TÓTH TAMÁS

HUMÁN KOCKÁZATOK A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁBAN

Bevezetés

A releváns információk ismerete elengedhetetlen a hatékony feladat-végrehajtáshoz, kellő minőségű és mennyiségű specifikus adat birtoklása nélkül nem lehet megfelelő döntéseket hozni. Mérhetetlen számú információ egyidejű, folyamatos áramlására van ahhoz szükség, hogy a „need to know" és a „need to share" elv érvényesülhessen a közszolgálati és magánszféra területén egyaránt. Ehhez kulcsfontosságú a kommunikációs képességek, csatornák komplex rendszerének, azaz az infokommunikációs infrastruktúrának a fenntartása és védelme. Az infokommunikációs rendszeren[143] belül pedig különös figyelmet kell fordítani a szenzitív, különösen fontos adatok áramoltatásának alrendszereire, azaz a kritikus információs infrastruktúra biztosítására (NATO Polgári Vészhelyzeti Tervezés, NATO Civil Emergency Planning – CEP, 2006).

Információs társadalomban élünk, ahol az adatok lehető leggyorsabb továbbításának fontossága kulcskérdés, legyen az honvédelmi, rendvédelmi, nemzetbiztonsági, gazdasági vagy egyéb jellegű adat. Egy megfelelő pillanatban érkező információ emberéleteket menthet, gazdasági érdekeket befolyásolhat, szavatolhatja a nemzetbiztonságot. A végtelenségig lehetne sorolni a pontos és időben érkező információ rendkívüli jelentőségét. Ugyanakkor ez fordítva is igaz, ha sikerül blokkolni az ellenérdekelt fél tér- vagy időbeli, digitális vagy analóg, verbális vagy nonverbális kommunikációs csatornáit, a jelentkező adathiány okán

[143] Infokommunikációs rendszer alatt az adatok gyűjtésére, felvételére, tárolására, feldolgozására (megváltoztatására, átalakítására, összegzésére, elemzésére, stb.), továbbítására, törlésére, hasznosítására (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozására használt elektronikus eszközök, eljárások, valamint az üzemeltető és a felhasználó személyek együttesét értem. *(.(Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, 16. o. Budapest, 2007)*

lépéselőnybe kerülhetünk, mi több, akár vissza nem fordítható folyamatokat generálhatunk a támadott fél részére.

Manapság az információk legtöbb esetben elektronikus jel, rádiófrekvenciás hullámok formájában, technikai úton terjednek, mivel ezek gyorsaságával a papír alapú kézbesítés nem veheti fel a versenyt. Ezen csatornák biztosítása a fentiek alapján kézenfekvő és indokolt, magában rejti az elvárást a védelem és biztonság iránt. (*Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17.)* De a leglényegesebb dolgot, miszerint ezeket humánerő, azaz személyek tervezik, alkalmazzák, üzemeltetik és tartják karban, nagyon nagy felelőtlenség lenne figyelmen kívül hagyni. Lehet egy digitális infokommunikációs csatorna akármennyire védett informatikai, fizikai szempontból, ha az azt alkalmazó személyek feladataik ellátása során nem elég körültekintőek, nem rendelkeznek a megfelelő biztonságtudatos magatartással, illetve alkalmasak ellenérdekelt befolyás hatására, ezen hálózatok szabotálására.
A lehető legjobban üzemelő, komplex biztonsággal rendelkező információs infrastruktúra hatékony működésének szavatolásában elengedhetetlen a személyi állomány biztonságának kialakítása a fizikai, elektronikus és adminisztratív védelem területén. Az elektronikus információs rendszerek teljeskörű védelemének biztosítása jogszabályi kötelemként jelenik meg a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 5§-ának b*)* pontjában.

1. Tudományos hipotézisek

- Az kritikus információs infrastruktúra fogalma nem egységes, így nélkülözhetetlen annak megalkotása.

- A humán kockázatok jelentősége egyre nő az információbiztonság területén, ezért átfogó vizsgálata, csoportosítása elengedhetetlen a megelőzés érdekében.

- A helyi humán kockázatok eszkalációjában rejlő veszélyek kialakulása globális problémákat jelenthet, melyek megelőzése nélkülözhetetlen a nemzeti és nemzetközi komplex biztonság megteremtése érdekében.

2. Pályázati célkitűzések

Kutatásom során az alábbi célokat tűztem ki:

- Definiálni a kritikus információs infrastruktúra fogalmát, tartalmát és alkotóelemeit, illetve felhívni a figyelmet a benne rejlő humán kockázati elemekre.

- A humán kockázatokat csoportosítani, a csoportokat elemezni, valamint szemléltetni esetleges eszkalációjukat, gyakorlati példákon keresztül.

- Felállítani egy komplex képet a humán kockázatokban rejlő rendkívül nagy veszélyforrásra, az infokommunikációs rendszerek vonatkozásában.

- Kiindulási alapot teremteni a kritikus információs infrastruktúra védelem jogszabályi biztosítékainak, kockázat kezelésének, valamint megelőzésének későbbi kutatásához.

3. Kutatási módszerek

A pályázat elkészítése során kezdetben, a korábbi tanulmányaim alatt megszerzett ismereteim kibővítése céljából, a kritikus infrastruktúrával, valamint a humán kockázatokkal kapcsolatos tudományos, szakirodalmi források kerültek feldolgozásra, majd ezt követően nyílt forrásokban megjelenő publikációkat elemeztem és emeltem be a tanulmányba.
Felhasználtam szakmai konferenciákon elhangzott előadások elemeit is, melyek még komplexebbé, és hitelesebbé teszik a kutatást.

1. Fejezet

Humán kockázatok értelmezése a kritikus információs infrastruktúra tükrében

1.1. A kritikus információs infrastruktúra meghatározása

A fogalom maradéktalan meghatározásához lényeges az egyes elemek értelmezése. Elsőként az infrastruktúra fogalmát szükséges meghatározni, ezt különböző szakirodalmak próbálják definiálni.

A Magyar Larousse Enciklopédia definiálása szerint az infrastruktúra „*a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér. Legfontosabb elemei a közművek, az energiaellátás rendszere és a közlekedési, hírközlési hálózat (utak, vasutak, telefonhálózat, stb.). Az ún. lakossági infrastruktúrához tartozik a lakásállomány, a kereskedelmi és szolgáltatási hálózat, az egészségügyi, szociális, kulturális ellátás, az oktatás eszközei és intézményrendszere (kórházak, rendelőintézetek, iskolák).” (Magyar Larousse Enciklopédikus szótár, Akadémiai Kiadó, Budapest, 1992.)*

A Magyar Értelmező Kéziszótár meghatározása szerint az infrastruktúra olyan angolszász eredetű szó, amely jelentése *„a társadalmi, gazdasági tevékenység zavartalanságát biztosító alapvető létesítmények, szervezetek (pl. lakások, közművek, a kereskedelem, a távközlés, az oktatás, az egészségügy stb.) rendszere.” (Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.)*

Egy másik meghatározás szerint az infrastruktúra nem más, mint *„egy adott rendszer (termelő vagy elosztó, szolgáltató rendszer, tudományos, állami, magán, nemzeti vagy nemzetközi szervezet, ország, város, vagy régió stb.) rendeltetésszerű működéséhez feltétlenül szükséges intézetek, intézmények, felszerelések és berendezések és a működtetést ellátó személyzet szabályszerűen működő összessége. Az infrastruktúra tehát a fizikai építményekből és berendezésekből és azokat szakszerűen működtetni tudó szakszemélyzetből áll.” (*Haig Zsolt, *Várhegyi István ezredes: Hadviselés az információs hadszíntéren, Zrínyi, Budapest, 2005.)*

A fenti meghatározások alapján, az infrastruktúra a gazdaságtudományban megjelenő fogalom, amely magában foglalja azon gazdasági javakat, folyamatokat, melyek közvetlenül nem, de közvetve befolyásolják a nemzetgazdaság elemeinek fejlődését, mind termelési, mind innovációs szinten.

