KOVÁCS TAMÁS *–JUHÁSZ GÁBOR JÓZSEF **

Az információbiztonság és információvédelem szerepe a hadiiparban 1. rész

Összefoglalás: Kutatásunk témája a hadiiparban kiemelt jelentőséggel bíró és a mindennapi élet területén is egyre jelentősebb az információbiztonság és információvédelem, a hadiiparban és a honvédelemben működő vállalatok és szervezetek vonatkozásában. A téma feldolgozása során külön vizsgáltuk a menedzsment és az információbiztonság kapcsolatát, ami a kritikus erőforrások védelme és alkalmazása miatt odafigyelést igényelnek.

Kutatásunk során első sorban az írásbeli kikérdezés módszerét és a kérdőív eszközét használtuk, amelynek kérdései a kutatási hipotézisek vizsgálatát szolgálták. Ez a metódus biztosította a résztvevő részére mind szervezeti, mind egyéni szinten a teljes anonimitást és részünkre ezáltal a lehető legőszintébb válaszokat a pontos kutatás érdekében.

A kérdőívekre adott válaszokat összesítést követően elemeztük, a számításokat a statisztikai adatokkal összevetve kiértékeltük. Az eredmények bemutatása a hipotézisek mentén történt, melyek a válaszadók egyértelmű véleményét és az azok mentén levont tapasztalásokat tükrözik. A kapott eredményeket a szakirodalomban feltártak alapján összegeztük, következtetéseket tettünk, melyeket a vizsgált szervezetek a biztonságpolitikájukba beépíthetnek.

Kutatásunk legfontosabb megállapításaként elmondhatjuk, hogy a szervezetek legnagyobb információkockázati tényezője továbbra is a humán erőforrás, amely megfelelő kiválasztása és szinten tartása elengedhetetlen.
Kulcsszavak: Információbiztonság, információvédelem, hadiiparban, honvédelemben működő vállalatok.

Abstract: The topic of our research is information security and information protection, which is of particular importance in the military industry and increasingly important in the field of everyday life, in relation to companies and organizations operating in the military industry and national defence.

* *Varsói Menedzsment Egyetem, egyetemi docens*
Email: drkovacst@nymu.hu

** *Varsói Menedzsment Egyetem, egyetemi hallgató*
Email: juhszgaborjozsef@gmail.com

During the processing of the topic, we separately examined the relationship between management and information security, which require attention due to the protection and application of critical resources.

During our research, we primarily used the method of written questioning and the instrument of the questionnaire, the questions of which were used to test the research hypotheses. This method ensured complete anonymity for the participant both at the organizational and individual level, and thus for us the most honest answers possible for accurate research.

The responses to the questionnaires were analyzed after aggregation, and the calculations were evaluated by comparing them with the statistical data. The results were presented along the lines of the hypotheses, which reflect the clear opinions of the respondents and the experiences drawn along them. We summarized the obtained results on the basis of what was revealed in the literature, and made conclusions that the examined organizations can incorporate into their security policy.

As the most important finding of our research, we can say that the biggest information risk factor for organizations is still human resources, which are essential to select and maintain at the right level.
Keywords: Information security, protection, companies, organizations, operating in the military industry.

Bevezetés

A hadiiparban az információbiztonság és információvédelem szerepe, kardinális jelentőségűek a vállalati menedzsment szempontjából, kiterjesztve hatásukat az információk integritásától és biztonságától kezdve a vezetők bizalmán és a jogi kötelezettségek betartásán át egészen a hírnév megőrzéséig. A megfelelő adatvédelmi intézkedések nem csupán a kockázatok minimalizálásához járulnak hozzá, hanem erősítik az információk minőségét, támogatva ezzel a stratégiai tervezést és végrehajtást. A menedzsment szintjén az adatvédelem felelős a vállalati titkok és stratégiák megőrzéséért, melyek kritikusak az üzleti sikerhez, melynek integrációja a vállalati kultúrába növeli a munkatársak információbiztonsági tudatosságát és az adatbiztonsági szabályok betartását. Az adatvédelem, amellett, hogy csökkenti a pénzügyi és adatvesztési kockázatokat, elengedhetetlen a pontos és megbízható információk biztosításához, amelyek szükségszerűek a döntéshozatalhoz. A vállalatok vezetései stratégiai szinten kell, hogy kezeljék az adatbiztonsági kérdéseket, mivel ezek közvetlen kapcsolatban vannak a hosszú távú üzleti sikerrel és fenntarthatósággal.

