HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

**Munk Sándor**
munk.sandor@zmne.hu

# A BIZTONSÁG KÉRDÉSEINEK DEKOMPOZÍCIÓJA

***Absztrakt***

*Napjainkban szinte minden alkalmazási területen általánosan elfogadottá vált a biztonság komplex megközelítésének igénye, a fenyegetések és a védelmi megoldások, intézkedések jellegüktől független, teljes körű vizsgálata. A komplex megközelítés szempontjából elvileg felmerülhet a speciális biztonsági szakterületek feleslegessége, vagy jelentőségük csökkenése, amit azonban a gyakorlati tapasztalatok nem igazolnak. A komplex megközelítésre épülő módszertanok és a részterületi dokumentumok, módszerek általában nem kapcsolódnak egymáshoz. Jelen publikáció célul tűzte ki a biztonság komplex megközelítéséhez kapcsolódó kérdések szakterületekre történő lebontása alapjainak vizsgálatát. Ennek érdekében: összegzi az összetett objektumok biztonságának alapvető kérdéseit; elemzi a biztonság kérdései dekompozíciójának alapjait; végül részletesebben vizsgálja a fenyegetések, sebezhetőségek, illetve a védelmi intézkedések dekompozíciójának lehetőségeit, szükségességét.*

*In our days complex approach of security, comprehensive analysis of threats and security controls, independent of their nature, became generally accepted on almost every application areas. From the point of view of the complex approach it would be possible that specialized security areas may become unnecessary, and their importance may decrease, but this is not justified by practical experiences. Complex approach based methodologies, and component area documents, methods usually not related. Recent publication aims at studying the basics of breakdown of questions related to complex approach of security into specialized security areas. For this purpose: summarizes the basics questions of security of complex objects; analyses the basics of security questions' decomposition; finally in greater detail examines possibilities, and necessity of decomposition of threats, vulnerabilities, and security controls.*

***Kulcsszavak**: biztonság, informatikai biztonság, kockázatmenedzsment, sebezhetőség, dekompozíció ~ security, information (IT) security, risk management, vulnerability, decomposition*

## BEVEZETÉS

Napjainkra a biztonság értelmezése gyakorlatilag minden alkalmazási területen – legyen az a politika, a kritikus infrastruktúrák, a katonai/védelmi szféra, a környezetvédelem, a gazdaság, vagy az informatikai rendszerek világa – a komplex megközelítések irányába mozdult el. A komplex megközelítés lényege leegyszerűsítve: jellegüktől függetlenül a biztonság alanyára ható valamennyi fenyegetés feltárása és a védelem összes lehetséges megoldásának, intézkedésének számbavétele, felhasználása.

A komplex megközelítés igényéhez, megjelenéséhez kapcsolódóan felvetődhet a kérdés, hogy vajon következik-e ebből a speciális – pld. szakterületi – biztonsági megközelítések feleslegessé válása, megszűnése, vagy jelentőségük csökkenése. Ez a következtetés előzetesen úgy tűnik, hogy sem logikai úton, sem gyakorlati tapasztalatok alapján nem igazolható. Az átfogó biztonság elvének elfogadása nem vonja maga után a katonai biztonság, a gazdasági biztonság, vagy a környezetbiztonság megszűnését és a komplex informatikai biztonság uralkodóvá válása sem teszi szükségtelenné, idejétmúlttá az olyan szakterületeket, mint a hálózati biztonság, az adatbázis-biztonság, a fizikai biztonság, vagy a humán biztonság.

A biztonság részterületeinek változatlan létjogosultságát, szükségességét elfogadva szükségesnek látszik megvizsgálni összefüggésrendszerüket, helyüket és szerepüket a komplex megközelítésű biztonsági elképzelésekben, módszertanokban. Ezt indokolja az is, hogy napjaink nemzetközi szabványaiban és legjobb gyakorlatokat rögzítő dokumentumaiban leírt komplex módszertanok többnyire csak átfogó jellegű feladatokat fogalmaznak meg, míg a részterületi dokumentumok és módszertanok mindmáig nem, vagy csak érintőlegesen foglalkoznak az átfogó keretekkel.

Mindezek alapján jelen publikáció célja a biztonság komplex megközelítéséhez kapcsolódó kérdések biztonsági szakterületekre történő lebontása, dekompozíciója és kapcsolatrendszerük alapjainak vizsgálata. Ennek érdekében:

- összegzi a biztonság összetett jellegének, az összetett objektumok biztonságának alapvető kérdéseit;
- elemzi a biztonság alanya és védendő tulajdonságai dekompozíciójának alapjait;
- végül részletesebben vizsgálja a fenyegetések, sebezhetőségek, illetve a védelmi intézkedések dekompozíciójának lehetőségeit, szükségességét és rendjét.

## A BIZTONSÁG ÉS ÖSSZETETTSÉGÉNEK ALAPJAI

A biztonság és egyes összetevői értelmezésének, számos más fogalomhoz hasonlóan – a közös jellemzők ellenére – nincs általánosan elfogadott változata. Ennek megfelelően a következőkben először összegezzük a publikációban felhasználásra kerülő alapvető értelmezéseket, megállapításokat, majd áttekintjük a biztonság összetett jellegének, az összetett objektumok biztonságának alapvető kérdéseit.

A továbbiakban a következő ***alapvető értelmezések*** kerülnek felhasználásra [részletesebben lásd 1]. A biztonság – általános értelemben – egy olyan állapot, amelyben valaki/valami a lehetséges fenyegető hatások ellen a kívánt mértékben védett, a védelem pedig a fenyegetések elleni, a biztonság megteremtésére és fenntartására irányuló tevékenységek, rendszabályok összessége.

A biztonság alapfogalma a biztonság alanya, a fenyegetések által veszélyeztetett objektum. A publikációban foglaltak törekszenek egy olyan általános megközelítésre, amelynek megállapításai, eredményei a biztonság kérdéseinek bármely alkalmazási területén, tetszőleges veszélyeztetett objektum esetében alkalmazhatóak, ezen belül azonban kiemelten figyelmet fordítanak az informatikai rendszerekre, mint a biztonság alanyára.