Az információ nem más, mint „bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.” *(2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 5§ 25)*)

A kritikusság lényegi megfogalmazása alapján, *„kritikus minden "dolog" amelyek megsemmisülése, működésének vagy szolgáltatásainak alacsonyabb szintje, elérhetőségének megszűnése vagy csökkenése valamilyen támogatott objektumra, folyamatra jelentős (ebben az esetben egyértelműen negatív) hatást gyakorol.” (Dr. Bognár Balázs PhD pv. őrnagy: A kritikus infrastruktúra, OKF Iparbiztonsági link, forrás: http://www.katasztrofavedelem.hu/index2.php?pageid=pvl_kritikus_infrastr-uktura (letöltés ideje: 2017.szeptember.12)*)
Mindezek alapján egy folyamat, vagy rendszer kritikusságát az határozza meg, hogy egy bekövetkező támadás, vagy kapacitáshiány, milyen negatív hatással lesz más, szorosan hozzá kapcsolódó rendszerekre, azaz a kármérték nagysága a viszonyítási alap.

Valójában értelmezési szempontból nem létezik kritikus információs infrastruktúra, hiszen e három szó összekapcsolása egy igen nehezen értelmezhető fogalmat alkotna.
„Már a kritikus jelző használata sem a legjobb, hiszen nem az infrastruktúra a kritikus, hanem annak elvesztése, sérülése válhat kritikussá, ezért célszerűbb lenne a – néhány fordításban használt – létfontosságú kifejezést használni. Az információs infrastruktúra sem igazán szabatos kifejezés magyarul, mert abba például a könyvtárakat is bele kell érteni, holott mindenki érti és érzi, hogy itt nem információs, hanem elektronikus információs infrastruktúrákról van szó.”(Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007. 11. o.) Ennek ellenére a kritikus információs infrastruktúra fogalom honosodott meg mind a köznyelvezetben, mind a tudományos nyelvezetben egyaránt, pedig szövegkohéziós szempontból a *„létfontosságú elektronikus információs infrastruktúra”* kifejezés alkalmazása lenne nyelvtanilag helyes. A tudományos nyelvezet használata okán továbbra is a kritikus információs infrastruktúra használatára kerül sor a pályázat további fejezeteiben is.

A fentiekből levezetve a kritikus információs infrastruktúra nem más, mint nemzeti vagy nemzetközi szinten, az általánosan értelmezett biztonság elemei számára, a szellemi és tárgyi életfeltételekhez szükséges információk áramlását biztosító szervezetek, létesítmények, hálózatok, információs-technológiai berendezések összessége, melyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése negatív hatással járhat.
Ez esetben a kármértéket, az információs infrastruktúra nem megfelelő működéséből adódó károk fogják meghatározni. Tehát azt kell vizsgálni, hogy az adat hiánya milyen kimenetelű döntések akadályozását, illetve ellehetetlenítését eredményezheti.

1.2. A humán kockázat meghatározása

Az információs infrastruktúrát vizsgálva, elsődleges humán kockázatokat a felhasználók, azaz a kommunikációs felek, valamint az üzemeltető-szakszemélyzet, vagyis a rendszergazdák, karbantartók, illetve a beszállítók jelenthetnek. A személyi állománynak tisztában kell lennie, milyen jelentőségű információk és döntési lehetőségek birtokába kerülhet, melyek privilegizált célpontjává tehetik őket bűnszervezetek vagy ellenérdekelt szolgálatok számára.

A humán kockázat fogalmi meghatározásához, meg kell vizsgálnunk a „humán” szó jelentését, illetve definiálni kell a kockázat fogalmat, mint biztonságot veszélyeztető tényezőt. Érdemes megvizsgálni a kockázat általános és nemzetbiztonsági meghatározását.
A kockázat általános megfogalmazása: *„a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.” (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1§ 28)*)
A kockázat meghatározása nemzetbiztonsági aspektusból nem mást, mint *„az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek.” (Dr. Resperger István mk. alezredes: Nemzetbiztonsági alapismeretek, 2. Fejezet Biztonsági kihívások, kockázatok és fenyegetések 2030-ig, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 31. o.)*

Mind a két fogalomban megjelenik a veszélyeztetettség lehetősége. Abban az esetben, ha ezeknek a kockázati tényezőknek a forrása, valamely személyhez köthető magatartás, humán kockázatokról beszélhetünk.
Humán kockázatnak minősülnek azok, a személyi állománynál fennálló körülmények, - különösen a negatív személyiségjegyek, konfliktusokkal terhelt környezeti vagy élethelyzetekből származó fenyegetettségek, életviteli és mentális problémák - amelyek fennállása önmagában nem, de az adott, fokozott kockázatú munkakörökben végzett feladattal összefüggésben, fenyegetettséget jelenthetnek az általánosan értelmezett biztonság egyes összetevőire.

Ilyen kockázati tényezőt jelenthet a nem megfelelő informatika-biztonsági ismeretek és a szabályozók hiánya, amelyek következtében a felhasználók magas kockázatú adatokat tárolhatnak, nem megfelelő biztonsági elemekkel ellátott adathordozón. A hordozóeszköz megszerzése esetén, az ellenérdekelt fél könnyen hozzájuthat az infokommunikációs rendszer titkosságát veszélyeztető adatokhoz, például felhasználó nevekhez, jelszavakhoz, kriptográfiai adatokhoz.
Egy megsértett, kiábrándult beosztott, szintén magában hordozza a kockázati tényezőt. Az ilyen alkalmazott elkeseredettségében, dühében a vezetővel szembeni személyes konfliktus okán, képes blokkolni az információáramlást, így nem jutnak el vagy téves adatok érkeznek a döntési folyamatban résztvevő személyekhez, elindítva akár mérhetetlen károkkal járó, egy rossz felsővezetői döntéshez vezető folyamatot.
Nem szabad megfeledkezni a bűnszervezetek és idegen titkosszolgálatok által egyre jobban kedvelt pszichológiai manipuláció módszeréről, azaz a social enginering alkalmazásáról sem. A folyamat célja, kiválasztani egy releváns adatokkal rendelkező, vagy ilyen adatokhoz hozzáférő beosztottat, vagy vezetőt a megtámadni kívánt szervezet állományából, majd a bizalmába férkőzve, ezen adatokat kiszivárogatni a támadás végrehajtásához, esetleg felhasználni a beszervezett egyént a végrehajtási folyamatokba is. *(Alissa Torres: A pszichológiai manipuláció (social engineering), OUCH, The SANS Instute 2014, 2014. 11. forrás: https://securingthehuman.sans.org/newsletters/ouch/ issues/OUCH-201411_hu.pdf (letöltés ideje: 2017. szeptember. 12)*

Ahhoz, hogy komplexen lássuk a kockázati amplitúdót és fel lehessen állítani egy kockázati rátát, szükséges a folyamat kiindulópontjaként az információ áramoltatás rendszerébe való bekerülést, azaz a humán „in-put”-ot meghatározni.

