M Ű E G Y E T E M **1 7 8 2**

**Budapesti Műszaki és Gazdaságtudományi Egyetem**
**Gazdaság- és Társadalomtudományi Kar**
**Információ- és Tudásmenedzsment Tanszék**

**BIZTONSÁGMENEDZSMENT KUTATÓ CSOPORT**

**VASVÁRI GYÖRGY CISM**
**Tiszteleti egyetemi docens**

# SZERVEZETI KULTÚRA, BIZTONSÁGI KULTÚRA

## AJÁNLÁS

**1.0 változat**

**2006**

**Az ajánlás 1. és 2. fejezeteihez, és a 8.1. ponthoz észrevételeket tett:**
POSZLER GYÖRGY akadémiai rendes tag (ELTE).

**Észrevételeket tett az ajánláshoz:**
Odor Zsuzsanna a kommunikáció tanára (HFGTSZ Főiskola).

**Az ajánlást megvitatták és észrevételeket tettek:**
a Biztonság Menedzsment Kutató Csoport tagjai:

BARTOK SÁNDOR P: CISA, CISM, ISACA Hungary Chapter alelnök.
EGERSZEGI KRISZTIÁN PhD hallgató (BME),
ERDŐSI PÉTER CISA, kutató (BME),
LENGYEL CSABA biztonsági vezető, informatikai ellenőrzési, és biztonsági szakértő (KELER Zrt.),
SÁNTHA PÉTER vezető szakértő (BME),
DR. SZÉKELY IVÁN adatvédelmi szakértő, egyetemi docens (BME),
VALÁDI ZOLTÁN informatikai biztonsági, és informatikai ellenőrzési szakértő, biztonsági vezető (GIRO BANKKÁRTYA Rt.).

# TARTALOMJEGYZÉK

# 1. BEVEZETÉS

A kultúra fogalma megjelent az informatikai szakirodalomban. A COBIT4, például egy sor magas szintű auditálási szempontban szerepelteti a kultúrát, mint ellenőrzési követelményt. Ugyanakkor ez a fogalom a COBIT4-ben nincs definiálva. Összehasonlítva az említett követelményeket, szempontokat a COBIT 3 megfelelő pontjaival (a COBIT3 [10]. megfelelősségeket a COBIT4 [11] táblázatban adja meg), következtetni lehet arra, hogy **a COBIT4** ***a kultúrán***

- *általában az erkölcsi tartást, az etikai érékeket, és a magatartást érti.*

Először szükséges tisztázni, támaszkodva az igen széles szakirodalomra, a kultúra fogalmát, majd a kisebb közösségekre vonatkozó szervezeti kultúra fogalmát. Ezek után lehet azzal foglalkozni, hogy mit értünk szervezeti kultúrán, beszélhetünk-e szervezeti kultúrán belül biztonsági kultúráról, és amennyiben igen, milyen viszonyban van az eddig használt biztonsági tudatossággal, és amit miként kell menedzselni.

Megközelítésünk alapja tehát

- a kultúra általános fogalma,
- a kisebb közösséget jellemző, a globális kultúrán belüli kultúra (-ák), mint a szervezeti kultúra és elemei, megjelenési formái,
- a biztonsági kultúra a szervezeti kultúrán belül, aminek elemeit és megjelenési formáit a szervezeti kultúra elemein, illetve megjelenési formáin belül határozzuk meg.

# 2. A KULTÚRA

## 2.1. A KULTÚRA FOGALMA

- A Magyar Nagy Lexikon és a Magyar Larousse Enciklopédia szerint a kultúra többek között:
  - az emberiség által létrehozott anyagi és szellemi értékek összessége;
  - egy adott korszak anyagi és szellemi javainak egysége;

- egy civilizáció jellemző tulajdonságai, beleértve a hitüket és szokásaikat. Az alapot képező értékek, a gyakorlat intézkedései és szabályai, amelyek egy közösséget azzá tesznek, ami;
- az embert az állatvilágtól megkülönböztető anyagi, szellemi, viselkedésbeli sajátságok összessége;
- műveltségi színvonal;
- a viselkedés kultúrája.

➢ A kultúra a COBIT4-ben a következő magas szintű ellenőrzési szempontokban szerepel:

- PO6.1. Politika és ellenőrzés
  A környezet egy kultúrán alapul, amely támogatja az értékteremtést, menedzseli a szignifikáns kockázatokat, támogatja a területek közötti együttműködést és a teammunkát, segíti a megfelelősséget és a folyamatos folyamatfejlesztést, kezeli a folyamtok eltéréseit (beleértve a hibákat is).
- PO8. Minőség menedzsment
  Folyamatok céljai: az IT folyamatokra állapít meg szabványokat és kultúrát.
- DS5. Gondoskodás a rendszer biztonságról
  DS5. 2. IT biztonsági terv. Az üzleti IT követelményeket alapul véve az IT konfigurációt, az IT kockázatkezelési tervet és az informatikai biztonsági kultúrát egy általános IT biztonsági tervben valósítja meg.
- ME3. Gondoskodás a szabályozott megfelelősségről. Érettségi modell 5. szint, optimalizált.
  A szervezet menedzsmentjének stílusa és kultúrája a megfelelősség vonatkozásában erős, az oktatási folyamatokat kielégítően fejlesztik az új alkalmazottak számára, valamint jelentős csere esetére.
- A belső ellenőrzés érettségi modellje (0. szint, nem létező) szerint, a belső ellenőrzés környezetének állapota:
  Nem ismerik fel a belső ellenőrzés szükségességét. Az ellenőrzés nem része sem a szervezeti kultúrának, sem a küldetésnek.

## *2.2. AZ INFORMATIKA ÁTALAKÍTJA A KULTÚRÁT*

A modern technológia, és a modern információ rendszer átjárja a kultúra minden területét. Az elektronikus globalizáció kialakítja az egyetemes kultúrán belül az elektronikus kultúrát. Ugyanakkor az informatikai technológia, hatással van az üzleti, és a magán életre egyaránt. Az informatika terjeszti az adott kultúra hitbeli, és értékbeli alapjait, a magatartás, és a viselkedés kultúrát, zsugorítja a kultúra megteremtésének, és elsajátításának idejét, míg a tér tényezőit kiterjeszti.

Az információ alakította kultúra (Information driven culture) komponensei, A. Tagorszki, és T. Rienzo munkája alapján (lásd [8]):

- az erkölcsi magatartás,
- az értékek,
- az életmód,
- a biztonság,
- az egészség,
- a magán élet.

Érdekes módon Heidrich [2-ben] a kultúra fogalmát, Hofstedre hivatkozva [16], a következőképpen adja meg:

„A kultúra az elme kollektív programozása, amely megkülönbözteti egy csoport tagjait vagy az emberkategóriákat a többitől”. Ezeket az érzelmi, cselekvési és gondolkodási mintaképeket Hofsted „az elme szoftverének” nevezte.

Az információs társadalom kialakulása során tehát a kultúra jelentős változáson megy át. AZ új technika átalakítja a viselkedés kultúrát is. Azonos folyamatok mennek végbe a vállalatok, szervezetek környezetében és magukban a szervezetekben is. Ezért az eddig tárgyaltak aláhúzzák a biztonsági kultúrával történő foglalkozás fontosságát.

# *3. A SZERVEZETI KULTÚRA*

## *3.1. A SZERVEZETI KULTÚRA FOGALMA*

A szervezetről írja W.E. Schneider [19-ben], hogy „minden szervezet élő társadalmi szervezet a saját kultúrájával, jellemzőivel, természetével, és azonosságaival.” Továbbá: „a szervezetek azonos küldetéssel rendelkező emberek közösségei”. A szervezetet megkülönböztetjük a rendszertől. L. Bertalanffy szerint:

„A rendszer elemek halmaza, amelyek egymással kölcsönös kapcsolatban állnak.”

