T. Dénes Tamás

„Maximális biztonság = minimális emberi tényező”

Vasvári György *A társadalmi és szervezeti (vállalati) biztonsági kultúra című könyvéről* (Budapest, Ad Librum Kiadó, 2009)

A köztudatban már-már közhelynek számít, hogy globalizálódó információs társadalomban élünk, amelyben alapvető szerepet játszik a tömeges mennyiségű információ létrehozása, áramoltatása és tárolása. Mindez egyre inkább elektronikus digitális rendszereken történik. Ennek az új és napjainkban is alakuló társadalmi formának a pontos leírása még a kutatók részéről is várat magára. Az azonban bizonyos, hogy az információ alapú e-társadalom kulcskérdése a biztonság. A biztonsággal, különösen az informatikai biztonsággal és az információbiztonsággal foglalkozó szakemberek általában mint technikai bravúrt fogják fel a biztonsági rendszerek kiépítését, így altatva el az alkalmazók veszélyérzetét. Éppen ezért fontos felhívni a figyelmet a kötet bevezetésének zárógondolatára, amely a további tartalom esszenciájának is tekinthető: „…a legelső veszélyforrás egy szervezetben maga az ember”.

A szerző jelen kötete hiánypótló a biztonsággal foglalkozó hazai szakirodalomban, mivel egészen új szemszögből világítja meg a kérdést. Rámutat, hogy egy adott társadalom kultúrájának részét képezi a biztonsági kultúra. A biztonságra vonatkozó leglényegesebb alapelv, az egyenszilárdság elve a technikai biztonsági rendszereken túl kiterjesztendő a teljes társadalomra (mint rendszerre), illetve annak alrendszereire (például a szervezetekre, vállalatokra) is. Így válik érthetővé, hogy a biztonsági kultúra a különböző rendszerszinteken fejleszthető, oktatható, a személyiségbe integrálható, sőt az újabb generációkra átörökíthető.

A kötet felépítése tökéletesen követi az ehhez a megközelítéshez elengedhetetlen rendszerszemléletet. Ez vonatkozik a biztonsági kultúra társadalmi rendszerszintjétől az alacsonyabb, szervezeti rendszerszintekre való modellanalógiák bemutatására, de a fogalmi rendszerépítésre is, amely az alapfogalmak (biztonság, társadalom, közösség, önvédelmi képesség stb.) definícióitól halad tovább a bonyolultabb fogalmakig (kultúra, szervezeti kultúra, biztonsági kultúra, biztonsági tudatosság).

Figyelemre méltó a szerzőnek az a törekvése, hogy az elmélet és az alkalmazható gyakorlati sémák közötti egyensúlyt megtalálja. Ennek alapjául szolgál az információ és a hatalom viszonyának tömör megfogalmazása az I. részben, a társadalmi biztonságot fenyegető veszélyforrások részletes felsorolása után: „Az információ ma már tömegcikk, és birtoklása nem utolsósorban hatalmat jelent.”

Mivel a szerző nem társadalomkutató, hanem informatikus szakértő, üdvözlendő a kitartó kutatása a háttérirodalomban, amely jól tükrözi az információs társadalommal kapcsolatos elméleti alapvetések hiányát. Ennek eredménye az I. rész elméleti záró-

gondolata, miszerint „…az új fenyegetések az információs társadalomban globálisak, kevésbé jelezhetők előre, gyorsan változnak, így kiszámíthatatlanok".

Ugyanebben az I. részben nemzetközi kitekintést (EU, NATO, ENSZ) is tartalmazó összefoglalását kapjuk a társadalmat, illetve a társadalmi biztonsági kultúrát meghatározó tényezőknek. Fontos és naprakészen alkalmazható az I. rész végén közölt COBIT érettségi modell, valamint az OECD tanácsa által 2002-ben elfogadott Új Biztonsági Kultúra program rövid ismertetése.

A kötet koncepcióját jól tükrözi, hogy a II. rész, amelynek címe „A szervezeti (vállalati) biztonsági kultúra", a gyakorlatban igen jól alkalmazható mellékletekkel együtt a könyv terjedelmének 75%-át teszi ki.

Általános vezérelvként fekteti le a szerző, hogy a kultúra afféle közösségi tudásbázis, amely kölcsönösen elfogadott, generációkon átnyúló (átörökíthető) tevékenységmintákat hoz létre. Az információs társadalom megkülönböztető jegye, hogy az informatika átalakítja a kultúrát (lásd 9.2. fejezet).

A szerző a társadalom szintjén megfogalmazott kultúrafogalmat alkalmazza a szervezetekre mint szubkultúrákra is. Megfogalmazza a vezetési alrendszer, azaz a menedzsment típusait és szerepét a szervezeti kultúra fejlesztésében és fenntartásában (lásd 2. táblázat). Mindezekre építve fog bele a szervezeti biztonság tárgyalásába, amely átvezet a biztonsági kultúra (lásd 3. ábra) és biztonsági tudatosság (lásd 4. ábra) területére.