Ez annyit jelent, hogy ellenőrizni kell a kockázati tényezők meglétét minden olyan személynél, aki a kritikus információs infrastruktúra rendszerében kíván feladatot ellátni, még a munkakör betöltése előtti előszűrés végrehajtásával. Azaz, az információs infrastruktúra szemszögéből vizsgálva, közvetett kockázat monitoring zajlik. Ez lényegében annyit jelent, hogy egy hatalmas kockázati halmazból ki kell szűrni azokat az elemeket, amelyek nem rendelkeznek kockázati tényezővel. A rendvédelmi szervek esetében, erre szolgál például a nemzetbiztonsági ellenőrzés *(1995. évi CXXV. törvény - a nemzetbiztonsági szolgálatokról 4§ 9) 5§ f) 6§ r) 8§ f)*), illetve a Nemzeti Védelmi Szolgálat által végrehajtott kifogástalan életvitel ellenőrzés *(293/2010. (XII. 22.) Korm. rendelet a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve kijelöléséről, valamint feladatai ellátásának, a kifogástalan életvitel ellenőrzés és a megbízhatósági vizsgálat részletes szabályainak megállapításáról 7§ (1) d)*). A rendvédelmi szervek állományába kerüléshez, az egészségügyi, pszichológiai alkalmassági vizsgálatokon történő megfelelés, szintén törvényi kötelem. *(2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról 33§ c)*). A szűrések végrehajtása során a munkakört betöltő személynél vizsgálják, hogy előélete során, milyen kockázatot jelentő élethelyzetbe került, milyen kapcsolati hálóval rendelkezik, megfelel-e a szenzitív adatok biztonságát biztosító markerek szintjének, nincsenek esetleges szervi, személyiségbeli, pszichés betegségei, amelyek alkalmatlanná teszik a beosztás betöltéséhez.

Az előszűrés végrehajtásának negatív eredménye előtt (pozitív kockázati tényező esetében alkalmatlan az „in-put”), a teljes folyamatot vizsgálva rendkívül magas a kockázati arány, ami persze leredukálódik a legoptimálisabb esetet vizsgálva, hiszen kockázati tényezőt nem tartalmazó humánerő kerül az információs infrastruktúra rendszerébe. Sajnos egyre nagyobb problémát jelent a nem kellő biztonságtudatos magatartás megléte, és továbbfejlesztésének lehetősége a potenciális munkaerő körében. Ennek szűrésére bizonyos rendvédelmi szervek kivételével, már a felvételi vizsgálatok alkalmával sem fordítanak kellő figyelmet a közigazgatási szervek, valamint a magánszektor elemei.

A felvételt megelőző időintervallumban a lehetséges kármérték igen alacsony, ami annak köszönhető, hogy a felvételiző nem rendelkezik valós ismeretekkel a kritikus információs infrastruktúra működésével kapcsolatban.

A következő szinten, a tényleges feladat-végrehajtás során felmerülő közvetlen kockázatok helyezkednek el. Ebben a szakaszban hajtódnak végre az információ létrehozásával, továbbításával, feldolgozásával kapcsolatos feladatok. Tényleges adatok birtokába kerül a humánerő, ez a legszenzitívebb része az információs rendszer működésének, hiszen ekkor van a legnagyobb relevanciája károsítani az infrastruktúra valamely elemét az alkalmazottnak. Ugyanakkor, egy megfelelően működő előszűrő rendszer esetén ekkor kellene a legalacsonyabb szintűnek lennie a kockázat fenyegetéssé alakulásának, mivel olyan személy került be a rendszerbe, aki nem rendelkezik biztonsági kockázattal. A munkáltató által a biztonságtudatos magatartás tovább fejlesztése, a közbenső szűrő és elhárító tevékenység is folyamatos kell, hogy legyen.
A kockázati ráta viszont nem redukálható le nullára, mivel az információkhoz való hozzáférés növeli a humán kockázat mértékét. Ebben a folyamatban van lehetőség az információ áram blokkolására, adatok kiszivárogtatására, a rendszer működésének akadályozására. A humán kockázat, ha az aktív munkavégzése során válik valós fenyegetéssé, vagy tényleges károkozássá, a kármérték ekkor lesz a legmagasabb. Ezen szakaszban van lehetőség a döntéshozó számára szükséges adat elérhetetlenné tételére, illetve a jogosulatlan szervezetek számára való hozzáférhetővé tevésére, akár aktív, akár passzív módon. A humán kockázat általi károkozás lehetősége, a tényleges munkafeladat végrehajtása során fenyeget a legnagyobb károkozással.

A harmadik fázis az „out-put” oldal, ekkor a munkaerő kikerül a kritikus információs infrastruktúra működtetésének rendszeréből. Ennek legoptimálisabb szakasza a nyugállományba vonulás. A kockázat egyik oldalról csökken, hiszen nem kerül a volt humánerő újabb aktuális információk birtokába, illetve a legoptimálisabb helyzetben a kialakult, magas szintű biztonságtudatos magatartás okán, nem is szivárogtathat ki korábban megszerzett adatokat, így a lehetséges kármérték újra leredukálódik.

Másik oldalról viszont nő a kockázat, hiszen a rezsimszabályok alóli kikerülés és egyéb, később vizsgált változó személyiség jegyek miatt, a biztonságtudatos magatartás csökken, megjelenhet az új környezet előtti megfelelési kényszer, ebből fakadóan a túlzott közlékenység. A teljes kockázati amplitúdót vizsgálva viszont megállapítható, hogy a károkozás mértéke szintén alacsony, akár csak az „in-put" szakaszban, hiszen a volt dolgozó nem rendelkezik töménytelen, aktuális döntési folyamatokat befolyásoló információval, illetve tényleges támadást nem tud végrehajtani a kritikus információs infrastruktúra ellen. *(1. számú melléklet)*

Kilépés, felmondás és elbocsájtás esetén a kockázatok nem redukálódnak ilyen alacsony szintre, inkább adott pillanatban jelentősek, hiszen a munkaviszony megszűnésének ezen eseteit kiválthatja valamilyen negatív érzés (sértődés, féltékenység, ellenszenv), amit kockázati tényezőnek kell értékelni.

A fentiek alapján kijelenthető, hogy vannak a kockázatot befolyásoló tényezők. Ilyen lehet az egyén biztonságtudatossága, a rendelkezésére álló információk mennyisége és minősége, a lehetséges károkozás mértéke, valamint egyéb külső ingerek. *(Dr. Kovács Zoltán András ezredes, Dr. Regényi Kund ezredes: Nemzetbiztonsági alapismeretek, 4. Fejezet Biztonság tudatosság: humán kockázatok, technikai kockázatok, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 73. o.)* A humánkockázat mértékét leghatásosabban személyi oldalról lehet csökkenteni, mivel a kármértéket nem egyedi tényezők, hanem komplex elemek alkotják. Ezért érdemes a személyi állomány oldaláról elemezni, majd csoportosítani a kockázatok jellemzőit, későbbi minimalizálásuk érdekében.

2. Fejezet
Humán kockázatok csoportosítása

Ahhoz, hogy a legátfogóbban ismerjük a humán kockázatok jellemzőit, és a leghatékonyabban lehessen fellépni ellenük, érdemes csoportosítani őket alanyi oldalról bűnösség szerint, a kockázatokat meg kell határozni eredet szerint, továbbá meg kell vizsgálni, hogy a kockázat milyen célzattal alakulhat ki.
A csoportosítás szempontjai az elemek bizonyos tulajdonságai alapján kerültek felállításra, de a csoportok között rendszerint átfedés van. Például attól, hogy valamely kockázati tényező szándékos magatartást feltételez, még lehet külső vagy belső tényező.