A kutatási téma aktualitását adta, hogy ezek az adatok egyre növekvő mértékben válnak célponttá a kiberbűnözők és illetéktelen szereplők számára, ezzel ösztönözve az érzékeny adatok megfelelő kezelésére és a biztonsági intézkedések fokozott figyelembevételére.

A munkánk célja az volt, hogy a modern munkakörnyezet dinamikájához igazodva feltárjuk és megértsük, hogyan alakulnak a munkavállalók kapcsolatai az adat- és információvédelem terén, valamint hogyan integrálódnak az adatelemzések a döntéshozatali folyamatokba. A kutatás során kiemelten vizsgáltuk, hogyan formálja a szervezeti kultúra, a képzések és a belső kommunikáció az alkalmazottak tudatosságát az adatvédelem terén, különös tekintettel a jelenlegi digitális környezet változására. Kiindulásként az alábbi 3 hipotézist állítottuk fel, melyek mentén a vizsgálatainkat lefolytattuk:

Az első hipotézisünk az adatvédelem és a hadiipari biztonság nemzeti és nemzetközi jogi és az iparágban alkalmazott nemzetközi minősítő szabványok előzetes kutatásán alapul, figyelembe véve a magyar munkaerőpiac jellemzőit és sajátosságait.

Hipotézis 1: Feltételezzük, hogy a vállalat alkalmazottai átfogóan ismerik az adatvédelmi szabályokat és maradéktalanul követik őket.

Másodhipotézisünk alapja az üzletág politikai megfelelési kényszere és a nemzetközi piaci verseny, amely a lehetőségekhez mérten a legmodernebb és leghatékonyabb adatfeldolgozást és elemzést teszi szükségessé, különös tekintettel a technológiai fejlődés ütemére.

Hipotézis 2: Feltételezzük, hogy a vállalat által gyűjtött, kezelt és feldolgozott adatok elemzett formában beépülnek a vállalat döntéshozatali folyamataiba.

A harmadik hipotézisünk szorosan ráépül a másodhipotézisre, mely szerint az adatvezérelt döntéshozatal a vállalat részére piaci versenyelőnyt, fenntarthatóságot és ellenálló képességet biztosít, amely a vállalatok szempontjából értéket és tőkét képvisel, ezáltal a szervezetek ezeket a szükséges mértékben védik.

Hipotézis 3: Feltételezzük, hogy a vállalat részére az adatok feldolgozása és elemzése után nyert információ érték.

Szakirodalmi hivatkozások – Az információbiztonság meghatározása

A biztonság megfogalmazását sokféleképpen magyarázták már. Csíkék szerint például *„a biztonság olyan kedvező állapot, amelynek megváltoztatása nem valószínű, de nem is zárható ki …”* [1] ez a megfogalmazás tudományos, de gyakorlatias szemszögből nézve is értelmetlen, ezzel szemben a Magyar Értelmező Kéziszótárban található

[1] Csík B.–Danyi P.–Egerszegi K. (2003): *Az informatikai biztonság fogalmainak gyűjteménye*. Budapest: BME GTK.

[2] Pusztai F. (Szerk.) (2003): *Magyar Értelmező Kéziszótár.* Budapest: Akadémiai.