A II. rész, de nyugodtan mondhatjuk, hogy az egész kötet csúcspontját a 11.2. fejezetben tárgyalt „emberi tűzfal" *(human firewall)* fogalmának bevezetése jelenti. Itt fogalmazódik meg az a biztonsági rendszerekkel kapcsolatos általános probléma, amely kiemeli az emberi tényező szerepét: „Az emberi tényező képezte kockázatokkal szembeni védelmi vonalak a technológiai megoldásnak nem részei. […] Ezeket a védelmi intézkedéseket egy szervezetenként kidolgozott *emberitűzfal-nyilatkozatnak* kell tartalmaznia…"

A szerző ismerteti a *Human Firewall Council* által ajánlott védelmi intézkedési lépéseket, amelyekre ez a nyilatkozat épül, majd sorra veszi a biztonsági kultúrát sértő magatartástípusokat. A 12. fejezetben részletesen tárgyalja a W. E. Deming által az 1980-as évek második felében kidolgozott *PDCA*- (*Plan*, *Do*, *Check*, *Act:* tervezés, megvalósítás, ellenőrzés, cselekvés) modellt, amelyet adaptáltak az Új Biztonsági Kultúra program megfogalmazói (lásd 3. táblázat). Ennek alapelvei szerint a programnak a biztonsági politikával összhangban kell készülnie, különös tekintettel a humán tényező fontosságára: a szervezetben kell lennie egy munkatársnak, aki a biztonsági kultúra koordinálásáért felelős. Ez a fejezet a biztonságszervezési folyamat leírásával és elemzésével (lásd 4. táblázat) támpontokat ad a teendők gyakorlati végrehajtásához is.

A 13. fejezet egy úgynevezett „érettségi modell" *(Control Objectives for Information and related Technology, COBIT)* segítségével mutatja be a biztonsági kultúra értékelését – lásd 5. táblázat. Az értékelés eredményeként meghatározhatók a biztonsági kultúra szintjei (lásd 6. táblázat), aminek az ad különös jelentőséget, hogy ráirányítja a figyelmet az egyenszilárdságú biztonsági rendszerek fontosságára: „A legújabb technika installálásának hatékony biztonsági kultúrával kell együtt járnia."

A szerző itt hívja fel a figyelmet az információbiztonság és az informatikai (számítógépes) biztonság közötti különbségre. Ennek lényege, hogy mindkettő a szervezeti

kultúra része, de a menedzsment részéről igen különböző védelmi intézkedéseket igényelnek (lásd 5. ábra).

Ki kell emelni a 17. fejezet („A biztonsági kultúra és az egyén") jelentőségét, amelyben nem csupán a Karl Gustav Jung típustanára épülő személyiségtipizálás részletes leírását és a biztonsági kultúra szempontjából történő elemzését találjuk meg, hanem figyelemre méltó új elemként „a szervezet személyiségtípusait" is (lásd 7. táblázat). Így egységes rendszerben válik magyarázhatóvá az egyén és az őt magában foglaló szervezet biztonságának összefüggése, valamint az, hogy az egyének, illetve az egyének és a szervezet különbözősége biztonsági szempontból kockázatot jelent.

Érdemes felhívni a figyelmet arra, hogy ezzel éppen ellentétes a célok elérése szempontjából hatékony, kreatív szervezet értékrendje, ahol a különbözőség a jó teammunka egyik meghatározó értéke. Itt tehát jelentős konfliktuskezelési feladatot kell megoldania a menedzsmentnek. E jelentős probléma elemzésének szenteli a szerző a 18. zárófejezetet („A vállalatirányítás, kockázat, megfelelőség és a kultúramenedzsment integrációja"), melynek végén „A kommunikáció és egyetértés alakulása a biztonsági kultúra kialakítása során" című ábrán összegzi a kötet mondanivalóját (lásd 10. ábra).

A kötet végén a témához kapcsolódó részletes irodalomjegyzéket, valamint a szakkifejezések és rövidítések rövid értelmezését találjuk. Ezek a mellékletek különösen alkalmassá teszik a kötetet oktatási célokra való felhasználásra, és segítik az olvasó további elmélyedését a témában akár kutatási szinten is.

A tartalmilag újszerű és kiválóan áttekinthető szerkezetű kötetben sajnos elég sok helyen fordulnak elő tördelőszerkesztői és technikai hibák (szövegbeli elütések, hibás elválasztások, a háttérnél és a szövegnél alkalmazott szürke árnyalatok rossz megválasztása miatt olvashatatlan ábrafeliratok).