2.1. Bűnösség szerint

Először alanyi oldalról vizsgálva, meg kell különböztetni a kockázati magatartást szándékos illetve gondatlan végrehajtási lehetőségek alapján. Kockázati tényező lehet nem megfelelő körültekintés eredményeként bekövetkező, hanyagul, gondatlanul elkövetett cselekmény, illetve akaratlagos, tettleges, azaz szándékos elkövetési magatartás is. *(Balogh Ágnes, Tóth Mihály: Magyar büntetőjog. Általános rész, TAMOP 4.2.5 Pályázat, Osiris Kiadó, Budapest, 2010, forrás: http://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_520_magyar_buntetojog/ch03s06.html (letöltés ideje: 2017.szeptember 15.)*

2.1.1. Gondatlan magatartás

A gondatlan kockázati tényezők legfőbb generálója, a nem megfelelő biztonságtudatos magatartás eredményezte hanyagság, mely következtében az infrastruktúra biztonságát hivatott szabályozók figyelmen kívül hagyása történik. Ilyen esetek lehetnek például a rendszer működtetéséhez szükséges adatok nem megfelelő kezelése, szenzitív információkat tartalmazó jegyzetek megsemmisítésének elmulasztása, mások számára is hozzáférhetővé tevése. Elektronikus adatok nem megfelelő hordozón történő tárolása, amely által könnyen megismerhetővé válnak inkompetens személyek számára. (Horváth Gergely Krisztián: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Kormányzati Informatikai Fejlesztési Ügynökség, Budapest, 2013. 26. o.)

Rendkívül nagy problémát jelent a túlzott közlékenység, amely során szenzitív információk szivároghatnak ki. A minősített adatkezelésben nincs bizalom, soha nem tudhatjuk, hogy hobbink, magánéletünk során kikkel kerülhetünk kapcsolatba. Igen felelőtlen dolog lenne azt hinni, hogy értékes információk birtokába lévő személyt leplezett módon nem kereshet fel ellenérdekelt szolgálat fedett alkalmazottja. Biztonsági kockázatként kell értékelni minden új kapcsolatot, aki túlzott bizalmaskodást és támogatást kínál, még ha eleinte ezt ellenszolgáltatás fejében is teszi.

Rendkívüli módon sértheti a biztonságot, a jó szándékból elkövetett normák megsértése. Az objektumokba való belépési feltételeket meghatározó szabályozók figyelmen kívül hagyása igen nagy kockázati elem, például egy kollégának kiadó személy belépésének biztosítása saját belépőkártyánkkal, belépő ponton keresztül, mivel arra hivatkozik, hogy otthon felejtette a sajátját. Ez a helyzet ellenőrző-áteresztő pontokon való áthaladáskor is igen nagy problémát jelenthet, mivel illetéktelen személyek védett objektumon belüli mozgását biztosítjuk, ami által blokkolhatják az infokommunikációs rendszert. Így az elkövetők mozgása nem lesz nyomonkövethető és dokumentált, amely által a védett információk könnyen megismerhetővé válnak inkompetens személyek számára.

Hatalmas kockázat rejlik a tudatmódosító szerek fogyasztásában is. Az ezek által előidézett kontrolálatlan pszichés állapotot, igen nagy hatékonysággal ki tudják használni az erre szakosodott személyek, így érzékeny adatokhoz jutva a kommunikációs rendszerről. Nem véletlenül szükséges az efféle kockázatokkal rendelkező humánerőt, már a szervezethez kerülés előtt kiszűrni, hiszen magas veszélyekkel járhat az adatszivárogtatás lehetősége.

A fenti példák jól mutatják, hogy nem károkozási céllal szegte meg a humánerő a biztonsági normákat, hanem hanyagságból, következetlenségből, mely abból ered, hogy nincs tisztában magatartásának esetleges biztonságot veszélyeztető következményeivel. Rendkívül fontos ez esetben a biztonságtudatos magatartás folyamatos fejlesztése, oktatása és szavatolása a munkáltató részéről, hisz másképp nem sikerülhet a mulasztás eredményezte humán kockázati elemeket leredukálni. *(Dr. Kovács Zoltán András ezredes, Dr. Regényi Kund ezredes: Nemzetbiztonsági alapismeretek, 4. Fejezet Biztonság tudatosság: humán kockázatok, technikai kockázatok, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013. 74-78. o.)*

2.1.2. Szándékos magatartás

A szándékos elkövetés büntetőjogi szankcionálása a legsúlyosabb, hiszen itt a károkozás bekövetkezése akaratlagos tevékenység útján valósulhat meg. (*2012. évi C. törvény a Büntető Törvénykönyvről/1998. évi XIX. törvény a büntetőeljárásról)*. A humánerő szándékos károkozásának kockázati lehetősége, mindig valamilyen inger hatására jön létre. Az előszűrések elvileg megakadályozzák a rendszerbe kerülését, olyan elemeknek, akik anyagi, ideológiai vagy pszichés okokból, károkozási szándékkal kívánnak az információs infrastruktúra rendszerébe bekerülni, de a hatalmas személyi állomány feladatának végrehajtása során, nagy kihívást jelent a folyamatos szűrés.
Kialakulhat olyan helyzet, amikor a munkavállaló munkáltatóval szembeni sértettsége, a rendszerbe való csalódottsága, kiábrándulása, esetleges bűnözői csoportokkal való kapcsolatba kerülése, magában hordozza a szándékos károkozás lehetőségét. Ilyen ok lehet az extrém munkahelyi stressz, a vezető nem megfelelő irányítási, személyügyi módszerei, az egyénben rejlő innovációs lehetőségek elfojtása, a munkatevékenység nem megfelelő értékelése.

Igen nagy kockázat rejlik már az előszűréskor is vizsgált függőségekben és szenvedélyekben egyaránt, akár legyen az az alkohol, a kábítószer, a szerencsejáték, valamint a nagy vagyoni hátteret kívánó luxus hobbik. A függőségét, szenvedélyét a dolgozó minden áron ki akarja elégíteni, ehhez nem sajnálva időt, anyagi fedezetet, amit egy idő után csak a munkabérén felüli forrásokból tud pótolni, így adósságcsapdába kerülhet. Amennyiben a kapott összeget nem tudja törleszteni a dolgozó, információkat kérhetnek tőle a „hitelezői", esetleg kereskedni kezdhet a birtokába lévő adatokkal, adathordozókkal. A közelmúltban a Brit Királyi Haditengerészet egy fegyvermérnöke, a rendszeresített rakétákra vonatkozó adatokkal teli laptopokat adott el ismeretleneknek, aminek bevételeit hatalmas kaszinó tartozásainak törlesztésére fordította. *(Humán kockázatok: a leggyengébb láncszem, Crisma, forrás*: *http://www.carisma.hu/cikkek/human_kockazatok.html. (letöltés ideje: 2017. szeptember. 17.)*

Nagy figyelmet igényel az is, ha a humánerő magánélete során szimpatizálni kezd ellenérdekelt szervezetek tevékenységével, esetleg bűnszervezet tagja lesz. A rendszerbe való passzív csalódottságát egyfajta aktív cselekvésre való akarat váltja fel, például ellenérdekelt hírszerző tevékenység támogatása során. Vallási radikalizálódás esetén, fennáll a lehetősége

egy terrortámadás támogatására a támadott fél kommunikációjának blokkolásával, mely hatására a reagáló erők nem lesznek képesek az információcserére, így meghiúsítva az elhárítás és mentesítés folyamatát. *(Dr. Kis-Benedek József: Célkeresztben az Iszlám Állam, Ludovika Szabadegyetem, Budapest. 2015.11.10.)*

2.2. Eredet szerint

A kockázatokat vizsgálni kell forrásuk szerint, vagyis meg kell határozni, hogy milyen eredetűek. Eszerint a kockázat lehet külső forrás, egy potenciális dolgozó jelölt, valamint lehet belső humán forrás, miszerint a kockázati tényezőt egy racionális munkatárs jelenti. A továbbiakban szétválasztásra kerül a külső támadó bejuttatása és a támadók által megtévesztett, vagy hanyag magatartást tanúsító humán kockázati elem fogalma, illetve köztes csoportként elemzésre kerül a menesztett alkalmazottak köre.