[3] Boytha Gy. (2003): A személyiségi jogok megsértésének vagyoni szankcionálása. In: *Polgári Jogi Kodifikáció,* 2003., (1.), Budapest: ORAC, pp. 3–6.

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény (hatályos: 2023.12. 01.)

megfogalmazás, mely szerint *„a biztonság veszélytől vagy bántódástól mentes, zavartalan állapot”* [2] szintén elég tudományos, de szakmailag nem elfogadható, mert zavartalan állapot a gyakorlatban nem létezik és ha az ingerküszöb alatti zavar mértéke elviselhető és gyakorisága sem okoz problémát akkor az szintén biztonságosnak tekinthető. Ebből kiindulva a biztonság az a kedvező állapot, ahol a fenyegetések mértékét és a fenyegetések által okozott kár mértékét képesek vagyunk minimalizálni.

Napjainkig a kár definíciója sem állandó, az is folyamatosan változik, s ezentúl mindig merülnek fel olyan értelmezésből eredő problémák, amelyek alapján érdemes újragondolni az eddig kialakult gyakorlatot. A legjobban a kár közgazdasági megközelítésű definíciója helytálló, ami Boytha [3] meghatározása alapján, a pénzben mérhető, ár- és piaci értékviszonyok alapján kiszámítható hátrány.

Az információ a vállalatok számára a kulcsfontosságú erőforrások egyike, a kiegyensúlyozott és hosszútávú működés alapja, ezért folyamatosan gondoskodni kell megbízhatóságáról és biztonságáról, hiszen alapvetően befolyásolhatja egy szervezet működését, szolgáltatásainak, termékeinek minőségét. A szervezeteken belüli követelmények mellett a *„társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sérthetetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal kibertér védelme.”* [4], amelynek az értelmében:

– a *bizalmasság* olyan biztonsági tulajdonság, amely lehetővé teszi, hogy az információ jogosulatlanok (emberek, folyamatok) számára ne legyen elérhető, vagy ne kerüljön nyilvánosságra. A bizalmasság elvesztése az információ illetéktelenek általi hozzáférését, megismerését jelenti;
– a s*értetlenség* olyan biztonsági tulajdonság, amely azt jelenti, hogy az adatot, információt vagy programot csak az arra jogosultak változtathatják meg és azok észrevétlenül nem módosulhatnak és nem törölhetők, semmisíthetők meg. A sértetlenség elvesztése az információ jogosulatlan módosítását vagy megsemmisítését jelenti. A sértetlenség fogalmába beleértendő az információk hitelessége és letagadhatatlansága is;
– a *letagadhatatlanság* olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az informatikai rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően;

– a hitelesség az entitás olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz. Egy információ akkor tekinthető hitelesnek, ha mind tartalmának, mind létrehozójának (küldőjének) sértetlensége garantálható;
– a *rendelkezésre állás* a biztonság azon szempontja, amely lehetővé teszi, hogy a feljogosított szubjektum (humán közreműködő vagy gépi folyamat) által támasztott igény alapján az adott objektum elérhető és használható legyen. A rendelkezésre állás elvesztése azt jelenti, hogy az információhoz vagy az informatikai rendszerhez való hozzáférés vagy annak használata akadályokba ütközik, vagy adott időtartamra vagy teljes mértékben megszűnik [5].

[5] Muha L. (2007): *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme.* Budapest: ZMNE.

