10.17625/nke.2012.002

**ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM**
**BOLYAI JÁNOS HADMÉRNÖKI KAR**
**HADMÉRNÖKI DOKTORI ISKOLA**

**Póserné Oláh Valéria**

# Közigazgatási informatikai rendszerek informatikai biztonsági kérdései

Doktori (PhD) Értekezés

**Témavezető:**
**Prof. dr. Haig Zsolt mk. ezredes, PhD**
**egyetemi tanár**

.....

**BUDAPEST, 2011.**

# TARTALOMJEGYZÉK

# BEVEZETÉS

Ma már a hétköznapi állampolgárok élete is elképzelhetetlen informatikai rendszerek nélkül, hiszen bárhova megyünk, nap, mint nap találkozunk velük. Vegyünk csak egy egyszerű példát. Amikor elmegyünk egy szakorvosi rendelésre és ott (azzal a célzattal, hogy hátha köze van a mostani problémánkhoz egy másik betegségnek is) megkérdezik, hogy egy másik szakrendelést milyen panasszal kerestünk fel, akkor saját bőrünkön tapasztalhatjuk az informatikai rendszerek jótékony hatását életminőségünkre. Meglepődve vesszük tudomásul, hogy életünket szép lassan beszövik az informatikai rendszerek.

Éppen ezért az informatikai biztonság – figyelembe véve a számítógép-hálózatok, az internet elterjedését és befolyását is úgy az állampolgárokra, mint a szervezetek sikeres működésére – egyre nagyobb jelentőséggel bír. Sajnálatos módon azonban tapasztalataim alapján azt kell megállapítanom, hogy nem csak a szervezetek vezetői, a tudatlan felhasználók, de még az informatikusok egy része sem érzékeli teljes felelősséggel az informatikai biztonság jelentőségét. Így van ez, akár az állami-, akár a civilszféra rendszereit vizsgáljuk is. Sok helyen még olyan alapkövetelménynek számító védelmi megoldásoknak sem tulajdonítanak jelentőséget, mint például a biztonsági mentés, vagy a jelszavas védelem kialakítása.

Az tapasztalható, hogy a felhasználók a megfelelő szabályozás vagy annak betartatása hiányában belátásuknak megfelelően használhatják az informatikai rendszereket, egyre több és több veszélyforrásnak kitéve ezzel a szervezet informatikai rendszereit.

Az informatikai biztonság azonban egy állapot, mely koránt sem állandó, így tehát folyamatos felülvizsgálatot igényel, nem elegendő egyszer kialakítani, állandóan oda kell figyelni és lépést kell tartani az újabbnál újabb fenyegetések ellen kialakított védelmi megoldásokkal. Ugyanis az informatikai biztonság hiánya nem érzékelhető, csupán az annak hiányából fakadó incidensek hatása, mint például adatvesztés, sérülés vagy lopás. Általában ezért nem hajlandó pénzt áldozni rá a felső vezetés mindaddig, amíg be nem következik a baj.

## A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Mivel az informatikai rendszerek az élet minden területén jelen vannak, így a közigazgatás feladatköreiben, szolgáltatásaiban is nagyobb teret hódítanak maguknak. A személyi számítógépek és a belőlük alkotott kisebb-nagyobb hálózatok elterjedésének, az első vírusok

megjelenésének, a számítástechnika felgyorsult fejlődésének köszönhetően az informatikai biztonság kérdése is egyre bonyolultabb lett. NATO és EU tagságunk is újabb információbiztonsági követelményeket támaszt hazánk informatikai rendszerei, köztük a közigazgatás informatikai rendszereivel szemben.

Belátható, hogy az informatikai biztonság csak akkor hatékony, ha az informatikai rendszer minden egyes elemére (szerverek, munkaállomások, operációs rendszerek, alkalmazások, hálózat, stb.) egységesen biztosított. Azonban a közigazgatási informatikai rendszerekről egyáltalán nem mondható el, hogy egyenszilárdságú védelemmel rendelkeznek. Vannak bizonyos területek, ahol közel megfelelő mennyiségben, minőségben és formában alkalmazzák a korszerű védelmi módszereket, de számos olyan közigazgatási informatikai rendszer is van, ahol az alapvető informatikai biztonsági intézkedéseket sem végzik el. Azért is nagy a jelentősége a közigazgatási informatikai rendszerek biztonsági hiányosságainak, mivel egy-egy incidens széles embertömegeket, akár a társadalom egészét is hátrányosan érintheti. Senki sem örülne például annak, ha bárki – a rendszer biztonsági problémáinak köszönhetően – a nevében mondjuk születési anyakönyvi kivonatot lenne képes igényelni, melynek segítségével már a teljes identitás is eltulajdonítható és visszaélésre ad lehetőséget.

Már a kutatásom kezdetekor megállapítottam, hogy hazánk közigazgatási informatikai rendszerei, csakúgy, mint sok egyéb rendszer is egyre több sérülékenységet tartalmaznak, a támadók köre, eszközeik, módszereik pedig rohamosan fejlődnek.

**A közigazgatási informatikai rendszereket fenyegető veszélyek feltárása, elemzése, valamint a korszerű védelmi módszerek alkalmazhatóságának vizsgálata** tudományos kutatást igényelt, amelyet az elmúlt években, az informatikai biztonság területén szerzett oktatói tapasztalataimra alapozva elvégeztem, és amelynek eredményeit jelen doktori értekezés kertében bemutatok. Az értekezés elkészítésének terjedelmi korlátaira való tekintettel kutatásom nem terjedt ki a minősített adatok kezelésével kapcsolatos informatikai biztonsági kérdések területeire, az további kutatást igényel.

## KUTATÁSI HIPOTÉZISEK MEGFOGALMAZÁSA

Kutatómunkám megkezdésekor az alábbi hipotéziseket állítottam fel:

1. A közigazgatási szervezetek informatikai rendszereinek informatikai biztonsága mind szabályzói oldalról, mind a működtető humánerőforrás szemléletmódjából adódóan nem kielégítő.
2. A közigazgatási informatikai rendszerek veszélyforrásai a támadók módszereit, eszközeit és motivációit tekintve nem különböznek a vállalati informatikai rendszerek elleni fenyegetésektől.
3. A közigazgatási informatikai rendszerek esetében, az azokban alkalmazott operációs rendszereket tekintve nem hátrányosabb a nemzetközi trenddel ellentétben a zárt forráskódú operációs rendszerek további alkalmazása.
4. A közigazgatási informatikai rendszerek biztonságának megteremtéséhez szükséges védelmi megoldások ugyanazok, mint egy vállalati informatikai rendszer esetében, de azok alkalmazása nem megfelelő mértékű a közigazgatásban.

## KUTATÁSI CÉLKITŰZÉSEK

A fentebb megfogalmazott kutatási hipotézisek igazolására vagy megcáfolására az alábbi kutatási célokat tűztem ki:

1. Megvizsgálni a közigazgatási szervek informatikai rendszereit, a rendszer modellezése alapján bemutatni és elemezni azok működési folyamatait, az alkalmazott informatikai biztonsági szabályzókat és a működtető személyzet szemléletmódját; feltárni azok hiányosságait és meghatározni fejlesztésük lehetséges irányait, követelményeit.
2. Elemezni a közigazgatási informatikai rendszerek elleni lehetséges támadókat, a támadások fajtáit és ez alapján rendszerezni és csoportosítani a veszélyforrásokat.
3. Az informatikai biztonság szempontjából elemezni, értékelni és összehasonlítani a közigazgatási informatikai rendszerekben leggyakrabban alkalmazott nyílt- és zárt forráskódú operációs rendszereket és javaslatokat tenni további alkalmazhatóságukra vonatkozóan.

4. Kockázatelemzési modellre alapozva megvizsgálni a közigazgatási informatikai rendszerekben alkalmazható korszerű védelmi megoldásokat, azok működési elveit és javaslatokat tenni alkalmazhatóságukra a közigazgatási informatikai rendszerek informatikai biztonságának növelése érdekében.

## KUTATÁSI MÓDSZEREK

Kutatásomat az informatikai rendszerek sérülékenységeire vonatkozó széleskörű **irodalomkutatásra épülő információk gyűjtésével, rendszerezésével elemzésével** kezdtem, melyet a későbbiekben kiegészítettem e sérülékenységek felderítésére, valamint az ellenük történő hatékony védelem kialakításának szemléltetésére, **modellezésére** irányuló **szimulációk** végrehajtásával. **Figyelemmel** kísértem a témával kapcsolatos elkészített és folyamatban lévő értekezések, tudományos diákköri dolgozatok megállapításait, a műszaki publikációkat, tudományos rendezvényeket és kiállításokat. Felhasználtam a közigazgatási szféra különböző vezető beosztású személyeivel folytatott **interjúk** során nyert információkat, tapasztalatokat. Az értekezés elkészítésekor a nemzeti és az EU információvédelemmel kapcsolatos jogszabályokra, szabályozókra, ajánlásokra, szabványokra támaszkodtam. Konzultáltam, tapasztalatokat gyűjtöttem, és a biztonságos informatikai rendszerek kialakítása, üzemeltetése, valamint ellenőrzése, felülvizsgálata témakörök **oktatása során szerzett tapasztalataimat felhasználtam** a kidolgozáshoz. Számos kutatás és tanulmány **másodelemzésével**, az **analízis** és **szintézis**, az **indukció** és **dedukció** módszereinek alkalmazásával törekedtem a kutatási céljaim elérésére és megvalósítására.

A kitűzött célok elérése érdekében végzett kutatásaimat a következő szerkezetű munkában foglaltam össze:

**Az első fejezetben** meghatároztam, pontosítottam az értekezésben használt fogalmakat, megvizsgáltam a közigazgatási informatikai rendszereket és azok működési folyamatait, megalkottam a közigazgatási informatikai rendszerek funkcionális és strukturális modelljét és meghatároztam a közigazgatási szervezetek informatikai biztonságát növelő informatikai biztonsági stratégia kialakításához szükséges szempontokat, feladatokat, bemutattam a stratégia felépítésének egy lehetséges változatát valamint feltártam a közigazgatási informatikai rendszerekre vonatkozó szabályozási hiányosságokat. Javaslatokat tettem a hiányosságok kiküszöbölését célzó megoldásokra.

**A második fejezetben** elemeztem és csoportosítottam a közigazgatási informatikai rendszerek informatikai biztonságát fenyegető veszélyforrásokat, támadási módszereket, megvizsgáltam a támadók körét, célpontjait, a támadások hatásait, valamint tesztelés alapján elemeztem és összehasonlítottam a közigazgatási informatikai rendszerekben leggyakrabban alkalmazott nyílt és zárt forráskódú operációs rendszereket, majd következtetéseket vontam le további alkalmazhatóságukra vonatkozóan.

**A harmadik fejezetben** megvizsgáltam az informatikai rendszerekben alkalmazható korszerű védelmi megoldásokat, azok működési elveit, majd a korábban feltárt fenyegetésekre és védelmi hiányosságokra koncentrálódó célzott, részleges kockázatelemzési modell és hatáselemzés alapján javaslatokat tettem alkalmazhatóságukra a közigazgatási informatikai rendszerek biztonságának növelése érdekében.

Az értekezés végén összegzem következtetéseimet, főbb megállapításaimat, megfogalmazom az általam elért új tudományos eredményeket és ajánlásokat fogalmazok meg a további felhasználásra vonatkozóan.

A dolgozatban az áttekinthetőség kedvéért dőlt betűkkel írom az idézeteket, félkövér betűkkel írom a kiemelendő, fontosnak tartott szavakat, kifejezéseket.

Az irodalmi hivatkozások tekintetében szögletes zárójelek között, a hivatkozott irodalom számát követően kettősponttal elválasztva tüntetem fel az azon belüli oldalszámot, ha szószerinti hivatkozást alkalmazok (például: [2: 21.p.] a 2. irodalom 21. oldalára való hivatkozás). Kivételt képez ez alól, ahol nem állapítható meg a konkrét oldal száma (weboldal, nincs oldalszámozás). Vesszővel választom el egymástól az irodalmak számát, ha egy adott gondolat több irodalom alapján fogant meg bennem (például: [3,7] a 3. és a 7. irodalomra való hivatkozást jelenti).

A saját publikációim közül azokat, melyekre az értekezésben is hivatkozom az egyszerűbb hivatkozási jelölhetőség kedvéért azon túl, hogy a publikációs jegyzékemben felsorolásra kerültek, megjelenítettem a felhasznált irodalmak között is.

Az adatgyűjtést 2011. május 15-én lezártam.

# 1. FEJEZET
# KÖZIGAZGATÁSI SZERVEZETEK INFORMATIKAI RENDSZEREI BIZTONSÁGÁNAK SZABÁLYOZÁSI KÉRDÉSEI

Ahhoz, hogy valamely szervezet informatikai rendszerének informatikai biztonságát megvizsgáljuk először is pontosan meg kell határozni, hogy mit is értünk informatikai rendszer és informatikai biztonság alatt. Elengedhetetlenül szükséges ez, mivel még szakmai körökben is gyakran keverednek az említett fogalmak az információs rendszer és információbiztonság fogalmaival. Így tehát kutatásom első lépcsőfoka a fenti fogalmak és további szükséges meghatározások tisztázása volt.

## 1.1. AZ ÉRTEKEZÉSBEN HASZNÁLT ALAPVETŐ FOGALMAK

Napjainkban az információs rendszer és az informatikai rendszer fogalmát igen gyakran keveredni láthatjuk. Előfordul, hogy egymás szinonimájaként alkalmazzák a két fogalmat, holott nem ugyanazt jelentik. Kétségtelen, hogy nem függetlenek egymástól, sőt valódi részhalmazuk van.

**Az információs rendszer** definíciójára a különböző szakterületeknek megfelelően több, akár egymástól eltérő meghatározást is találhatunk. Így pl. a közgazdaságtan területén a vállalati környezetre vonatkoztatva Chikán Attila megfogalmazásában *„Az információs rendszer a vállalatok környezetére, belső működésére és a vállalat - környezet tranzakciókra vonatkozó információk begyűjtését, feldolgozását, tárolását és szolgáltatását végző személyek, tevékenységek és technikai eszközök összege.”* [1: 293.p.] Mint e definícióból is látható megadja a szakterületi sajátosságát, vagyis, hogy a vállalatok környezetére, a vállalat – környezet tranzakcióira vonatkoztatja a definíciót.