2.2.1. Külső forrás

Külső forrásként kell tekinteni azokra az elemekre, akik a kritikus információs infrastruktúrán kívülről érkező veszélyeztető tényezők, még akkor is, ha egyes tagjaikat sikerült a rendszerbe betelepíteniük. Fontos a külső humán kockázati tényezők kategorizálása az információs infrastruktúrához viszonyított elhelyezkedésük alapján.

Legtávolabb állnak a passzív közvetett tényezők. Ezek az elemek azok a bűnszervezetek, ellenérdekelt szolgálatok, akik veszélyeztethetnék a rendszer működését, de a vizsgált időszakban ilyen irányú szándék, vagy tevékenység nem jellemzi működésüket. Rendkívül nagy jelentősége van a hírszerző modulok működésének a számunkra negatív elemek feltérképezésében és lokalizálásában.
Őket követik az aktív közvetett tényezők, akik már tevőlegesen törekednek a szervezetbe férkőzni. Ez annyit jelent, hogy tagjaikat megpróbálják felvételiztetni, bejuttatni valamely részegység állományába, így előkészítve a műveleteikhez szükséges stratégiai pontokat. Ezen tényezők blokkolását az előszűrő rendszerek kifogástalan működésének kellene szavatolnia.
Következő szinten számolunk az igen nagy fenyegetést jelentő passzív közvetlen humán kockázati tényezőkkel, akik a nem megfelelően működő lokalizációs hírszerző tevékenység és előszűrő rendszerek okán bekerültek az infokommunikációt biztosító szervezetbe. Itt már a tényleges károkozás lehetőségével kell számolni, hiszen valós adatokhoz jutnak a kockázati

tényezők a rendszer működésével kapcsolatban, így azt blokkolhatják is. Ezen a szinten a szervezet belső elhárító mechanizmusai hivatottak az illegális szándék feltérképezésére és a rendszerből való kiemelésére a lehetséges károkozás megelőzése céljából.
A negyedik lépcső, amikor a humán kockázat a fenyegetésen túl tényleges károkozásként jelenik meg, vagyis aktív közvetlen kockázati tényező realizálódik a kritikus információs infrastruktúrában. Ekkor beszélhetünk racionális támadóról, aki ténylegesen információkat szolgáltat ki a rendszer működéséről, akadályozza a kommunikációt, háttértámogatást nyújt illegális tevékenységek végrehajtásához az ellenérdekelt küldő szerv részére. Ebben a szakaszban a belső elhárító egységek mellett a külső társszervek feladata a támadás lokalizálása és elhárítása. Abban az esetben, ha idáig képes egy bűnszervezet valamely tagját eljutatni, akkor a biztonsági elemek működése rendkívül sok kívánni valót hagy maga után, hiszen minimum három biztonsági lépcsőt sikerült deaktiválnia a támadó félnek.

2.2.2. Belső forrás

Belső kockázati tényezőként kell tekinteni az információs infrastruktúrát működtető személyi állományt és a hozzájuk köthető egyéb humán kapcsolataikat. Belső forrásnak számít a dolgozó abban az esetben is, ha egy külső kockázati forrás befolyásával, megtévesztésével hajt végre akciót, illetve ha fennáll a lehetősége, hogy mulasztással szivárogtat ki információkat.
A munkaviszony ideje alatt a munkavállaló magánéletében számos olyan esemény történhet, amely magatartását negatív irányba befolyásolhatja. Ebben az esetben azok a személyek, akik nem rendelkeznek kellő biztonságtudatos magatartással, és elég fegyelemmel a normák betartása iránt, sajnos könnyen megszeghetik az előírásokat. Nem tudnak magánéleti problémáik miatt kellően koncentrálni a munkafolyamatok kifogástalan végrehajtására, így károkat okoznak a rendszer működésében. Nem kellő odafigyeléssel kezelik a rájuk bízott adatokat, amelyek megsemmisülhetnek, megsérülhetnek vagy hiány keletkezhet bennük.
Például egy rendszergazda úgy telepít újra egy operációs rendszert, hogy nem mentett le minden adatot merevlemezre, így az újratelepítés során azok megsemmisülnek.
Magas kockázati elemeket hordoz magában az alkalmazott kiégése, sértettsége, kapzsisága. Ez esetben elég csak azt megvizsgálni, milyen károkkal járhat, ha egy dolgozó, hon- vagy rendvédelmi alakulatok által használt rádiójel átjátszó tornyoknak a pontos helyére, és védelmi fokára vonatkozó adatokat csempész ki anyagi ellenszolgáltatás fejében bűnözői

csoportok, vagy ellenséges államok számára. Így pontos ismeretek kerülhetnek a birtokukba a kommunikációs hálózat megbénításának végrehajtásához, egy esetleges katonai művelet során.
Ezen példák jól mutatják, hogy a humán „in-put”-ra jellemző kockázatok, a munkaviszony ideje alatt is kialakulhatnak.

Rendkívüli nagy kockázati tényező a világháló, azon belül is a közösségi oldalak, levelező rendszerek nem kellően körültekintő alkalmazása. Ezeken a humánerő, hanyag biztonságtudatos magatartásának következtében, mindenki számára hozzáférhető adatokat adhat meg magáról, családjáról, barátairól, hobbijáról, munkahelyéről és az ott végzett tevékenységéről.
Léteznek mindenki számára hozzáférhető adathalász programok, melyek segítségével bárki a számára érdekes személyről, mérhetetlen mennyiségű, az internetre feltöltött és hozzájuk kapcsolható információt gyűjthet össze. Ezeket számos bűnszervezet is alkalmazza, így szerezve megtévesztéshez, befolyásoláshoz, zsaroláshoz szükséges adatokat a ” leggyengébb láncszemről”. *(Horváth Gergely Krisztián: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Kormányzati Informatikai Fejlesztési Ügynökség, Budapest, 2013. 36-66. o.)*

Az Egyesült Királyságbeli Sophos Group Plc. egy 2010-es jelentése szerint, a közösségi oldalakon robbanásszerűen megnőtt a kártékony programok és spamek száma. A jelentés szerint 2009-ben a közösségi oldalakat használók 57%-a számolt be arról, hogy profilját spamelték[144]. Ez 70%-os növekedést jelent 2008-hoz képest. A vizsgált 500 vállalat vezetőjének ¾-e úgy tartja, hogy alkalmazottai humán kockázatot jelentenek, hiszen munkaidőben látogatják a biztonsági szempontból nem megfelelő közösségi oldalakat. *(Durbák Ildikó: Ellopott céges információk, Profession, 2010, Forrás: https://www.profession.hu/cikk/20100722/ellopott-ceges-informaciok/401#, (letöltés ideje: 2017. szeptember 17.)*

[144] Spam: elektronikus úton továbbított kéretlen reklámlevél *(Dr. Dósa Imre: A Spam jogi szabályozása, 2004. 1. o. forrás: https://nws.niif.hu/ncd2004/docs/ehu/112.pdf (letöltés dátuma: 2017. szeptember 22.)*