Az információbiztonság területei

Ahogy azt fentebb kifejtettük az információbiztonság célja, hogy tevékenységekkel és intézkedésekkel megakadályozzuk az általunk kezelt és védett információkhoz való jogosulatlan hozzáférést, valamint azok kísérleteit nyomon kövessük és kiértékeljük. Így a biztonsági intézkedéseket az alábbi területekre oszthatjuk fel:
– a személyi biztonság területe azt szabályozza, hogy a minősített információ csak olyan személynek juthat birtokába, aki megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelel, illetve az adott minősítésű információ megismerése számára hivatalos célból szükséges;
– a fizikai biztonság azon fizikai akadályok összessége, amelyek megfosztják az illetékteleneket a minősített, kritikus információkhoz, dokumentumokhoz, eszközökhöz való hozzáféréstől, és meghiúsítják vagy megakadályozzák a fizikai támadást;
– a dokumentumbiztonság azt jelenti, hogy az összes dokumentumot minősítésének, érzékenységének, vagyis titkossági osztályba sorolásának megfelelően kell védeni. Az érzékeny adatokat tartalmazó dokumentumokhoz való hozzáférés azon körre kell, hogy korlátozódjon, akik számára feltétlenül szükséges, hogy annak tartalmát megismerjék;
– az elektronikus információbiztonság (INFOSEC) a távközlési és informatikai, valamint egyéb elektronikus rendszerekben és támogató infrastruktúráikban alkalmazott rendszabályok összessége. Az elektronikus információbiztonság területei:

– az átviteli biztonság (TRANSEC);
– a kompromittáló kisugárzás elleni védelem (EMSEC);
– a rejtjelezési biztonság (CRYPTOSEC);
– a számítógépbiztonság (COMPSEC) és
– a hálózati biztonság (NETSEC) [6].

[6] Haig Zs. (2006): Az Információbiztonság komplex értelmezése. In: Kovács L.: *Hadmérnök Különszám 2006.* Robothadviselés 6. tudományos szakmai konferencia. Nemzetvédelmi Egyetem, Zrínyi Miklós Kiadó, pp. 6–8.

[7] Yejun, W.–Fan-Song, M. (2019): Categorizing for Security Management and Information Resource Management. In: *Journal of Strategic Security,* 2., (11.), pp. 72–84.

Az információ védelmi szempontú kategorizálása

Az információk biztonsági kategorizálása és megfelelő osztályba sorolása nélkülözhetetlen lépés a modern társadalmi és gazdasági környezetben, ahol az adatok értéke és veszélyeztetettsége kiemelt jelentőséggel bír.

Az információk és adatok biztonsági kategorizálása szempontjából több különálló kategorizálási tényezőt és szabályzót is figyelembe kell vennünk. Ebből kifolyólag az információk biztonsági osztályozása a különböző szempontok szerint eltérő és állandó kihívást jelent a biztonság kezelésében [7]. Ez különösen igaz a hadiipari információk területére, ahol az információk a felhasználás tekintetében akár több különálló biztonsági minősítést is kaphatnak. Ezeket szabályozza a minősített adat védelméről szóló 2009. évi CLV. törvény, a 41/2015. (VII. 15.) BM-rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről, az ISO/IEC 27002 szabvány és még folytathatnánk tovább a felsorolást, azonban a lényegi tartalmat tekintve mind a védelem minimális követelményeit fogalmazza meg. A minősített információk a felhasználási terület tekintetében lehetnek:
– banktitok a 2013. évi CCXXXVII. törvény szerint;
– orvosi titok a 1997. évi CLIV. törvény szerint;
– ügyvédi titok a 2017. évi LXXVIII. törvény szerint;
– üzleti titok a 2018. évi LIV. törvény szerint;
– nemzeti minősített adat a 2009. évi CLV. törvény értelmében;
– külföldi minősített adat (Európai Uniós vagy NATO szabályozás alapján).

A vállalat vagy szervezet által birtokolt és kezelt adatokat információbiztonsági tervében megfogalmazottak alapján a kockázatelemzés az, amely meghatározza, hogy az adott információ milyen mértékű kár okozására alkalmas a szervezet életében vagy üzemszerű működésében. Ezen elemzések eredményeit, valamint a törvényi szabályokat figyelembe véve kell az adatokat biztonsági osztályba sorolni. A biztonsági osztály határozza meg a továbbiakban, hogy az adott információ milyen szintű védelmet igényel.