Ladó L. [28] a különbségről azt írja, hogy:: A szervezet rendszerként értelmezhető. A szervezet, a vállalat mikro gazdasági rendszer (míg fordítva nem lehetséges). A szervezet feltételezi emberek részvételét, míg a rendszer lehet csak gépi. A szervezet az szabályozó, a rendszer szabályozott.

A szervezeti kultúra alapvetően a szervezet személyisége [2,4,5,6,], az alkalmazottak véleményének, szokásainak, értékítéletének, magatartásának, gondolkodási és cselekvési módjainak összessége, (Buchowicz szerint [12]).

A [13-ban] Dr. G. Hinson azt írja, hogy „a cél kialakítani és fenntartani egy szervezeti kultúrát, ahol az informatikai biztonság minden munkavállaló második természete”.

A szervezeti kultúra (a vállalati kultúra szinonimája azzal, hogy a szervezet tágabb fogalom, mint a vállalat, hiszen vannak szervezetek, amelyek nem vállalatok) magába foglalja a szervezet tagjainak a felelősség vállalásait, az etikai értékeket, a normatívákat, ezeknek a megjelenési formáit, a szervezet magatartását, a vezetési filozófiát.

A szervezeti kultúra a szervezet közös gondolkodása, amit a szervezet a közös problémáinak megoldása során tanul meg.

A szervezeti/vállalati kultúra integrálja a szervezetet, és elősegíti a környezethez történő alkalmazkodást, amelyen elsősorban az üzleti célok, követelmények változását követő *változásmenedzsmentet értjük.*

## *3.2. A SZERVEZETI KULTÚRA ELEMEI, MEGJELENÉSI FORMÁI*

C. Handy a szervezeti kultúrát négy összetevőre bontja:

- szerepkultúra,
- feladatkultúra,
- hatalomkultúra és
- személykultúra, amelyeket

ki kell egészítenünk a biztonsági kultúrával, amely valójában mind a négy összetevő zavartalan, rendeltetésszerű működésének feltétele, mivel biztonság nélkül nincs szervezet, amely a küldetésének meg tudna felelni.

Heidrich Balázs [2] szerint a szervezeti kultúra elemei:

- a környezet (társadalmi, gazdasági),
- az értékek (amelyek a szervezeti kultúra alapját képezik),

- a hősök és tekintélyek (akik a szervezet céljai elérésében kiemelkedőt tettek),
- a ceremóniák és szertartások (rendezvények a szervezet összetartásáért),
- a kulturális hálózat (a kulturális elemek terjedésének közege).

Továbbá [2] alapján *a szervezeti kultúra megjelenési formái*:

- a szimbólumok (tárgyak, berendezések, vezetők, hősök, szerepek),
- a nyelvezet (zsargon, gesztusok, jelek, dalok, viccek, kifejezések, szólások),
- a történetek (legendák, mítoszok, sztorik),
- a szokások (szertartások, tabuk, rituálék, ceremóniák).

Bodor Márton szerint [15] a szervezeti kultúra elemei:

- a normák, értékek, gondolkodás, magatartás az egyén és a vállalat szintjén,
- a problémamegoldás módja,
- a szerep-, feladat-, hatalom- és személykultúra (lásd C. Handy szerint is).

A munkatársak mintákra támaszkodnak, amelyeket a vezetőktől és a társaiktól látnak. Ilyen minták például a viselkedés módok, a normák, értékek és más formális vagy informális eszközök.

A Mc Kinsey féle 7S modell [14] szerint *a szervezeti kultúra elemei* két csoportba oszthatók:

⇒ **kemény elemek, azok a szabályozási elemek,** amelyek kezelésére modellek, számszerűsíthető módszerek, menedzsment eszközök állnak rendelkezésre. Ezek a következők:

- a szervezeti stratégia, a szervezeti célok és a megvalósítás eszközei, követelményei,
- a struktúra szervezetirányítása, felépítése és módszere,
- az üzleti, termelési és információ rendszerek,

⇒ **lágy elemek, azok a motivációs elemek,** amelyek nem írhatók le modellekkel, és nem léteznek menedzselésükre számítástechnikai eszközök, de ezeknek kiemelkedő szerepe van a szervezet kultúrájának alakításában. Éspedig:

- képességek, a szervezetnek az alapvető értékeken alapuló képessége,
- az alkalmazottak képzettsége, ismeretei, tudása, elkötelezettsége, érdekeltsége,

- a szervezet értékrendje, amely a szervezet magatartását, viselkedését, például a humán kultúrát határozza meg.

A példaképpen bemutatott meghatározások közül az ajánlás készítőjéhez a 7S modell áll legközelebb, amelyet felfoghatunk úgy is, hogy Bodor és Handy elemei megtalálhatóak benne. Ugyanis a normák, értékek, gondolkodás kemény elemeknek tekinthetők, míg a szerep, feladat, hatalom, személyi (pl. magatartás) kultúra motivációs elemek, azaz lágy elemeknek tekinthetők.

## *3.3. A SZUBKULTÚRÁK*

A szakirodalomban több szerzőnél felmerül, például [2]-ben, hogy a szervezeti kultúra, különösen nagyobb szervezeteknél, vállalatoknál nem teljesen egységes, kialakulhatnak eltérő megjelenési formákkal leírható szubkultúrák

Ezekben a szubkultúrákban a megjelenési formák közül egyesek megegyeznek a szervezeti kultúrával, míg egyesek eltérnek attól. A szubkultúrák kialakulásának az egyes elkülönült szervezetek, funkcionális vagy területi sajátosságok lehetnek az okai. Gondoljunk csak a nyelvezetre (zsargon), a speciális szokásokra, a saját történetekre. A szubkultúrák lehetnek a felső vezetéssel kialakult viszonyt

- *támogató,*
- *ellentétes, illetve*
- *semleges* megjelenési formák.

Természetesen a szubkultúrák szükségszerűen nem képeznek káros jelenséget, hozzájárulhatnak a csoportszellem erősödésével a szervezeti kultúra erősödéséhez. Például az informatikai területen a szoftveresek, műszakiak, szervezők képezhetnek szubkultúrát a szervezeti kultúra egyes megjelenési formáit tekintve. Azonban törekedni kell az alapvető értékrendek, a szervezet iránti elkötelezettség vagy a magatartáskultúra tekintetében egységes szervezeti kultúrát létrehozni, fenntartani, a szubkultúrák támogató jellegét erősíteni., a szubkultúrák egymásra hatását is figyelembe véve.

A szervezeti kultúra a nemzeti kultúrán belül egy szubkultúra.

Itt kell megemlíteni az **ellenőrzési kultúrát** (a fentiek szerint egy funkcionális eredetű szubkultúra), amely azt jelenti [18], hogy a szervezet kihangsúlyozza és demonstrálja az alkalmazottak minden szintjén a belső ellenőrzés fontosságát. Azaz az ellenőrzési kultúra

- a vezetés szavainak, magatartásának, a board tevékenységeinek és a felső vezetésnek a viszonya (felelősség érzete) a szervezet ellenőrzési kultúrájának a sértetlenségéhez, etikájához (ez a számon kérhetőség és a következetes számonkérés követelménye),
- a további szinteken annak a felismerése, hogy mindenkinek a felelősségét hatékonyan kell megvalósítania, és a működés bármely problémáját, az illegális tevékenységeket, illetve politikák megsértését a vezetés megfelelő szintjével közölni kell (ez az események rendeltetésszerű kezelésének követelménye).