A gondatlan eredetű humán kockázatok felhasználásával bűnözői csoportok, ellenérdekelt szervezetek, könnyen alakíthatnak ki szándékos károkozó magatartást az alkalmazottaknál.
A nem megfelelő biztonságtudatos magatartást kihasználva pszichológiai manipuláció, azaz Social Engineering (SE) alkalmazásával könnyen bűnszervezetek, vagy ellenérdekelt szolgálatok célpontjává válhat a humánerő. Itt mutatkozik meg leginkább a túlzott közlékenységben rejlő kockázat, hiszen a közösségi oldalak elemzésével, olyan személyes adatokhoz juthat a támadó, amelyek segítségével ki tudja választani melyik, az infrastruktúra egyik elemével munkaviszonyban álló személy lesz a legalkalmasabb a megkörnyékezésre. A kiválasztásnál szempont a személlyel kapcsolatos nyilvánosan elérhető adatok mennyisége. *(Christopher Hadnagy: Social Engineering: The Art of Human Hacking, John Wiley & Sons, USA, 2010. nov. 29)*
A kiválasztott személy profiljának elemzése során a támadó beszerzi a manipulálásához szükséges adatokat - hobbi, szórakozás, munkahelyi jellemzők, család, barátok vonatkozásában - majd felépíti a kapcsolatépítéshez szükséges legendát. Ezt követi a megkeresés, majd a bizalomba férkőzés fázisa. Amikor sikerült a külső személynek kialakítania a kellő bizalmi viszonyt az alkalmazottal, megkezdődhet a manipuláció végrehajtása az információk kiszivárogtatása érdekében. *(Tóth Tamás: Az új irány, üzleti hírszerzés és elhárítás, OTDK dolgozat, Budapest, 2017. 45-46. o.)*
Ebben az esetben a humán kockázat kialakulása a nem megfelelő biztonságtudatos magatartásnak köszönhetően fennálló, túlzott közlékenység kapcsán vált veszélyeztető tényezővé. Azaz a kockázat belső eredetű, hiszen a manipulált humánerő önként adott át bizalmasan kezelt információkat illetéktelen, harmadik fél részére, ezáltal realizálódott a humán kockázatban rejlő veszélyforrás.

A levelező rendszerek kockázata is igen magas, hiszen ha a vállalati dolgozók magán e-mail fiókjukat használják az információs infrastruktúra működése szempontjából fontos és érzékeny adatok fogadására vagy továbbítására, az ellenérdekelt felek könnyen hozzájuthatnak adathalász e-mailek segítségével. A magán e-mail fiókok munkahelyi számítógépeken történő használata is igen nagy veszélyeket rejt magában. A PishMe e-mailfigyelő szolgáltatás jelentése szerint, 2016 első negyedévében vizsgált spamek 93%-a ransomware terjesztésére volt hivatott, ez az arány 2015 utolsó negyedévéhez képest 789 %-os növekedést mutat. *(Csizmazia Darab István, Az adathalász levelek legalább 93%-a zsaroló*

vírus, Antivírus Blog, 2016.06.07. forrás: http://antivirus.blog.hu/2016/06/07/az_adathalasz_levelek_93_-a_zsarolo_virus (letöltés ideje: 2017. szeptember 27.)

2.2.3. Köztes csoport

Köztes csoportként definiálható az elbocsájtott, kilépett alkalmazottak köre. Ez a csoport a szervezetről való ismeretei segítségével, legyen a célzat bármi, igen jelentős károkat tud okozni az információs infrastruktúra számára. Az ilyen alkalmazottak célpontjai lehetnek külső veszélyforrásoknak, hiszen a menesztett humánerő birtokában lévő információk megszerzése, lényeges eleme lehet az infrastrukturális elem működésének megismerésében..

„A sértődött vagy elbocsájtott emberek, a rendszer-ismeretükkel nagy károkat okozhatnak. Az okok általában; irigység, sértettség, bosszú, vandál pusztítási vágy, rosszindulat, hirtelen felindulás, hírszerzés és ipari kémkedés támogatása, információszerzés anyagi vagy egyéb előnyökért" (Schutzbatz Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004. 83. o.)

Elég, csak a biztonságvédelmi elemekkel kapcsolatos ismeretek átadása egy ellenérdekelt állam számára, így megkönnyítve a felkészülést egy csapásmérés végrehajtásához. A humánerő elcsábítása, illetve szolgálatokhoz történő beszervezése igen nagy kockázati tényező, hiszen a magasabb bér vagy a jobb munkakörülmények szavatolásának ígérete, a legtöbb alkalmazottban felkelti az érdeklődést. A kármértéket ebben az esetben az csökkenti, hogy a volt munkavállaló nem rendelkezik fizikális hozzáféréssel az infrastruktúra elemeihez, illetve nem jut újabb naprakész információkhoz.

2.3. Eszkalálódás alapján

A megfelelő védelem kialakításához, ismernünk kell a kockázatokat indukáló tevékenységek célját, vagyis, hogy milyen célzattal történik a humán kockázat eszkalációja. Alapvetően három nagy csoportra sikerült tagolni a kockázatokat végkimenet szempontjából, az első az anyagi haszonszerzés, ezt követi az ellenérdekelt információgyűjtés, végül pedig a károkozás. Azért lényeges vizsgálni a humán kockázatokat eszkaláció szempontjából, mivel így, még a kockázat kialakulása során tudunk következtetni arra, hogy esetlegesen milyen típusú fenyegetéssé terjedhet ki.

2.3.1. Egyéni anyagi haszonszerzés

Egyéni anyagi haszonszerzés alatt, a belső alkalmazottak részéről végrehajtott illegális akciókat értünk jogosulatlan profitszerzés céljából. Ebbe a csoportba csak az illegális, közvetlen haszonszerző tevékenységek kerülnek definiálásra, mint például a lopás, sikkasztás és egyéb vagyonelleni bűncselekmények, szabálysértések.

Kifejezetten az alkalmazott által végrehajtott, a saját szükségletei kielégítésére, önmagában generált igény alapján elvégzett akciókat vizsgál a kutatás.

A humánerő, saját célra történő haszonszerzését leggyakrabban az alábbi kockázati tényezők eredményezhetik, mint például az alacsony bérezés, valamely függőségének és pénzügyi tartozásának kielégítése. A legnagyobb csábító erőt az adatokkal való illegális kereskedelemre, jelenleg a „bérkiegészítés" teszi ki. Fontos kihangsúlyozni, hogy ebben az esetben nem az információk átadása, hanem az ellenszolgáltatás, azaz a jogtalan anyagi haszonszerzés a cél.

Ezt bizonyítja James Goodnow jogász CNBC-nek tett nyilatkozata is: *"Bár a külső, hackerektől érkező támadások száma a digitalizációval párhuzamosan 2007 óta az egekbe szökött, az alkalmazottak által elkövetett adatlopások inkább a gazdaság állapotával állnak összefüggésben: recesszió idején csúcsokat dönt, míg javuló gazdasági környezetben csökken az ilyen visszaélések száma. Amikor a gazdaság nem teljesít jól, az emberekre nagyobb nyomás nehezedik, hogy olyasmiből is profitáljanak, amiből nem kellene"* (Kerkuska Viktórira: Belső ellenségek Adatlopások és visszaélések, 2016. 06. 03. (XX/22), Hetek, forrás: http://www.hetek.hu/hatter/201606/belso_ellensegek, (letöltés ideje: 2017. október 02.)

Ebbe a kategóriába tartozik az információkereskedés mellett, az adathordózók, technikai berendezések feketepiacon történő forgalomba hozatala is, mely visszaszorítása, illetve megakadályozása a fizikai biztonság növelésével valósulhat meg. Nagy jelentőséget kell fordítani a technikai eszközöket használó alkalmazottak gépjármű és csomagátvizsgálására, így megakadályozva a hardverek kicsempészését a munkafolyamatok végrehajtására szolgáló létesítményekből. Az élőerős átvizsgálás mellett, tovább növelheti a biztonságot a fémdetektoros kapuk, a gépjármű átvilágító röntgenberendezések vagy más biztonságtechnikai berendezések telepítése. *(Kálmán László: A csomagvizsgálati röntgenberendezés alkalmazási lehetősége, Hadmérnök, X. Évfolyam 3. szám, 15. o., 2015. szeptember)*

2.3.2. Illegális információgyűjtés

Az illegális információgyűjtés, legyen szó ipari kémkedésről, vagy gazdasági hírszerzésről, túlmutat az egyéni anyagi haszonszerzés generálta ingeren, hiszen itt már egy csoport információ igényének kielégítésére kerül sor. Ezen a szinten általános információgyűjtő tevékenység zajlik, amely célja minél szélesebb körű adatok begyűjtése, elemzés és tárolás céljából.