Egy másik meghatározás szerint *„…az információs rendszer az információ megszerzésével, rögzítésével, generálásával, létrehozásával, tárolásával, kikeresésével, feldolgozásával, átalakításával, csoportosításával, továbbításával, vételével, megjelenítésével megsemmisítésével foglalkozó rendszer.”* [2: 16.p.] Mint látható itt elsősorban az információs tevékenységekre helyeződik a hangsúly és nem említi például a személyzetet és a technikai eszközöket.

Az információs rendszerek vonatkozásában megállapítható, hogy közös jellemzője mindegyik meghatározásnak, hogy az információs rendszer lehetőséget nyújt az adatok gyűjtésére, tárolására, visszakeresésére, strukturálására, szűrésére, összefoglalására, és továbbítására, egyszóval az információs tevékenységek megvalósítására. Tágabb értelemben mindez értelmezhető akár manuális, akár automatizált (elektronikus) információs rendszerekre is, bár napjainkban már az elektronizáltság a jellemző.

Fentiek alapján **információs rendszer alatt az alábbi meghatározást értem**: az információs rendszer az információ gyűjtését, rögzítését, létrehozását, tárolását, feldolgozását, továbbítását, megjelenítését és megsemmisítését végző technikai eszközök, folyamatok és a működtető szakszemélyzet összessége.

Munk Sándor Katonai informatika II. Katonai informatikai rendszerek, alkalmazások című egyetemi jegyzetében [3] körbejárta az **informatikai rendszer** fogalmának lehetséges értelmezéseit, ezen belül a NATO által elfogadott és más katonai informatikai értelmezéseket is megfogalmazott, mely alapján „*Egy **funkcionális informatikai rendszer** egy adott információs rendszer, egységes szabályozás hatálya alá tartozó információs tevékenységek összességének megvalósítására, támogatására szolgáló eszközök, programok, adatok, valamint működtető személyzet összessége.*" [3: 21.p.], míg „*A funkcionális megközelítésmód alapján **legszűkebb értelemben** az informatikai rendszerek közé azon rendszerek sorolhatók, amelyek elsődleges rendeltetése az információk feldolgozása (átvétele, tárolása, átalakítása és rendelkezésre bocsátása).*" [3: 19.p.]

Muha Lajos megfogalmazása alapján az „***Informatikai rendszer** az adatok kezelésére[1] használt elektronikus eszközök, eljárások, valamint az ezeket kiszolgáló és a felhasználó személyek együttese.*" [4: 142.p.] E definícióból szükséges kiemelni az „elektronikus" jelzőt, amely hangsúlyosan utal arra, hogy e rendszerben az adatok kezelése elektronikus úton történik.

Az információs rendszer és az informatikai rendszer fogalom keveredésének az okát egyrészt az angol megnevezésben látom, ugyanis angolul mindkettőre az „information system" megnevezést használják, és csak a szövegkörnyezetből derül ki, hogy melyik fogalomról van szó konkrétan. Másrészről pedig, az informatikai és a kommunikációs technológiák konvergenciája, integrációs folyamatai is bonyolítják a helyzetet. Az adatok (in-

[1] Adatkezelés: „az adatok gyűjtése, felvétele, tárolása, feldolgozása (megváltoztatása, átalakítása, összegzése, elemzése stb.), továbbítása, törlése, hasznosítása (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozása." [4]

formációk) megszerzését (előállítását), tárolását, feldolgozását, továbbítását biztosító különböző elektronikai, informatikai eszközök és rendszerek közötti legátfogóbb, legmeghatározóbb jelenség ezen területek konvergenciája, amit infokommunikációs konvergenciának nevezünk.

Az infokommunikációs rendszereken alapuló információs infrastruktúrák egymásba kapcsolódó komplex rendszere elengedhetetlenül szükséges feltétele az információs társadalom működésének. „*A rendszerek komplexitását bizonyítja, hogy a távközlési, informatikai rendszerek, a hozzájuk kapcsolódó távérzékelő, távfelügyeleti, navigációs rendszerekkel, szenzorhálózatokkal és más elektronikai rendszerekkel egységes rendszert képeznek, ami által képesek teljes hatékonysággal működni.*" [5] Azaz itt jóval többről van szó, mint csupán az informatikai és távközlési rendszerek konvergenciájából kialakuló rendszerekről, mivel az infokommunikációs rendszerekbe beletartoznak az érzékelés, irányítás, vezérlés funkcióit ellátó rendszerek is (mint pl. a távközlési rendszereken és a számítógéphálózatokon keresztül más rendszerekhez kapcsolódó repülőtéri leszállító és irányító rendszerek).

Ezeknek a korszerű, igen fejlett információtechnológián alapuló infokommunikációs rendszereknek a vállalati alkalmazásukon túl a különböző kormányzati, gazdálkodó, védelmi szervezetek, intézmények területén történő alkalmazására is lehetőség nyílt. „*Amennyiben e szervek ezeket a rendszereket megfelelően tudják működtetni, ki tudják használni a bennük rejlő lehetőségeket, és ugyanakkor a biztonságos működtetésüket is meg tudják teremteni, akkor ez egy igen komoly erősokszorozó, hatásnövelő képességjavító és integráló hatású tényezővé válik.*" [5]

A felvetett fogalmi keveredésekkel kapcsolatban egyetértek Munk Sándorral, abban hogy sokkal nagyobb a jelentősége az adott fogalom tartalmának, mint, hogy éppen hogyan nevezzük, hiszen, ha az egyik kommunikáló fél egy adott kifejezéshez pontosan meghatározza a tartalmát, akkor a másik fél képes lesz azt annak pontos értelmezése alapján lefordítani az ő általa elfogadott megnevezésre. „*Az azonos tartalomhoz rendelt különböző elnevezések általában nem akadályozzák (csak nehezítik) az információcserét, egymás információinak jelentésmegőrző átvételét. … Ehhez persze a fogalom meghatározás sajátosságaiból következően rendszerint szükség van a definícióban szereplő további, pld. általánosabb fogalmak tartalmának egyeztetésére.*" [6]

Ezzel természetesen nem azt kívántam kifejezni, hogy nincs szükség a fogalmak egységesítésére, hanem csak vázoltam a nehézségeket, melyek az informatikai és a kommunikációs technológiák konvergencia és integrációs folyamatainak befejeződéséig nehezíteni fogják a különböző fogalmak egységesítését.

A fentebb leírtakra tekintettel **véleményem szerint** az **informatikai rendszer az infokommunikációs rendszernek része**, egy olyan részhalmaza, amely a már összegyűjtött (megszerzett) adatok (akár hálózatos környezetben való) tárolására, feldolgozására, továbbítására szolgál.

Mindezeket figyelembe véve a fenti definíciók közül Munk Sándornak a funkcionális megközelítésmód alapján legszűkebb értelemben vett megfogalmazása, valamint a NATO szabályozókban előforduló meghatározás[2] alapján az **informatikai rendszereket a következőképpen értelmezem**: eszközök, programok, adatok, valamint a működtető személyzet összessége, amely **a már összegyűjtött (megszerzett) adatok (akár hálózatos környezetben való) bevitelére, tárolására, feldolgozására, továbbítására szolgál.** Ebből adódóan a kutatási témámhoz nem tartozott hozzá az adatok gyűjtésére alkalmas távérzékelő, távfelügyeleti, navigációs rendszerek, szenzorhálózatok és más, az informatikai rendszerekhez kapcsolható elektronikai rendszerek vizsgálata. Ugyanakkor e fogalom körébe sorolandó a már meglévő (összegyűjtött) **adatok bevitele** az informatikai rendszerbe, ami e rendszer szempontjából adatgyűjtésnek is tekinthető.

Az előbbiek alapján az is kijelenthető, hogy az információbiztonság sem egyenértékű az informatikai biztonsággal. Ugyanis az információs társadalomban, az egymásba kapcsolódó komplex infokommunikációs rendszerek korában, az információbiztonság fogalmát is komplexen kell értelmezni.

Az információbiztonság komplexitásából adódóan megállapítható, hogy az nem csak technológiai kérdés, bár megteremtésében és fenntartásában jelentős szerepe van a különböző információvédelmi eszközöknek, eljárásoknak. A komplex információbiztonság az informatikai biztonságnál jóval több és komplexebb, bonyolultabb tervezési, szervezési és végrehajtási folyamat. [7] A korábban megfogalmazott infokommunikációs rendszer és informatikai rendszer viszonyának analógiáján kijelenthető, hogy az informatikai biztonság része, részhalmaza a komplex információbiztonságnak.

---

[2] Information system (IS): Eszközök, módszerek és eljárások, illetve működtető személyzet, információfeldolgozási funkciók megvalósítására létrehozott rendszere. [3: 7.p.]

Mindezek alapján egyetértek Muha Lajos informatikai biztonság definíciójával, miszerint: „*az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága*[3]*, sértetlensége*[4] *és rendelkezésre állása*[5]*, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szemponjából zárt, teljes körű, folytonos és a kockázatokkal arányos*" [4: 145.p.]. A továbbiakban értekezésemben **az informatikai biztonságot e meghatározás alapján értelmezem**.

Miután tisztáztam az informatikai rendszer és az informatikai biztonság fogalmakat szükséges még a közigazgatás és a közigazgatási informatikai rendszer fogalmak behatárolása.

„*Az igazgatás, mint tevékenység két fő elemből tevődik össze, jelesül a magánigazgatásból (civil szféra, gazdasági élet) és közigazgatásból. A* ***közigazgatás*** *olyan tevékenység, amely közösségi célok megvalósítására irányul, a közösség érdekében. A közigazgatási tevékenységet közigazgatási szervek végzik.*" [8: 8.p.]

A közigazgatási szerveket két fő jellemző határoz meg, az egyik az illetékességük, melyet területi szempontok határoznak meg, a másik pedig a hatáskörük, mely az általuk lefolytatható eljárások, ügyintézések típusától függ.

A közigazgatás feladata: „*... az adók, illetékek, bírságok behajtása, nyilvántartása, az állam vagyonának óvása, gazdaságos felhasználása, a közszükségletek kielégítésének megszervezése, köznyilvántartások vezetése, közbiztonság megteremtése, stb., ...*" [9]

A közigazgatási szervek jogkövetkezményekkel járó, konkrét ügyintézési folyamatait mindig egy döntés zár le, mely meghozatalához jogilag releváns és hiteles információkra van szükség, melyek elsősorban közhitelű vagy csak deklaratív erejű országos alapnyilvántartásokból származnak. [8] Az egyes ügyintézési folyamatok lezárását szolgáló döntések meghozatalához szükséges információknak a biztosítása ma már elképzelhetetlen informa-

---

[3] Bizalmasság (ang.: confidentiality ): „az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról." [4: 144.p.]

[4] Sértetlenség (ang.: integrity ): „az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanság8) is, illetve a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható. [4: 144.p.]

[5] Rendelkezésre állás (ang.: availability): az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható. [4: 144.p.]

tikai támogatás nélkül.

Az Új Magyarország Fejlesztési Terv keretében, az Államreform Operatív Program támogatásával, az „Elektronikus közigazgatási keretrendszer" tárgyú kiemelt projekt megvalósításának részeként készült dokumentumban a **közigazgatási informatikai rendszert** a következőképpen definiálják: „*a közigazgatási területen alkalmazott, központi szolgáltatásokat megvalósító, vagy támogató, vagy ilyen célt szolgáló informatikai rendszer.*" [10]

A fenti fogalmi behatárolások alapján kutatásomat a **közigazgatási informatikai rendszerek** informatikai biztonságára fókuszáltam.

## 1.2. KÖZIGAZGATÁSI INFORMATIKAI RENDSZEREK

### 1.2.1. A KÖZIGAZGATÁSI INFORMATIKAI RENDSZER – MINT KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA – MODELLJE

Az előző alfejezetben letisztáztam az értekezésemben alkalmazott alapvető fogalmakat, így a közigazgatási informatikai rendszerek fogalmát is, mint kutatási témám központi kérdését. Mivel a közigazgatási informatikai rendszereket a biztonság szempontjából vizsgáltam, ezért szükségesnek tartottam feltárni e rendszerek és a kritikus információs infrastruktúrák viszonyát.

Hazánk kritikus infrastruktúráinak védelme érdekében az Európai Unió Zöld Könyvének figyelembevételével 2008-ban a kormány kiadta a 2080/2008. (VI. 30.) Korm. határozatát a Kritikus Infrastruktúra Védelem Nemzeti Programjáról, melynek 1. melléklete (Zöld Könyv) szerint „*Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.*

*Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorol-*

*hat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.*" [11: 220.p.]

A fenti meghatározás alapján, a rendelet Magyarországon a kritikus infrastruktúrák 10 ágazatát és 43 alágazatát különbözteti meg, ugyanakkor nem említi a kritikus információs infrastruktúrákat. A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló zöld könyv azonban megadja a definícióját, miszerint: „*Kritikus információs infrastruktúrák közé azok sorolandók, melyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlés, számítógép hardver/szoftver, Internet, műholdak stb.)*". [12]

A 2080/2008 korm. rendelet kritikus infrastruktúra ágazati besorolása és az EU zöld könyv kritikus információs infrastruktúra meghatározása alapján a magyarországi kritikus információs infrastruktúrák az alábbiak szerint kategorizálhatók:

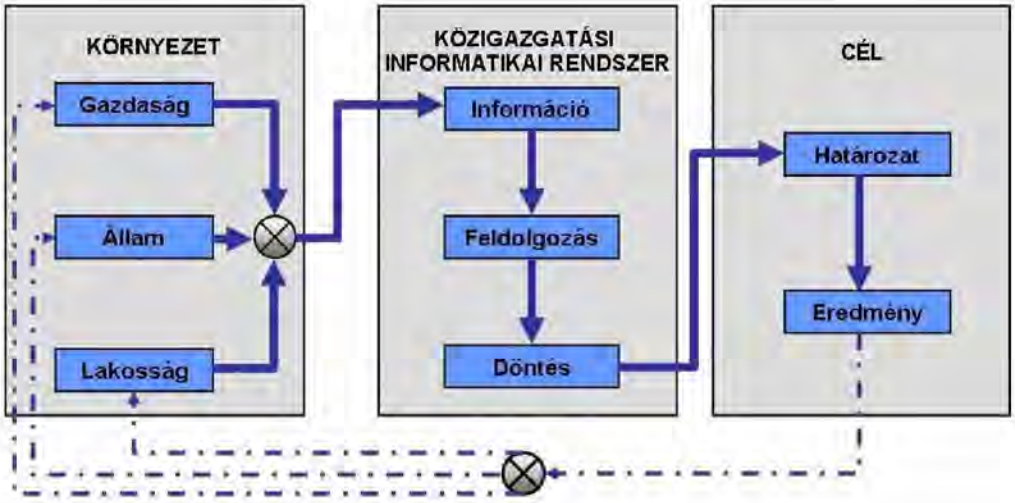
- energiaellátó rendszerek rendszerirányító infokommunikációs hálózatai;
- infokommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás infokommunikációs hálózatai;
- vízellátást szabályzó infokommunikációs hálózatok;
- élelmiszerellátást szabályzó infokommunikációs hálózatok;
- egészségügyi rendszer infokommunikációs hálózatai;
- pénzügyi-gazdasági rendszer infokommunikációs hálózatai;
- ipari termelést irányító infokommunikációs hálózatok;
- kormányzati és önkormányzati szféra infokommunikációs hálózatai
- védelmi szféra infokommunikációs hálózatai. [7]

A fentiek alapján megállapítható, hogy **a közigazgatási informatikai rendszerek,** mint a kormányzati és önkormányzati szféra infokommunikációs rendszereinek részhalmaza **kritikus információs infrastruktúrának minősülnek**.

