KOVÁCS TAMÁS *–JUHÁSZ GÁBOR JÓZSEF **

Az információbiztonság és információvédelem szerepe a hadiiparban 2. rész

Összefoglalás: Kutatásunk témája a hadiiparban kiemelt jelentőséggel bíró és a mindennapi élet területén is egyre jelentősebb 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 kiemelt fontosságú.

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 beépíthetik a biztonságpolitikájukba.

Kutatásunk legfontosabb megállapításaként elmondhatjuk, hogy a szervezetek legnagyobb információkockázati tényezője továbbra is a humán erőforrás, amelynek 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. During the processing of the topic, we separately examined the relationship

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

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

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.

Saját vizsgálatok – A kutatási eredmények ismertetése

A kutatási vizsgálat érdekében 25 célirányos kérdésből felépített kérdőívet alakítottunk ki több terület vonatkozásában, mellyel a feltételezéseinket kívántuk reprezentálni. A kérdőívek kitöltésénél a kitöltési időre külön figyelmet fordítottunk és figyelembe vettük azt, hogy a munkavállalók leterheltsége, időszakos távolléte ne okozzon problémát az adatok gyűjtése során. A felmérés során az előzetesen bevont személyek pontos száma nem került meghatározásra, azonban megfelelő hozzáférést biztosítottunk azoknak a személyeknek, akik köre a vizsgálathoz relevánsnak bizonyult, azonban az ebből fakadó részvételi hajlandóságot az adatok minősítésére való tekintettel nem vizsgáltuk. Így végül összesen 54 fő vett részt a folyamatban, melyből 53 fő szolgáltatott értékelhető adatokat. 1 főt az adatok kiértékelése során kompetencia hiánya (kapcsolat hiánya a kiértékelt terület vonatkozásában) miatt a vizsgálatok elvégzése előtt kizártunk a folyamatból.

A kérdőíven található kérdéseket 4 csoportban fogalmaztuk meg és ezeknek megfelelően vizsgáltuk (demográfia, szakmai tapasztalat, információbiztonság, adatvezérelt döntéshozatal). Ez azonban nem jelentett kérdések szerinti elkülönülést, vagyis az egy kérdésre adott választ, a relevancia fennállása esetén több csoport elemzése során is felhasználtuk.

A kérdőív első csoportjában a demográfiai adatokat vizsgáltuk meg. Megállapítottuk, hogy a kérdőíves felmérésben jelentősebb arányban vettek részt a férfiak, kisebb arányban nők, ami az iparág sajátosságából, a munkavállalók összetételéből is adódik.

A válaszokat 66,04%-ban férfiak adták, míg 33,96 %-ban nők válaszoltak a feltett kérdésekre. A válaszadókat ezt követően generációk szerint is elkülönítettük, melynek során a Meretei (2017) által meghatározott kategóriákat és besorolásokat vettük alapul. Ezek alapján megállapítottuk, hogy a válaszadók 13,2%-a Z-generációhoz (18–30 év közötti korosztály), 34%-a Y-generációhoz (31–43 év közötti korosztály), 45,3%-k X-generációhoz (44–58 év közötti korosztály) tartozott, mindössze 7,5%-a a válaszadóknak a „boomer"-k generációja (59–65 év közötti korosztály). A demográfiai adatok közül még az iskolázottság mértékét tartottuk relevánsnak a vizsgált kérdéskörök tekintetében. A legmagasabb iskolai végzettség tekintetében a vett minta 60,4%-a főiskolai vagy egyetemi végzettséggel, 39,6% érettségivel zárult középfokú végzetséggel bír. A fenti demográfiai adatokat összegezve és elemzésüket kiértékelve kijelenthetjük, hogy a minősített adatokat elsődlegesen kezelő munkavállalók iskolai végzettsége a hadiipari szektorban magasabb, mint más gazdasági szektorok tekintetében.