A gazdasági társaságok és az állami szervek egy része a külső támadások kivédése mellett, nem fordít kellő figyelmet a belső mulasztások, adateltulajdonítások megelőzésére illetve elhárítására. Adatbiztonsági szempontból megengedhetetlen, hogy a munkatársak hozzáférhessenek az információs infrastruktúra működéséhez szükséges adatállományokhoz, valamint, hogy azokat módosítani tudják. Jelentős visszatartó ereje van az adatbázis kezelés naplózásának, a jogosultsági szintek, valamint a hozzájuk kapcsolódó műveletek megfelelő meghatározásának.

Abban az esetben, ha nincs ellátva az informatikai rendszer efféle biztonsági elemekkel, egy külső befolyás alatt álló alkalmazott segítségével könnyen juthatnak információkhoz ellenérdekelt szolgálatok, vagy konkurens szervezetek az infrastruktúra egy meghatározó eleméről.

Ezt az állítást támasztja alá Lengyel Csaba, a Hungard Kft. szakmai vezetőjének 2015-ben tett nyilatkozata is: *„A biztonsági vizsgálatok során számos alkalommal találkozunk azzal, hogy egy kívülről nehezen feltörhető rendszer a belülről érkező veszélyek ellen teljesen védtelen.*" (*Olyan a céges pajzs, mint a szita, 2015.08.08. P/AC & PROF/T forrás: http://www.piacesprofit.hu/infokom/it_biztonsag/olyan-a-ceges-pajzs-mint-a-szita/ (letöltés ideje: 2017. október 03.).*

Az adatlopások kapcsán nem feltétlenül a kész információkat kell csak védeni, hanem a hozzájuk kapcsolódó metaadatokat is, hiszen ezek az adott információra jellemző adatállományok, amelyekkel átfogóbb ismereteket szerezhetnek a célinformációról.

Rendkívül nagy problémát jelent az adatszivárogtatásban a humán „in-put" nem megfelelő előszűrésének végrehajtása. Igen magas a száma a Kínai Népköztársaság által telepített ügynököknek, például az Amerikai Egyesült Államok területén működő multinacionális vállalatoknál, melyek egy része az USA kritikus információs infrastruktúrájában jelen van. Ezek a személyek az oktatási rendszert kihasználva bekerülnek a célország egyetemeire. Tanulmányaikat elvégezve, a nem megfelelően működő biztonsági szűrőrendszerek folytán

munkaviszonyt létesítenek telekommunikációs vállalatoknál. Ezáltal hozzáférnek szenzitív információkhoz és hozzájuk kapcsolódó metaadatokhoz, amelyeket kicsempészhetnek a küldő országba. (*Csíki Ádám: Hogyan vigyázzunk a szellemi termékeinkre – avagy a kritikus digitális vagyontárgyak védelme. K+F és Innováció – 2016 Fókuszban az iparági fejlesztési trendek, Konferencia és kiállítás, 2016.12.06.)*

A leggyakoribb humán kockázati tényezők a nem megfelelő biztonságtudatos magatartás, mely következtében könnyen hozzájuthatnak védendő adatokhoz illetéktelen személyek, például a nem megfelelően kezelt e-mail fiókok tekintetében. Továbbá jelentős problémát okozhatnak a nem megfelelően működő előszűrő rendszerek, melyeket kihasználva külső humán kockázat kerülhet az infrastruktúra működésébe. Ezek eszkalációja vezethet az adatvesztéshez, adatszivárogtatáshoz.

2.3.3. Károkozás

Az egyéni anyagi haszonszerzésen, valamint az adattár létrehozásra és kibővítésére irányuló illegális információgyűjtésen kívül, számolni kell a tényleges károkozás generálta akciók végrehajtására is. Ezeket szinten indukálhatja ellenérdekelt hatalom, az infrastruktúrát alkotó szervezet konkurens vállalata, illetve maga a humánerő egyaránt.

A károkozás legszignifikánsabb kockázati tényezője a sértettség. Az aktív alkalmazottaknál kialakulhat a sértettség munkahelyi féltékenységből, rossz vezetői értékelésekből, döntésekből. Ekkor a legérzékenyebb a humánerő ellenérdekelt, külső megkeresésekre, amik vagy információ igényben, vagy fizikai károkozó akciók végrehajtásban realizálódnak.

Fontos megemlítetni, hogy ebben az esetben az eszkalálódott humán kockázat valós eredménye a károkozás, ami független a tartó szerv adat-felhasználási igényeitől.

Igen jól szemlélteti a humán kockázatokban rejlő veszélyt a 2017-ben Európán végigsöprő zsarolóvírussal végrehajtott támadás.

Az Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) biztonsági réseket fedezett fel a Windows operációs rendszereiben. Ezek kihasználására megalkották az EnternalBlue elnevezésű exploitot[145]. Ezt az információt, és az exploitot, nagy

[145] Informatikai biztonsági fogalom: olyan forráskódban terjesztett vagy bináris program, adathalmaz vagy parancssorozat, amely alkalmas egy szoftver vagy hardver biztonsági résének, illetve hibájának kihasználására, így érve el a rendszer tervezője által nem várt viselkedést. *(forrás: http://searchsecurity.techtarget.com/definition/exploit)*

valószínűséggel egy belső munkatárson keresztül, sikerült kicsempésznie a The Shadow Brokers nevű hackercsoportnak, akik a birtokukba került adatok felhasználásával megalkották, a WannaCry nevezetű ransomwar, leállító kód nélküli változatát. A zsarolóvírus felhasználta az EnternalBlue parancssorozat tulajdonságait, amely által blokkolni tudta a Windows alapú operációs rendszerrel rendelkező számítógépeket. Pár nap leforgása alatt, számos a nemzetközi szinten működő telekommunikációs vállalat adatállományát titkosította a vírus. Összesen 74 országban észlelet támadást a Kasperky Lab orosz számítógépes biztonsági cég. A támadott telekommunikációs vállalatok mindegyike része a kritikus információs infrastruktúra nemzeti, illetve nemzetközi platformjainak. Spanyolországban a Telefonica és a Vodafon, Portugáliában a Telecom, Oroszországban a MegaFon multinacionális távközlési vállalat számolt be arról, hogy kibertámadás érte a rendszereiket. A fenti esemény során adatállományok kerültek titkosításra, a kommunikációs csatornák csak azért nem omlottak össze, mert a vírus nem ilyen feladat végrehajtására volt megalkotva.

Ez a példa jól mutatja, hogy egy ellopott adatállomány, illegális felhasználása mekkora méretű veszélyforrás lehet egy globális kiterjedésű kibertámadás végrehajtása során. Ezt az egész eseménysorozat, nagy valószínűséggel egy eszkalálódott humán kockázati tényező indukálta. *(Nicole Perlroth, David E. Sangermay: Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool, The New York Times, 2017.05.12.)*

4. Konklúziók és eredmények

A pályázat során sikerült megvizsgálni a ’kritikus információs infrastruktúra’ kifejezés alkotóeleminek különböző szempontú meghatározásait, továbbá ezek alapján megalkotni egy általános és pontos definíciót a kritikus információs infrastruktúra vonatkozásában. Jól látható, hogy az infrastruktúra meghatározása ágazatonként más és más, ezért volt szükség a közös tartalmi elemek ismertetésére.

Ezt a gondolatmenetet követve bemutatásra került a ’humán kockázat’ kifejezés tartalmi eleminek meghatározása. Sikerült prezentálni a kockázat általános és a biztonság aspektusaiból történő megfogalmazását is.