A közigazgatás, mint rendszer két alrendszerből áll, az egyik az államigazgatás a másik az önkormányzati igazgatás vagy nevezhetjük helyi közigazgatásnak is. A közigazgatási informatikai rendszerek célja ezen alrendszerek működési folyamatainak támogatása, a megfelelő információ biztosítása a konkrét ügyintézési folyamatok lezárását szolgáló döntésekhez.

Mint minden rendszer, így a közigazgatási informatikai rendszer is kétféle modellel írható le: az egyik a működési folyamatot bemutató **funkcionális modell**, a másik pedig a

szervezeti struktúrát ábrázoló **strukturális modell**. Egy rendszer **bemeneteit** a **környezetéből** származó erőforrások, igények, és feltételek adják, **kimeneteit** pedig mindazon **célok**, amelyek valamilyen eredmény elérésére irányulnak. [13] Az 1. ábrán a közigazgatási informatikai rendszerek funkcionális modellje látható, melyet Seres György „Fenntartható fejlődés – fenntartható nemzetvédelem" című tanulmányában [13] publikált univerzális rendszermodelljének felhasználásával készítettem. A közigazgatási informatikai rendszerek **környezetét az állam, a gazdaság és a lakosság alkotják**. Funkcionális szempontból ezektől az elemektől származnak a közigazgatási informatikai rendszerek bemeneti adatai, (például egy állampolgár útlevelet igényel), melyek feldolgozását követően döntés, majd határozat születik (az útlevél kiállításáról), mellyel a rendszer teljesítette az elérendő célt. Az eredmény visszacsatolódik a környezetbe, annak megfelelő elemébe (jelen példában az útlevél eljut az igénylőhöz).

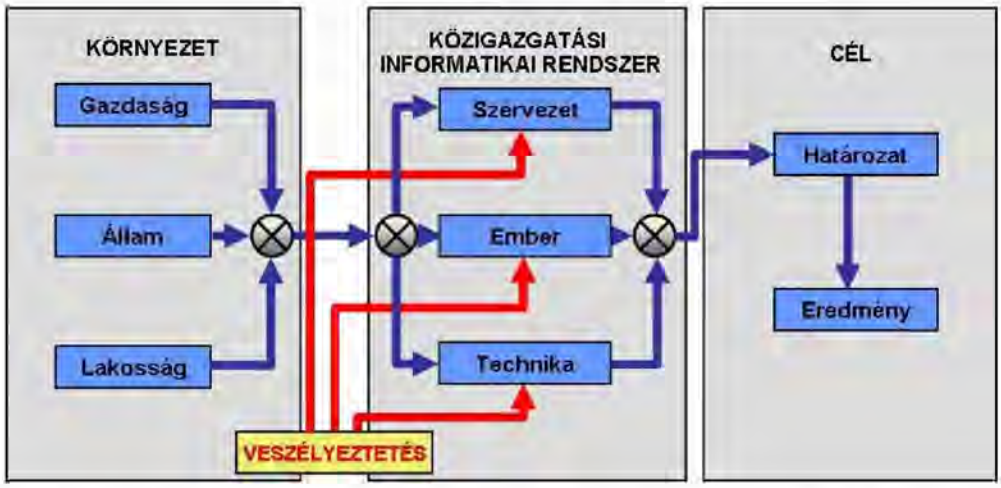



1. ábra: A közigazgatási informatikai rendszerek funkcionális modellje [13 alapján szerkesztette a szerző]

A funkcionális modell a közigazgatási informatikai rendszer működésének bemutatására alkalmas, de a veszélyeztetés szemléltetése rendkívül bonyolult lenne.

Ezért az előző modell analógiájára elkészítettem a közigazgatási informatikai rendszerek strukturális modelljét is (2. ábra), melyben a rendszer környezete és az elérendő cél is változatlan formában jelenik meg. A különbség, a rendszer ábrázolásában van, ahol jelen esetben nem a működési folyamat a lényeges, hanem a közigazgatási informatikai rendszer strukturális felépítése. Ez esetben a szervezet lehet például egy adóhivatal, ahol a rendszer része az ember és a technika. E modell alapján látható, hogy közigazgatási informatikai

rendszer veszélyeztetése a környezetéből és a rendszeren belülről a technikán, az emberen és/vagy a szervezeten keresztül valósulhat meg, például a technika hibájából, emberi gyengeség kihasználásából, vagy esetleg a szervezet nem megfelelő felépítéséből, szabályozási hiányosságokból adódóan.




2. ábra: A közigazgatási informatikai rendszerek strukturális modellje [13 alapján szerkesztette a szerző]

*„Az **elektronikus közigazgatás** megvalósításának **alapját** a **Központi Elektronikus Szolgáltató Rendszer** (Központi Rendszer) biztosítja, amely a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) rendelkezése alapján együttesen **magába foglalja** az **Elektronikus Kormányzati Gerinchálózatot** (EKG), a **kormányzati portált**, a **kormányzati ügyféltájékoztató központot**, az ott megjelenő szolgáltatásokat és ügyintézési lehetőségeket, valamint azok fenntartóit és üzemeltetőit, továbbá biztosítja az **ügyfelek számára az elektronikus ügyfélkapu** létesítésének lehetőségét."* [14: 122.p.]

Az elektronikus kormányzás alapinfrastruktúráját az Elektronikus Kormányzati Gerinchálózat (EKG) biztosítja, míg az ügyfelek számára az informatikai rendszerekhez való kapcsolódás lehetőségét az ügyfélkapu adja, ezért ezeket a következőkben szükségesnek látom részletesebben bemutatni.

### 1.2.2. AZ ELEKTRONIKUS KORMÁNYZATI GERINCHÁLÓZAT

*„Az EKG egy olyan informatikai hálózat, amelynek feladata, hogy a kormányzati és közigazgatási adatbázisokat, hálózatokat és informatikai rendszereket összekapcsolja a vonat-*

*kozó kormányrendeletben meghatározott kormányzati körnek, - valamint a különböző kormányzati szolgáltatások elérhetőségét biztosítsa a civil szféra számára.*" [14: 122.p.]

Az európai folyamatok hatására 2000-ben kormányhatározat formájában is testet öltött a megvalósításának gondolata. Mára a kapcsolódott szervezetek számát tekintve már Európa második legnagyobb hálózata lett.

Az EKG célja és rendeltetése:

1. *„nagy sebességű, nagy üzembiztosságú és magas biztonsági követelményeknek megfelelő, egységes architektúrájú hálózati infrastruktúra biztosítása a civil szféra számára az állami intézmények által nyújtott szolgáltatások eléréséhez (Front-Office feladatok);*
2. *az új infrastruktúrára épülő szolgáltatások és egyes eddig elszigetelt (pl. ágazati) hálózatok elérhetővé tétele a jogosult felhasználók számára (Back–Office feladatok);*
3. *a kormányzati szervek közötti kommunikáció, az adatátvitel költségeinek csökkentése, minőségi szintjének emelése;*
4. *kormányzati szintű, több felhasználó által használt alkalmazások hatékony működtetése;*
5. *olyan infrastrukturális háttér biztosítása, amely alkalmas az elektronikus ügyvitel és ügyintézés feltételeinek megteremtésére, a jövőbeli elektronikus közigazgatás koncepciójának, vagyis az állampolgár és a kormányzat újszerű kapcsolatának kiszolgálására;*
6. *a kétirányú kormányzati kapcsolatok biztosítása a brüsszeli adminisztráció rendszereihez (csak az EKG-n keresztül lehetséges);*
7. *a minisztériumok és a központi intézmények részére biztosítson védett, – security, – szolgáltatások nyújtását és elérését.*" [15]

Az EKG **fő célkitűzése**, a jelenlegi széttagolt, gyakran nem megfelelő kapacitású és biztonságú hálózatok helyett egy nagy sávszélességű, üzembiztos, országos elérhetőséget lehetővé tevő egységes gerinchálózat biztosítása, melyen keresztül nyújtott szolgáltatások üzembiztonsága kiemelten kezelendő és kezelhető. A biztonság növelése céljából minden csatlakozott intézmény kapcsolatrendszere önálló magánhálózatként kerül kialakításra.

Egy másodlagos célja a költségek csökkentése azáltal, hogy ha az intézményeket egy közös hálózatba kapcsolják, akkor a működtetés jóval költséghatékonyabb, mintha minden

intézmény önálló rendszert építene ki és üzemeltetne.

Az EKG hálózata 2004 februárja óta kapcsolódik az Európai Unió TESTA[6] hálózatához, mely a központi alkalmazások elérését biztosítja a tagországok számára.

A kormányzati informatikai rendszerek üzemeltetését a Miniszterelnöki Hivatal megbízásából a Kopint-Datorg Infokommunikációs Zrt. üzemelteti. Napi 24 órás rendszerfelügyeletet, intézménytámogatást és hibaelhárítást biztosítanak az infrastruktúra felhasználóinak és a proaktív EKG HelpDesk támogatás mellett jelentős szakmai segítséget is nyújtanak az intézményi hálózatüzemeltetés számára is. [15]

### 1.2.3. AZ ÜGYFÉLKAPU

*„Az **Ügyfélkapu** a magyar kormányzat elektronikus ügyfél-beléptető és azonosító rendszere. Biztosítja, hogy felhasználói a személyazonosság igazolása mellett, egyszeri belépéssel biztonságosan kapcsolatba léphessenek elektronikus közigazgatási ügyintézést és szolgáltatást nyújtó szervekkel.*" [16] A Központi Rendszer természetes személyek részére nyújtott azonosítási szolgáltatásainak belépési, illetve szolgáltatási pontja.

**Célkitűzése**: a közigazgatásban egykapus, kényelmes, online ügyintézési lehetőség biztosítása az állampolgárok és a szervezetek részére.

*„Az elektronikus Ügyfélkapu szolgáltatásai:*

- *az ügyfél biztonságos, egyszeri azonosítása, majd összekötése az elektronikus szolgáltatást nyújtó intézmény alkalmazásaival;*
- *az ügyfelek a rendszert magát, valamint az egyes elektronikus intézményi szolgáltatásokat böngészőn keresztül érik el (kiegészítve esetleges letöltődő alkalmazásokkal);*
- *a piacon lévő szabványos elektronikus aláíró alkalmazások fogadása;*
- *a rendszer felkészült a jövőbeni alternatív aláíró eszközök (pl. mobiltelefon) használatára, szabványos kapcsolódási felületek kialakításával.*" [16]

Az Ügyfélkapuhoz kötött szolgáltatások:

- eBev szolgáltatások;
- anyakönyvi kivonatok ügyintézése;
- egyéni vállalkozói igazolvánnyal kapcsolatos ügyintézés;

---

[6] A TESTA egy zárt, internettől független gerinchálózat, amely az Európai Unió adminisztrációja és a tagországok kormányzatai közötti információcserét teszi lehetővé.

- forgalmi engedéllyel kapcsolatos ügyintézés;
- adatszolgáltatás letiltása;
- TAJ- szolgáltatások;
- nyugdíj e-ügyintézés;
- foglalkoztatott bejelentése
- magánnyugdíjpénztári szolgáltatások;
- elektronikus felvételi;
- gépjármű-igazgatási ügyekkel kapcsolatos ügyintézés;
- lakcímigazolvánnyal kapcsolatos ügyintézés;
- nemzetközi vezetői engedéllyel kapcsolatos ügyintézés;
- Okmányiroda az interneten. Az egyes ügyek intézésének előkészítése érdekében adatok megadása, időpont foglalása, egyéb szolgáltatások (SMS, ügykezelés, stb.) vehető igénybe. [17]

Az Ügyfélkapu **előzetes regisztrációs folyamat** végrehajtása után vehető csak igénybe, melynek **elengedhetetlen feltétele a személyazonosság igazolása**. Ez történhet **személyes megjelenéssel** valamelyik okmányirodában vagy regisztrációs joggal rendelkező hivatalban (kormányhivatali ügyfélszolgálati irodában, adóhatóság ügyfélszolgálatán vagy külképviseleten), ahol **az ügyintéző végzi el a személyazonosítást és hitelesítést**. Ezen kívül történhet **elektronikus úton** az Ügyfélkapun keresztül a Regisztrációs adatlap kitöltésével és annak **digitális aláírásával**. Az elektronikus aláíráshoz az Elektronikus Aláírás Törvénynek megfelelő **minősített tanúsítvánnyal** kell rendelkezni. Az Ügyfélkapu azon **Hitelesítés szolgáltatók** tanúsítványát fogadja el, amelyek annak kiadásakor **garantálják a személyes megjelenést**, azaz a személyazonosság igazolását. Tehát semmiképpen nem kerülhető el a személyazonosság személyes megjelenéssel történő igazolása.

A **véleményem** az, hogy ez a megoldás **nem túlságosan felhasználóbarát** és nem sokat javít a biztonságon, mivel személyes megjelenéskor is **igazolhatja magát bárki hamis iratokkal**. Ráadásul jogosan azt gondolhatnánk, hogy ha az ügyfél rendelkezik a megfelelő tanúsítvánnyal és elektronikus úton regisztrál, akkor hamarabb igénybe tudja venni az Ügyfélkapu szolgáltatásait, mivel megspórolja a személyes megjelenéssel járó, sok esetben igencsak időigényes várakozási folyamatot, de ez nem így van, mert **a tanúsítványának ellenőrzése 24 óráig tart**. További negatívum az elektronikus aláírásos regisztrációval kapcsolatban, hogy **csak 32 bites Internet Explorer böngészőben működik**,

így a nyílt forráskódú rendszereket használó ügyfelek ezt a lehetőséget nem vehetik igénybe.

