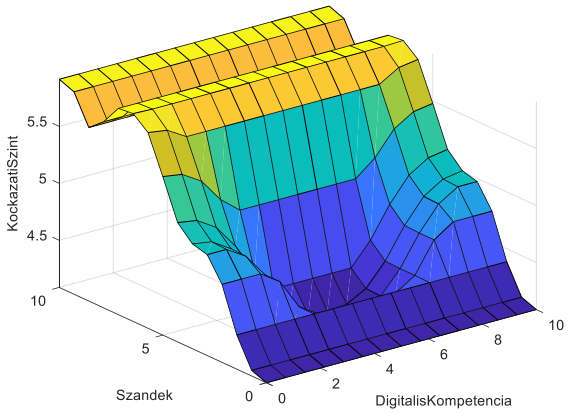


8. ábra: A karakter kockázati szintje

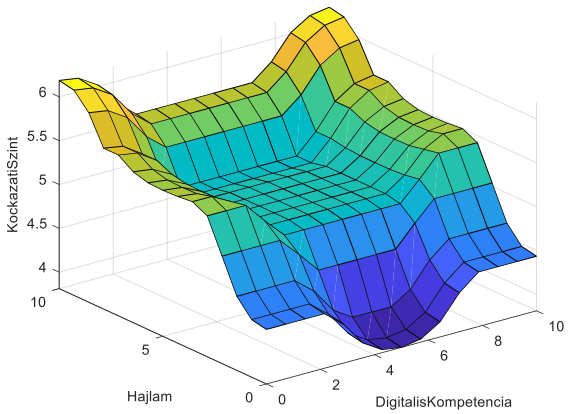
A bemenetek megváltoztatásával a modell eltérő eredményeket mutat. A vállalaton belüli megbecsülést 4-ről 8-ra növelve a kockázati szint változatlanul közepes szintű maradt, azonban kisebb eredménnyel (5). A szándékot 4-re csökkentve a kockázati szint 4,17-re változik.

7.2 A bemenetek hatásai

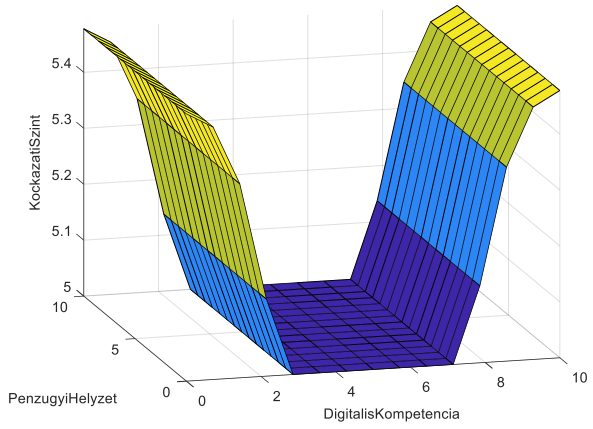
A módszer felhasználásával a különböző bemeneti értékek, így a kockázati szintre gyakorolt hatásuk is könnyen megvizsgálható. Ennek eredményeképpen a digitális kompetencia fontosságát a többi bemenethez képest az alábbi ábrák mutatják: szándék (9. ábra), hajlam (10. ábra), pénzügyi helyzet (11. ábra) és munkahelyi környezet (12. ábra).



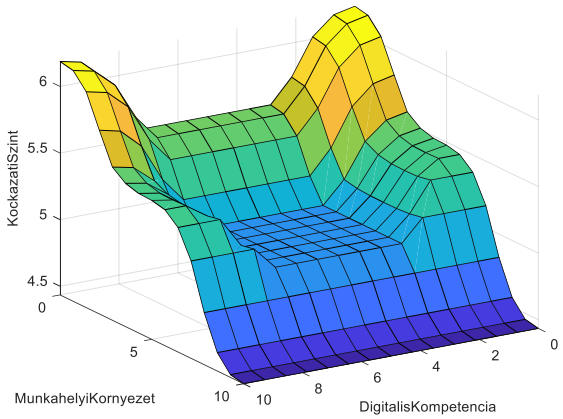
9. ábra: A Szándék és a Digitális Kompetencia hatása a kimenetre



10. ábra: A Hajlam és a Digitális Kompetencia hatása a kimenetre



11. ábra: A Pénzügyi helyzet és a Digitális Kompetencia hatása a kimenetre



12. ábra: A Munkahelyi környezet és a Digitális Kompetencia hatása a kimenetre

7.3 Validálás

A modell validálását mélyinterjúk segítségével végeztük, melyek a terület neves szakembereivel készültek: Hegyi Krisztián (Belügyminisztérium Titokvédelmi Irodájának volt helyettes vezetője), Hegedűs Judit (egyetemi docens, Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Rendészeti Magatartástudományi Tanszék), Fehér Sándor (a White Hat IT Security ügyvezetője).