Ennek során informatikai rendszer alatt – a tágabb értelmezésnek megfelelően – eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására létrehozott rendszerét értjük. [2, 21. o.] Ez a meghatározás magában foglalja a szűkebb értelemben vett számítógépes, kommunikációs (távközlési, híradó), navigációs, információszerző (felderítő, szenzor-), vezetéstámogató, folyamatirányító, stb. rendszereket, valamint az ezek integrációjára, összeolvadására épülő, a különböző szakmai közösségekben infokommunikációs, információtechnológiai, vagy IT jelzőkkel megnevezett technikai rendszereket.

A biztonság értelmezéséhez hozzátartoznak a biztonság összetevői (aspektusai), a biztonság alanyának azon tulajdonságai, amelyeknek a megengedett mértéktől eltérő megváltozása a biztonság sérülését, megsértését jelenti. A szakirodalomban ezek általában biztonsági célkitűzések[1] megnevezéssel szerepelnek [lásd pld. 3, 7. o.; 4, E-2. o.]. Az informatikai rendszerekhez és az általuk kezelt információkhoz kapcsolódóan ezek közé elsősorban a bizalmasságot, a sértetlenséget és a rendelkezésre állást, továbbá a hitelességet, letagadhatatlanságot, számonkérhetőséget, stb. sorolják.[2]

A biztonság alapvető fogalmai közé tartoznak még a fenyegetések, a biztonság alanyát veszélyeztető, a védendő tulajdonságokat károsan, a meg nem engedett/elfogadható mértéknél jobban befolyásoló potenciálisan káros [kölcsön]hatások. A sebezhetőségek a biztonság alanyának – illetve tágabb értelemben a biztonság fenntartására irányuló tevékenység- és eszközrendszernek – olyan tulajdonságai (biztonsági szempontból hiányosságai, gyengeségei), amelyek lehetőséget teremtenek a fenyegetést megvalósító kölcsönhatások érvényesülésére. Végül a veszélyforrások azok az objektumok, amelyek a biztonság alanyát veszélyeztető hatást közvetlenül, vagy közvetve (áttételesen) kiváltják, vagy a veszélyeztető kölcsönhatásokban érintettek.[3]

Egy adott objektum vonatkozásában joggal állítható, hogy ***a biztonság összetett fogalom***. Összetett egyrészt abból a szempontból, hogy az objektum biztonsága különböző megőrzendő tulajdonságokkal írható le, illetve a biztonságot különböző jellegű, sokszor egymástól teljesen független fenyegetések veszélyeztetik. Ezek egymással sok esetben szoros kapcsolatban állnak, meghatározott védendő tulajdonságokat meghatározott fenyegetések veszélyeztetnek.

Egy nemzet, egy állam biztonságát különböző fenyegetések, kockázatok és kihívások veszélyeztetik. A Magyar Köztársaság Nemzeti Katonai Stratégiája szerint "A Magyar Köztársaság kormánya a biztonságot átfogó módon értelmezi, amely a politikai és katonai tényezőkön túl magában foglalja annak gazdasági, pénzügyi, energiaellátási, rendvédelmi, emberi jogi és kisebbségi, információs és technológiai, környezeti, demográfiai és civilizációs, közegészségügyi, valamint nemzetközi jogi dimenzióit is.". [5, 6. o.] Hasonlóképpen különböző fenyegetések veszélyeztetnek kritikus infrastruktúrákat, kritikus információs infrastruktúrákat,

[1] Security objective, security goal.
[2] Confidentiality, integrity, availability, authenticity, non-repudiation, accountability.
[3] Threat, vulnerability, threat source.

illetve informatikai rendszereket is. A fenyegetések érkezhetnek a természeti, a technikai és az információs környezetből, hatásmechanizmusukat illetően lehetnek fizikai, információs, vagy pszichológiai jellegűek.

A fentiek alapján a komplex biztonság felbontható különböző részterületekre, amelyek egy meghatározott védendő tulajdonságra, vagy ezek összetartozó körére, illetve az ezeket veszélyeztető fenyegetésekre összpontosítanak, korlátozódnak. Ennek megfelelően beszélhetünk a bevezetőben már említett katonai biztonságról, gazdasági biztonságról, környezeti biztonságról, stb., vagy hálózati biztonságról, adatbiztonságról, fizikai biztonságról, humán biztonságról. A biztonság részterületekre bontásához kapcsolódóan azonban nyilvánvaló, hogy a komplex biztonság nem egyszerűen az egyes részterületek szummatív összegzése, egyre jelentősebb szerepet játszik a közöttük fennálló összefüggésrendszer: az egymásra épülés, a kölcsönös függőség (az interdependencia) kérdésköre, ami napjaink egyik jelentős vizsgálati területe.

A biztonság összetettnek tekinthető abból a szempontból is, hogy az objektumok általában maguk is összetettek, így a teljes objektum biztonsága többek között összetevői biztonságára épül. Az objektum adott követelményekkel meghatározott biztonságához szükség van arra, hogy az egyes összetevői is megfeleljenek meghatározott – az átfogó követelményekből levezethető – biztonsági követelményeknek. Emellett persze egy adott objektum biztonsága függhet olyan más – általa felhasznált, vagy vele együttműködő – objektumok biztonságától is, amelyek nem képezik részét, amelyek felett nincs rendelkezési joga. Összetett objektumok esetében a biztonsághoz kapcsolódó elemek (fenyegetések, sebezhetőségek, védelmi tevékenységek) nem kezelhetőek kizárólag az adott objektum szintjén, elemzésük, megvalósításuk végeredményben csak a konkrét összetevőkre lebontva, illetve ezekből összeállítva lehetséges.

A biztonság vizsgálatának, kialakításának és fenntartásának alapvető eszköze a ***kockázat-menedzsment***. A kockázat-menedzsment alapfogalma – a szintén különböző módokon értelmezett – kockázat. Ehhez kapcsolódóan a következőkben a jövőbeni esemény következményeihez rendelt érték-központú megközelítést használjuk, amelynek megfelelően a kockázat egy adott sebezhetőséget kihasználó fenyegetés bekövetkezésének valószínűségére, illetve az ennek következtében jelentkező biztonságsértés "értékére" (súlyosságára, kár-mértékére) épül. A kockázat-menedzsment alapvető összetevőinek a kockázat-értékelést és a kockázat-kezelést[4] tekintjük.