[8] Haig Zs. (2006): Számítógép-hálózati hadviselés rendszere az információs műveletekben. In: *Bolyai Szemle 2006.* Nemzetvédelmi Egyetem, Zrínyi Miklós Kiadó, pp. 54–58.

Információbiztonság fenyegetései

A vállalatok védett információira leselkedő veszélyek jelentős része a termelési infrastruktúrát támadja. Ezzel annak megfelelő szintű működését próbálja befolyásolni. „*A támadások származhatnak egyes személyektől, jogosulatlan felhasználóktól, csoportoktól, terroristáktól, valamint különböző nemzeti szervezetektől, külföldi hírszerző szolgálatoktól, katonai szervezetektől. Szakértők véleménye szerint a rendszerbetörések nagy többségében, mintegy 70–90%-ban belső munkatárs, vagy volt munkatárs is közreműködik.*" [8]. Az információbiztonsági intézkedések egyik fő célkitűzése a fenyegetettségek megakadályozása, felismerése, kezelése, a kockázatok minimalizálása és az eredeti állapot visszaállításának megkönnyítése.

A fenyegetések keletkezésének tekintetében megkülönböztetünk emberi közreműködés nélküli, azaz természeti eredetű fenyegetéseket és közvetlen emberi közreműködés eredetű fenyegetéseket. A természeti eredetű fenyegetések közé soroljuk továbbá az ember által közvetlenül nem befolyásolt tevékenységeket, mint földrengés, árvíz, viharok vagy napkitörések. A védekezés során az ember ezen eseményekbe csak rövidtávon és kis mértékben képes beavatkozni és a védelmi intézkedések teljesen megegyeznek a természeti fenyegetések elleni védelmi intézkedésekkel.

Emberi tevékenység okozta fenyegetések közé soroljuk azon fenyegetéseket, melyek közvetlen emberi tevékenység eredményeként jönnek létre függetlenül az elkövető szándékától és a cselekmény okától. A szándékosságot tekintve, lehetnek gondatlan veszélyeztetés, amely elsősorban a tudás és biztonságtudatosság hiányának következménye, mint a szoftverhibák, vagy üzemeltetési folyamatok megsértése, másrészről lehet szándékos tevékenység, amikor is személyek vagy csoportok célzottan támadják a szervezetet annak üzemszerű működését megzavarva vagy az általa

kezelt információkat kompromittálva, mint a terrorizmus, hacking, szabotázs vagy iparikémkedés. A belső veszélyeket elsősorban a saját alkalmazottak okozzák, akik a biztonsági előírásokat és eljárásokat szándékosan vagy hanyagságból figyelmen kívül hagyják, ezzel jelentős problémák forrásaivá válnak. A külső veszélyek minden esetben a szervezeten kívüli forrásból származnak és a támadás célja anyagi-, gazdasági- vagy katonai előnyszerzés. Az infokommunikációs eszközök térhódításával és fejlődésével egyenes arányban nőtt a támadások száma is.

A különböző természeti veszély típusok elemzését követően könnyen felismerhető, hogy a természeti katasztrófák elleni felkészülés gondos tervezéssel biztosítható, és ezáltal a kár bekövetkezése a lehetőségekhez képest a minimalizálható, valamint a kárelhárítás gyorsan és hatékonyan kivitelezhető.

Az emberi közreműködés eredetű veszélyek jelentős része a megfelelő tervezéssel, kidolgozott protokollokkal és megfelelő képzéssel megelőzhető és minimalizálható. A kárelhárítás az esemény nagyságától függően hatékonyan végrehajtható. Ugyanakkor a védekezés a szándékos károkozás, illetve nem ismert támadási technika (pl. nulladik napi sérülékenység) kihasználása esetén jelentős nehézséget okozhat.