**Mindkét regisztrációs módot követően** a megadott **e-mail címre** elküld a rendszer egy egyszer használatos, az aktiváláshoz szükséges belépési kódot, amelyet az Ügyfélkapu felületén öt napon belül **aktiválni kell** (első belépés). Tehát, a személyes megjelenéssel történő regisztráció esetén akár még aznap használhatja is az ügyfél a rendszert, szemben az előbbiekben vázolt elektronikus regisztráció hátrányaival.

Amennyiben az aktiválás nem történik meg időben, illetve elektronikus aláírással történő regisztráció esetében a tanúsítvány ellenőrzési időszakában az ügyfél, mint **ideiglenes regisztrált** is igénybe veheti az elektronikus közigazgatási **szolgáltatások** egy **szűkebb körét**, melyet a közigazgatási szolgáltatók határoznak meg, de például ügyek indítására nincs lehetőség. **Ha 30 napon belül a regisztráció nem kerül hitelesítésre** (elektronikus regisztráció, de elektronikus aláírás nélküli esetben azonosítás bármelyik okmányirodában), az adatokkal együtt **törlődik a regisztráció**.

A **felhasználói név** kis- és nagybetű érzékeny, kizárólag a magyar abc betűiből állhat, számokat és szóközt tartalmazhat. Minimális hossza 4 karakter és tartalmaznia kell minimum 3 különböző karaktert.

A hivatalos informatikai biztonsági protokollnak megfelelően az első belépés alkalmával **meg kell változtatni a jelszót** és az **új jelszónak** legalább nyolc karakternek kell lennie, nem lehet benne ékezetes betű, "@" karakter, nem lehet azonos a felhasználói azonosítóval, kis- és nagybetű érzékeny és meg kell felelnie a bonyolultsági követelményeknek, azaz tartalmaznia kell legalább két számot, valamint kis- és nagybetűt egyaránt.

Az Ügyfélkapu használatakor az ügyfél egyedi azonosító kódja illetve elektronikus aláírás használatával történő regisztráció esetén az aláírt egyedi azonosítója azonosítja az ügyfelet. Sikeres azonosítás esetén, az Ügyfélkapun belépve kiválasztható a kívánt elektronikus szolgáltatást biztosító intézmény, és az ügyfélkapu továbbítja az azonosítási információt a megfelelő intézményi alkalmazás számára. Az intézmény bekérheti az ügyfél intézményi azonosítóját (pl.: adószám), hogy az alapján viszontazonosítást végezzen a központi rendszer felé az általa tárolt ügyféladatok segítségével, viszont a kapun nem kell az ügyfélnek többször azonosítania magát, ha egy bejelentkezés során több szolgáltatást kíván igénybe venni.

Az elektronikus ügyintézés támogatására időbélyeg szolgáltatás és biztonságos ideiglenes tároló hely háttérszolgáltatásokat biztosít az Ügyfélkapu. Az időbélyeg szolgáltatás az adott tranzakció időbeli hitelességének biztosítására szolgál, az ideiglenes tároló hely pedig, lehetőséget nyújt, hogy az ügyfél át tudja venni az intézmény határozatát egy adott ügyben, mely egyben a posta tértivevényes kézbesítésének felel meg, ahol az ügyfél megfelelő kiértesítése az intézmény feladata. [16]

Az ügyfélkapuval voltak problémák, például a 2009. január 20-i ügyfélkapu lassulásának elemzése során az üzemeltető gyorsítási lehetőséget talált és a módosítást elvégezte előzetes egyeztetés és éles üzemben történő tesztelés nélkül, ami viszont február 7-én a Központi Rendszer azonosításkeveredését okozta. Azaz a kapcsolati kód keveredésének köszönhetően 832 esetben a bejelentkezett felhasználó nem a saját adatait láthatta, hanem véletlenszerűen valaki másét. A leginkább érintett az APEH rendszer volt, mivel ismételten nem végezte el a bejelentkező azonosítását. Azonban dokumentumfeltöltés esetén, ha a beküldő és a dokumentumban szereplő személy vagy meghatalmazottja nem volt azonos, akkor a rendszer a dokumentumot nem dolgozta fel, csak értesítést küldött a beküldőnek és a dokumentumon szereplő személynek. A napló elemzéséből, melyet független szakértő végzett el, kiderült, hogy a 832 eset mintegy 90%-a az értesítési tárhely dokumentumainak a listáját érintette, azok kinyitására 100 alatti esetben került sor és ezek közül is csak a visszaigazolások váltak olvashatóvá, mert a többi dokumentum titkosítva volt. **Mindez az éppen bejelentkezett felhasználók adatait érintette, célzottan, más felhasználó adataival történő bejelentkezés lehetősége nem állt fenn.** [18]

## 1.3. AZ INFORMATIKAI RENDSZEREK ALAPVETŐ FOLYAMATAI

Informatikai rendszereink egyre gyakrabban érintettek különböző forrásból származó biztonsági fenyegetésekkel, bizalmas információk illetéktelen megszerzésére irányuló törekvésekkel szemben. Ezért fontos megvizsgálni a rendszerekben lezajló fontosabb folyamatokat. A 3. ábrán vázlatosan egy informatikai rendszer általános folyamatai láthatóak, melyek megtalálhatóak minden informatikai rendszerben, legyen szó akár gazdálkodó célú vállalati rendszerről, akár közigazgatási célú szervezet rendszeréről.


3. ábra: Informatikai rendszer folyamatai [szerkesztette a szerző]

A **bemeneten** juttatjuk be az adatokat az informatikai rendszerbe. Itt történik a tényleges adatfelvételen kívül az adatok osztályozása és a bevitel ellenőrzése is. A közigazgatási rendszerek esetében ez egy igen **sérülékeny pont**, ugyanis ma már az állampolgárok számára számos szolgáltatás (elektronikus ügyintézés) igénybe vehető web alkalmazásokon keresztül. Ezt a sérülékenység forrást a következő fejezetben részletesebben tárgyalom.

A **feldolgozási** folyamatok alakítják át a nyers adatokat értékes, hasznos információvá. Olyan folyamatok halmaza ez, mint például az adatrendezés, összegzés, elemzések, karbantartás, különböző matematikai műveletek, stb.

A **tárolás** során az adatokat valamilyen rendszerezett formában – azok kiterjedésétől és nagyságától függően rekordokba, fájlokba, adatbázisokba, adattárházakba szervezve – elraktározzuk későbbi felhasználás vagy archiválás céljából. Ez egy másik igencsak **sérülékeny része egy informatikai rendszernek**. A leghatékonyabb védelmi lehetőség a megfelelő szabályozás és annak betartása.

Minden informatikai rendszernek rendelkeznie kell továbbá valamilyen visszacsatolással, azaz folyamatosan figyelni kell a rendszer kimenetét, és ha a működés nem megfelelő, akkor a **vezérlő** folyamatok fognak beavatkozni.

A **kimenet** biztosítja az adatok „kivételét" a rendszerből, vagyis az információ közvetítését. Mivel elsődlegesen ezen a ponton lehet hozzájutni az értékes információkhoz, ezért a rendszernek ez a része is **kiemelt odafigyelést igényel**.

Mindezek a folyamatok a rendszer működéséhez szükséges **erőforrásokra** (mint a hardver és szoftver elemek, adatok és a működtető személyzet) támaszkodva működnek. Mint az informatikai biztonság területén már szálló igévé vált mondás is tartja egy informatikai rendszer leggyengébb láncszeme az ember, tehát erre is kiemelt figyelmet kell szentelni.

A 3. ábrán szemléltetett folyamatok során **érzékeny adatok elérése, továbbítása, tárolása, feldolgozása is történik**. Az adatok jelzőjeként használt „érzékeny" szó – melyet mindennapjainkban számtalanszor hallunk ebben a szókapcsolatban – azonban elgondolkodásra késztet. **Mi is számít valójában „érzékeny" adatnak?**

Az adatokból származó információt több szempontból is lehet osztályozni. Például az érzékenységet tekinthetjük úgy, hogy az adott információnak **mekkora a jelentősége** az információ **tulajdonosának szempontjai szerint**, míg fontosságot is megállapíthatunk úgy, hogy a támadó szempontjai szerint mennyire meghatározó a kérdéses információ.

Az információ érzékenysége alapján lehet:

- nyilvános (mindenki számára elérhető);
- személyes (nem tartozik a nyilvánosságra, de ha megtudják, nem okoz nagy problémát);
- bizalmas (olyan információ, amelynek ismerete a versenytársaknak gazdasági előnyt jelent) és
- titkos (ha illetéktelenekhez kerül, akkor a szervezet versenyhelyzetét, akár működését is jelentősen rontja).

A szervezetek hatékony vezetéséhez, rendeltetésének megfelelő működtetéséhez ma már elengedhetetlenül szükséges az informatikai rendszerek használata, az adatok tárolása feldolgozása, esetlegesen továbbítása. Tudvalevő azonban, hogy egy informatikai rendszer előbb említett funkciói számtalan veszélyforrást rejtenek (az információ sérülhet, elveszhet, illetéktelen kezekbe juthat, stb.), melyek jelentős anyagi és erkölcsi károkat okozhatnak, így tehát az alkalmazott informatikai rendszerek biztonságának kialakítása, fenntartása elsődleges szempont kell, hogy legyen. Különösen igaz ez a közigazgatásban alkalmazott informatikai rendszerekre, ahol egy esetleges incidens széles embertömeget érinthet hátrányosan. A megfelelő biztonság többek között csak akkor biztosítható, ha az információ azonos szintű védelméről gondoskodunk, legyen szó akár elektronikus, akár ismeret, vagy papír alapú megjelenési formájáról. Kutatásom során én az elektronikus formával

foglalkoztam részletesen, de természetesen nem lehet figyelmen kívül hagyni a másik két megjelenési formát sem.

A közigazgatási szervezetekben az elektronikus információ **bizalmasságának**, az információ és az azt kezelő rendszer **sértetlenségének**, **rendelkezésre állásának** biztosítása érdekében szükség van **személyi-, fizikai-, dokumentumbiztonsági és elektronikus információvédelmi intézkedések** meghatározására, alkalmazására. Mindezek hatékony megvalósítása érdekében **informatikai biztonsági célok** (egy bizonyos idő alatt milyen biztonsági szintre kívánják eljuttatni az informatikai rendszert) és a **megvalósításuk módjának** meghatározása, a végrehajtandó **feladatok** megfogalmazása, a **végrehajtás nyomon követése és ellenőrzése** szükséges. A célkitűzések elérését elősegítendő, **informatikai biztonsági stratégiát kell kidolgozni**.

## 1.4. A KÖZIGAZGATÁSI SZERVEZETEK INFORMATIKAI BIZTONSÁGI STRATÉGIÁJA ÉS POLITIKÁJA

A megfelelő informatikai biztonságpolitika kialakításának elengedhetetlen követelménye az informatikai biztonság egységes értelmezése, informatikai biztonsági célok és a megvalósításukhoz vezető út, az elvégzésre váró feladatok meghatározása, és végrehajtásuk figyelemmel kísérése, rendszeres felülvizsgálata. [19]

Az e-közigazgatási keretrendszer informatikai biztonsági követelményrendszere a meglévő törvényi és szabályozási környezetre épülő hierarchikus, felülről – a stratégiai szintről – kibontakozó szabályozási rendszert definiál. A legfelső szinten, a **stratégia szintjén** kell lefektetni az alapelveket, ezen a szinten történik a biztonsági célkitűzéseknek és biztonsági elvárásoknak a meghatározása. **A politikák szintjén** kell a stratégiában meghatározottak szerint specifikálni a biztonsági rendszer működését ellátó biztonsági szervezetet, a technikai és szervezési védelmi intézkedéseket. **A szabályzatok szintjén** (melyet részletesen az 1.5 fejezetben tárgyalok) kell leírni, hogy a politika szintjén leírt biztonsági rendszert, az ott meghatározott védelmi intézkedéseket hogyan kell működtetni, ki, miért felelős, stb. [20]

A fentiekből következik, hogy a legfőbb cél – a kockázatokkal arányos biztonsági rendszerek kialakítása – elérésében meghatározó szerepe van a stratégiai szinten lefektetett alapelveknek, célkitűzéseknek, biztonsági elvárásoknak.

Stratégia tervezésére van szükség, ha a megoldandó problémák az intézmény egészére vagy nagy részére kihatással vannak, időben hosszú lefutásúak, jelentős erőforrásokat igényelnek, nagyobb változásokhoz vezethetnek a szervezetben. Az informatikai biztonsági stratégia kialakításának irányvonalát, módját alapvetően meghatározza a szervezet felépítése és információszükséglete.

Az egyértelműen meghatározott célok alapvető feltételei a jó informatikai biztonsági stratégia kidolgozásának, mivel ezek határozzák meg az informatikai biztonsági rendszer fejlesztésének kulcskérdéseit, figyelembe véve a szervezet felépítésének, működésének és informatikai rendszerének jövőbeli alakulását is.

A célkitűzéseket nem csak rövidtávra (1 évnél rövidebb), hanem közép- (1-3 év) és hosszú távra (> 3 év) is meg kell határozni. Ki kell terjedniük a célállapotokra, azaz **az intézmény jelenlegi informatikai biztonsági szintjéből kiindulva meg kell határozni**, hogy az egyes állapotjelző paraméterek (pl. az elérendő biztonsági szint, egy-egy rendszer megengedett maximális kiesési ideje, két kiesés közötti megengedett minimális idő, a rendelkezésre állás, hatékonysági mutatók, stb.) **a jövőben milyenek legyenek**. Valamint ki kell terjedniük az akció célokra is, melyek a folyamat lefolyásával kapcsolatos célkitűzéseket és paramétereket írják elő (például egy-egy új informatikai eszköz beszerzése, új szabályzatok bevezetése, az üzemeltető szervezet átalakítása, a személyzet képzése, stb.). [19]

Muha Lajos megfogalmazásában az infokommunikációs biztonsági stratégia általános célkitűzése „*... a nemzet biztonságának megőrzése azáltal, hogy megakadályozza, vagy elviselhető mértékűre csökkenti a kritikus információs infrastruktúrák elleni sikeres támadások lehetőségét, valamint a bekövetkezett támadások hatását a lehető legkisebbre csökkentse. Ennek érdekében a következő célokat tűzi ki:*

- *a kritikus információs infrastruktúrák elleni támadások hatékony megelőzése;*
- *a kritikus információs infrastruktúrák elleni támadások hatékony kivédése;*
- *a kritikus információs infrastruktúrák elleni támadások hatékony kezelése.*" [21]

Fenti megfogalmazással **egyetértve**, **annak analógiáján** (tekintve, hogy a közigazgatási informatikai rendszerek is a kritikus infrastruktúrák közé tartoznak) a közigazgatásban **az informatikai biztonsági stratégia általános célkitűzése** a közigazgatási szervezet biztonságának megőrzése azáltal, hogy megakadályozza, vagy elviselhető mértékűre csökkenti a szervezet informatikai rendszerei elleni sikeres támadások lehetőségét, valamint a

bekövetkezett támadások hatását a lehető legkisebbre csökkenti, azaz a szervezet informatikai rendszerei elleni **támadások hatékony megelőzése, kivédése, kezelése**.