A biztonság kérdéseinek dekompozíciója alatt egy összetett objektum biztonsági kérdéseinek összetevői biztonsági kérdéseire történő lebontását, illetve az ezek között fennálló összefüggések meghatározását értjük. Ezen belül viszonylag önállóan vizsgálható a biztonság alanyának és a védendő tulajdonságoknak, a sebezhetőségeknek és a fenyegetéseknek, valamint a védelmi intézkedéseknek a dekompozíciója.

## A BIZTONSÁG ALANYÁNAK ÉS VÉDENDŐ TULAJDONSÁGAINAK DEKOMPOZÍCIÓJA

A ***biztonság alanyának összetevőkre bontása*** általánosságban különböző kritériumoknak megfelelően is lehetséges. Ilyenek lehetnek többek között: a funkcionális kritériumok; a ren-

[4] Risk assessment, risk mitigation

delkezési jog, működtetési felelősség kritériumai; a térbeli (földrajzi) kritériumok; esetleg műszaki-technikai kritériumok. Bármelyik felbontás esetén meg lehet, meg kell határozni az adott objektum összetevőinek körét és ezek egymás közötti – a vizsgálat szempontjából érdeklődésre számot tartó – kapcsolatrendszerét. A felbontás során olyan összetevőket célszerű meghatározni, amelyek biztonsági szempontból viszonylagosan "homogének": hasonló fenyegetettségeknek vannak kitéve, hasonló sebezhetőségekkel rendelkez(het)nek, hasonló védelmi tevékenységeket, intézkedéseket igényelnek.

***Informatikai rendszerek, hálózatok biztonsági szempontból történő részekre tagolása*** a gyakorlatban általában két szempont alapján történik. Magasabb szinten a részekre tagolás alapja az azonos helyszín és az azonos informatikai biztonsági politika, amely szerint egy összetett informatikai rendszer, biztonsági tartományokra, úgynevezett enklávékra bomlik. Az enklávé "(helyi informatikai környezet) a teljes fizikai és szervezeti környezet, beleértve a végberendezéseket és kommunikációs rendszereket (kapcsoló eszközöket), amelyek egyetlen felelős irányítása és egy közös, egységes biztonsági politika hatálya alatt állnak." [6, 4. o.]

Az egyes tartományok további összetevőkre bontása az informatikai rendszerek általános technikai architektúrális elveinek megfelelően történhet. Ennek megfelelően a felbontás első szinten hálózati infrastruktúrára és a végberendezésekre, ez utóbbiak esetében pedig kiszolgáló eszközökre és munkaállomásokra lehetséges. A végberendezések esetében további felbontás lehetséges hardver platformra, szoftver platformra (operációs rendszerre és környezetére), alkalmazói rendszerekre (szoftverekre), valamint adatbázisokra.

A ***biztonság összetevői, a védendő tulajdonságok dekompozíciója*** az összetett objektum, valamint összetevői megőrzendő, védendő tulajdonságainak és az ezek között fennálló kapcsolatrendszer meghatározását jelenti. Ennek során először azt kell meghatározni, hogy az összetevők mely tulajdonságainak megléte szükséges ahhoz, hogy az összetett objektum védendő tulajdonságai a kívánt mértékben fenntarthatóak legyenek. Ugyanez ellenkező oldalról megközelítve azt vizsgálja, hogy az összetevők mely tulajdonságainak, milyen mértékű megsértése eredményezi az összetett objektum megőrzendő tulajdonságának sérülését. Informatikai rendszerek esetében például feltehető az a kérdés, hogy a rendszer rendelkezésre állásának meglétéhez az egyes összetevők – hálózati infrastruktúra, hardver összetevők, alapszoftver platform, alkalmazói szoftverek, adatbázisok, működtető állomány, elhelyezési környezet, stb. – milyen tulajdonságainak fennállása szükséges.

A védendő tulajdonságok dekompozíciója elméletileg lehet homogén és heterogén. Homogén esetben az összetett objektum adott tulajdonsága kizárólag az összetevők azonos, vagy lényegében azonos tulajdonságai fennállásának függvénye. Ez a függőség kiterjedhet valamennyi összetevőre, vagy csak azok egy részére. Ez utóbbi esetben az összetevők között megkülönböztethetőek a tulajdonság szempontjából 'lényegesek' ('kritikusak') és 'lényegtelenek'. Heterogén összefüggés esetében az összetett objektum adott tulajdonsága az összetevők azonos tulajdonságai mellett más tulajdonságaiknak is függvénye. Informatikai rendszerek esetében példa lehet erre egy rendszer sértetlensége, amely egy összetevő bizalmasságának (csak jogosultak számára történő elérhetőségének) megsértése esetén veszélyeztetetté válik.

Mivel a védendő tulajdonságok szorosan kapcsolódnak az adott objektummal szemben támasztott biztonsági követelményekhez (amelyek lényegében bizonyos tulajdonságok fennállását, vagy ezen tulajdonságok meghatározott értéktartományba esését írják elő), a védendő tulajdonságok dekompozíciója a gyakorlatban az egyes összetevőkkel szemben támasztott biztonsági követelmények és az ezekben szereplő tulajdonságok meghatározását, 'levezetését'

jelentik. Az összetett objektum és az összetevők védendő tulajdonságai közötti kapcsolat nem mindig, sőt sok esetben nem közvetlen. Ebből következően az összetevők védendő tulajdonságainak meghatározása is egy iteratív, az összetevők közötti kapcsolatokat is figyelembe vevő folyamat kell legyen, amely már átvezet a sebezhetőségek, fenyegetések következő pontban tárgyalt kérdéséhez.

A védendő tulajdonságok dekompozíciója ezen tulajdonságok meglétének – a biztonsági követelmények érvényesülésének – megítélése, vagyis ***biztonsági ellenőrzések, értékelések*** során is lényeges lehet. Általánosságban megállapítható, hogy összetett objektumok esetében számos, biztonsági szempontból lényeges tulajdonság nem önmagában, hanem összetevői tulajdonságain keresztül mérhető, ítélhető meg. Egy objektum sértetlensége például nem értelmezhető, nem vizsgálható összetevői sértetlensége nélkül. De természetesen vannak olyan, elsősorban az adott objektum működéséhez, az általa nyújtott szolgáltatásokhoz kapcsolódó tulajdonságok is, amelyek megléte, értéke, vagy szintje az objektumot 'fekete doboznak' tekintve is megállapítható.