Az ellenőrzési kultúra elemei:

⇒ **kemény elemek:**

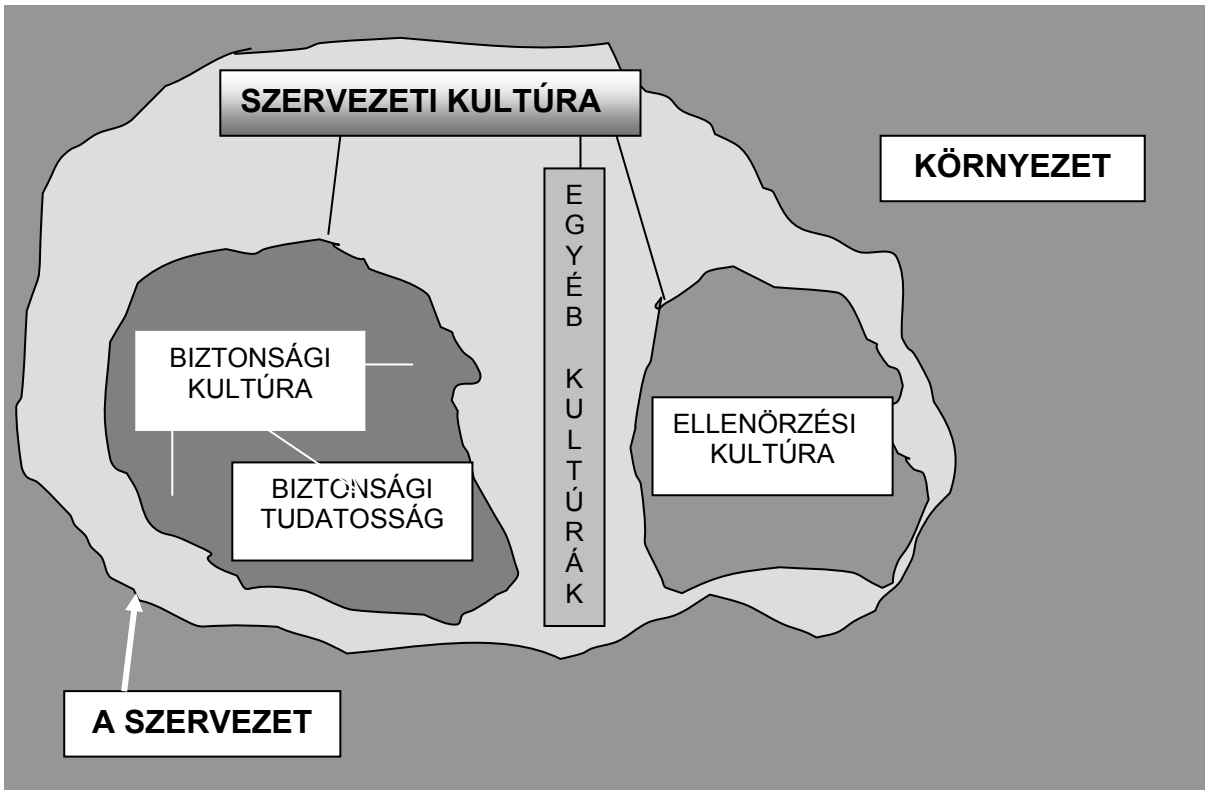
- az ellenőrzési stratégia és célok a szervezeti stratégia és célok függvényében, valamint a megvalósítás eszközei, követelményei,
- az ellenőrzési struktúra, az ellenőrzési szervezet irányítása, felépítése és módszerei,
- az ellenőrzés rendszere az alrendszerekben.

⇒ **lágy elemek:**

- az ellenőrzési szervezetnek az alapvető értékeken alapuló képessége,
- az ellenőrök képzettsége, ismerete, tudása, elkötelezettsége, érdekeltsége,
- az ellenőrzés helye a szervezet értékrendjében, a vezetés, és az alkalmazottak viszonya az ellenőrzéshez.

A biztonsági kultúra az ellenőrzési kultúra nélkül nem képes a vezetés által meghatározott biztonsági szintet biztosítani. A hatékony és eredményes ellenőrzési kultúra a biztonság potenciális megsértőit, akár szervezeten belül, akár szervezeten kívül elrettentheti, csökkentheti szándékolt cselekedetük (a támadás) motivációját az elkövetésére. Az ellenőrzési kultúra a vezetési stílus, a hatalom gyakorlásának a függvénye.

A szervezeti kultúrán belül tehát szubkultúrák jönnek létre, illetve állnak fenn, és ezt a fentiek szerint, az alábbi ábrán mutathatjuk be, miközben a szervezet egy környezetben létezik (például jogi, piaci, társadalmi, természeti stb.), amely befolyással van rá, és amely első sorban a nemzeti kultúra része.




A fentiekben kifejtettek alapján, az ábrán feltüntetett két szubkultúrán kívül, szervezetenként eltérően, a küldetésük és a vezetés, valamint az alkalmazottak adottságai függvényében, funkcionális vagy szervezeti okokból más szubkultúrák is létrejöhetnek, fennállhatnak. A biztonsági kultúra szempontjából meghatározó e szubkultúrák megítélésében, a szükséges teendők meghatározásában e kultúrák támogató, ellentétes, vagy semleges viszonya a vezetéshez, a szervezeti célokhoz.

## *3.4. A SZERVEZETI BIZTONSÁG*

A szervezet küldetését, üzleti célját akkor tudja megvalósítani, ha az üzleti folyamatok és az azt kiszolgáló folyamatok, illetve az alaptevékenysége és az irányítási tevékenysége zavartalanul, rendeltetésszerűen valósul meg. Azaz a szervezet erőforrásai bizalmasságának, sértetlenségének és rendelkezésre állásának fenyegetettsége minimális, a szervezet biztonsága zavartalan.

*A szervezet biztonsága a szervezet kedvező állapota, amelynek megváltozása nem valószínű, de nem is kizárt.*

A szervezet biztonsága mindezek alapján csak akkor biztosítható, ha az erre irányuló intézkedések, integráltan, egységes irányítás mellett kerülnek kialakításra, végrehajtásra [21]. Ebből egyértelműen következik,

hogy a biztonsági kultúrát is a szervezet egészére (a vagyon-, termelési-, és informatikai biztonságra egyaránt) kell értelmezni.

# *4. A BIZTONSÁGI KULTÚRA*

A biztonsági kultúra meghatározása előtt idézni kell az EU Bizottság következő Közleményét, amely alapvetően politikai állásfoglalás, és amely nem a szervezetek biztonsági kultúrájára, hanem az EU biztonsági kultúrájára vonatkozik. Ugyanakkor figyelembe vétele indokolt, mert mint annyi sok nemzeti védelmi, biztonsági megoldásnak, ennek hatása is várhatóan megjelenik a kereskedelmi, és privát szférában követelményként, illetve felhasználható védelmi eszközként.

- Az EU Bizottság 2004-ben kiadott Közleménye szerint [3]:
  - Európának be kell ruháznia a „biztonsági kultúrába”, amely a kombinált, és relatíve ki nem használt erősségű biztonsági ipart, és kutatást, a jelen, és jövő biztonsági kihívásai alapján, a hatékonyság, és az innovativitás irányába tereli.
  - A közlemény, a kihívásokból kiindulva, a következő három célt állítja az Unió elé:
    1. a fenyegetések kezelése, mint terrorizmus, a fegyveres tömeg demonstrációk terjedése, a tönkrement államok, regionális konfliktusok és a szervezett bűnözés;
    2. biztonság kialakítása szomszédinknál;
    3. nemzetközi együttműködés kialakítása a fenyegetésekkel szemben.