Szándékos emberi tevékenységből fakadó fenyegetések nagymértékben függenek a támadó fél szakmai tudásától, motivációjától, illetve a rendszer védelmi képességeitől. A napvilágra került sikeres, kritikus infrastruktúrákkal szembeni támadások szinte mindegyikéről elmondható, hogy a támadás előre jól megtervezett módon, korábban nem ismert technikákkal történt, a támadók kihasználták a támadott rendszerek nulladik napi (0-day) sérülékenységeit és azon keresztül bejutva az információs rendszerbe végezték tevékenységüket [9].

Az ENISA (2022) kutatása alapján a kibertámadások terén 8 fő csoport létezik:

1. *zsarolóprogramok:* a hackerek átveszik az irányítást valakinek az adatai felett, és váltságdíjat követelnek a hozzáférés visszaállításáért,
2. *rosszindulatú programok:* a rendszert károsító szoftverek,
3. pszichológiai manipuláció okozta fenyegetések: az emberi hiba kihasználása információkhoz vagy szolgáltatásokhoz való hozzáférés érdekében,
4. *az adatokkal szembeni fenyegetések:* az adatforrások célzása jogosulatlan hozzáférés és nyilvánosságra hozatal érdekében,
5. *az elérhetőség elleni fenyegetések:* szolgáltatásmegtagadás: olyan támadások, amelyek megakadályozzák, hogy a felhasználók hozzáférjenek az adatokhoz vagy szolgáltatásokhoz,

[9] Sági G. (2016): Megvédhetőek-e a kritikus információs infrastruktúrák? In: *Hadmérnök,* 9., (2.), Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar. pp. 154–169.

6. *elérhetőség elleni fenyegetések:* internetes fenyegetések: az internet elérhetőségét fenyegető veszélyek,
7. *dezinformáció/félretájékoztatás:* félrevezető információk terjesztése,
8. *az ellátási láncot ért támadások:* szervezetek és beszállítók közötti kapcsolatot célozva.

Az eddigi szakmai tapasztalataink, valamit a kutatásunk alatt áttekintett esettanulmányok alapján megállapíthatjuk és kijelenthetjük, hogy a támadások jelentős része egy egyszerű, általánosnak mondható katonai séma alapján kerültek végrehajtásra, amelyet a következő forgatókönyvben foglaltunk össze.

A védelmi rendszer műszaki tesztelése, amely akár a támadás első előkészítő lépéseként is felfogható, célja azonban mindösszesen az informatikai, infrastrukturális és humán környezet felmérése és az ezekről való teljes információ szerzés.

Ehhez a mai felhőalapú társadalom információs adattárai jelentős segítséget nyújtanak a támadóknak, a célpontok profilozása tekintetében, azonban az egyéb hagyományos hír- és információszerzési technikák és csatornák sem elhanyagolhatók.

Az internet korában a szervezetek és a magánszemélyek is egyre több információt osztanak meg magukról akarva és akaratlanul is, így szinte lehetetlen, hogy ne rendelkezzenek digitális lenyomattal. Ez egy szervezetre kifejezetten igaz, hiszen a szervezeten kívül az alkalmazottai és a vele együttműködők is hagynak róla információkat. Az igazán jelentős célpontok nagyok, így az ilyen jellegű információ szivárgása is nagy. A szervezetek honlapján megosztott információk is rengeteg kiindulási lehetőséget adnak a támadóknak. Mindemellett a mai kutatások alátámasztják, hogy minden jelentős személy rendelkezik valamely szociális hálón fiókkal, vagy fiókokkal és ott sok mindent megoszt, amit egy személyes találkozón nem tenne.

Egy másik hasznos erőforrás az internetes keresőmotorok, amelyek a megfelelő kulcsszavak segítségével akár a célpont teljes életútját feltárhatják. Számos esetben igazolódott, hogy ezen módszerrel akár belső üzleti dokumentumok és iratok is előkereshetőek. Amennyiben az eddigiekkel szerzett információ nem elégséges, célravezető a célpont telefonos vagy írásos megkeresése, ez azonban jelentős kockázatot hordoz a támadók számára, mivel a legtöbb szervezet ellenőrzi és kontrollálja ezeket a kommunikációs csatornákat. Ha semmi más nem vezetett a kívánt eredményre, a támadó személyesen keresi fel a célpontot.