Az ellenőrzéshez, értékeléshez kapcsolódó kérdéskör annak meghatározása is, hogy egy összetett objektum valamely, biztonsági szempontból lényeges tulajdonságát (pld. sértetlenségét, rendelkezésre állását, stb.) mérhető, megítélhető módon milyen feltételek mellett tekintjük fennállónak, illetve milyen módon határozhatjuk meg fennállásának mértékét. Egy objektum sértetlensége például fennállhat úgy is, hogy – időlegesen – vannak sérülést szenvedett összetevői és szolgáltatásai rendelkezésre állhatnak úgy is, hogy egyes összetevői nem állnak rendelkezésre.

Az előzőekben elmondottak konkrétan is megjelennek az összetett termékek, illetve a rendszerek értékelési rendjét leíró magyar kormányzati dokumentumokban is. "Összetett termék … értékelése esetén is követelmény, hogy az egyedi komponenseket függetlenül értékeljék, mivel az összeállítás értékelése az egyedi komponens értékelések eredményeire alapoz." [7, 14 o.] "A rendszer szintű értékelés jelentős mértékben támaszkodik a rendszer komponenseire (termékekre és összetett termékekre) korábban már elvégzett értékelések eredményeire." [8, 9 o.] "A több funkciós rendszerek különböző alrendszereire eltérő biztonsági szabályzatok vonatkozhatnak. Egy ilyen rendszer ugyanazon biztonsági szabályzat alá eső részeit biztonsági tartománynak is nevezik. Minden biztonsági tartományra külön megadhatók a funkcionális és garanciális követelmények, így minden tartomány rendelkezni fog egy saját biztonsági szabályzattal, biztonsági probléma meghatározással, biztonsági célokkal, követelményekkel és specifikációkkal. Minden tartomány egyúttal a nagyobb rendszer általános szabályai, biztonsági problémái, céljai, követelményei és specifikációi körén belül működik." [8, 20 o.]

***Összességében megállapítható***, hogy a biztonság alanya, ezen belül például egy kritikus információs infrastruktúra, vagy egy informatikai rendszer különböző – sajátos alkalmazási, funkcionális, technikai és biztonsági jellemzőkkel rendelkező – összetevőkre, alrendszerekre tagolható. Összetett rendszerek biztonságának összetevői, megőrzendő tulajdonságai – mint követelmények – meghatározó szerepet játszanak összetevőik megőrzendő tulajdonságainak meghatározása során. Biztonsági ellenőrzések, értékelések során egy összetett rendszer biztonsága többnyire – bár nem kizárólagosan – összetevői biztonságának, megőrzendő tulajdonságai meglétének értékelésén keresztül mérhető, ítélhető meg. A biztonsági ellenőrzések, értékelések egy, jellemzően kisebb része megvalósítható globális módon, az összetett rendszert "fekete doboz"-nak tekintve, azonban nagyobb részt az egyes összetevőkhöz kapcsolódó biztonsági ellenőrzésekre, értékelésekre épülnek.

## A SEBEZHETŐSÉGEK, FENYEGETÉSEK DEKOMPOZÍCIÓJA

A ***sebezhetőségek dekompozíciója*** az összetett objektum sebezhetőségeinek, illetve összetevői sebezhetőségeinek, valamint a közöttük fennálló kapcsolatrendszernek a meghatározását jelenti. Összetett objektumok, például informatikai rendszerek esetében a sebezhetőségek jelentős része lebontható egyes összetevők sebezhetőségeire, vagyis olyan tulajdonságokra (hiányosságokra, gyengeségekre), amelyek már kizárólag egyetlen összetevőhöz, alkotóelemhez kapcsolódnak. A sebezhetőségek egy másik – általában kisebb – része nem, vagy nem teljes egészében vezethető vissza összetevő szintű sebezhetőségekre, hanem az összetett objektum egészéhez, vagy annak felépítéséhez kapcsolódik.

Egy adott objektum sebezhetőségeinek feltárása, számbavétele háromféleképpen is lehetséges. Az első – amennyiben ilyen létezik – az adott objektumtípus nyilvánosságra került potenciális sebezhetőségeinek elemzése és annak meghatározása, hogy a közreadott sebezhetőség az adott objektumban fennáll-e, vagy sem. A második az adott objektum tervszerű, biztonsági szempontú vizsgálata a védendő tulajdonságok (biztonsági célok) potenciális megsértésére vezető hiányosságok, gyengeségek keresésére. Végül a harmadik – és legkevésbé kívánt – lehetőség a sebezhetőségek bekövetkező biztonságsértéshez kapcsolódó felfedezése. Ez utóbbiak általában ezt követően be is kerülnek a nyilvános sebezhetőség listákba.

A gyakorlatban közreadott, rendszerezett ***sebezhetőség katalógusok*** az informatikai eszközök és rendszerek, ezen belül is elsősorban a szoftverek területén léteznek. Ide tartozik mindenekelőtt a MITRE cég által kezelt Közös Sebezhetőségek Listája (CVE)[5], amely egy korai célkitűzés [9] szerint: "egy szabványosított lista, amely:

- számba veszi és megkülönbözteti az összes ismert sebezhetőséget;
- minden sebezhetőséghez hozzárendel egy szabványos, egyedi megnevezést;
- független a sebezhetőség különböző megközelítéseitől;
- és nyilvános, minden elosztási korlátozás nélkül hozzáférhető."

A lista 2010 elején több mint 40 ezer sebezhetőséget tartalmazott.

A Közös Sebezhetőségek Listájához szorosan kapcsolódik, a sebezhetőségek körében lényegében azzal megegyezik az Egyesült Államok Nemzeti Sebezhetőségi Adatbázisa[6], amely a sebezhetőség-kezelési adatok kormányzati szintű tárháza és amelyet a Belbiztonsági Minisztérium Cyber Biztonsági Osztályának támogatása mellett a Nemzeti Szabványügyi és Technológiai Intézet (NIST) Számítógép Biztonsági Osztálya[7] kezel.