## *4.1. A BIZTONSÁGI KULTÚRA FOGALMA*

Ezek után **a biztonsági kultúra** az, amikor az emberek tudják jogaikat, kötelezettségeiket, és ami a legfontosabb, érvényesítik azokat, és akik egy biztonsági kultúrához tartoznak, tudják, mi kompromittálja a biztonságot, és oktatják, elmarasztalják azokat az embereket, akik tudatlanságból, feledékenységből vagy személyes gyengeségből nem biztonságos magatartást tanúsítanak [17].

A biztonsági kultúra egy funkcionális alapon kialakuló szubkultúra. Minden alkalmazottnak van meghatározott szintű felelőssége, szerepe a szervezeten belül. Ezen kívül a szervezetbe érkezésekor mindenki hoz

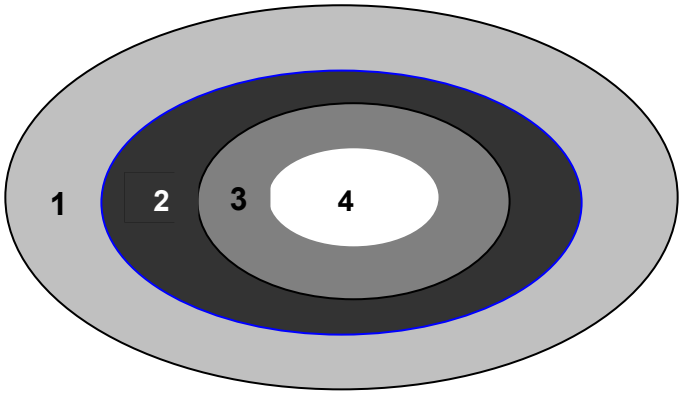
magával gondolkodásmódot, viselkedés- és magatartásjegyeket, többek között a biztonsággal kapcsolatban, amelyeknek azonosulniuk kell a szervezet kultúrájával, biztonsági kultúrájával.

A biztonsági kultúrát ki kell alakítani nem csak az alkalmazottak és az időszakos alkalmazottak, szerződéssel munkát vállalók körében, hanem a szervezettel foglalkozó, tevékenységében résztvevő harmadik felek munkatársaiban is. A biztonság tudatosan egy kultúrává válik, ha a szervezet, mint egész, a biztonság megsértését szociálisan és erkölcsileg a szervezetben elfogadhatatlannak tartja, és a biztonság, pedig átfogja, a szervezetet, és mindenhol és mindenkinek része van a biztonságért való felelősségben (egyenszilárdság elve, humán vonatkozásban), amelyet a szervezet számon is kér tőle. Alá kell húzni, hogy az emberi tényező (erőforrás) a biztonság szempontjából a leggyengébb, a legkritikusabb tényező, amelyet feltétlenül a biztonsági kultúra vizsgálatánál, kialakításánál, fenntartásánál szem előtt kell tartani. Egy szervezetben a végbemenő folyamatokat és tevékenységeket bárki végzi, annak van szerepe és felelőssége a hatékonyságért és az eredményességért, amelynek számon kérhetőnek kell lennie [1].

A biztonsági kultúra alkotó eleme, hogy a humán erőforrások biztonsági ismereteinek részét képezik az alábbiak [27]:

- a biztonsági kultúra központi elve, hogy az emberek nem automatikusan érdekeltek abban, hogy érzékeny információkat nem szükséges tudniuk;
- a biztonsági kultúra az etikett egy formája, egy út a fölösleges félreértések és a lehetséges konfliktusok elkerülésére;
- a kockázatok csökkentésével a biztonsági kultúra nem intézményesített gyanakvás, hanem az egészségtelen gyanakvás elkerülése;
- a biztonsági kultúra tartalmazza a hallgatás szabályait, de nem a némaság szabályait.

A biztonsági kultúra vizsgálatánál figyelembe kell venni a kultúrák egymásra hatását, egymásba ágyazódásukat, amelyet BAKACSI [26] a következőképen mutat be:




**1**=nemezetközi befolyás.
**2**= nemzeti,
**3**= szervezeti, és
**4**= biztonsági kultúra

## *4.2. A BIZTONSÁGI KULTÚRA ELEMEI*

A biztonsági kultúra elemei a szervezeti kultúra elemeinek részét képezik, kiegészítik azokat. A biztonsági kultúra elemei a Mc Kinsey 7S modellje alapján tehát:

⇒ **kemény elemek:** a biztonságirányítás struktúrája**,** és módszerei, a biztonsági stratégia, a biztonsági alrendszerek (vagyon, üzem és informatikai biztonsági alrendszer),

⇒ **lágy elemek:** a biztonsági tudatosság színvonala a szervezet és az egyének szintjén, az alkalmazottak elkötelezettsége, képzettsége, biztonsági szakképzettsége és biztonsági ismeretei, a biztonsági értékrend, a környezet.

Szükséges, különösen biztonsági szempontból, a lágy elemek közé **a környezetet (**pl. társadalmi, jogi, piaci, természeti**)** is felvenni. Ezt alátámasztja Bakacsi előadása is [26].

A kemény és a lágy elemek egyaránt arra utalnak, hogy a biztonsági kultúráról a szervezet, a vállalat és az egyének szintjén beszélhetünk. A szervezeti kultúrával kapcsolatban, a fentiekben azt állapítottuk meg, hogy „a szervezeti kultúra a szervezet közös gondolkodása, amelyet a szervezet közös problémáinak megoldása során tanul meg.” A biztonsággal összefüggő problémák megoldása a szervezet ilyen közös problémája. Ebből következik, hogy a biztonsági kultúráról is a szervezet és az egyének szintjén beszélhetünk. A [20] azzal foglalkozik, hogy a fizikai és logikai biztonság integrálása a szervezeti biztonság-menedzsment egyik nagy kihívása, amelynek fel nem ismerése veszélyforrást képez.

# 5. A BIZTONSÁGI TUDATOSSÁG

## 5.1. A BIZTONSÁGI TUDATOSSÁG FOGALMA

**A tudatosság meghatározott** kérdésben a kérdés ismerete, tekintetbe vétele, az azzal történő törődés, és az annak megfelelő cselekvés.

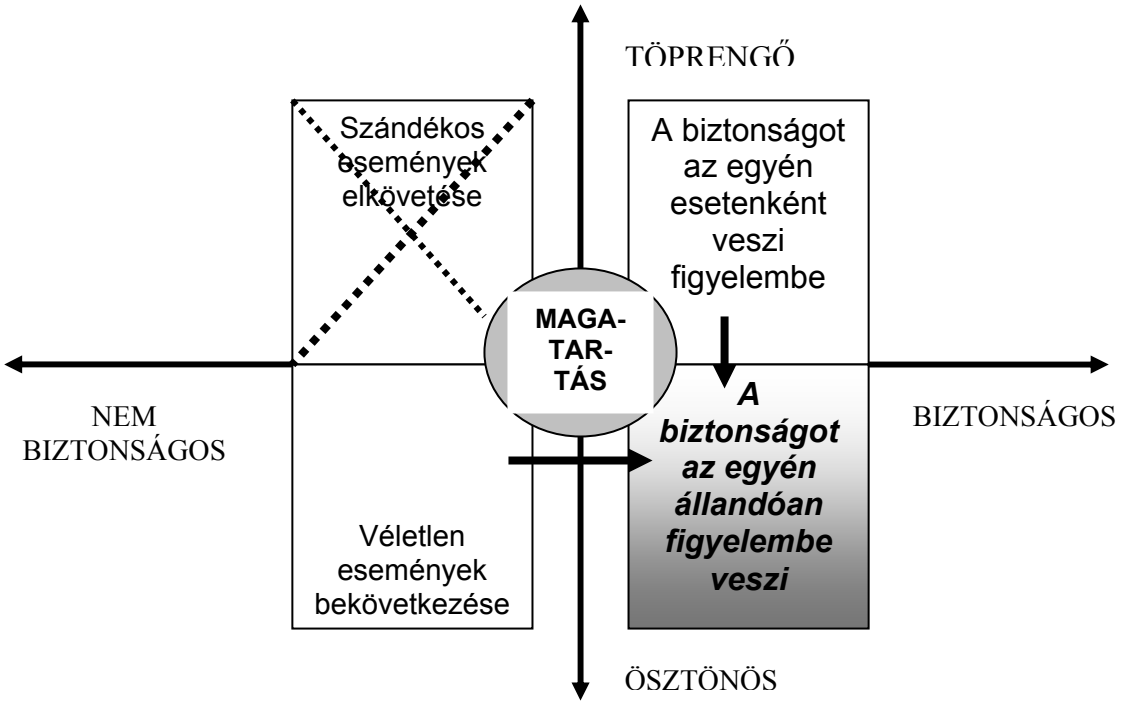
**A biztonsági tudatosság** a szervezet biztonsági szintjének, mint követelménynek, elfogadása és esetleges hiánya következményeinek elismerése, valamint a felelősség vállalása a szervezet biztonságáért a biztonsági szempontból erkölcsös, etikus magatartás kultúra alapján, azaz annak felismerése, hogy