Ez a megoldás kockázatos, de a tapasztalatok alapján olyan információkkal is szolgálhat, amivel más csatornák nem. Az ezzel kapcsolatos hátteret a következő fejezetben részletesebben tárgyaljuk. A fent leírtakat követően a megszerzett információkat és kapcsolatokat felhasználva valósul meg a támadás. Amint itt is rámutattunk, a védelem leggyengébb pontja az emberi tényező, és ezt a szervezet riválisai és támadói ki is fogják mindig használni.

Az egyik kiemelkedő példa, a világ egyik legnagyobb cége elleni észak-koreai programozó csoport által elkövetett támadás, amely többek között arra is rávilágított, hogy Észak-Koreában hozzávetőleg 6000 katonai hackert képeztek ki és bármikor alkalmazhatják őket. A hackertámadások többek között az állam egyik jelentős bevételi forrása ott. (Simon, 2016).

Információbiztonság a vállalati menedzsmentben

Az egyre inkább tudásalapúvá váló társadalomban és gazdaságban az információ a gazdálkodó szervezet számára olyan érték, amely a vezetői döntések, az üzleti sikeresség alapja és a működés hatékonyságának meghatározó eleme. Legyen szó termékről, szolgáltatásról, technológiáról, a rendelkezésre álló erőforrásokról, vagy akár az üzleti partnerekről. Amennyiben az adatok vagy információk hiányosak, pontatlanok, vagy nem a megfelelő időben állnak rendelkezésre, esetleg illetéktelenek kezébe kerülnek, akkor ez a vállalat számára károkat okozhat. Az információt tehát szükséges védeni [11].

Az információbiztonság területén való hatékony működéshez szükséges a vállalatvezetés elkötelezettsége a biztonsági elvek iránt. A vezetőknek teljes mértékben érteniük kell, hogy az információ nem csupán egy technológiai eszköz, hanem egy olyan érték, amelynek védelme stratégiai prioritás kell legyen. Ennek érdekében a menedzsmentnek ki kell dolgoznia és be kell vezetnie azokat a keretszabályozásokat, folyamatokat és irányelveket, amelyek biztosítják az információbiztonság megfelelő szinten tartását és fejlesztését. Ezzel megteremtve a vállalati biztonsági kultúra alapjait.

„*A biztonsági kultúra szervezeti biztonság felfogása szerint tehát egy hatékony és hatásos szervezeti biztonsági rendszer akkor hozható létre, ha a személyes (értékek, attitűdök, hiedelmek, észlelés és felfogókészség) és a viselkedési tényezők (megértés, bizalom, elkötelezettség, motiváció/szándék és az éberség) egyszerre irányulnak a szervezeti biztonság megteremtésére, megtartására*" [12].

[10] Simon L. (2016): Az információ, mint fegyver? Katonai Nemzetbiztonsági Szolgálat, *Szakmai Szemle,* 2016/1., pp. 34–60.

[11] Michekberger P. (2018): *Információ-, folyamat-, és vállalatbiztonság.* Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[12] Lazányi K. (2015): A biztonsági Kultúra = Security Culture. In: *Taylor,* 7., (1–2.), pp. 398–405.

Az információbiztonság emberi tényezői

A humánerőforrás az, aki az információs erőforrást kezeli, értelmezi és hasznosítja, de hozzájuk vezethetők vissza (szándékosan vagy gondatlanul) az információbiztonsági eseményeket előidéző hibák is. A vállalati információbiztonságot érintő fenyegetések jelentős része, az informatikai tervezési hibák mellett, a szervezetben dolgozó munkavállalóktól származik. Ezeket kiküszöbölni nem, de a kockázati szintet csökkenteni lehet. A személyzet kiválasztási folyamatokba, az alkalmazásba vétel és a kilépés szabályozásába információbiztonsági szempontokat is be kell építeni. Fontos szempontok a már megszerzett informatikai képzettség, a megbízhatóság, az életkor, vállalati méret és a munkakörnyezet, a szervezeti kultúra, valamint a rendszeres fejlődés iránti igény [11].