A ***sebezhetőségek tervszerű elemzésre épülő feltárása*** célszerűen az összetett objektumok (pld. informatikai rendszerek, szoftver rendszerek) fejlesztéséhez kapcsolódó feladat, hiszen így a sebezhetőségek megfelelő védelmi megoldásokkal még a tervezés, illetve megvalósítás fázisában – tehát hatékonyabban és olcsóbban – kiküszöbölhetőek, csökkenthetőek, vagy megmaradásuk esetén számba vehetőek. A biztonságos rendszerek kialakítására az elméletben és gyakorlatban több módszer is megjelent, melyek közé tartoznak a biztonsági fenyegetések modellezésének sokban hasonló, de egyes jellemzőikben eltérő módszerei: a fenyegetés-fa

[5] Eredetileg Common Vulnerability Enumeration, ma Common Vulnerabilities and Exposures. Részletesebben lásd cve.mitre.org.
[6] National Vulnerability Database. Részletesebben lásd nvd.nist.gov.
[7] National Institute of Standards and Technology, Computer Security Division.

(támadás-fa) elemzések, valamint a hagyományos forgatókönyv módszerekre épülő negatív/támadási forgatókönyv módszerek[8]. [10, 11, 12, 13]

Az előzőekben említett módszerek közvetlenül nem a sebezhetőségek feltárására irányulnak, azonban eredményeik közé ez utóbbi is beletartozik. A feltárt fenyegetések és támadások esetében ugyanis meghatározható, hogy az adott fenyegetés/támadás ellen létezik-e védelmi intézkedés, megoldás, ekkor az objektum (rendszer) egészét tekintve az adott fenyegetéshez kapcsolódóan nincs sebezhetőség. Amennyiben azonban ilyen védelem nem létezik, lényegében az objektum általános, vagy konkrét sebezhetősége került feltárásra.

A ***fenyegetés-fa elemzés*** lényege a konkrét fenyegetések és részleteik fokozatos meghatározása. A módszer kiinduló pontja a fenyegetések lehető legáltalánosabb meghatározása, amely, vagy amelyek fenyegetés-fák gyökér-csomópontját alkotják. Ezek a – kezdetben absztrakt – fenyegetések kerülnek lebontásra az adott csúcshoz kapcsolódó további, konkrétabb fenyegetéseket reprezentáló csúcspontok formájában. A lebontás lehetséges változatai közé tartozhat: az adott objektum összetevői (egy rendszer alrendszerei), vagy a fenyegetések típusai[9] szerinti lebontás. A módszer hiányossága, hogy nehéz szabályokat, segítséget nyújtani a lebontás módjára és sok esetben nehéz biztosítani, ellenőrizni e lebontás teljességét, alaposságát. Ezen kívül a módszer nem nyújt segítséget új, vagy ismeretlen fenyegetések feltárására.

A ***támadás-fa elemzés*** lényege a biztonságot fenyegető támadási célokhoz vezető "utak" fokozatos meghatározása. A fa-szerkezetű modell gyökerében egy konkrét támadási cél áll, amely lépésenként kerül lebontásra támadási részcélokra, amíg konkrétan végrehajtható támadásokhoz nem jutunk. A részcélok egymással ÉS, vagy VAGY kapcsolatban állva vezetnek a lebontott cél eléréséhez. A támadási fa csúcspontjaihoz különböző értékek (pld. bekövetkezés/végrehajtás valószínűsége, a cél eléréséhez szükséges ráfordítás mértéke, stb.) is rendelhetőek és elemezhetőek. A módszer erőteljesen épít az előre elkészíthető, vagy korábbi elemzések során kidolgozott részfák, valamint az úgynevezett támadási sémák, minták[10] (újra)felhasználására.

A részcélok meghatározása, bár a fenyegetés-fa elemzéshez képest logikailag valamivel megalapozottabb, még mindig informális – intuíción, gyakorlati tapasztalatokon – nyugvó módszer. Összetett rendszerek esetében a támadási részcélokra történő lebontásnak szintén egyik alapvető lehetősége az összetevőket érő támadásokra, mint részfeladatokra bontás.

A ***negatív/támadási forgatókönyv módszerek*** a hagyományos forgatókönyv módszerek kiterjesztéseként, új célra történő felhasználási módjaként jelentek meg. A forgatókönyv módszerek lényege az adott objektum szolgáltatásai igénybevételének, működésének felhasználóközpontú folyamatszemléletű modellezése, a "hogyan kell a rendszernek működnie" leírása. A negatív/támadási forgatókönyv ezzel szemben, általában a hagyományos forgatókönyv lépéseihez kapcsolódóan, azt kiegészítve, a "hogyan lehet rosszindulatú tevékenységet megvalósítani" feladatok modellezése, leírása. A módszer eredménye az előzőekhez hasonlóan a sebezhetőségek és támadási lehetőségek feltárása, ennek alapján a védelmi megoldások, intézkedések megvalósítása.

[8] Threat tree modelling, attack tree modelling, use cases, misuse/abuse cases.
[9] Az eredeti megoldásban szereplő fenyegetés-típusok: a bizalmasságot, a sértetlenséget és a működőképességet érintő fenyegetések (disclosure, integrity, denial of service).
[10] Attack pattern.

A forgatókönyv-alapú módszerek során különböző megközelítésű és hatókörű, illetve részletezettségű megvalósítások lehetségesek. A megközelítés lehet alkalmazás-, vagy rendszer központú. Az előbbi tárgya a szervezet és a szervezeti folyamatokra összpontosít, az utóbbi tárgya pedig egy rendszer és a rendszer funkcióira összpontosít. A hatókör alapján készülhetnek forgatókönyvek egy szervezeti folyamat, vagy egy rendszer működésének egészére, illetve egyes részfolyamatokra, vagy alrendszerek működésére. Ez utóbbi gyakorlatilag részekre bontást és részletesebb kifejtést jelent, ami rendszerek esetében jellemzően alrendszerekre tagolást és azokhoz kapcsolódó részfunkciók leírását foglalja magában. [14, 9. o.]

