

Vasvári György CISM

A társadalmi és szervezeti (vállalati) biztonsági kultúra

AD-LIBRUM Kiadó, Budapest, 2009.

(recenzió)

„Maximális biztonság = Minimális emberi tényező”
(T.D.T.)

A köztudatban már-már közhely, hogy globalizálódó információs társadalomban élünk, amelyben alapvető szerepet játszik a tömeges mennyiségű információ létrehozása, áramoltatása, illetve tárolása. Mindez egyre inkább elektronikus digitális rendszereken történik. Eme új és napjainkban is alakuló társadalmi forma 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, illetve információbiztonsággal foglalkozó szakemberek, általában mint technikai bravúrt fogják fel a biztonsági rendszereket, így altatva el az alkalmazók veszélyérzetét. Éppen ezért fontos felhívni a figyelmet a kötet bevezetésének záró gondolatára, amely a további tartalom eszenciájának is tekinthető: „... a legelső veszélyforrás egy szervezetben maga az ember.”

A Szerző jelen kötete hiánypótló a biztonsággal foglalkozó hazai szakirodalomban, mivel egy egészen új szemszögből világítja meg a kérdést. Rámutat, hogy egy adott társadalom kultúrájának részét képezi a biztonsági kultúra. A biztonságra vonatkozó leglényegesebb alapelvek, az *egyensúlytalanság elve*, a technikai biztonsági rendszereken túl kiterjesztendő a teljes társadalomra (mint rendszerre), illetve annak alrendszerreire (pl. a szervezetekre, vállalatokra). Így válik érthetővé, hogy a biztonsági kultúra a különböző rendszerszinteken fejleszhető, 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 definícióitól (biztonság, társadalom, közösség, önvédelmi képesség, ...), a bonyolultabb fogalmakig (kultúra, szervezeti kultúra, biztonsági kultúra, biztonsági tudatosság, ...) halad.

Nem elhanyagolható a kötet azon törekvése, hogy az elmélet és az alkalmazható gyakorlati sémák közötti egyensúlyt megtalálja. Ennek alapjául szolgál az információ és 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.”¹

Mivel a Szerző informatikus szakértő, nem társadalomkutató, üdvözlendő az a kitartó háttér irodalomkutatás, amely jól tükrözi az információs társadalommal kapcsolatos elméleti

¹ A megfogalmazás tökéletesen igazolja vissza N.Wiener több mint 60 évvel ezelőtt, az információ tömegcikké válásának hajnalán leírt látónoki gondolatait: "A tipikus amerikai világban az információ sorsa az, hogy áru lesz, venni és eladni lehet. Nem az én dolgom, hogy azon akadékoskodjam, hogy ez a kereskedői álláspont erkölcsös-e vagy nem, durva-e vagy finom. Az én dolgom az, hogy kimutassam: ez az álláspont az információ és a vele kapcsolatos fogalmak félreértéséhez és félrekezeléséhez vezet." (Norbert Wiener)

alapvetések hiányát. Ennek eredménye az I. rész elméleti zárógondolata, miszerint „Végül az új fenyegetések az információs társadalomban globálisak, kevésbé jelezhetők előre, gyorsan változnak, így kiszámíthatatlanok.”

Másrészt 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, illetve az OECD Tanácsa 2002-es *Új Biztonsági Kultúra Programjának*² 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 egyfajta közösségi tudásbázis, amely kölcsönösen elfogadott, generációkon átnyúló (átörökíthető) tevékenységmintákat hoz létre. Az információs társadalom differenciaspecifikuma, hogy az informatika átalakítja a kultúrát (lásd 9.2.fejezet).

A társadalom szintjén megfogalmazott kultúra fogalmat alkalmazza a szervezetekre, mint szubkultúrákra. 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) fogalmi bevezetése jelenti. Itt kerül megfogalmazásra 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 *EMBERI TŰZFAL NYILATKOZAT*-nak 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 magatartás típusokat.

A 12. fejezetben részletesen tárgyalja W.E. Deming 1980-as évek második felében kidolgozott PDCA (Plan, Do, Check, Act) modelljét adaptáló *Biztonsági Kultúra Programját* (lásd 3.táblázat). Ennek alapvető elve, hogy a programnak a Biztonsági politikával összhangban kell készülnie, egyúttal megfogalmazza a humán tényező fontosságát, vagyis, hogy a szervezetben kell lennie egy biztonsági kultúra koordinálásáért felelős munkatársnak.

A fejezet továbbá támpontot ad az alkalmazáshoz, a biztonságszervezési folyamat leírásával és elemzésével (lásd 4.táblázat).

Majd a 13. fejezet a biztonsági kultúra értékelését mutatja be a *Control Objectives for Information and related Technology* (COBIT) érettségi modell segítségével (lásd 5.táblázat). Az értékelés eredményeként meghatározhatók a biztonsági kultúra szintjei (lásd 6.táblázat), amelynek különös jelentősége, hogy ráirányítja a figyelmet az *egyenszilárdságú biztonsági rendszerre*. Azaz, hogy „A legújabb technika installálásának hatékony biztonsági kultúrával kell együtt járnia.”

² Ezt a 12. fejezet részletesen tárgyalja.

A szerző itt hívja fel a figyelmet az *információbiztonság* és *informatikai (számítógépes) biztonság* közötti különbségre. Ennek lényege, hogy mindkettő a szervezeti kultúra része, de a menedzsment számára igen különböző védelmi intézkedéseket igényelnek (lásd 5.ábra).

Ki kell emelni a 17. fejezet jelentőségét (*A biztonsági kultúra és az egyén*), amelyben nem csupán a biztonsági kultúra szempontjából vizsgált Karl Gustav Jung típusánára épülő személyiség tipizálás részletes leírását és elemzését találjuk, hanem figyelemreméltó új elemként írja le a „*szervezet személyiségtípusait*” (lásd 7.táblázat). Így egységes rendszerben válik magyarázhatóvá az egyén és az őt befoglaló szervezet biztonságának összefüggése, valamint az, hogy az egyének, illetve *az egyének és a szervezet különbözősége biztonsági szempontból kockázatot jelent*.

Érdeemes felhívni a figyelmet arra, hogy ezzel éppen ellentétes, a célok elérése szempontjából hatékony, kreatív szervezet értékrendje, ahol a különbözőség a jó team munka egyik meghatározó értéke. Itt tehát jelentős konfliktuskezelési feladatot kell megoldania a menedzsmentnek.

Eme jelentős probléma elemzésének szenteli a Szerző a záró 18. fejezetet (*A vállalatirányítás, kockázat, megfelelés és a kultúramenedzsment integrációja*), melynek végén *A kommunikáció és egyetértés alakulása a biztonsági kultúra kialakítása során* című ábrában összegzi a kötet mondanivalóját (lásd 10.ábra).

A kötet végén található mellékletekben a témához kapcsolódó részletes irodalomjegyzéket, valamint a szakkifejezések és rövidítések rövid értelmezését találjuk.

A kötet tartalmi újszerűségét és kiválóan áttekinthető szerkezetét elég sok helyen zavarják meg a tördelő-szerkesztés hibái (szövegbeli elütések, hibás elválasztások, a háttér és szöveg szürkeárnyalatának rossz megválasztása miatt olvashatatlan ábrák).

Budapest, 2010. január

Dénes Tamás
matematikus