Elsődlegesen a humán kockázatok, büntetőjogi ismérv alapján kerültek elemzésre, méghozzá a bűnösség szempontjából. E szerint a gondatlan és a szándékos magatartás, mint kiváltó ok volt a csoportosítás fő irányvonala. Sikerült szemléltetni a hanyagság következtében kialakuló

nem megfelelő biztonság tudatos magatartás kockázati elemeit, valamint a közvetlen és közvetett, aktív és passzív kockázati tényezőkben rejlő kihívásokat.

Ezt követte az eredet szerinti felbontás, miszerint sikerült infrastruktúrán belüli és külső forrásra tagolni a humán kockázatokat, valamint a volt alkalmazottak köre is vizsgálat tárgyát képezte. Ez a fajta szegmentálás segíti a megelőzést, és a kockázat felderítését az előszűrések és a folyamatos humán audit szempontjából.

Végső soron, a humán kockázatokon túlmutató kockázati eszkaláció szempontja volt a fő motívum, a csoportosításban. Ez alapján egyértelműen meghatározható az egyéni anyagi haszonszerzés, mely során a kockázat jogosulatlan haszonszerzés céljából eszkalálódik. A következő részhalmazt az illegális információgyűjtés alkotja, mely végrehajtása során az információigény biztosítása az eszkalációs folyamat indukáló tényezője. A legsúlyosabb következményekkel járó humán kockázati eszkaláció a károkozás, ekkor a kockázati tényező továbbfejlődését szándékos károkozás indukálja, aminek globális jelentőségét a 2017-es év során végrehajtott, nemzetközi zsarolóvírus támadás is alátámaszt.

A fentiek tükrében kijelenthetem, hogy a pályázati célkitűzések megvalósultak, miszerint elkészült egy kellő mélységű elemzés a humán kockázatok prezentálása céljából, ami jó alapot teremt későbbi kutatási folyamatok elvégzéséhez a kritikus információs infrastruktúra védelem jogszabályi biztosítékainak, kockázat kezelésének, valamint megelőzésének vonatkozásában.

Irodalomjegyzék

Szerzői művek

1. Christopher Hadnagy: Social Engineering: The Art of Human Hacking, John Wiley & Sons, USA, 2010. nov. 29

2. Dr. Kovács Zoltán András ezredes, Dr. Regényi Kund ezredes: Nemzetbiztonsági alapismeretek, 4. Fejezet Biztonság tudatosság: humán kockázatok, technikai kockázatok, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013.

3. Dr. Resperger István mk. alezredes: Nemzetbiztonsági alapismeretek, 2. Fejezet Biztonsági kihívások, kockázatok és fenyegetések 2030-ig, szerk: Dr. Kobolka István, Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013

4. Haig Zsolt, Várhegyi István ezredes: Hadviselés az információs hadszíntéren, Zrínyi, Budapest, 2005.

5. Horváth Gergely Krisztián: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, Kormányzati Informatikai Fejlesztési Ügynökség, Budapest, 2013.

6. Kálmán László: A csomagvizsgálati röntgenberendezés alkalmazási lehetősége, Hadmérnök, X. Évfolyam 3. szám, 15. o., 2015. szeptember.

7. Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.

8. Magyar Larousse Enciklopédikus szótár, Akadémiai Kiadó, Budapest, 1992.

9. Muha Lajos: A Magyar Köztársaság Kritikus Információs Infrastruktúráinak Védelme, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.

10. Nicole Perlroth, David E. Sangermay: Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool, The New York Times, USA, 2017.05.12.

11. Schutzbatz Mártonné: Az informatikai rendszerek biztonságának kockázatelemzése a védelmi szférában PhD értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004.

12. Tóth Tamás: Az új irány, üzleti hírszerzés és elhárítás, OTDK dolgozat, Budapest, 2017.

Konferenciák

1. Csíki Ádám: Hogyan vigyázzunk a szellemi termékeinkre – avagy a kritikus digitális vagyontárgyak védelme. K+F és Innováció – 2016 Fókuszban az iparági fejlesztési trendek, Konferencia és kiállítás, 2016.12.06.

2. Dr. Kis-Benedek József ezredes: Célkeresztben az Iszlám Állam, Ludovika Szabadegyetem, Budapest. 2015.11.10.

Jogszabályok

1. 1995. évi CXXV. törvény - a nemzetbiztonsági szolgálatokról

2. 1998. évi XIX. törvény a büntetőeljárásról

3. 2012. évi C. törvény a Büntető Törvénykönyvről

4. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

5. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

6. 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról

7. 293/2010. (XII. 22.) Korm. rendelet a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve kijelöléséről, valamint feladatai ellátásának, a kifogástalan életvitel ellenőrzés és a megbízhatósági vizsgálat részletes szabályainak megállapításáról

8. NATO Polgári Vészhelyzeti Tervezés, NATO Civil Emergency Planning – CEP, 2006

9. Zöld Könyv a kritikus infrastruktúrák védelem európai programjáról. Európai Közösségek Bizottsága, Brüsszel, 2005. 11. 17.

Internetről származó hivatkozások

5. Alissa Torres: A pszichológiai manipuláció (social engineering), OUCH, The SANS Instute 2014, 2014. 11. forrás: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH201411_hu.pdf (letöltés ideje: 2017. szeptember. 12)

6. Balogh Ágnes, Tóth Mihály: Magyar büntetőjog. Általános rész, TAMOP 4.2.5 Pályázat, Osiris Kiadó, Budapest, 2010, forrás: http://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_520_magyar_buntetojog/ch03s06.html (letöltés ideje: 2017.szeptember 15.)

7. Csizmnazia Darab István, Az adathalász levelek legalább 93%-a zsaroló vírus, Antivírus Blog, 2016.06.07. forrás: http://antivirus.blog.hu/2016/06/07/az_adathalasz_levelek_93_a_zsarolo_virus (letöltés ideje: 2017. szeptember 2.)

8. Dr. Bognár Balázs PhD pv. őrnagy: A kritikus infrastruktúra, OKF Iparbiztonsági link, forrás: http://www.katasztrofavedelem.hu/index2.php?_pageid=pvl_kritikus_infrastr-uktura (letöltés ideje: 2017.szeptember.12)

9. Durbák Ildikó: Ellopott céges információk, Profession, 2010, Forrás: https://www.profession.hu/cikk/20100722/ellopott-ceges-informaciok/401#, (letöltés ideje: 2017. szeptember 17.)

10. Humán kockázatok: a leggyengébb láncszem, Crisma, forrás: http://www.carisma.hu/cikkek/human_kockazatok.html (letöltés ideje: 2017. szeptember. 17.)

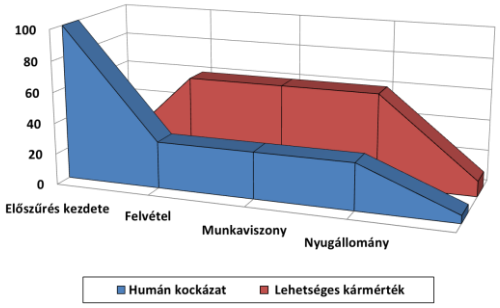
11. Kerkuska Viktórira: Belső ellenségek Adatlopások és visszaélések, 2016. 06. 03. (XX/22), Hetek, forrás: http://www.hetek.hu/hatter/201606/belso_ellensegek (letöltés ideje: 2017. október 02.)

12. Olyan a céges pajzs, mint a szita, 2015.08.08. P/AC & PROF/T forrás: http://www.piacesprofit.hu/infokom/it_biztonsag/olyan-a-ceges-pajzs-mint-a-szita/ (letöltés ideje: 2017. október 03.)

Mellékletek

1. számú melléklet:

A humán kockázatok és a lehetséges kármérték összefüggése



Forrás: „saját szerkesztés”