Az informatikai biztonsági stratégia célkitűzésének ki kell terjednie az informatikai rendszer összes területére, elemére és résztvevőjére, figyelembe véve azok szerepét, funkcionális módosítási igényeit.

Az informatikai biztonsági célkitűzések elérését biztosító feladatokat, a felülvizsgálati szempontokat és a stratégiával szembeni követelményeket az „A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei" című cikkemben [19] tárgyaltam, mely alapján a közigazgatási szervezetek biztonságát szavatoló informatikai biztonsági stratégia akkor éri el az elvárt eredményeket, ha előre definiált követelményeknek eleget tesz. Kutatásaim alapján az **informatikai biztonsági stratégiával szemben az alábbi követelmények határozhatók meg**: [19]

- a felső vezetésnek megfelelő szintű elkötelezettséggel kell bírniuk az informatikai biztonsági rendszer szervezetükben betöltendő szerepével kapcsolatban;
- tartalmaznia kell az informatikai rendszerek fejlesztésére, üzemeltetésére vonatkozó szabályozási és műszaki terveket;
- képezze alapját az informatikai biztonság kialakításához, fenntartásához, fejlesztéséhez szükséges finanszírozással kapcsolatos döntéseknek;
- meg kell határoznia a szükséges változtatásokhoz, tervezéséhez és ellenőrzéséhez szükséges mechanizmusokat;
- ha az intézmény különböző szervezeti egységekből tevődik össze, szervezeti (rész)stratégiákra bontható legyen (ebben az esetben szükség van az egész intézményre vonatkozó ún. vezérstratégiára is);
- bele kell illeszkednie az intézmény működési kereteit meghatározó éves tervezési ciklusokba. [19]

Muha Lajos „A Magyar Köztársaság kritikus információs infrastruktúráinak védelme" című [81] doktori értekezésében többek között meghatározta a Magyar Köztársaság infokommunikációs stratégiájának szerkezeti követelményeit. Az ott leírtakat elfogadva és adaptálva valamint a fentebb általam megfogalmazott követelményeknek megfelelve, a közigazgatási szervezetek informatikai biztonsági stratégiájának kronológiai felépítésére egy változatként az alábbiakat javaslom: [21, 81]

- **a védelem tárgya**: a legfőbb védendő érték az intézményi információk, mert ha

az információ nem elérhető, elvész vagy illetéktelen kezekbe jut, az jelentős anyagi és erkölcsi károkat okozhat;

- **a védelem alanyai**: ki kell terjednie az informatikai rendszer összes területére, elemére és résztvevőjére, beleértve az ügyfeleket, és azokat a szervezeteket is, amelyek az informatikai rendszereket működtetik, vagy ezzel összefüggő szolgáltatásokat nyújtanak;
- **a védendő érdekek**: a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állásának, valamint a rendszer elemeinek sértetlensége és rendelkezésre állásának megőrzése kell, hogy legyen;
- **a szervezet helyzete** a fenyegetések, kockázatok, kihívások tükrében;
- **a fenyegetések,** amelyek a szervezet működését, informatikai biztonságát negatívan befolyásolhatják;
- **a célok a fentebb leírt általános célkitűzéseknek megfelelően**: fel kell készíteni a szervezet működéséhez létfontosságú informatikai rendszereket a támadások hatékony megelőzésére, kivédésére, kezelésére a védendő kör beazonosításával, a potenciális támadások észlelésével és a támadók jogi-technikai elrettentésével, a megfelelő reagáló-kapacitások kialakításával. A védelem terjedjen ki a bekövetkezett támadások hatásának csökkentésére, a helyreállítási idő minimalizálására;
- **a célok megvalósításához szükséges feladatok**: szervezeti koordináció, valamint a már meglévő eredményekre épülő monitorozás és reagálás elmélyítése. További feladat az informatikai biztonsági szabályozók aktualizálása, illetve megteremtése, valamint a biztonságtudatosság és az ismeretek fejlesztése.

Az informatikai biztonsági stratégiában meghatározott feladatok lebontása a politikák szintjén kell, hogy megtörténjen, így a fentiek alapján **az informatikai biztonságpolitikában meghatározandó legfontosabb feladatok** a következők: [19]

- az egész szervezetre vonatkozólag feltérképezni a jelenlegi, és rögzíteni a jövőbeli tervezett informatikai biztonsági rendszer működését, a változások vázlatos határidőinek és mérföldköveinek rögzítése mellett;
- a célteljesítés mérési módjának, időléptékének meghatározása;
- az informatikai biztonsági rendszer céljaira vonatkozó prioritás meghatározása;

- az informatikai biztonsági rendszer fejlesztéséhez szükséges befektetési erőforrások vázolása;
- az adott intézmény szükségleteinek megfelelő informatikai biztonsági javaslatok kidolgozása;
- az informatikai biztonsági szabályozások aktualizálása, illetve megalkotása;
- a már meglévő eredményekre épülő monitorozás és reagálás elmélyítése;
- az alkalmazott informatikai biztonsági megoldások hasznának értékelése;
- a biztonságtudatosság és az ismeretek fejlesztése. [19]

Természetesen ezen feladatok nem állandóak, azokat rendszeresen aktualizálni kell, melynek alapját a rendszeres felülvizsgálatok adják. Vizsgálataim alapján a rendszeres (legalább éves) felülvizsgálatok során az alábbi kérdésekre kell választ adni:

- milyen változások következtek be a szervezet struktúrájában, működésében, illetve a támogató informatikai rendszerben;
- aktuálisak-e az informatikai biztonsági célkitűzések;
- el tudták-e fogadni és be tudták-e tartani az intézmény vezetői és dolgozói az informatikai biztonsági célkitűzéseket;
- mik a vezetők és a dolgozók véleménye és tapasztalata;
- ha nem sikerült megvalósítani a célkitűzéseket, ki vagy mi a felelős;
- ha sikerült, akkor milyen eredménnyel, és mik a tapasztalatok;
- az informatikai beruházások és fejlesztések összhangban voltak-e a célkitűzésekkel;
- a célkitűzéseken milyen módosításokra van szükség? [19]

Az informatikai biztonsági stratégiában kitűzött célok az informatikai biztonsági rendszer fejlesztésének kulcskérdései, így az informatikai biztonsági stratégia kialakításában résztvevők alapvetően meghatározzák a szervezet informatikai biztonságának minőségét, ennek megfelelően véleményem szerint a legfontosabb szerepkörök az informatikai biztonsági célkitűzések meghatározása során a következők:

- **A szervezet felelős informatikusai** végzik el a tervezési szakaszban az informatív adatgyűjtést a külső és belső informatikai környezetről (az intézmény jelenlegi és tervezett jövőbeli felépítése, biztonságának színvonala, a hazai és a nemzetközi trendek, irányelvek, más intézmények informatikai biztonsági fejlesztései, stb.), azok elemzését, a lehetőségek és a még nem látható fenyegetések fel-

derítését. Dokumentálják az információgyűjtés folyamatát, rendszerezik, nyilvántartásba veszik az összegyűjtött információkat, koordinálják azok feldolgozását. **Ők szolgáltatják a célkitűzések megfogalmazásához szükséges háttérinformációkat**, figyelembe véve a belső elvárásokat, a hazai és nemzetközi informatikai biztonság jövőbeli helyzetére vonatkozó előrejelzéseket, az intézmény környezetében (pl.: jogi, gazdasági, politikai, üzleti, piaci, természeti, stb.) bekövetkezett változásokat. [19]

- **Az intézmény felső vezetése és az informatikai vezetők,** beleértve **az informatikai biztonsági felelős (vezető)** személyét is, az informatív adatgyűjtés eredményei alapján **határozzák meg az informatikai biztonsági célokat**, mely alapján kidolgozzák az informatikai biztonsági stratégiát, amit legalább évente egyszer ajánlatos felülvizsgálniuk. Meghatározzák továbbá a szükséges feladatokat és ellenőrzik a végrehajtásukat. [19]

## 1.5. A KÖZIGAZGATÁSI SZERVEZETEK INFORMATIKAI BIZTONSÁGI SZABÁLYOZÁSA

A megfelelő informatikai biztonság kialakítása fokozott körültekintést igényel a közigazgatás rendszereit tekintve, hiszen a közigazgatási informatikai rendszerek nem megfelelő volta miatt bekövetkezett problémák tömegeket érinthetnek.

Kutatásom során a magyar közigazgatás informatikai rendszereinek informatikai biztonsági szabályozási kérdéskörét két szempont szerint vizsgáltam: az egyik a szabályozás oldala, a másik pedig a megfelelő szemléletmód, az informatikai biztonsági kultúra fejlettségének foka. Kutatásom alább részletezett eredményeit „A magyar közigazgatás az informatikai biztonság szemszögéből" című cikkemben publikáltam, melyben felhívtam a figyelmet a meglévő hiányosságokra is. [22]

**Ma már az informatikai biztonság** – figyelembe véve a számítógép-hálózatok, az internet elterjedését és befolyását a szervezetek sikeres működésére – **nem oldható meg pusztán a korábban alkalmazott eszközökkel**, mint ahogy az az ISO/IEC 27001:2005 nemzetközi szabványból is látszik. [23] Tovább súlyosbítja a helyzetet, hogy tapasztalataim alapján sajnos nem csak a szervezetek vezetői, de még az informatikusok egy része sem veszi eléggé komolyan a biztonság fontosságát. Sok helyen még az internet megjelenése

előtti biztonsági tevékenységeket sem alkalmazzák, mint a biztonsági mentés, archiválás, vagy a jelszavas védelem. **Az egyik legnagyobb problémát a megfelelő szabályozás hiányában**, (részleges) megléte esetén a **be nem tartásában** látom. **A másik fő problémakör a megfelelő szemléletmód, informatikai biztonsági kultúra hiánya.** Gyakran anyagi megfontolásokra hivatkozva, időnként időhiányra panaszkodva magyarázzák az informatikai biztonság megteremtésére, fenntartására irányuló alapvető eljárások elmulasztását. Pedig ma már elengedhetetlen a megfelelő informatikai biztonság kialakítása (a befektetett anyagi- és humán erőforrás megtérül), és folyamatos felülvizsgálata. Lépést kell tartani az újabbnál újabb fenyegetések ellen kialakított védelmi megoldásokkal, ugyanis az informatikai biztonság hiánya nem érzékelhető, csupán az annak hiányából fakadó adatvesztés, adatsérülés vagy adatlopás. Általában ezért nem hajlandó pénzt és energiát áldozni rá a felső vezetés mindaddig, amíg be nem következik a baj. Megfelelő kockázatelemzéssel viszont megállapíthatók a rendszer működési hibáiból, az esetleges adatvesztésből fakadó károk és ezek alapján meghatározhatók mindazon intézkedések, amelyekkel e károk csökkenthetők, minimalizálhatók.

A közigazgatás közhatalmat gyakorolva, az állam vagy az önkormányzat nevében **közfeladatokat lát el és jogszabályokat hajt végre.** Figyelembe véve ezt a tényt, továbbá korunk technikai vívmányait alkalmazó e-közigazgatás és az azt kiszolgáló informatikai rendszerek, funkciók rohamos terjedését, belátható, hogy **a közigazgatás területén különösen fontos az informatikai biztonság megteremtése, fenntartása**, mivel annak nem megfelelő voltából adódó problémák **jelentős embertömegeket érinthetnek hátrányosan**. Az 1.3 alfejezetben vázoltam az informatikai rendszerek általános folyamatait és kiemelten kezelendő területként jelöltem meg a tárolás és a humánerőforrás elemeit. Ezen potenciális sérülékenységekre a megfelelő biztonságot támogató technológiák mellett (mint az adatmentés, archiválás automatizálása, stb.), jelentős biztonságnövelő megoldás a kellő szabályozási rendszer kialakítása. Ezért az általam nagyon fontosnak tartott két szempont (szabályozók és a kialakult/átalakulóban levő szemléletmód) alapján vizsgáltam meg a magyar közigazgatás informatikai biztonság oldalát.

### 1.5.1. A SZABÁLYOZÓK

Az informatikai biztonság megteremtésével nemzetközi szervezetek, nemzetközi szabványok foglalkoznak, amelyeknek **egy része** NATO és EU tagságunknak köszönhetően **kötelező érvényű**, **mások** pedig **ajánlások**.