Az ***informatikai rendszerek sebezhetőségeinek, támadásainak rendszerezése*** régóta vizsgált kutatási terület. A nyilvános sebezhetőség-adatbázisok, listák konkrét – elsősorban szoftver, de részben hardver – összetevők sebezhetőségeit tartalmazzák és nyilvánvaló, hogy ezek között hasonló jellegű, vagy meghatározott szempontok alapján egy kategóriába sorolható sebezhetőségek is vannak. Az egyes, több ezer elemet is tartalmazó sebezhetőség-listák könnyebb kezelhetőségének, a különböző listák közötti kapcsolat kialakításának igénye vezetett az úgynevezett sebezhetőség taxonómiák kialakítására, vizsgálatára. Ezek közül napjainkig számos javaslat látott napvilágot [lásd pld. 15, 16, 17, 18], de egységesen elfogadott taxonómia még nem alakult ki.

A javasolt taxonómiák között több olyan is van, amely egyik osztályozási szempontként az informatikai rendszerek összetevőit (mint a sebezhetőséget hordozó, a fenyegetés célpontját képező objektumokat) használja. Egy hálózati és számítógépes támadás taxonómia második szintű osztályozási szempontja például a támadás (elsődleges) célpontja, ami lehet:

- hardver összetevő, ezen belül számítógép, hálózati eszköz és periféria (majd ezek tovább bontva konkrétabb eszköztípusokra);
- szoftver összetevő, ezen belül operációs rendszer és alkalmazás (utóbbi tovább bontva kiszolgáló jellegű – pld. adatbázis-kezelő – és ügyfél-oldali szoftverekre);
- végül hálózati összetevő (ezen belül pld. protokollok). [17, 8-10. o.]

Egy másik taxonómia [18] egyik osztályozási szempontja szintén a támadás célpontja, ami lehet: az operációs rendszer, a hálózat, a helyi számítógép, a felhasználó maga, valamint az alkalmazás (ami lehet ügyfél-oldali, vagy kiszolgáló oldali alkalmazás).

***Összességében megállapítható***, hogy összetett objektumok, köztük az informatikai rendszerek sebezhetőségeinek jelentős része lebontható, visszavezethető egyes összetevőik sebezhetőségeire, vagyis olyan tulajdonságokra (hiányosságokra, gyengeségekre), amelyek már kizárólag egyetlen összetevőhöz, alkotóelemhez kapcsolódnak. Az összetett objektumok sebezhetőségeinek feltárására leggyakrabban használt módszerek (fenyegetés-fa elemzés, támadás-fa elemzés, negatív/támadási forgatókönyvek) alapvető jellemzője a fenyegetések, sebezhetőségek egyre elemibb részekre bontása, amelyek egy szint elérését követően a legtöbb esetben már meghatározott rendszer-összetevőkhöz kapcsolódnak. Az említett módszerek esetében eredményesen használhatóak fel az egyes rendszer-összetevő specifikus fenyegetés-fák, támadás-fák és részforgatókönyvek.

## VÉDELMI RENDSZABÁLYOK, INTÉZKEDÉSEK DEKOMPOZÍCIÓJA

A biztonság megőrzésének egyik alapvető feladata a kockázatok kezeléséhez szükséges védelmi rendszabályok, intézkedések, eszközök meghatározása, megvalósítása és alkalmazása. Ezen intézkedések irányulhatnak a fenyegetéseket lehetővé tévő sebezhetőségek kiküszöbölé-

sére, vagy csökkentésére, valamint a fenyegetések elrettentésére, megelőzésére, észlelésére, az ellenük való védelemre, bekövetkezésük esetén káros hatásaik csökkentésére, majd következményeik felszámolására. A továbbiakban vizsgálatainkat leszűkítjük az informatikai biztonsághoz kapcsolódó kérdésekre.

A kívánt mértékű biztonság fenntartására irányuló, a kockázatokat elhárító, vagy elfogadható mértékre csökkentő ***védelmi megoldások, eszközök*** megnevezése az angol nyelvű szakirodalomban 'security control'. Az ISO 27000 fogalomjegyzék szerint a 'control' "a kockázatok kezelésének eszköze, beleértve politikákat, eljárásokat, irányelveket, gyakorlati megoldásokat, vagy szervezeti struktúrákat, amely lehet adminisztratív, technikai, igazgatási, vagy jogi jellegű. Megjegyzés: a 'control' használatos a védelmi intézkedés, vagy ellenintézkedés szinonimájaként is." [19, 2. o.]

Az Egyesült Államok Szabványügyi Hivatalának vonatkozó dokumentuma szerint a 'security control'-ok "az informatikai rendszerek számára előírt, a rendszerek és információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére irányuló igazgatási, eljárási és technikai védelmi intézkedések és ellenintézkedések[11]". [20, 1. o.] A védelmi intézkedések magukban foglalnak "biztonsági jellemzőket, igazgatási korlátozásokat, a személyi biztonságot, valamint a fizikai struktúrák, területek és eszközök biztonságát." [21, 8. o.] Az ellenintézkedések pedig "tevékenységek, eszközök, eljárások, módszerek és más rendszabályok, amelyek egy informatikai rendszer sebezhetőségét csökkentik". [21, 6. o.]

Az Egyesült Államok hadereje vonatkozó dokumentuma szerint az 'IA [Information Assurance] control' "a sértetlenség, a rendelkezésre állás, vagy a bizalmasság objektív IA feltétele, amely meghatározott védelmi intézkedések alkalmazásával, vagy meghatározott tevékenységek szabályozásával érhető el és amely meghatározott formában van megfogalmazva ('control' szám, 'control' név, 'control' szöveg és egy 'control' osztály)." [22, 20. o.] A szabályozó szerint az 'IA control' olyan feltétel, vagy állapot, amely tesztelhető, teljesülése mérhető, illetve a megvalósulásához szükséges tevékenységek hozzárendelhetőek, így számonkérhetőek. [22, 48. o.]