- a biztonsági követelmények elfogadása a veszélyérzeten alapul, és egyaránt vonatkozik a biztonsági intézkedéseknek, elvárásoknak való megfelelősségére, valamint a biztonsági események kezelésére;
- a veszélyérzet hiányának hatása a következmények biztonsági kockázatának fel nem ismerését eredményezi, amely az üzleti cél és a rendeltetésszerű üzletmenet sérüléséhez vezethet.

A szervezet tagjainál, az egyéneknél a biztonsági tudatosság elérése, fenntartása a cél, amely [1] alapján a biztonsági tudatosság összefüggései a következő oldalon elhelyezett ábrán mutathatók be.

A biztonsági tudatosság ösztönös, biztonságos magatartást eredményez a töprengő, nem biztonságos helyett, és minimalizálja a szándékos biztonsági események elkövetésének valószínűségét, de nem zárja ki a véletlen biztonsági eseményeknek a bekövetkezését.

K. Rudolph, CISSP írja [4]: Egy személy, aki tudatában van a veszély jeleinek (felismeri azokat), az úgy tud működni, mint a szervezet érzékeny jelző készüléke. Azoknak az eseményeknek a felismerése, amelyek biztonsági eseménnyé válhatnak, ösztönösen kell történnie. A biztonsági tudatosság ezt a képességet alakíthatja ki.




A legjobb gyakorlat szabványa [9] azt mondja a számítástechnikát üzemeltetők és felhasználók legyenek *tudatában* a következőknek:

- az informatikai biztonság jelentőségének (az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelmével kapcsolatban);
- miért van szükség az informatikai biztonságra az installáció védelméhez;
- az informatikai biztonságpolitika és az alkalmazott szabványok/folyamatok teljesítésének fontosságának;
- az informatikai biztonsággal kapcsolatos személyes felelősségüknek.

Hinson [13]. az informatikai biztonsági tudatosság növelésére a következőket ajánlja:

- a biztonsági tudatosságnak, gyakorlatnak és képzésnek a menedzsment ellenőrzése mellett megkülönböztetett helyzetet kell biztosítani;
- gondoskodni kell a vezetési és mérési kerettevékenységekről, a közlési technikák és eszközök választékáról;
- támogatni kell a fegyelmező és jogi akciókat azokkal szemben, akik nem tesznek eleget az informatikai biztonsági kötelességeiknek;
- fejleszteni kell az informatikai biztonsági ellenőrzés alkalmazásának megfelelősségét, hatékonyságát;

- teljesíteni kell a szervezet biztonsági tudatossággal kapcsolatos jogszabályi kötelezettségeit (pl. SOX).

## *5.2. NÉHÁNY PÉLDA A BIZTONSÁGOT SÉRTŐ MAGATARTÁSOKRA*

Az alkalmazottak között lehetnek olyanok, akiknek személyiségjegyei hajlamossá teszik őket a biztonsági követelmények be nem tartására, a biztonság megsértésére, továbbá nem elkötelezettek a szervezet iránt. A biztonsági kultúra, és a biztonsági tudatosság programjának törekedni kell arra, hogy a szóban forgó alkalmazottaknál ellensúlyozza ezeket a tulajdonságokat, érje el magatartásuk megváltoztatását. A [17] alapján néhány példa a biztonságsértő magatartásra:

- *hazudozó* - másokat befolyásol illegális tevékenységre;
- *pletykálkodó* - gyenge jelleműek azt gondolják, hogy így szerezhetnek speciális információkat;
- *kérkedő* - az illegális tevékenységével kérkedő másoknak rossz példát szolgáltathat.
- *indirekt kérkedő* - aki „ki, ha én nem” alapon egy nagy illegális akciót valósít meg, ahol névtelenül a háttérben akar maradni, és reméli, hogy szükség esetén ki tudja menteni magát.

A biztonsági tudatosságnál el kell érni, hogy a felhasználók számon kérhetőek legyenek tevékenységükről, elismerjék, hogy elolvasták, megértették és elfogadták a magatartás szabályait.

A NIST Special Publication 800 -100, amely 2006. júniusában jelent meg [22], jó példákat hoz arra, hogy hol kell a felhasználó magatartását szabályozni. Az alábbiakban megadott szabályozási előírások igen biztonság kritikus tevékenységekre vonatkoznak. Éspedig:

- felelősség a működő rendszer használatáért és a felhasználói magatartásért,
- megfelelő összekapcsolási korlátozások,
- a szerviz ellátás és a helyreállítás priorításai,
- a szabályoknak nem megfelelő magatartás következményei,
- továbbá a szabályozások tartalmazzák a következő témákat:
  - otthoni munka,
  - dial-in hozzáférés,
  - internet csatlakozás,
  - szerzői joggal védett munka használata,

- a rendszer jogosultságok és az egyéni számonkérhetőség
- jelszóhasználat,
- keresés adatbázisban és információk kifecsegése.

## *5.3. A BIZTONSÁGI KULTÚRA ÉS A BIZTONSÁGI TUDATOSSÁG VISZONYA*

A biztonsági tudatosság a biztonsági kultúra előfeltétele, valamint alakítója. A biztonsági kultúra a vezetés, és a munkatársak viszonya biztonsághoz, míg a biztonsági tudatosság a biztonsági kultúra egyik lágy eleme, amely lényegesen hozzá járulhat a biztonsági kultúra kialakításához, fenntartáshoz. A biztonsági kultúra csak tudatos magatartás eredménye lehet, amikor a szervezetben az egyéneknek a biztonságos magatartás ösztönös magatartás jegye.

A biztonsági kultúra tehát bővebb tartalmú, mint a biztonsági tudatosság.

# *6. A BIZTONSÁGI KULTÚRA ÉRTÉKELÉSE*

## *6.1. A BIZTONSÁGI KULTÚRA MEGJELENÉSI FORMÁI*

A biztonsági kultúra mutatói, megjelenési formái [2] alapján a következők (amelyek az értékelés alapját szolgálhatják):

- *szimbólumok:* biztonsági szaktekintélyek, biztonsági szerepek és felelősségek allokációja, a biztonság események gyakorisága, biztonság szükségességének elfogadottsága a gyakorlatban, biztonsági elvárások és tabuk.
- *nyelvezet:* biztonsági zsargon (nyelvezet), gesztusok, humán kommunikáció,
- *történetek:* biztonsági események,
- *szokások:* a rendszeres biztonsági szokások (értekezletek, képzések).

.

## *6.2. NÉHÁNY ELLENŐRZÉSI SZEMPONT*

- A menedzsment biztonság iránti elkötelezettsége megfelel-e a szervezet biztonsági stratégiájának, annak meghatározó eleme-e?