Nemzeti szinten az első komolyabb ajánlásgyűjteményt a Miniszterelnöki Hivatal Informatikai Koordinációs Iroda Informatikai Tárcaközi Bizottsága adta ki 1996-ban. Az ITB ajánlásai közül a 8. a 12. és 16. számú foglalkozott az információs rendszerek biztonságával. [24, 25] Erre az ajánlásgyűjteményre támaszkodtak a jogszabályok, kormányrendeletek egészen 2008-ig. 2008 júniusában váltotta fel a Miniszterelnöki Hivatal megbízásából a Közigazgatási Informatikai Bizottság által létrehozott Magyar Informatika Biztonsági Ajánlások (MIBA). A MIBA a jogszabályok által előírt dokumentumok összeállításához, az eljárásrendek kialakításához, valamint a biztonságos elektronikus szolgáltatások megvalósításához szükséges ajánlásokat tartalmaz. [26]

A MIBA három fő részből áll: [27]

- A **Magyar Informatikai Biztonsági Keretrendszer** (MIBIK) az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokra, és az irányadó EU és NATO szabályozásokra támaszkodik. A biztonságos információs rendszerek irányításáért felelős vezetőknek, a szervezetre vonatkozó követelményeket auditáló szakembereknek ad iránymutatást. Részei a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására fókuszáló Informatikai Biztonsági Irányítási Rendszer (IBIR) [28], az informatikai biztonság hatékony kezelésére irányuló Informatikai Biztonság Irányítási Követelmények (IBIK) [29], valamint az informatikai biztonság ellenőrzéséhez módszertani segítséget nyújtó Informatikai Biztonsági Irányítás Vizsgálata (IBIV). [30]
- A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** az ISO/IEC 15408:2005 és ISO/IEC 18045:2005 nemzetközi szabványokra épül, figyelembe véve a nemzetközi legjobb gyakorlatokat és nemzeti sémákat. Az informatikai biztonság technológiai oldaláról nyújt segítséget elsősorban az informatikai rendszerek fejlesztéséért felelős vezetők illetve az informatikai termékek (operációs rendszerek, hardverek, szoftveralkalmazások) és rendszerek biztonsági megfelelőségét ellenőrző és tanúsítását végző szakemberek számára. [31]

- Az **Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)** olyan kis méretű szervezetek számára nyújt segítséget, ahol nem üzemeltetnek jelentősebb információs rendszert, és/vagy nem rendelkeznek megfelelő szakértelmű humánerőforrással. [32]

A MIBA a Közigazgatási Informatikai Bizottság (KIB) 25. számú ajánlásának egy része. Nem tartalmaz olyan koherens követelményeket és konkrétumokat, mint a KIB 28. ajánlása. Az E-közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár hatalmas terjedelmű és a régi ITB ajánlásokkal ellentétben már tényleg naprakész, rengeteget merítettek az ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 15408:2005, ISO/IEC 18045:2005 és az ISO/IEC TR 13335 nemzetközi szabványokból, valamint az irányadó EU és NATO szabályozáson alapul.

A fentiek azonban csak ajánlások nem jogszabályok, nem kötelező érvényűek.

Néhány éve folyamatosan figyelemmel kísérem a magyar közigazgatás informatikai rendszereinek biztonságára vonatkozó szabályozások alakulását. 2009 őszéig elsősorban a 2005 novemberében életbe lépett Közigazgatási Eljárási Törvény előírásait kellett figyelembe vennünk. Ezért először részletesen áttanulmányoztam és értékeltem a 2005-ös 195/2005 (IX.22) Korm. rendeletet [33], mivel a közigazgatási informatikai rendszerek biztonságát a benne foglaltaknak alapvetően meg kellett volna határoznia. „Az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról" szóló **195/2005. (IX. 22.) Korm. rendelet** (különösen a biztonsági követelményekkel foglalkozó V. fejezet) tanulmányozása során **több hiányosságra, pontatlanságra bukkantam**, melyekkel kapcsolatos észrevételeimet „A magyar közigazgatás az informatikai biztonság szemszögéből" című cikkemben közzé is tettem, és amelyekből néhányat alábbiakban is ismertetek. [22]

A rendelet a biztonsági követelményeket csak olyan informatikai célrendszerre írta elő, amelyben olyan hatósági ügyre vonatkozó elektronikus dokumentumokat tárolnak, amelyek egyidejűleg papír alapon nem állnak teljes körűen a hatóság rendelkezésére, vagy tartós üzemzavar esetén a hatóság nem tudja a folyamatban lévő közigazgatási hatósági ügyet további öt napon belül papír alapon folytatni. [33]. Ezzel kapcsolatban akkor több kérdés is megfogalmazódott bennem, melynek hangot is adtam cikkemben, nevezetesen: Mit kell figyelembe venni a többi rendszer esetében? Ha az információ papír alapon is rendelkezésre áll, akkor már nem is lényeges az elektronikus változatának védelme?

A 15. § (1) a felelősségre vonás alóli kibújás lehetőségét rejtette magában, mivel a műszaki lehetőségeknek megfelelően írta elő az egyszer már azonosított ügyfél vagy hatóság helyébe jogosulatlan harmadik személy belépésének kizárását, de nem határozta meg, hogy mi az a minimális műszaki lehetőség, amit mindenképp meg kell teremteni.

A 16. § (1) előírta ugyan a rendszer működése szempontjából meghatározó folyamat valamennyi eseményének naplózását, de nem rendelkezett a naplók ellenőrzéséről, feldolgozásáról, elemzéséről, pedig anélkül csak felesleges erőforrás pazarlás a naplózás beállítása.

A rendelet 20. § (1) pontja megkövetelte a vírusokkal és más rosszindulatú programokkal szembeni arányos védelmet, de például nem írta elő, hogy minden munkaállomáson legyen megfelelően konfigurált és naprakész adatbázissal rendelkező vírusvédelem, a védelem kivitelezését az adott szervezetre bízta.

Ugyancsak problémás volt a 22. § (1), amely az ügyfelekkel a nyilvános csomagkapcsolt adathálózaton történő kommunikációval foglalkozott, de csak a külön jogszabályban meghatározott párbeszédre épülő elektronikus ügyintézésre vonatkoztatva tette kötelezővé az elektronikus dokumentumok megfelelő rejtjelezési eljárást használva történő küldését és fogadását. Egyéb esetekben az ügyfél külön kérésére biztosíthatta a hatóság azt, de véleményem szerint ma még az ügyfelek nagy része azt sem tudja, hogy van ilyen lehetőség és mit is jelent ez pontosan.

Ugyanilyen hiányosságokra, pontatlanságokra bukkantam a „Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről" szóló 84/2007 (IV.25.) Korm. rendelet vizsgálata során, de már jóval kevesebbel. Ilyen hiányosság volt például az adatbiztonság pontban a mentés résznél *„A Központi Rendszerben tárolt és feldolgozott minden adatról üzemzavar elhárítása céljából adatmentés készül. Ezen mentések biztosítják, hogy adatvesztéssel járó üzemzavar esetén az adatvesztés mértéke még elfogadható mértékű legyen. A kialakított mentési stratégia olyan, hogy legrosszabb esetben is csak korlátozott adatvesztés lehetséges."* [34: 3401.p.] Itt is hiányzott a pontos, konkrét meghatározás, követelmény, ami szerint kidolgozható lett volna a mentési stratégia. A biztonsági naplózásra ez a rendelet is kitért, ugyan már jóval részletesebben, de még mindig nem elég konkrétan.

A fenti hiányosságok kiküszöbölésére való törekvés tapasztalható **a jelenleg érvényben levő 223/2009. (X. 14.) Korm. rendeletben** [35], melyről általánosságban elmondha-

tó, hogy **felhasználásra került benne a KIB ajánlásgyűjteménye**. Ennek következményeként sokkal részletesebb, konkrétabb paragrafusokból tevődik össze, mely sokkal egyszerűbben használható. Például a fentebb kifogásolt naplózás témakörben sokkal részletesebb előírásokat tartalmaz a naplóállományok megőrzési idejére, védelmére, tárolására, ellenőrzésére vonatkozóan is.

Azonban **még mindig tartalmaz hiányosságokat és hasonlóan jelen van benne a pontatlanság**. Például rögtön az elején az 1. § (2) pontja szerint a minősített információt kezelő rendszerekben a rendeletben rögzítetteken kívül külön jogszabályokban foglaltak alkalmazása is szükséges, de jó lett volna, ha bele is kerül legalább a hivatkozás, hogy mely jogszabályokra gondolt a jogalkotó.

Az értelmező rendelkezések 2. § e) pontja szerint az „*információbiztonsági fenyegetés: mindazok az események, amelynek bekövetkezése esetén a rendszerhez fűződő érzékeny információk jogosulatlanul kerülnek más birtokába, vagy válnak megismerhetővé, vagy válnak elérhetetlenné, vagyis sérülnek az e rendeletben megfogalmazott adat- és információbiztonságra meghatározott követelmények*". [35] Ebből arra lehet következtetni, hogy az adat- és információbiztonságra meghatározott követelmények csak akkor sérülnek, ha jogosulatlanul más birtokába, vagy nyilvánosságra kerülnek, esetleg elérhetetlenné válnak, de ezek szerint, ha például módosítják, meghamisítják, akkor nem sérülnek az információbiztonsági követelmények.

Említésre méltó továbbá az informatikai biztonsági felügyelet rendszere részben megfogalmazottak is, melyek szerint az informatikai biztonsági felügyelő „*folyamatosan figyelemmel kíséri a központi rendszert üzemeltető szervezetekkel, valamint a központi rendszer számára szolgáltató szervezetekkel kötött megállapodásokban foglalt informatikai biztonsági követelmények betartását; … véleményt nyilvánít a központi rendszerhez csatlakozni kívánó szervezetek és szolgáltatások biztonságáról, … jogosult a … feladatkörébe tartozó szervezet informatikai biztonsággal összefüggő tevékenységének és ellátottságának ellenőrzésére; … jóváhagyja a központi rendszer üzemeltetője, adatkezelője biztonsági irányelveit, szabályzatait és eljárásrendjeit; … az arra jogosult jóváhagyását megelőzően szakmailag ellenőrzi az elektronikus közszolgáltatást nyújtó szervezetek biztonsági irányelveit, szabályzatait és eljárásrendjeit; … határidő tűzésével felhívja az érintett szervezetek vezetőit a … tudomására jutott eltérések felszámolására, ellenőrzi a követelmények megvalósítását; … kapcsolatot tart a Nemzeti Hírközlési Hatóság … a biztonságos elektronikus*

*szolgáltatásokat nyilvántartó szervezeti egységével; ... ellenőrzi a biztonságirányítási rendszerek működtetését.*" [35] Még felsorolni is sok, nem hogy végrehajtani. Véleményem szerint **egy ember** felelősségteljesen, maradéktalanul **képtelen ennyi feladatot ellátni**. Mindezek végrehajtására megfelelő apparátust **kell létrehozni**, amit irányít, felügyel, ellenőriz az informatikai biztonsági felügyelő.

A rendelet egyáltalán nem foglalkozik az informatikai szolgáltatások tanúsítási kérdéskörével, ami egy ilyen mértékű szolgáltatást végző szervezetrendszer esetében, mint a közigazgatás elengedhetetlen az informatikai biztonság területén.

Még lehetne sorolni a további problémákat, de már a fenti példákból is jól látható, hogy bár a korábbi rendeletek hiányosságait javították e rendeletben, ugyanakkor újabb pontatlanságokat is vittek bele. A rendelet terjedelme is bizonyítja, hogy megalkotói törekedtek mindenre kiterjedő, teljes körű jogszabályt alkotni, ami azonban még mindig korrekciókra szorul.

A közigazgatás területén kardinális kérdés a személyes adatok védelme, mivel a rögzített adatok igen jelentős hányada – véleményem szerint több mint 90 százaléka – személyes adat vagy személyes adathoz kötődik. **Az adatok védelme** azonban **nem oldható meg csupán a technika védelmére koncentrálva**, meg kell óvni azt a szervezet tagjaitól is különböző szabályok felállításával és betartatásával. Ezért olyan nagy a jelentősége a megfelelő szabályok pontos megfogalmazásának és a szabályozás betartatásának. A **humán biztonság**nak természetesen belső és külső aspektusa is van, amely során egyrészt a szervezetnek törekednie kell a saját dolgozóinak a tevékenységét minél jobban beszabályozni, másrészt az idegenek jogosulatlan adathozzáférését lehetetlenné tenni.

A magyar közigazgatás informatikai rendszereinek a törvények, szabályzatok, előírások oldaláról történő vizsgálata során arra a megállapításra jutottam, hogy a kialakításukra, biztonságos üzemeltetésükre vonatkozóan **a törvényi előírások legfelső szinten többékevésbé megszülettek** ugyan, azonban **nem teljes körűek**, félreértelmezhetőek. Igaz, hogy léteznek a részletekre vonatkozó **ajánlások, szabványok**, azonban azok **implementációi az alsóbb szinteken sok esetben nem, vagy csak részlegesen kerülnek megvalósításra**. Jó példa volt ennek magyarázatára a Belügyminisztérium Informatikai Biztonsági Politikája kiadásáról szóló 12/2004. (BK 12.) BM utasítás, mely a felettes szerveknek feladatul szabta, hogy kényszerítsék rá az alárendelt szerveket a felsőbb szinten meghatározott biztonságpolitika illetve az informatikai biztonsági szabályzat alapján megfogalmazott

szabályozások, technológiai eljárások végrehajtására, de finanszírozási támogatás nem volt mögötte. Így a 2004-es utasítás nem gerjesztette azt a folyamatot a rendőrségnél, amit kellett volna. Ezt a megállapításomat támasztották alá a Budapesti Rendőr-főkapitányság informatikai osztályán Csillag Imrével 2008-ban folytatott interjúm során elhangzottak. Mindenhol egységesen meg kellett volna valósítani az informatikai biztonság szabályozásának kérdéseit. Bizonyos területeken, mint az adatvédelemmel kapcsolatos szabályozások, műszaki normák, iratkezelési szabályzatok, elektronikus adathordozók kezelésével kapcsolatos szabályzatok, stb. azért megvalósultak, mint az informatikai biztonság kérdésének szegmensét képező szabályozások, csak nincsenek egységes keretbe foglalva. Katasztrófa tervek, mentési szabályzatok léteznek ugyan, de az aktualizálásukkal gondok vannak, melynek legfőbb oka humánerőforrás problémákkal magyarázható (személyi állomány csökken, a megfelelő képességekkel nem rendelkeznek, külső auditáló szakemberek bevonása a bizalmasság megsértését eredményezheti).