A továbbiakban a 'security/information assurance control' fogalomra a védelmi rendszabály, intézkedés kifejezést használjuk, amely bár nem teljes egészében fejezi a fentiekben körülírt tartalmat, de megítélésünk szerint közelebb áll és közérthetőbbnek tűnik, mint az ellenőrzés, könyvvizsgálat szakterületéhez kapcsolódó – a COBIT módszertan magyar változata által is használt – kontroll. A COBIT a 'control' kifejezés további fordítási változatára többek között az irányítási és ellenőrzési eljárást tartalmazza. [23, 3. o.] A Magyar Informatikai Biztonsági Ajánlások párhuzamosan, lényegében érdemi megkülönböztetés nélkül használják a védelmi intézkedések, biztonsági intézkedések és kontroll kifejezéseket. [Lásd pld. 24]

A ***védelmi rendszabályok, intézkedések*** jellegük, megvalósításuk alapján különböző csoportokba sorolhatóak. Egyes osztályozások [pld. 19] adminisztratív, technikai (logikai) és fizikai védelmi intézkedéseket különböztetnek meg. Egy másik, széles körben használt osztályozás szerint vannak igazgatási (menedzsment), eljárási és technikai[12] védelmi rendszabályok, intézkedések. A három alapvető kategória a funkcionális hasonlóság alapján aztán tovább

[11] Safeguards, countermeasures.

[12] Az igazgatási rendszabályok, intézkedések a kockázatkezeléshez, illetve az informatikai rendszer biztonságának kezeléshez kapcsolódnak, az eljárási rendszabályok, intézkedések sajátossága, hogy azokat emberek, míg a technikai jellegűeket az informatikai rendszer hardver és szoftver összetevői valósítják meg, hajtják végre

osztható védelmi rendszabály, intézkedés családokra (négy igazgatási, kilenc eljárási és négy technikai). [20, 6 o.]

A védelmi rendszabályok, intézkedések kiválasztása, meghatározása az informatikai biztonság kialakítása és fenntartása folyamatának egyik alapvető feladata. Alapját a kockázatelemzés eredményei képezik és a feladatrendszer a kockázatkezelés része, lényegi összetevője. A biztonságpolitika és a biztonsági célkitűzések által meghatározott biztonság eléréséhez szükséges rendszabályok, intézkedések meghatározása alkotó folyamat, amelyet azonban jelentős mértékben segítenek különböző védelmi rendszabály, intézkedés katalógusok, listák. Ezek részben a háttértámogatás szándékával kerültek összeállításra, másrészt meghatározott területeken, például különösen a kritikus infrastruktúrák, vagy a katonai (védelmi) informatikai rendszerek esetében a minimális védelmi rendszabályok, intézkedések előírásához is alapul szolgálnak.

***Átfogó védelmi rendszabály, intézkedés listák*** találhatóak többek között az ISO 27001 szabványban [25], amely tizenegy kategóriába, azon belül mintegy negyven alcsoportba sorolva száznál több rendszabályt, intézkedést tartalmaz; a NIST 800-53-ben [20], amelynek tizenhét családjába közel 200 rendszabály, intézkedés tartozik; vagy a DoD 8500.2 Utasításában [22], amely nyolc kategóriába sorolva közel száz rendszabályt, intézkedést rögzít. A NIST 800-53 a felsorolt intézkedéseket a szövetségi informatikai rendszerek számára javasolja, a DoD 8500.2 pedig a katonai informatikai rendszerek számára – működésbiztonsági kategóriájuktól és a kezelt információk bizalmassági szintjétől függő módon – minimálisan írja elő.

Az említett átfogó rendszabály, intézkedés listák mellett, azokat kiegészítve részterületenként ***részletes védelmi rendszabály, intézkedés listák*** is készültek. Ezek közé tartoznak például a biztonsági beállítási (konfigurációs) útmutatók és a biztonsági technikai megvalósítási útmutatók[13]. Ezek között megtalálhatóak szakterületekhez, objektumtípusokhoz – például hozzáférés ellenőrzés, adatbázis-kezelő rendszerek, stb. – tartozó és konkrét termékekhez (termékcsaládokhoz) – például Microsoft IE6, Oracle 8i, stb. – kapcsolódó útmutatók is.

Egy konkrét rendszerben érvényesítendő védelmi rendszabályok, intézkedések meghatározásának célszerű rendjét az alapvető módszertanok a lépésenkénti közelítés módszerével javasolják. Ennek első lépése a kiinduló[14] rendszabály, intézkedés lista kiválasztása, amelyet az egyes dokumentumok közös, vagy minimális rendszabályokként, intézkedésekként határoznak meg. Ezek egy része választható összetevőket és meghatározandó értékeket tartalmaz, amelyek segítségével második lépésként a rendszabályok, intézkedések "testre szabhatóak".[15] Végül az így kialakult lista bővíthető az adott rendszerre specifikus védelmi rendszabályokkal, intézkedésekkel.

Összetett objektumok, például informatikai rendszerek esetében a védelmi rendszabályok, intézkedések jelentős része, különösen alacsonyabb szinten – a sebezhetőségekhez és fenyegetésekhez hasonlóan – hozzárendelhető annak összetevőihez. A rendszabály, intézkedés listákban szereplő átfogó kategóriák nem elsősorban rendszer-összetevők szerint tagolódnak,

[13] Security Configuration Guide, Security Technical Implementation Guide (STIG).

[14] Baseline.

[15] Például: AC-7 Sikertelen bejelentkezési kísérletek: Az informatikai rendszer egy adott felhasználó számára [*meghatározott szám*] számú sikertelen bejelentkezést engedélyez [*meghatározott időtartam*] időtartamon belül. A megengedett számú sikertelen bejelentkezés túllépése esetén a rendszer [*[meghatározott idő] időre lezárja az azonosítót/eszközt; [meghatározott idő] időtartamig késlelteti a bejelentkezési kérdést*]. [20, F-6. o.]

azonban ezek többsége értelmezhető összetevőnként is. Például a hozzáférés ellenőrzés, a biztonsági mentések, az auditálás és megfelelőség-ellenőrzés konkrétan megvalósítandó feladatok a fizikai környezet, az operációs rendszerek, vagy az alkalmazások, köztük kiemelten az adatbáziskezelő rendszerek esetében.

***Összességében megállapítható***, hogy a védelmi rendszabályok, intézkedések jelentős része kapcsolódik közvetlenül összetett objektumok egyes összetevőihez. Ennek megfelelően találkozhatunk a szakirodalomban a hálózati védelmi intézkedések; az alkalmazás-szintű védelmi intézkedések, vagy az adatbázis védelmi intézkedések fogalmakkal, illetve listákkal.