- A szervezet üzleti céljának, küldetésének megvalósítására vonatkozó stratégia követelményként menedzseli-e az elérendő biztonsági szintnek megfelelő színvonalú biztonsági kultúrát?
- A védelmi intézkedések között szerepel-e a biztonsági kultúra megteremtése, fenntartása, ellenőrzése céljára szolgáló folyamatos és hatékony Biztonsági Kultúra Program?
- A biztonsági kultúra a szervezetben egyenszilárdságú-e?
- A Biztonság Kultúra Program minden megjelenési formát figyelembe vesz-e?
- Van-e rendszeresen ismétlődő biztonsági kultúra és biztonsági tudatossági kampány, oktatás?
- Világosan meg vannak-e határozva a tulajdonosok és a felelősségek (szerepek)?
- Az üzleti kockázatok milyen súllyal szerepelnek a biztonsági kultúrában?
- A biztonsági események, biztonsági audit értékelése után intézkednek-e?
- Van-e menedzser szintű munkakör (koordinátor) a biztonsági kultúrára, biztonsági tudatosságra?
- A biztonsági tudatossági kampány oktatás magába foglalja-e átfogóan a védelmi intézkedéseket?
- Az ellenőrzési kultúra szintje megfelelő-e?
- Van-e a biztonsági kultúra vonatkozásában folyamatos, az üzleti célokat, követelményeket követő változás menedzsment?

A lehetséges válaszok (pl. igen, nem megfelelő, nem) veszélyforrásokra mutathatnak, amelyek természetesen csökkentendő kockázatokat képezhetnek.

A veszélyforrások között kell megemlíteni a kiszervezés (outsourcing) esetén, a kiszervező szervezet, és kiszervezést vállaló szervezet biztonsági kultúrája közötti eltérést. Természetesen ez nem zárjaki a kiszervezést, hanem kihangsúlyozza e probléma kezelésének fontosságát.

## *6.3. A BIZTONSÁGI KULTÚRA SZERVEZETI SZÍNTŰ ÉRTÉKELÉSI MODELLJE*

A COBIT érettségi modellt felhasználva, egy szervezet biztonsági kultúrájának színvonalát a következő értékelési modellel (amely önvizsgálatra is alkalmazható) mérhetjük meg, A biztonsági kultúra

mérésére, egy tudatos program keretében, sikerességének meghatározása végett van szükség. A mérés a biztonsági auditálás, a biztonsági helyzetkép feltárásának eszköze, amely az auditálás eredményeként jelenhet meg az auditori, illetve évente esedékes belső ellenőrzési jelentésben. A biztonsági kultúra színvonalának összhangban kell lennie a vezetés által meghatározott biztonság erősségi szinttel.

Az érettségi modell:

| Ssz. | SZÍNVONAL | A SZÍNVONAL JELLEMZŐI |
|---|---|---|
| 0 | Nem létező | Teljesen hiányzik |
| 1 | kezdeti/ad hoc | A szervezet felismerte a biztonsági kultúra fontosságát, de megteremtése nem szabályozott, nem tudatos. |
| 2 | Ismétlődhet, de nem tudatos | A felismerés elvárásként jelenik meg, de nem törekszenek a megvalósítására. |
| 3 | Definiált folyamatok | Biztonsági Kultúra Program van, de a gyakorlatban gyengén valósul meg, a biztonsági kultúrát nem oktatják. |
| 4 | Menedzselt | A gyakorlatban a Program megvalósul, az egyének tudatosan vesznek részt benne, de nem átfogóan, és nem ellenőrzik. |
| 5 | Optimalizált | A biztonsági kultúra az egyének, a szervezet magatartásának jellemzője, átfogóan jelen van a szervezetben, és folyamatosan napra készen tartják, ellenőrzik. |

Az informatikai biztonság erőségének garancia szintjeit magyar szabvány adja meg, de jelenleg még akkreditált biztonságértékelési, tanúsítási szervezet hazánkban nincs. Ettől függetlenül egyes biztonság érzékeny termékek vásárlásánál, fejlesztésénél a (külföldi) minősítés megkövetelhető. Az MSZ-ISO/IEC 15408:2002. „Az informatikai biztonság értékelésének közös szempontrendszere” című szabvány (a Common Criteria, CC alapján készült szabvány fordítása), hét szintet ad meg. Ezek az Evaluation Assurance Level (Értékelési Garancia Szint), EAL 1-7.

Célszerű egy szervezet biztonsági követelményei között meghatározni az elvárt biztonsági szintet, amely egyúttal meghatározhatja a szervezet számára az elérendő, fenntartandó biztonsági kultúra szintjét is. Nyilvánvaló, hogy meghatározott erősségű biztonság csak megfelelő biztonsági kultúrával is rendelkező szervezetnél érhető el. Az egyes EAL értékek által kívánt biztonsági kultúra szintet, a fentiekben megadott értékelési modellt alkalmazva, az alábbiakban adhatjuk meg:

| MSZ-ISO/IEC15408:2002 | | Értékelési modell | |
|---|---|---|---|
| Szint | Megnevezés | Szint | Megnevezés |
| EAL1 | Funkcionálisan tesztelt | 1 | Kezdeti/ad hoc |
| EAL2 | Strukturálisan tesztelt | 2 | Nem tudatos |
| EAL3 | Módszeresen tesztelt és ellenőrzött | 3 | Definiált folyamatok |
| EAL4 | Módszeresen tervezett és ellenőrzött | 4 vagy 5 | Menedzselt vagy Optimalizált |
| EAL5 | Fél formálisan Tesztelt és ellenőrzött | 5 | Optimalizált |
| EAL6 | Fél formálisan, ellenőrzötten tervezett és tesztelt | 5 | Optimalizált |
| EAL7 | Formálisan, ellenőrzötten tervezett és tesztelt | 5 | Optimalizált |

Az üzleti, privát szféra általában az EAL 1-4 szinteket használja, míg az EAL 5 -7 szintek az állami, védelmi szervezetek követelményeit képezik.

Összefoglalva, a biztonsági kultúra szintjei tehát a fenti összehasonlítás alapján a védelem erősségének szintjeihez vannak rendelve. Ezzel az is kimondásra került, hogy a biztonsági kultúra szintjének, erősségének emelése, vagy fenntartása **védelmi intézkedés, az egyenszilárdságú biztonság alakító eleme.** Amennyiben az elvárt EAL szintnek nem felel meg a biztonsági kultúra szintje, az gyengíti a védelmet, és kockázat növelő tényező.

# *7. A BIZTONSÁGI KULTÚRA MEGTEREMTÉSE, FENNTARTÁSA*

## *7.1. A BIZTONSÁGI KULTÚRA PROGRAMJA*

A biztonsági kultúra megteremtése, és fenntartása tehát a Biztonsági Kultúra Programja szerint valósul meg, amelynek eleme a Biztonsági Tudatosság Programja is, és amely része a Biztonsági Programnak. Ez a program a biztonság sajátossága szerint nem egyszeri, hanem folyamatos tevékenységeket kell tervezzen. Ugyanis például egy biztonsági esemény ellenőrzés értékelését követően is meg kell, hogy határozza a javító intézkedések, változtatások megtételét.

A Biztonsági Program DEMING (1989-ben) PDCA (Plan, Do, Check, Act) modellje alapján készítendő, és így a Biztonsági Kultúra Program is eszerint készítendő el.