Az előbbieknek azért is egyre nagyobb a jelentősége, mivel a hatályos magyar jogszabályok szerint 2009-től az összes közfeladatot ellátó szervezetnek kötelező a minősített elektronikus iratkezelő szoftvertermékek használata. [36]

### 1.5.2. A SZEMLÉLETMÓD

A megfelelő szabályozás mellett nem elhanyagolható tényező a döntéshozásban, a kivitelezésben, felhasználásban és az üzemeltetésben résztvevők hozzáállása, szemléletmódja. Az elkötelezettség ugyanis elengedhetetlen a kívánt minőségű informatikai biztonság kialakításához, fenntartásához. Ennek demonstrálására jó példa a következő: Krasznay Csaba és Szigeti Szabolcs 2006. októberi tanulmányában [37] elemezte és megkérdőjelezte az Ügyfélkapu biztonságát. A tanulmány megállapításaira hivatkozó képviselő felvetésére az Országgyűlés 2007.10.29-i ülésén a következőképpen reagált a MeH EKK államtitkára: „*A hackerek számára is nyitott az ügyfélkapu, mint minden magyar állampolgár számára természetesen, szabályosan a hackerek is használhatják; ha megpróbálják hackelni, annak következményei vannak.* ***Nyilvánvalóan tettek már kísérletet, és ön sem tud beszámolni arról, hogy sikeres lett volna egyetlenegy kísérlet is. Azt tudom tehát kijelenteni felelősen, hogy az Ügyfélkapu természetesen biztonságos****, biztosítja azt, hogy a magyar állampolgárok és a magyar vállalkozások nyugodtan, minden behatástól mentesen bevallhassák adataikat.*" [38]

Arra alapozva, hogy nincs tudomásunk sikeres támadásról, nem jelenthető ki felelősen, hogy egy informatikai rendszer biztonságos-e, vagy sem. Az Ügyfélkapu egyébként is a manapság egyre divatosabb támadási célpontok közé sorolható, mivel a felmérések azt mutatják, hogy drasztikusan növekednek a web alkalmazások elleni támadások. Köszönhető ez annak, hogy a hagyományos (a hálózati réteg és az operációs rendszer gyengeségeit kihasználó) támadások oly régen folynak már, hogy a védelem ezen a területen igencsak megerősödött. Ennek köszönhetően mára már annyira megnehezítették a hackerek dolgát, hogy inkább máshol (a kisebb ellenállás irányában) próbálkoznak, ami ma az alkalmazások sebezhetőségeinek kihasználása.

Egy másik, ugyan 2004-es példa, de a helyzet sajnos nem sokat változott azóta: Csillag Imre a Baranya Megyei Rendőr-főkapitányság auditjával kapcsolatosan megjelent cikkében leírta, hogy az audit riportjára az ORFK gazdasági főigazgatójának reakciója az volt, hogy amíg a rendőrautókat nem tudják tankolni, addig nem tud erőforrásokat fordítani az informatikai biztonság területére. Véleménye szerint kisebb a kockázata, ha egy szabályozás nem változik, mintha egy rendőrautó nem tud kimenni az utcára, mert nincs elegendő pénzügyi erőforrás az üzemeltetésére. [39]

A fentieken kívül még számos példát lehetne bemutatni arról, hogy felelős beosztásban levő döntéshozók mennyire elhanyagolhatónak tartják azt, hogy informatikai rendszereik biztonságosak-e vagy sem. Az elsődleges szempont, hogy működjön, amíg valami nagy baj nem történik.

## 1.6. JAVASLATOK A SZABÁLYOZÁSI ÉS SZEMLÉLETMÓDBELI PROBLÉMÁK MEGOLDÁSÁRA

**Megállapítható**, hogy a **hiányosság** a magyar közigazgatás informatikai rendszereinek biztonsága területén **nem elhanyagolható**. Ahhoz, hogy a felvetett problémákra megoldásokat keressünk, több oldalról kell megvizsgálnunk a kérdést. A megközelítés függ az adott informatikai rendszer nagyságától, fajtájától, védettségétől, fejlettségétől, erőforrásaitól, a tárolt, feldolgozott, illetve továbbított információ minőségétől, a rendszer felhasználóitól és a rá vonatkozó szabályozóktól.

Az egyik fő probléma tehát, hogy **az alsóbb szintű közigazgatási informatikai rendszerek esetében** főleg finanszírozási problémákra és szakember hiányra hivatkozva **az irányadó rendeleteket, ajánlásokat nem veszik figyelembe**. Ennek legfőbb okát a

meglévő jogszabályi hiányosságban, pontatlanságban, valamint a megfelelő, rendszeres ellenőrzés és tanácsadás hiányában látom. **Javaslom** e probléma megoldásának elősegítésére, egy olyan, nemzetközi szabványon és jó gyakorlatokon alapuló **információbiztonsági törvény kidolgozását**, amely a közigazgatási szervek informatikai biztonságát széleskörűen szabályozná. Jó alapot biztosít hozzá a **223/2009. (X. 14.) Korm. rendelet, de a törvényben szükségesnek látom a megfogalmazások pontosítását**, a hiányosságok pótlását. A törvény szintű jogszabályi javaslatom indokaként említhető, hogy az magasabb szintű jogszabály, mint egy kormányrendelet, ezért annak elfogadása és esetleges módosítása országgyűlési hatáskörbe tartozik. Ennélfogva joggal várható, hogy a jogalkotók annak elkészítésekor és elfogadásakor nagyobb körültekintéssel járnak el.

Javaslom továbbá egy szakértőkből álló **információbiztonsági szervezet létrehozását**. Az információbiztonsági szervezet szakértői – az érvényes jogszabályok (pl. az általam javasolt törvény), ajánlások alapján – meghatározott rendszerességgel belső auditot végeznének az egyes közigazgatási szervezetek információs rendszerein, **feltárnák** azok **hiányosságait**. **Javaslatokat tennének, iránymutatást, esetleg szakmai segítséget adnának** a hiányosságok kiküszöbölési lehetőségeire. Munkájuk során olyan hasznos tapasztalatokra is szert tennének, mellyel a javasolt információbiztonsági törvény kidolgozását, majd későbbi korrekcióját is hatékonyan tudnák segíteni. Létezik ugyan a Nemzeti Hálózatbiztonsági Központ, amely alapvetően internetes incidenskezelést végez, de a fentebb említett tanácsadói és belső auditori feladatokat nem lát el. Az általam javasolt szervezet megalakulhat a Nemzeti Hálózatbiztonsági Központ bázisán is, kiegészülve a fentebb felsorolt feladatokkal és jogkörökkel.

Az is előfordul, hogy a rendszer üzemeltetői, a felhasználók tisztában vannak a felelősségükkel és tájékozottak az informatikai biztonság terén, de az adott szervezet **informatikai biztonsági szabályzat**a (IBSZ) már elavult, vagy nem létezik. Ennek **megújítása**, vagy **létrehozása** jelentős segítséget nyújthat. Ha az IBSZ megújítása, vagy elkészítése nem elegendő, előfordulhat, hogy a komplett informatikai biztonsági stratégiát, számítógépes hálózatot, szerepköröket újra kell tervezni. Ez rengeteg munkát és szakértelmet kíván, azonban, ha egyszer jól létrehozzuk, akkor már egyszerűbb a felügyelete, szabályozása. Ebben az esetben is célszerű külső szakértő bevonása.

Egy másik igen jelentős sérülékenységi forrás a nem megfelelő szemléletmód. Ez a legnehezebben kiküszöbölhető hiányosság is egyben. Tapasztalatok szerint a multinacioná-

lis cégeknél, ha valami új, vagy szokatlan (informatikai rendszer) kerül bevezetésre, egyrészt kisebb ellenállást vált ki, másrészt rövidebb ideig tart. Ez véleményem szerint betudható a magasabb szintű szakértelemnek, naprakészségnek és a vezetői hatásnak, illetve a szabályrendszer felelősségteljesebb betartásának. **A szemléletmód megváltoztatásához vezető út első lépcsőfokának azt tartom**, hogy ne csak a biztonsági rendszer hiányosságaként fellépő, olykor súlyos károk hatására gondoljunk az informatikai biztonság elemzésére, hanem **próbáljuk megelőzni** azt. Ez persze nem egyszerű feladat, rengeteg tényező játszik szerepet a probléma megoldásában. Az emberi erőforrásokat jóval nehezebb a biztonságos működtetésre bírni, mint az informatikai eszközöket. Egy mondás szerint a fő biztonsági rés mindig a szék és a számítógép között áll.

E fő probléma megoldására a következőket javasolom:

- szerepkörök pontos meghatározása;
- számítógép kezelői, üzemeltetői oktatások szervezése, akár intraneten keresztül;
- informatikai biztonsági oktatások tartása célirányosan üzemeltetőkre illetve felhasználókra (gyakorlati is);
- felelősségek tudatosítása.

A „social engineering”[7] típusú támadás sikerességét is jelentős mértékben csökkenti a minél több informatikai biztonsági **tréning, szituációs gyakorlatok és biztonságtudatossági oktatás**.

Véleményem szerint ezek a javaslatok nagymértékben segítenének a közigazgatási informatikai rendszerek egységes biztonságossá tételében.

[7] Az emberi hiszékenység, segítőkészség kihasználása.

# KÖVETKEZTETÉSEK

**Néhány alapvető fogalom**, – mint informatikai és információs rendszer, informatikai- és információbiztonság – **tisztázását,** valamint a közigazgatási informatikai rendszer **meghatározását** követően **megalkottam** a közigazgatási informatikai rendszerek **funkcionális és strukturális modelljét.**

**Bemutattam** az elektronikus kormányzás alapinfrastruktúráját alkotó Elektronikus Kormányzati Gerinchálózatot és **elemeztem** az ügyfelek számára az informatikai rendszerekhez való kapcsolódás lehetőségét biztosító Ügyfélkaput.

**Megvizsgáltam az informatikai rendszerek alapvető folyamatait** (bevitel, feldolgozás, tárolás, vezérlés, kimenet) és arra a **megállapításra jutottam**, hogy ezek közül a közigazgatás rendszereit tekintve **a legkritikusabb az adatok rendszerbe kerülési, kivételi folyamata, valamint a tárolás**. Ezeknek a folyamatoknak **a megfelelő szabályozása** jelentős mértékben **növelheti** az informatikai biztonság szintjét.

Fenti okokból kifolyólag részletesen tanulmányoztam az e-közigazgatási keretrendszer informatikai biztonsági követelményrendszerét, **elemeztem** a szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételeit és **megfogalmaztam az informatikai biztonsági stratégia célkitűzéseit**.

Ezt követően **meghatároztam** az **informatikai biztonsági stratégiával szemben** támasztott **követelményeket és** bemutattam egy lehetséges **felépítését**.

A célkitűzések alapján **megállapítottam** az informatikai biztonság kialakítása során a célkitűzéseknek megfelelő legfontosabb végrehajtandó **feladatokat, azok rendszeres felülvizsgálatának kérdéseit és követelményeket**.

Megállapítható, hogy a kellő mértékű és részletességű, ugyanakkor nem túlzott **szabályozás kardinális kérdés** a biztonságos informatikai rendszerek kialakításának és működtetésének területén. Ennek következetes kivitelezéséhez **elengedhetetlenül szükség van egyértelmű, pontosan megfogalmazott törvényi szabályozásra**.

Ezért megvizsgáltam a közigazgatás rendszereire informatikai biztonság szempontjából jelenleg érvényben levő, **irányadó kormányrendeletet,** valamint elődeinek tartalmát, és **azt állapítottam meg**, hogy a felsőszintű jogszabályok, előírások is **mutatnak hiányosságokat**. Véleményem szerint a nagyobb probléma mégis az, hogy **a megfelelő implementációk az alsóbb szinteken nem, vagy csak részben jönnek létre**. Ennek okát legfőképpen a megfelelő szakember és a finanszírozás hiányában látom.

**Javaslatot tettem** egy nemzetközi szabványon és jó gyakorlatokon alapuló, a közigazgatási szervezetek informatikai biztonságát széleskörűen szabályozó **információbiztonsági törvény kidolgozására**, továbbá egy szakértőkből álló **információbiztonsági szervezet létrehozására**, mely a közigazgatás egyes szervezeteinél rendszeres **belső auditori** és **tanácsadói** feladatokat látna el. Munkájuk során szerzett hasznos tapasztalataikat pedig a javasolt információbiztonsági törvény kidolgozásában, majd későbbi korrekciójában hasznosíthatnák.

**Megvizsgáltam** a közigazgatási informatikai rendszerek kialakításában, szabályozásában, működtetésében, felhasználásában részt vevő humán oldal **biztonságtudatosságának fejlettségi szintjét** és **arra a megállapításra jutottam**, hogy **hiányzik az összhang az informatikai vezetők, igazgatók és döntéshozók szemléletében,** mely **túlzott, vagy nem elégséges befektetéseket** és nem hatékony informatikai kockázatkezelési programokat **eredményez**.

**A megfelelő szemléletmód kialakítása** törvényi szabályzásokkal, **előírásokkal nem megvalósítható**, de jelentős szerepet játszhat benne az oktatás. **Javaslom** a közigazgatás különféle informatikai felkészültségi szintű dolgozói számára számítógép kezelői, üzemeltetői és **informatikai biztonsági oktatások szervezését**, akár intraneten keresztüli **tréningek** formájában, **szituációs gyakorlatok** és **tesztvizsgák** bevezetését az egy szintre hozás és továbbfejlesztés érdekében.

# 2. FEJEZET
# A KÖZIGAZGATÁSI INFORMATIKAI RENDSZEREK ELLENI TÁMADÁSI FORMÁK, SÉRÜLÉKENYSÉGEK

A 21. század természetes és egyben megállíthatatlan folyamata az egyes országok informatikai infrastruktúrájának rohamos fejlődése. Ezzel egyidejűleg azonban az informatikailag fejlettebb országok egyre nagyobb veszélynek vannak kitéve, hiszen az internet a világgazdaság civilszférájától egészen a kormányzatokig mára csaknem mindenhol jelen van. Beláthatjuk, hogy minél nagyobb, átfogóbb és fejlettebb egy adott ország informatikai infrastruktúrája, annál nagyobb károkat lehet okozni egy informatikai rendszer elleni támadással. Ezt bizonyítja az is, hogy az elmúlt években számtalan hacker-akcióról hallhattunk, melyek túlnyomó része az informatikailag legfejlettebb ország, az Egyesült Államok ellen irányult. Célpontnak számítanak többek közt a katonai létesítmények, a bankok, a pénzügyi rendszerek, a közlekedés, a távközlés, a rendőrség, valamint az energiaellátás egyaránt[8], melyek esetleges támadása során az állami infrastruktúra is érzékenyen károsodhat, de célpont lehet akár az otthoni személyi számítógépünk is. Egyedi gépeket támadhatnak pusztán szórakozásból, de azzal a céllal is, hogy a későbbiekben felhasználják azt egy komolyabb rendszer ellen indított támadás során. Téves és egyben veszélyes elképzelés egy hétköznapi állampolgártól az, hogyha betörnek a gépükbe semmi gond, amíg az nem zavarja látványosan munkájukat, hiszen úgysincs semmi rejtegetni valójuk, nincs a gépükön semmi fontos dolog, amit különösebben védeni kellene. Nem számolnak azzal a lehetőséggel, hogy számítógépük kapacitását felhasználhatják például egy DDoS[9] támadás végrehajtásához, mint egy Botnet[10] hálózat tagja, mellyel a támadók nagyobb eséllyel képesek fontos rendszerek feltörésére. Bármely információs rendszer elleni támadás kritikus lehet, de a közigazgatás informatikai rendszerei elleni támadások nagy jelentőséggel bírnak, hiszen míg a gazdál-

---

[8] Egy viszonylag friss példa, a 2010 júniusában felfedezett, eddig egyedülálló, komoly biztonsági védelemmel ellátott ipari folyamatirányító rendszereket megcélzó Stuxnet féreg, melynek valószínűsíthető célpontja az iráni atomlétesítmények működésének leállítása. A féreg 4 zero-day sérülékenységet használ ki. [40]

[9] Distributed Denial of Service: Olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatás igénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet. [41]

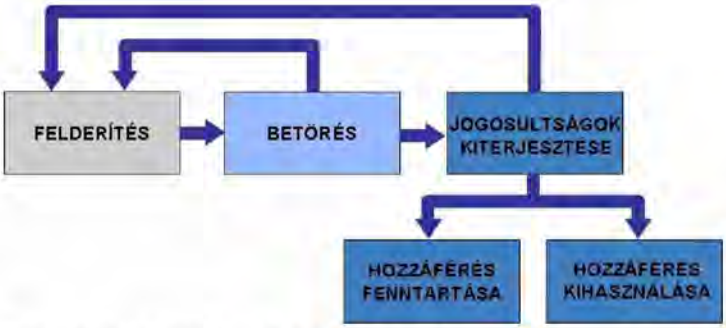
[10] Különböző vírusokkal és trójai szoftverekkel a támadó irányítása alá vett számítógépek hálózata, melynek erőforrásait a saját céljára használja fel.

kodó szervezetek vagy az otthoni felhasználók saját biztonságukat kockáztatják, addig a közigazgatás informatikai rendszereinek támadása esetén széles körben az állampolgárok adatai megsérülhetnek, nyilvánosságra kerülhetnek, meghamisíthatják és vissza is élhetnek vele, így ezen a területen kiemelt fontosságú a megfelelő védelem kialakítása.