A demográfiai bevezető kérdéseket követően a válaszadók szakmai tapasztalatát vizsgáltuk, mivel ennek relevanciája a szervezeti menedzsment szempontjából kiemelkedő fontosságú, a jól képzett és tapasztalt szakemberek és vezetők nagyban hozzájárulnak a szervezet sikeres működéséhez és fejlődéséhez. Ezenfelül jelentős tényezőként bírnak a szervezeti kockázatcsökkentés szempontjából, mivel segítenek a kockázatok azonosításában és csökkentésében a szervezeten belül. Tapasztalataik alapján felismerik a potenciális problémákat és kockázati tényezőket, és rendelkeznek a szükséges képességekkel, hogy azok hatásait stratégiai, műveleti vagy operatív szinten is minimalizálni tudják.

A kapott válaszokból megállapítottuk, hogy a vizsgált mintában a többség jelentős szakmai tapasztalattal bír. A válaszadók 47,2%-a rendelkezik 20 évnél is több tapasztalattal, 24,5%-a 10 és 20 év közötti szakmai múlttal, 10 évnél kevesebb tapasztalattal összesen 28,3% rendelkezett, amelyből a pályakezdők 11,3%-t tettek ki a felmérésben. Az adatok alapján megállapíthatjuk, hogy a szektor és az azon belül vizsgált szervezetek munkavállalói összetétele közel optimális. Megfelelő képzett és tapasztalt munkavállalóval rendelkeznek, hogy hatékonyan működjenek és a friss szemléletet behozó kezdő munkavállalókat fennakadás nélkül tudják mentorálni. A fenti számok azonban tisztán jelzik, hogy a szervezetekben túlsúlyban vannak a tapaszaltabb munkavállalók, amely egy elöregedő munkaerő negatív hatásait vetíti elő hosszú távon.

Az adatokat mélyebben megvizsgálva és figyelembe véve a munkakörök jellegét, ahol a válaszadók 34%-a nyilatkozott arról, hogy vezető beosztásban van alkalmazva azonban csak 66% jelölte meg a beosztott munkakört, illetve munkaköröket, kiderült, hogy vezető munkakörökben az átlagos szakmai tapasztalat 17 és 20 év között mozog, míg a beosztott munkakörökben 10–15 év között volt. A felsorolt adatok alapján jogos a feltételezésünk, hogy a válaszadók rendelkeznek kellő szakmai tapasztalattal ahhoz, hogy az információbiztonság jelentőségének tudatában legyenek. A vizsgált szervezetek részéről az információbiztonsági tudatosság átlagosnál magasabb szintje az iskolai végzettségeket és a szakmai tapasztalatokat figyelembe véve egyértelmű következtetésnek tűnt, azonban ez nem kezelhető tényként, csak megalapozott feltételezésként.

Az információbiztonságra irányuló kérdések során megmutatkozott, hogy az minden vizsgált szervezet vezetési és irányítási rendszerének szerves része, azonban minden szervezetnél kimutatható egy jelentős réteg, aki annak tartalmával nincs tisztában, a vizsgált sokaság tekintetében ez az alábbiak szerint jelentkezett: a válaszadók 88,7%-a tisztában van, 9,4%-a nincs tisztában és 1,9% szerint nincs ilyen. Ez a tény önmagában is jelentős biztonsági kockázatot rejt. A biztonsági szempontból tájékozatlan vagy figyelmetlen alkalmazottak alapvető forrásai a támadók által kihasznált sebezhetőségeknek, mivel a hiányos ismereteik révén könnyebben manipulálhatók vagy kihasználhatók, ezzel növelik a támadási felületeket. A 10% feletti információbiztonságilag alulképzett réteg a szervezetekkel szemben bizalmatlanságot és bizalmi veszélyeket teremt.

A további vizsgálatok mentén kiderült, hogy a megkérdezettek 69,8 %-a rendelkezik nyílt internet hozzáféréssel és közülük 67,9%-a intézi ezen magán jellegű ügyleteit, ami további kockázatot hordoz a rendszer biztonsága számára. A válaszadók az internet böngészőben tárolt adataik biztonsága szempontjából jelentősnek mondható kérdésre 71,7%-ban azt a választ adták, hogy nem törlik ezen adatokat, mielőtt azokhoz más is hozzáférne.