Az alábbi tényezők vagy folyamatok vezethetnek odáig, hogy a vállalat aktív vagy volt munkavállalója védett információt juttat illetéktelenek részére:

- tudatlanság, az alkalmazott nem ismeri, hogy ez a cselekmény nem engedélyezett, tehát a munkavállaló képzetlen;
- fegyelmezetlen a felhasználó, a biztonsági előírásokat és protokollokat szándékosan figyelmen kívül hagyja;
- figyelmetlen, hanyag, azaz a biztonsági előírásokat nem szánt szándékkal, de megszegi;
- megtévesztették és úgy érzi, hogy ki kell adni az információt;
- megfenyegetik, megzsarolják;
- bosszút áll (vélelmezett sérelem érte a vállalat irányából);
- a szervezeti működési szabályzat nem tér ki az információ biztonságra, ebből adódóan az csak józan belátás szerint működik;
- az információbiztonsági szabályozás elavult, nem követi a technológiai fejlődést.

A szervezeti audit kockázatelemzése során az információs- és folyamattechnológia, valamint az azt üzemeltető emberi erőforrás nem választható szét. A munkavállaló által végrehajtott károkozás mindig több veszélyt hordoz magában, mint a külső támadás. Míg a vállalatok első sorban a külső fenyegetésekre készülnek, a belső támadó az, aki ismeri az információs rendszerek gyenge pontjait, tudja, hogy melyek a szervezet számára értékes információk és tisztában van az üzleti és ügyviteli folyamatok sebezhetőségével [13].

[11] Michekberger P. (2018): *Információ-, folyamat-, és vállalatbiztonság.* Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar.

[13] Colwill, C. (2009): Human factors in information security: The insider threat – Who can you trust these days? In: *Information Security Technical Report*, 14., pp. 186–196.

Az információbiztonságot érintő, emberi tevékenység okozta fenyegetések bekövetkezéséhez három tényező együttes megléte szükséges:
– motiváció;
– lehetőség (hely és idő);
– és képesség „támadás" végrehajtására.

Ha ezek közül egy is hiányzik, akkor a támadás, fenyegetés nagy valószínűséggel meghiúsul. A nem szándékos baleseteket külön kell kezelni, mivel azok nem a közvetlen célzottak, hanem lehetőségfókuszúak és elsősorban a gyors és nem megfelelően követett információtechnológiai és szervezeti változásokból adódnak.

A leggyakoribb gondatlan esetek közé tartoznak a magánjellegű információs rések, mint közösségi oldalak vagy a magán adathordozó használata a szervezeti információs rendszeren. Illetve a távmunkás eszközök otthoni használata esetén a biztonsági előírások elhanyagolása, be nem tartása.

A távmunkás eszközök mellett a kapcsolt külső partnerek hozzáférései is jelentős kockázatot jelentenek, hiszen az ő munkavállalóik az eredeti vállalat biztonsági előírásait nem törvényszerűen tekintik magukra érvényesnek vagy ismerik részleteiben. További, a kockázatot befolyásoló tényezők lehetnek a képzettség, a generációs sajátosságok, a munkakörnyezet kialakítása és a témához kapcsolódó képzések hiánya, valamint a szervezeti kultúra is [11].

Az írás második részét a következő, júnusi számunkban közöljük.

[11] Michekberger P. (2018): *Információ-, folyamat-, és vállalatbiztonság.* Budapest: Óbudai Egyetem, Keleti Károly Gazdasági Kar.