Az eredmények alapján a modell szabályainak további finomhangolására van szükség, hogy minél pontosabb eredményt adjon a kimeneti oldalon. A különböző személyiség típusok felállítása a következő lépés a szándék, hajlam, pénzügyi helyzet, munkahelyi környezet és digitális kompetencia figyelembevételével. Ezt követően új interjúk készítése szükséges a korábbi interjú alanyok körét bővítve. Ekkor már konkrét kockázati értéket kell kapcsolni az egyes személyiségtípusokhoz a teszt kitöltésekor.

Ha a szakértők által adott válaszok (kockázati értékek) nem közelítik meg a modell által kimeneti oldalon megadott értékeket, akkor szükséges a szabályrendszer elemzése, finomhangolása. Másik továbbfejlesztési irány a bemeneti értékek átgondolása, kiegészítése, módosítása vagy tovább bontása.

8 Összegzés

Ebben a cikkben egy fuzzy modellt javasoltunk a humán faktor kockázati szintjének feltárására a digitális minősített információszivárgás fókuszával. Hipotéziseket fogalmaztunk meg arról, hogy mely tényezők befolyásolhatják a munkaerő kiberbiztonsági kockázati szintjét (bemenetek) és ezek különböző értékei milyen hatással bírnak a kockázati szintre (szabályok). A hipotézisek igazolására interjúkat készítettünk a terület neves szakembereivel, majd az így kapott visszajelzések alapján a fuzzy modell szabályait módosítottuk. A fuzzy modell megbízhatóságának igazolására további interjúk készítése szükséges, ahol az egyes személyiségek kockázati értékének összehasonlítására kell nagyobb hangsúlyt helyezni. A megfelelő modell alkalmazásával a munkavállalók számára meghatározható a megfelelő képzések szintje, így csökkenthető az általuk okozott kockázat szintje.

KÖSZÖNETNYILVÁNÍTÁS

Ez a cikk az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar és a Magyar Fuzzy Társaság támogatásával készült.

HIVATKOZÁSOK

[1] ISACA, The Business Model for Information Security, ISACA.

[2] P. Shakarian, J. Shakarian, A. Ruef (2013). Introduction to Cyber-Warfare. *Elsevier*. pp. 223–239, ISBN: 9780124078147

[3] M. Alotaibi, W. Alfehaid, (2019). Information Security Awareness: A Review of Methods, Challenges and Solutions. *Internet Technology and Secured Transactions*. ICITST-2018.

[4] J. Lukács (2020). A Fuzzy Approach for In-Car Sound Quality Prediction. *Acta Polytechnica Hungarica*. Vol. 17, No. 6, pp. 75-94.

[5] C. Hadnagy, Cristopher (2011). Social Engineering – The Art of Human Hacking. *Wiley Publishing, Indianapolis.* ISBN: 9780470639535

[6] D. Kiss, D. Váczi (2018). Analysis of dangers and attacks against the human network of companies and critical infrastructures based on complex networks. *Hadmérnök.* 2018/1, pp. 151-168, ISSN: 17881919

[7] A. K. Sood, R. Enbody (2014). Targeted cyber attacks. *Elsevier*. pp. 13-18, ISBN: 978-0-12-800604-7

[8] P. Papadimitriou1, H. Garcia-Molina (2009). A Model for Data Leakage Detection. *IEEE 25th International Conference on Data Engineering, ICDE 2009*, China. ISBN: 978-1-4244-3422-0

[9] Security and Privacy Controls for Federal Information Systems and Organizations (2013). *NIST Special Publication* 800-53 Rev. 4.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[11] International Organization for Standardization, "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements", 2013

[12] International Organization for Standardization, ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management (third edition ed.)", 2018.

[13] Zadeh, L. A. (1965) Information and control. *Fuzzy sets*. Vol. 8, No. 3, pp. 338-353

[14] J. Dombi, E. Tóth-Laufer (2020) Reducing the Computational Requirementsin the Mamdani-type Fuzzy Control. *Acta Polytechnica Hungarica*, Vol. 17, No. 3, pp. 25-41.

[15] A.R, Várkonyi-Kóczy (2009). Model Based Anytime Soft Computing Approaches in Engineering Applications. *Balas, V., J. Fodor, A.R. Várkonyi-Kóczy (eds.), Soft Computing Based Modeling in Intelligent Systems (Ser. Studies in Computational Intelligence), Springer Verlag, Berlin, Heidelberg*. pp. 63-92, DOI: 10.1007/978-3-642-00448-3_4

[16] I. Ajzen (1991) The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, vol. 50(2), pp. 179—211.

[17] E. Snowden (2019) Permanent Record. *Metropolitan Books* ISBN: 1250237238

[18] J. F. Gomes, P. Ahokangas, K. A. Owusu (2016). Business modeling facilitated Cyber Preparedness *The Business and Management Review*, Vol. 7 No. 4.