Az említett – és más hasonló – informatikai rendszer-összetevő orientált védelmi rendszabályok, intézkedések jelentős szerepet játszanak az informatikai biztonság kezelésének rendszerében azonban megítélésem szerint hiányos az összhang az átfogó biztonság-, illetve kockázat-kezelési módszertanok és háttéranyagok, valamint a szakterületi megközelítések között. A gyakorlatban viszont egyaránt szükség van az átfogó megközelítésre és az ebből levezethető szakterületi szintű részletekre, illetve a bevált megoldásokra.

## ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegzésképpen abból az általános megállapításból kell kiindulnunk, hogy a biztonság alanyai általában különböző – sajátos alkalmazási, funkcionális, technikai és biztonsági jellemzőkkel rendelkező – összetevőkre, alrendszerekre tagolhatóak. Ez mindenképpen igaz a vizsgálatunk szempontjából kiemelt kritikus információs infrastruktúrák, illetve informatikai rendszerek esetében. Ezek technikai összetevői közé tartoznak végső soron a hálózati infrastruktúra, valamint a végberendezések hardver, operációs rendszer, alkalmazói szoftver és adatbázis komponensei.

Az összetett objektumok, köztük az információs infrastruktúrák és informatikai rendszerek biztonsági vonatkozásai, kérdései – megőrzendő tulajdonságok, fenyegetések, sebezhetőségek, védelmi intézkedések – értelmezhetőek, vizsgálandóak és meghatározandóak az objektum egészére, illetve külön-külön egyes összetevőire. Az egyes biztonsági kérdések dekompozíciója alatt egy összetett objektum biztonsági kérdéseinek összetevői biztonsági kérdéseire történő lebontását, illetve az ezek között fennálló összefüggések meghatározását értjük.

A publikációban vizsgált kérdések mindegyikénél megállapítható volt, hogy szoros kapcsolat áll fent az összetett objektum szempontjából vett és az egyes összetevők szerinti megközelítések (vizsgálat, meghatározás, megvalósítás, ellenőrzés, értékelés, stb.) között. A két szint között elsődlegességet az összetett objektum egészére vonatkozó átfogó megközelítés élvez, azonban a gyakorlatban – sőt az elméletben – megkerülhetetlen az összetevő, ezzel egyben szakterületi szintű megközelítések (sajátosságaik, módszereik, eszközeik, megoldásaik) érvényesülése is. Következtetésként tehát megfogalmazható, hogy az átfogó biztonsági módszertanokhoz illeszkedő módon továbbra is szükséges és érdemes vizsgálni a biztonság különböző - összetevő-típusok szerint elkülönülő – részterületeit.

## FELHASZNÁLT IRODALOM


[1] Munk Sándor: Informatikai biztonság vs. információbiztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám.

[2] Munk Sándor: Katonai informatika II., Katonai informatikai rendszerek, alkalmazások. Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006.

[3] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Third Edition. – 2009.

[4] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. – National Institute of Standards and Technology, 2002

[5] A Magyar Köztársaság Nemzeti Katonai Stratégiája. Összefoglaló. – HM Zrínyi Kommunikációs Szolgáltató Kht. – Zrínyi Kiadó, Budapest, 2009.

[6] Information assurance through defense in depth. – Directorate for C4 Systems, US DoD Joint Chiefs of Staff, Washington, 2000.

[7] Összetett termékekre vonatkozó értékelési módszertan. – Miniszterelnöki Hivatal, Budapest, 2008.

[8] Rendszerekre vonatkozó értékelési módszertan. – Miniszterelnöki Hivatal, Budapest, 2008.

[9] Mann, David E.-Christey, Steven M.: Towards a Common Enumeration of Vulnerabilities. – MITRE Corporation, Bedford, 1999.

[10] Amoroso, Edward G.: Fundamentals of Computer Security Technology. – Prentice Hall, Englewood Cliffs, 1994

[11] Schneier, Bruce: Attack trees – modeling security threats. – Dr. Dobbs Journal, 1999/12., 21-29.o.

[12] McDermott, John-Fox, Chris: Using Abuse Case Models for Security Requirements Analysis. – Proceedings of the 15th Annual Computer Security Applications Conference, Phoenix, Arizona, 1999, 55-66. o.

[13] Sindre, Guttorm-Opdahl, Andreas L.: Capturing Security Requirements through Misuse Cases. – Proceedings of Norsk Informatikkonferanse NIK'2001, Trondheim, 2001. 11.26-28., 219-230. o.

[14] Kettenis, Jan: Getting Started with Use Case Modeling. An Oracle White Paper. – Oracle Corp., Redwood Shores, 2005.

[15] Landwehr, Carl-Bull, Alan R.-Mcdermott, John P.-Choi, William S.: A Taxonomy of Computer Program Security Flaws, with Examples. – ACM Computing Surveys, 1994/3, 211-254 o..

[16] Bishop, Matt-Dailey, David: A Critical Analysis of vulnerability taxonomies. TR CSE-96-11. – Dept. of Computer Science University of California, Davis, 1996.

[17] Hansmann, Simon-Hunt, Ray: A taxonomy of network and computer attacks. – Computers & Security, 2005/1, 31-43 o.

[18] Shiva, Sajjan-Simmons, Chris-Ellis, Charles-Dasgupta, Dipankar.-Roy, Sankardas-Wu, Qishi: AVOIDIT: A cyber attack taxonomy. Technical Report CS-09-003. – University of Memphis, 2009.

[19] ISO/IEC 27000:2009(E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. – International Organization for Standardization/International Electrotechnical Commission, 2009.

[20] NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. Revision 2. – National Institute of Standards and Technology, 2007.

[21] FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. – National Institute of Standards and Technology, 2006.

[22] DoD Instruction 8500.2, Information Assurance (IA) Implementation. – US Department of Defense, 2003.
[23] COBIT 4.1 Szószedet. Szakmai szótár. – ISACA Budapest Chapter, 2007.
[24] KIB 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások (MIBA). 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK). 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR). 1.0 verzió – Közigazgatási Informatikai Bizottság, 2008.
[25] ISO/IEC 27001:2005(E), Information technology – Security techniques – Information security management systems – Requirements. – International Organization for Standardization/International Electrotechnical Commission, 2009.