A Program főbb elemei a következők:

| A BIZTONSÁGI KULTÚRA PROGRAM FŐBB ELEMEI | | |
|---|---|---|
| 1. | A program céljai (a biztonsági tudatosság is benne szerepel) | MIT? |
| 2. | A program célterületei | HOL? |
| 3. | Tevékenységek, módszerek | HOGYAN? |
| 4. | A program értékelése | EREDMÉNY? |
| 5. | Programjavító intézkedések | TEENDŐ! |

Az egyes elemekről:

1. A program célja intézkedések a biztonsági kultúra és ezen belül a biztonsági tudatosság erősítésére, fenntartására, a top management által meghatározott biztonsági szintnek megfelelő szinten.
2. A program célterületei: a menedzserek, a biztonsággal foglalkozó alkalmazottak, a közvetlenül nem érintett alkalmazottak és a szerződéssel a szervezet számára munkát végzők (a szervezet területén, vagy a saját munkahelyükön).
3. Oktatás, workshop, kampány, szimbólumok alkalmazása.
4. Ellenőrzés, célvizsgálat (a programkészítés, végrehajtás, karbantartás ellenőrzése).
5. A vizsgálati eredmény vagy a biztonsági esemény értékelése, vagy az üzleti cél változása miatt szükségessé váló változáskezelés.

A programnak összhangban kell készülnie a biztonságpolitikával, amely az alapját képezi, és a biztonsági szervezetben kell lennie biztonsági kultúra koordinálásáért felelős munkatársnak.

## A biztonságszervezés folyamata és a biztonsági kultúra

Björck [24]-ben a biztonságszervezési (Security Management Process) folyamat egyes tevékenységei (Plan-tervezés, Do-megvalósítás, Check-ellenőrzés, Act-intézkedés) output-jait kemény és lágy output-okra ossza, ahol a lágy output-ok a biztonsági kultúrára, a biztonsági tudatosságra vonatkoznak.

| Out-Putok | BIZTONSÁGSZERVEZÉSI FOLYAMAT | | | | |
|---|---|---|---|---|---|
| | PLAN | | DO | CHECK | ACT |
| | Helyzet-feltárás, értékelés | Kidolgozás | Megvalósítás | Ellenőrzés | Intézkedés |
| **Kemény** | **kockázatok** | **SMS (ISMS)** | **alkalmazás** | **megvalósulás gyengeségei** | **SMS változtatása** |
| **Lágy** | **tudatosítás** | **Biztonsági Kultúra Program** | **a kívánt biztonsági kultúra kialakítása** | **tudatosítás** | **biztonsági kultúra fejlesztése** |

### A Biztonsági Kultúra Programjának vázlata

1. *A program célja*
2. *A program célterületei*
3. *A program (a PDCA modell alkalmazásával)*
   - Tervezés
     ⇒ feladat
     ⇒ végrehajtás [felelős (munkakör), határidő]
     ⇒ költségigény
   - Megvalósítás
     ⇒ feladat
     ⇒ végrehajtás [felelős (munkakör), határidő]
     ⇒ költségigény
   - Ellenőrzés
     ⇒ feladat (belső, külső ellenőrzés)
     ⇒ végrehajtás [felelős (munkakör), határidő]
     ⇒ költségigény
   - Intézkedés (értékelések alapján a szükséges intézkedések)
     ⇒ feladat
     ⇒ végrehajtás [felelős (munkakör), határidő]
     ⇒ költségigény
4. *A felelősök, végrehajtók jelentési kötelezettségei*

## *7.2. A BIZTONSÁGI KULTÚRA, ÉS A SIKERES BIZTONSÁGI PROGRAM*

A szervezet tagjainak, az egyéneknek az azonosulása a szervezeti kultúrával és a szervezet biztonsági kultúrájával egy véget nem érő

folyamat. Ezt a folyamatot célirányos tevékenységgel, a biztonsági kultúra vonatkozásában, a Biztonsági Kultúra Programja útján lehet és kell napra készen tartani. A Biztonsági Kultúra Program megvalósulása pedig egyik feltétele a biztonsági követelmények teljesülésének. Az ISACA anyaga [7] a sikeres biztonsági program kritikus tényezői között adja meg a következőket:

- a felső vezetés kötelezettségvállalását a biztonsági iniciatívákért,
- a biztonsági témák megértését a felső vezetés részéről, és
- a szervezet elkötelezettségét a biztonsági célokra nézve.

A kiegészítő kritikus elemek között pedig

- az erőforrások védelmének szükségességét,
- az alkalmazottak megfelelő oktatását,
- a biztonsági tudatosságot adja meg.

A Biztonsági Program kritikus siker tényezői tehát a biztonsági kultúráról is szólnak. *Ebből következik, hogy a biztonsági kultúra színvonala befolyásolja a védekezés (defenzív és proaktív) hatékonyságát is.*

## *7.3. A BIZTONSÁGI KULTÚRA ÁLLANDÓSÁGA, FEJLESZTÉSE*

A biztonsági kultúra, mint minden kultúra, annak ellenére, hogy látszólag az állandóság alapvető követelmény, nem szükségszerűen állandó. A biztonsági kultúrában változtatás okai lehetnek például:

- a biztonságon belüli okok, mint
  - a biztonsági követelmények megvalósulásának problémái,
  - a biztonsági szubkultúrák problémái (ellenséges vagy semleges jelleg),
  - a biztonsági technológia fejlesztése,
  - a támadási módszerek alapvető változása,
- a szervezeti változtatások
  - az üzleti követelmények változása miatt a biztonsági követelmények, a biztonsági stratégia változása,
  - az üzleti, termelési technológia változása, változtatása,
  - a szervezet növekedése [telephelyek létrejötte, kapcsolatok kiterjedése (bizalmas, nem bizalmas hálózatok)],
  - a szervezeti struktúra, a szervezetirányítás változásai.

A biztonsági kultúra változtatása egy folyamat, amelynek a Biztonsági Kultúra program keretében kell megvalósulnia. A 3.1 pontból idézve, amely a biztonsági kultúrára is igaz:

> "A szervezeti kultúra a szervezet közös gondolkodása, amelyet a szervezet közös problémáinak megoldása során tanul meg. A szervezeti/vállalati kultúra integrálja a szervezetet, és elősegíti a környezethez történő alkalmazkodást, amelyen elsősorban az üzleti célok, követelmények változását követő *változás menedzsmentet értjük."*

Hirtelen, drasztikus változtatás nem lehetséges, de nem is vezetne eredményre, hiszen a szervezet biztonsági kultúrája az egyének biztonsági kultúrájának összessége. A változtatás a biztonsági kultúra fejlesztése, amelyet a 7.4 pont szerinti módszerekre épülő folyamattal, programmal érhetünk el.

A szakirodalom alapján a biztonsági kultúra fejlesztése, általában négy szakaszból áll:

- a biztonsági kultúra állapotának felmérése,
- a biztonsági kultúra fejlesztésének, céljának közös munkával (workshop-okkal) történő meghatározása,
- a program kialakítása (akcióterv jelleggel),
- változtatások lépésenkénti bevezetése magatartástudományt felhasználó fejlesztési lépésekkel, módszerekkel (lásd a következő pontban).

## *7.4. BIZTONSÁGI TUDATOSSÁG FEJLESZTÉSE*

A biztonsági kultúra fejlesztésének folyamatos programjában kiemelt szerepet kell kapnia a biztonsági tudatosság növelésének, az USA Szabványügyi Hivatalának NIST vonatkozó szabvány publikációi alapján, a következők tevékenységekkel (amelyek a biztonsági kultúra fejlesztésére is mértékadóak, és együttesen is kell végrehajtani):

⇒ **Oktatással** [22]. Igen figyelemre méltó, hogy e szabvány nem általában a biztonsági tudatosság oktatásáról beszél, hanem szerep bázison határozza meg (négy szinten), hogy kiknek mit kell oktatni. Azaz „a szükséges tudás, szükséges cselekvés" elvének alkalmazása, vagy ahogy a szabvány írja „szerep alapú képzés". Felhasználva ezt az oktatási koncepciót, a négy szintet a következők szerint adjuk meg:

- **1.) Oktatás,** *biztonsági szakemberek, profik részére*:

Tárgya: a különböző funkcionális specialitások biztonsági céljainak és a kompetenciáknak közös tudás bázisba integrálása, kiegészítve a technológiai és szociális koncepciók, eredmények és elvek multidisciplináris tanulmányozásával. A biztonsági szakemberek képessé tétele az előrelátásra, a megelőző válaszokra.