A megkérdezettek 54,7%-a a saját modern kommunikációs eszközeit részesíti előnyben, míg 45,3% a szervezeti kommunikációs eszközöket. Az arány alapvetően azzal magyarázható, hogy a szervezetek a vezetők és a kulcsfontosságú beosztott munkavállalók részére biztosítanak elsősorban „szolgálati" kommunikációs eszközöket és ezek működését a szervezetek infokommunikációs szakemberei kontrollálják.

A vizsgált szervezetek a törvényi előírásoknak és saját biztonsági szabályzatuknak megfelelve évente több alkalommal is szerveznek információbiztonsági képzéseket a munkavállalók részére, amin mindenkinek legalább évi egy alkalommal kötelező részt vennie. Ennek ellenére a megkérdezettek nyilatkozataiból az derül ki, hogy a válaszadók 30,2%-a vagy nincs tudatában, vagy a rendszert kijátszva, csak papíron vesz részt ezen képzéseken, amely eredmény az érdektelenség mértékéről ad visszajelzést.

Mivel a kutatások során megismert és feltárt infokommunikációs ismeretek nem teljes mértékben publikusak, ezért a fenti adatok csak részlegesen kerültek bemutatásra. Azok részletes elemzési és értékelési metodikájának bemutatása sértette volna az érintett szervezetek biztonsági érdekeit. Azonban az tisztán megállapítható, hogy COVID–19-járvány okozta hatások a hadiipari szektort sem kerülték el és a fenntartható kiegyensúlyozott működés érdekében át kellett alakítaniuk az infokommunikációs eljárásaikat és szabályzóikat. A költséghatékonyság érdekében korlátozottan, de elérhetővé kellett tenni a szervezeti hálózat bizonyos nem minősített részeit az alkalmazottak személyes eszközeiről a távutas munkavégzés érdekében. Habár a szervezetek gyorsan és hatékonyan alkalmazkodtak a kihívásokhoz, alkalmazottaik már nem voltak képesek a kontrollált környezetből való kiszakadás mellett is megtartani az információbizonsági fegyelmet.

A válaszadók túlnyomó része (66%) élete során dolgozott, vagy jelenleg is dolgozik olyan munkakörben, ahol nemzeti vagy nemzetközi minősített adatot kezel(t) és a szükséges biztonsági ellenőrzésen átesett. Ezek a munkavállalók nagyrészt tisztában vannak a titoksértés következményeivel. Ez tisztán rámutat arra, hogy az információbiztonsági szabályszegések elsősorban az alacsonyabb biztonsági területen dolgozók körében fordulnak elő. Emiatt a szervezetek nem is fordítottak rá akkora figyelmet, kisebb belső szankciókkal igyekeztek szabályozni azokat. Többek között ez is hozzájárulhat, hogy az információvédelmi incidenseket a feltett kérdések alapján a válaszadók jelentős része, 60%-a nem jelenti, annak ellenére, hogy tudatában vannak, hogy ez kötelességük lenne.

A bérképzés tekintetében folytatott elégedettségi vizsgálat során megállapíthattuk, hogy a munkavállalók 54,7%-a elégedett a jelenlegi bérezésével, míg 45,3%-k elégedetlen és a konkurencia bérezését versenyképesebbnek tartja. Ez az adat első ránézésre riasztónak hat, hiszen egy ilyen szektorban ez kifejezetten jelentős kockázati tényezőnek mutatkozik. Azonban, ha ezt az adatot a legfrissebb hasonló magyarországi általános kutatásokkal összevetjük, melyek eredményeiben az elégedettség mindösszesen 38%-os, akkor a szegmens nemzeti viszonylatban nagyon is jól áll. Az általános kutatások azt is kimutatták, hogy az átlag magyar munkavállaló 10% körüli bérkülönbözetért hajlandó váltani, míg a szektorban ennyire nem jelentős a szinten belüli bérkülönbözet.

Kutatásunk következő részének fókuszában maga az információ és az adat állt. Ahhoz, hogy megállapíthassuk ez mekkora valós értékkel bír a szervezetek részére, fel kellett mérnünk, hogy az mennyire szerves része a belső folyamatoknak és sérülékenysége okoz-e valós kárt a szervezet részére. A szervezetek által kezelt adatok minőségének és megbízhatóságának, az elemzésükhöz használt analitikai megoldások és a szervezeti monitorozás kérdéseinek válaszai alapján az alábbi következtetések vonhatók le a szervezetek döntéshozatali folyamataiban résztvevők hozzáállásáról és gyakorlatairól. Az eredmények alapján a válaszadók között jelentős eltérés mutatkozik az adatminőséghez és megbízhatósághoz való hozzáállásban. A válaszadók 20,8%-a teljes mértékben megbízik a rendelkezésére bocsátott adatokban, míg 47,2% alapvetően megbízik, de szükség szerint ellenőrzi azokat. Egy jelentős kisebbség (18,9%) csak kényelemből nem ellenőrzi az adatokat, míg 13,2% csak a saját adataiban bízik.

Az analitikai eszközök és programok használata tekintetében mindösszesen a válaszadók 39,6% felelt igennel. Ez azt jelzi, hogy a vállalatok többsége felismeri és kihasználja az analitikai rendszerek nyújtotta előnyöket a döntéshozatali folyamatokban, azonban a munkavállalók jelentős része még mindig nem képes azokat használni. Az analitikához kapcsolódó technológiai kérdés válaszai alapján a piaci szegmens jelentős részén hasonló technológiai szinten elemzik és dolgozzák fel az adatokat (válaszadók 39,6%-a szerint), ugyanakkor elsősorban a fiatalabb generáció tagjai ezen eljárásokat elavultnak ítélik (válaszadók 28,6%-a).

A monitorozás kérdésében a válaszadók túlnyomó többsége (79,2%) erősítette meg, hogy a szervezet menedzsmentje monitorozza a szervezetet. Ez azt mutatja, hogy a vállalatok jelentős része elismeri a mo-

nitorozás szükségességét a teljesítményük és hatékonyságuk folyamatos javítása érdekében. A még mindig jelentős kisebbség (20,8%), aki nemmel válaszolt, talán kevésbé hangsúlyozza ezt a szempontot, vagy náluk más módon valósul meg a teljesítményértékelés és ellenőrzés a vállalaton belül.

A kutatási eredményeinek összegzéseképpen megállapítottuk, hogy az adat és az információ a hadiipari szektor szereplői részére szervezeti szinten értéket képviselnek és a döntéshozatali, valamint döntés támogató rendszerekbe szervesen beépülnek. A szektoron belül az analitikai eszközök alkalmazása haladó, de nem a leginnovatívabb szinten található. Elsősorban a fiatal generáció tagjai tartják elavultnak az alkalmazott analitikai módszereket, azonban gazdasági szempontból ez nem kap jelentőséget tekintve, hogy a szektor gazdasági szereplőinek többsége azonos adatelemzési technológiai szinten mozog. A szektor analitikai szempontból legnagyobb problémáját kutatásuk alapján a munkavállalók felelőtlensége és közömbössége jelenti. A munkavállalók korábban már említett jelentős kisebbsége tisztában van az adatok és információk értékével, azonban közömbös a szervezet eredményessége iránt, ezért az információ helytállóságára nem fordít megfelelő figyelmet.

A kutatásunk kérdéseinek záró szakaszát a biztonság és a munkaerőkezelés szempontjából Magyarországon elhanyagolt pszichológiai profilozáshoz használtuk fel. A válaszadók személyiségi profilalkotásához alkalmazott kérdés esetében az vizsgáltuk, hogy a potenciális kibertámadás-célpontokra jellemző főbb tulajdonságok milyen arányban és csoportban jelennek meg a válaszadóknál. Az adatok elemzését és értékelését követően megállapítottuk, hogy a 3 legjellemzőbb tulajdonság az együttműködő, érdeklődő és a kompromisszumkereső, míg a leggyakoribb tulajdonságcsoport az együttműködő, nyílt és kompromisszumkereső jellemzők együttese. A kérdőívek kiértékelésének eredményeképpen megállapítottuk, hogy a vizsgált szegmens kutatásban résztvevő szervezeteinek mindegyike rendelkezik egy közel 10%-s olyan alkalmazotti réteggel, akik a szervezet számára fontos információt kezelnek és optimális célpontjai egy esetleges támadásnak, akár saját tudtukon kívül is.