- **2.) Képzés**:

  *a.) Biztonsági szerepet, felelősséget betöltők részére*
  *b.) Az üzleti és az információ rendszerben a felhasználók részére.*

  Tárgya: Integrált releváns és szükséges biztonsági tudás, jártasság, biztonsági cél elsajátítása, kompetencia fejlesztés támogatása, a munkatársak segítése a szerepük megértésében és hogy hogyan hajtsák azt végre.

- **3.) Ismertetés:** Az e*gyéb munkatársak részére.*

  Tárgya: Biztonsági ismeretek nyújtásával a tudatosság figyelem-középpontba állítása. Ez valójában nem egy oktatás, hanem egy folytonos program, amely a biztonsági üzeneteket különböző formában eljuttatja a munkatársakhoz.

Az 1., és 2. szinten szaktudás és szerep alapú biztonsági tudatosság képzés, míg a 3. szinten biztonsági ismeret alapú képzés történik.

⇒ **Eszközökkel** [23], mint kampányok, propagandaanyagok a biztonságról, a magatartás szerepéről.

⇒ **Közléssel** [23], mint biztonsági értékelések, stratégiai tervek és programok bevezetése a felhasználók, menedzserek és végrehajtók részére.

⇒ **Befolyásolással** [23], a biztonsági tudatosság legjobb gyakorlatával.

⇒ **Méréssel** [23], mint a biztonsági tudatossági program hatékonyságának a mérése.

## *7.5. A BIZTONSÁGI KULTÚRA HELYE A BIZTONSÁGSZERVEZÉSI FOLYAMATBAN*

A biztonsági kultúra hordozói a humán erőforrások. Így a biztonsági kultúra a humán biztonság része, amelyből következik, hogy azzal a biztonságszervezési folyamatban mindig a humán biztonságnál kell foglalkozni.

A biztonságszervezési folyamat, mint ismert, a veszélyforrások, fenyegetések feltárása, a kockázatok, a védelmi intézkedések, meghatározása, bevezetése, ellenőrzése. A biztonságszervezés végtermékei, dokumentumai a következők:

- A Biztonsági Program:
  - a Biztonsági Átvilágítás,
  - a Biztonsági Stratégia,
  - a Biztonsági Politika (Biztonsági Szabályzat),
  - az Üzletmenet Folytonossági Terv,
  - a Biztonság Ellenőrzése.

A biztonságszervezési folyamat egyes lépései és a végtermékek pedig a következő biztonsági struktúrával foglalkoznak:

- Szervezési biztonság:
  - adminisztratív biztonság,
  - humán biztonság **(többek között a biztonsági kultúra).**
- Technikai biztonság:
  - fizikai biztonság,
  - logikai biztonság.

# 8. MELLÉKLETEK

## 8.1. NÉHÁNY HASZNÁLT KIFEJEZÉS ÉRTELMEZÉSE

Az ajánlásban szereplő alábbi kifejezéseket a következőképen értelmezzük:

- **biztonság** valakinek vagy valaminek kedvező állapota, minimális fenyegetettsége, amely megváltozásának minimális a valószínűsége, de nem kizárt**,**
- **egészség** az életműködés zavartalan, betegségmentes, állapota,
- **életmód** az a magatartásforma, ahogy valaki szellemi, anyagi, illetve erkölcsi vonatkozásban él, és tevékenykedik,
- **erkölcs** egyéneknek vagy csoportoknak a magatartását irányító és annak megítélését segítő, társadalmilag helyesnek tekintett szabályok, követelmények összessége,
- **etika** az erkölcs filozófia-elméleti alapjaival foglalkozó tudományág,
- **etikai értékek** az erkölcsön alapuló magatartás jegyek,
- **magánélet** valaki életének a hivatalos elfoglaltságán kívüli része,
- **magatartás** egyéneknek vagy csoportoknak a környezettel, az élet, a társadalom jelenségeivel szembeni állásfoglalási módja,
- **rendszer** egymással kölcsönhatásban lévő elemek halmaza**,**
- **szervezet** több, valamilyen közös feladat megoldásán rendszeresen és szabályozott módon dolgozó ember együttese,
- **vállalat** közvetlen gazdasági tevékenységet végző, jogilag önálló szervezet**,**
- **viselkedés** az a mód, ahogy valaki vagy valami valamilyen magatartást tanúsít.

## *8.2. FELHASZNÁLT IRODALOM*

[1] Security Awareness. ISACA. 2005.

[2] Heidrich Balázs: Szervezeti kultúra és interkultúrális menedzsment. Human Telex Consulting Kft. 2001.

[3] On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security research. EU Commission. Commission Communication. 2004.

[4] K. Rudolph, CISSP. Computer Security Handbook. Chapter. 29. Security Awareness. 2001. www.nativeintelligence.com.

[5] Carter McNamara: Organizational culture.2006.

www.managementhelp.org

[6] Bodor Márton: Erős szervezeti kultúra titka. IQ Consulting Szervezetfejlesztő, és tanácsadó Kft. 2003.

[7] Critical Elements of Information Security Program Success. ISACA. 2005.

[8] A. Targovski, T. Rienzo: Enterprise Information Infrastructure Paradox Associates,Inc. 2004.

[9] Information Security Forum: Good Practice of Information Security. 2.1. 2005.

[10] Control Objectives for Information and Related Technology. IT Governance Institute. 2000.

[11] COBIT 4. IT Governance Institute. 2005.

[12] B. Buchowicz: Cultural Transition and Attitudes Change. Journal of General Management.1990/4.

[13] Dr. G. Hinson: The value of information security awareness". www.NoticeBored.com. 2005.

[14] Pascale,A. and Whipp, R. : Managing Change for Competitive Success.Blackwell.1991.

[15] Bodor Márton: Az erős szervezeti kultúra titka. IQ Consulting. 2003.

www.iqconsulting.hu

[16] G. Hofsted: Cultures and Organizations- Software in the Mind. McGraw-Hill Book Co. 1991.

[17] Security Culture. IMF/World Bank. 2001.

http://mlcastle.net/raisethefist/security.html

[18] Framework for Internal Control Systems in Banking Organisations. Basle Committee on Banking Supervision. 1998.

[19] W.E.Schneider: Why Good Management Ideas Fail – The Neglected Power of Organizational culture. The CEO Refresher Archives. 2002.

[20] Enabling Comprehensive Security Management. Open Security Exchange. www.opensecurityexchange.org

[21] Booz, Allen, Hamilton: Convergence of Enterprise Security Organizations. ASIS, ISACA, ISSA. 2005.

[22] NIST Special Publication 800-100. Information Security Handbook: a Giude for Managers. 2006.

[23] Information Security Handbook: a Guide for Managers. NIST Special Publication 800-100. 2006.

[24] Björck: Security Scandinavian Style. Stockholm University. 2001.

[25] NIST SPECIAL PUBLICATION 800-50. Building an Information Security Awareness and Training Program.

[26] Bakacsi Gy.: Minőség és biztonsági kultúra. BME. Ergonómiai Tanszék.

[27] Security culture. Guerilla news network. 2005.

[28] Ladó László: Szervezéselmélet és módszertan. Közgazdasági és jogi könyvkiadó. 1979.