A szervezetek vezetőivel készített mélyinterjúk rávilágítottak, hogy a védelmi- és hadiipari szektorban résztvevő vállalatoknak és szervezeteknek a biztonsági területen adott szabad mozgása jelentős mértékben korlátozott. Az ügyféligényeknek és ügyfélbizalomnak, valamint a piacnak való megfelelés érdekében nagyon szigorú és szoros külső szabályozásnak kell megfelelni. Ezeket rendszeres, a szabványokban előírt akkreditációs eljárásban bizonyítják.

Az interjúalanyok mindegyike külön kiemelte, hogy a szervezetek erősek a fizikai biztonság területén és ehhez kapcsolódó intézkedéseiket proaktívan végzik. Az infokommunikációs biztonság témakörében a lehető legtöbb védelmi megoldást alkalmazzák (tűzfalak, szeparált hálózati szegmensek, IPS, IDS-eszközök). Az intézkedések egy része nem saját döntés alapján történik, hanem audit megfelelés céljából, vagy az audit során feltárt hiányosságok kezeléseként. A személyzet részére biztonsági oktatások vannak, de a szervezet egyes területeinek a biztonságtudatossága ennek ellenére elmarad az elvárt szinttől.

Az információbiztonság kihívásai között említhetjük a folyamatosan változó kiberfenyegetéseket és az alkalmazottak hozzáférési jogosultságainak kezelését. A kiberbiztonsági részlegeknek folyamatos proaktivitást kell tanúsítaniuk a kihívásokra, a biztonsági rések felderítésére és megszüntetésére. Ezeket a problémákat a vállalatok nem önmagukban kezelik, hanem nagyban támaszkodnak és aktívan részt vesznek az ipari partnerségekben és együttműködnek a nemzeti- és katonai biztonsági szolgálatokkal. A belső fenyegetéseket szigorú szabályozással és monitorozással igyekeznek kezelni, a szoftverek folyamatos naprakészen tartása és az erős titkosítás alkalmazása mellett.

Az interjúalanyok egybehangzó szakvéleménye alapján egyértelműen kijelenthetjük, hogy a vizsgált ipari szereplők részére az információbiztonság nem csupán kötelező technikai kérdés, hanem egy vállalatstratégiai szempont, amely meghatározza az adott vállalat sikerességét és fenntarthatóságát, amely a folyamatos fejlesztésen és a jövőbeni kihívásokhoz való rugalmas alkalmazkodás képességén alapul.

Összegzés

A vizsgálat és a komplex elemzés kiterjedt a hadiipari szegmens résztvevőinek tekintetében a vizsgált szervezetek döntéshozatali és analitikai folyamataira. A vizsgálatok során számos olyan tényezőt megfigyeltünk, amelyek egymástól elkülönülve és együttesen is befolyásolják az információbiztonságot, többek között a szervezeti kultúrát, a munkavállalók hozzáállását, a technológiai eszközök alkalmazását vagy a szervezet belső monitorozási folyamatait.

Az eredmények alapján meggyőződésünk, hogy a munkavállalók hozzáállásában szükséges a változás és ezt a nélkülözhetetlen szemléletváltást a középvezetői szinten javasolt kezdeni, az érintett vezetők továbbképzésével és megfelelő felkészítésével. A jelenlegi felgyorsult, változó környezetben a vezetőknek is szükséges közel azonos ütemben proaktívan megújulni és fejlődni, más esetben a szervezet elveszti versenyképességét és ellenállóképességét. A naprakész vezetők az egyéni és a szervezeti célok összehangolásával motiválják és fejlesztik a beosztott munkaerő információbiztonsági tudatosságát, ezzel javítva és fejlesztve a szervezeti kultúrát.