Az informatikai rendszerek elleni támadási módszereket több szempontból, különféle módon lehet csoportosítani. **Véleményem szerint** a közigazgatási informatikai rendszerek esetében **a leghatékonyabb védelmi politika kialakítása szempontjából döntő jelentősége van, hogy az adott támadást helyileg honnan hajtják végre**. Ugyanis más jellegű védelmi intézkedést igényel, ha a rendszeren kívülről, esetleg belső segítséggel, vagy belülről hajtják azt végre. Ennek megfelelően a közigazgatási informatikai rendszereket tekintve, a veszélyeztetés forrásának szempontjából a következő típusú csoportosítás szerint vizsgáltam a támadási módszereket, sérülékenységeket:

- **Külső támadás**: amikor a szervezet ellen kívülről, hálózaton keresztül az informatikai rendszer építőelemeinek valamely sérülékenységét kihasználva, belső segítség nélkül indítanak támadást. Azaz a fenyegetés valamilyen külső forrásból származik és célja anyagi- politikai-, gazdasági- vagy katonai előnyszerzés; [42]
- **Belső támadás**: amikor a szervezeten belülről indítva, a rendszer valamely humán eleme által, vagy annak tudatos illetve akaratlan segítségét igénybe véve történik a támadás;
- **Külső és belső támadás kombinációja**: amikor a szervezeten kívülről indítva, a rendszer valamely humán elemének tudatos illetve akaratlan segítségét igénybe véve kívülről történik a támadás.

Ahhoz azonban, hogy hatékonyan tudjunk védekezni a támadások ellen pontosan tisztában kell lennünk azzal, hogy mi is az, ami ellen ki kell alakítani a megfelelő védelmet. A fenyegetések meghatározásához ismernünk kell a támadások felépítését. Ha megértjük a támadók által használt alapvető megközelítéseket, jobb és hatékonyabb védelmi intézkedéseket tudunk alkalmazni, mivel tudjuk, hogy mire számíthatunk. Egy támadás alapvető lépéseit a 4. ábrán foglaltam össze.




4. ábra: Egy támadás alapvető lépései [szerkesztette a szerző]

**Felderítés:** első lépésként a támadó megvizsgálja a célpontot, hogy felmérje a jellemzőit, és azonosítsa a gyenge pontjait. Ezek nem csak technikai jellegű információk, hanem beleértendő a támogatott szolgáltatások, protokollok, potenciális sebezhetőségek, a rendszer belépési pontjai, az áldozat domain nevei, IP címei, az e-mail címek szerkezete, és a weblapok tartalma mellett a szervezet felépítése, az alkalmazottak elérhetőségei, az irodák elhelyezkedése, a beléptető-rendszer, a munkarend is, mely jellemzők mind-mind fontos segítséget nyújtanak a támadások kivitelezéséhez. A felderítő fázisban információ a rendszerről kézi és automatizált technikával is szerezhető. Például egy nem biztonságos web alkalmazás esetén már kézi technika (erőteljes böngészés, hibaüzenetek provokálása, stb.) segítségével lehet azonosítani az internetes alkalmazást, annak felépítését, meg lehet tudni, hogy van-e információszivárgás és milyen információ szivárog, fogékony-e az alkalmazás injekciós támadásra, stb. Az 5. ábrán látható hibaüzenetből megállapítható, hogy az alkalmazás nagy valószínűséggel Microsoft adatbázist használ (az SQL hibaüzenetből látszik) és a fájljai a d:\downloads\AltoroMutual_v6\website\bank\ könyvtárban tárolódnak. Egy ilyen hibaüzenet provokálása még csak riasztást sem eredményez a célpont rendszerében. A támadó az így megszerzett információk alapján tervezheti meg a támadást.

**An Error Has Occurred**

Summary:

**Syntax error (missing operator) in query expression 'username = '' AND password = 'a''.**

Error Message:

System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression 'username = '' AND password = 'a''. at System.Data.OleDb.OleDbCommand.ExecuteCommandTextErrorHandling(OleDbHResult hr) at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMS dbParams, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteCommandText(Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteCommand(CommandBehavior behavior, Object& executeResult) at System.Data.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.OleDb.OleDbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) at System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbCommand command, CommandBehavior behavior) at System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) at Altoro.Authentication.ValidateUser(String uName, String pWord) in d:\downloads\AltoroMutual_v6\website\bank\login.aspx.cs:line 68 at

5. ábra: Provokált hibaüzenet

**Betörés:** a célpont felmérése után a következő lépés a hibák kihasználásával hozzáférés a rendszerhez. A védelmi megoldásoktól függően elképzelhető, hogy a támadónak a betörést több lépésben kell végrehajtania melyekhez újra felderítő műveleteket kell végrehajtania.

**Jogosultságok kiterjesztése:** miután a támadó hozzáférést szerzett a célrendszerhez, megpróbálja fokozni a privilégiumait. Adminisztrátori jogosultságokat vagy olyan jogokat próbál megszerezni, amelyekkel a legtöbb alrendszerhez hozzáférhet. Itt is szükség lehet újabb felderítő folyamatokra és az egyes alrendszerekbe való betörésekre.

**Hozzáférés fenntartása:** a rendszerbe való bejutás után a támadó lépéseket tesz annak érdekében, hogy a jövőben könnyebben bejusson (backdoor programokat telepít, vagy kihasznál egy olyan felhasználói fiókot, amely nem rendelkezik védelemmel).

**Hozzáférés kihasználása:** egyértelmű meghatározója a támadó motivációja és, hogy milyen jogosultságot sikerül megszereznie. A támadó célja lehet a rendszer forgalmának lehallgatása, abból információ gyűjtése, saját célú felhasználása, adatbázisában tárolt adatok megszerzése, megrongálása, meghamisításuk következtében téves döntések előidézése, szolgáltatások működésének akadályozása, megbénítása. Bármely célból történjen is a támadás, még ha a támadó tevékenysége során a rendszer nem is sérül, az információk illetéktelen kezekbe kerülésével azok bizalmassága (mely az informatikai rendszerekkel szemben támasztott egyik alapkövetelmény) mindenképpen sérül, és jelentős veszteséget okozhat a támadást elszenvedőnek, nem beszélve arról, hogyha fizikai károkozás is történik. [42]

Minden lépés végrehajtása során a támadó törekszik arra, hogy eltüntesse a betörésre utaló jeleket (naplófájlok módosítása, törlése).

Kutatásom következő jelentős mérföldköve a fenti lépéseket segítő különböző támadási formák, sebezhetőségek feltérképezése volt. Ezt a fejezet elején bemutatott csoportosítás alapján, vagyis külső-, belső- és kombinált veszélyforrások szerint végeztem el. Ehhez a területhez kapcsolódva megvizsgáltam továbbá a támadók különböző csoportjait, motivációit, eszközeit, célpontjaik alakulását, valamint a támadások hatásait is.

## 2.1. KÜLSŐ VESZÉLYFORRÁSOK

Mára az otthonok nagy részében ugyanúgy megtalálható az internet, mint a kormányhivatalokban, vagy épp az üzleti életben. Az internetre kapcsolódó szerverek mindegyike szá-

mos adatbázist tartalmaz, vagy különböző, valamilyen egyéb szolgáltatást nyújt. A felhasználók és a kiszolgálók száma napról napra növekszik, csakúgy, mint a szolgáltatások sokrétűsége. Az, hogy a háztartások felhasználói nem, vagy csak részben alakítják ki a megfelelő védelmet, mondván, hogy nekik nincs védeni való információ a számítógépükön, nagymértékben segíti a fontosabb rendszerek elleni támadások sikeres kimenetelét. Ugyanis ez a hiányzó vagy gyenge védelem lehetőséget biztosít például az adott számítógép botnetbe szervezésére, melynek kapacitásával már sokkal gyorsabban meg lehet fejteni akár egy komolyabb rendszerbe való bejutáshoz szükséges titkosított információt is.

A közigazgatási informatikai rendszerek ellen végrehajtható külső támadások lehetőségeit, eszközeit három szint sérülékenységeinek kihasználása szempontjából vizsgáltam, a hálózat, az operációs rendszer és a rendszereken telepített alkalmazások szintjén.

### 2.1.1. A HÁLÓZAT SÉRÜLÉKENYSÉGEIT KIHASZNÁLÓ MÓDSZEREK

**A közigazgatás számítógépes-hálózaton keresztül nyújtott szolgáltatásai, annak igénybevétele, az igénybevevők köre napról-napra nagyütemben bővül és szélesedik**, amiből eredően az üzemeltetett informatikai rendszerei egyre nagyobb mértékben válnak sebezhetővé számítógép-hálózati támadások kapcsán. **Naponta akár több ezer sikeres, regisztrált feltörés történhet a világhálón**. Ebből legalább **két-, háromnaponta egy nagyobb rendszer** esik áldozatul valamilyen hacker-támadásnak. [43] Az Amerikai Védelmi Minisztérium évente 200-300 ezer sikertelen betörési kísérletet ismer el, de ez közel sem egyezik meg a tényleges kísérletek számával, mert elég sok kísérlet nem kerül a nyilvánosság elé.

Egy számítógépes-hálózat erőforrásai elleni támadások a legtöbb esetben kívülről egy külső hálózatból érkeznek, leggyakrabban az internet felől. Az ilyen külső támadások a teljes hálózat internetre vezető átjáróját illetve a részhálózatok kapcsolódási pontjait érintik először. Ezért aztán a hálózati kapcsolatok kialakítása során a megbízhatóság, a rendelkezésre állás növelése érdekében egyre nagyobb számú kapcsolók alkalmazásával jelentős veszélyforrásokat is vihetünk a rendszerbe, mert a hozzáértés hiánya, a nem megfelelő konfigurálás épp ellenkező hatást gyakorolhat védeni kívánt hálózatunkra. A kapcsolók megfelelő körültekintés nélküli alkalmazása, biztonsági lehetőségeinek nem megfelelő konfigurálása jelentős sérülékenységet jelenthet rendszerünkben. [44]

Kutatásaim során feltérképeztem azokat a számítógép-hálózatokat fenyegető leggyakoribb támadási módszereket, melyek bárki által az internetről letölthető és némi hozzáértéssel alkalmazható eszközök segítségével végrehajthatók, és amelyek alkalmazására a közigazgatási informatikai rendszerek esetén is számítani kell [45]:

- aktív szolgáltatások keresése, elemzése;
- hallgatózás;
- hamisítás;
- kapcsolat lopás;
- hamis bejelentkező felület;
- fragment támadás;
- elárasztásos támadás;
- puffer túlcsordulás;
- szolgálatmegtagadás típusú támadások.

Az **aktív szolgáltatások keresése, elemzése** a támadások 1. lépésének (felderítés) kiváló módszere. Az éppen hallgató portok átvizsgálásával ugyanis megállapítható, hogy milyen elérhető szolgáltatások vannak a rendszerben, de még akár az is, hogy a célpont operációs rendszere Microsoft termék-e[11]. A támadó a felderített szolgáltatások ismert sérülékenységeit kihasználhatja, vagy alkalmazhat automatikus sérülékenység-keresőket, illetve további fontos információhoz juthat a web szerver válaszainak részletes elemzése által. A talált nyitott portokon kapcsolódhat a célgéphez, vagy nagy mennyiségű adatot küldve megpróbálhatja kiváltani a puffer túlcsordulás (buffer overflow) állapotát, mely veszélyeztetheti a hálózat és a benne lévő számítógépek biztonságát, érzékeny információk felfedéséhez illetve elvesztéséhez esetleg a munka megbénításához vezethet.

A **hallgatózás** (sniffing vagy snooping) szintén a felderítés „hasznos" eszköze, melynek segítségével a támadó a hálózati interfész úgynevezett promiscious, válogatás nélküli módba kapcsolása révén megszerezheti, lehallgathatja a helyi hálózat forgalmát, így könnyen hozzájuthat minden, a hálózatra kiküldött nem titkosított adathoz. Azonban ez a módszer csak akkor alkalmazható, ha a helyi hálózat minden csomagot elküld az adott gépnek (pl. hub esetén), vagy ha valamilyen ARP[12] táblát illetve kapcsolót befolyásoló

[11] A Microsoft operációs rendszerek portjai semmilyen előzmény nélküli FIN (final data from sender: a TCP kapcsolat végét jelző flag) csomagra nem válaszolnak.

[12] ARP (Address Resolution Protokol): számítógépes hálózatokon használatos módszer egy ügyfél hardvercímének meghatározására, ha annak csak az IP-címe ismeretes.

módszerrel ráveszi a köztes elemeket, hogy felé is továbbítsák az adatcsomagokat. Az ilyen ARP táblát befolyásoló aktív támadási módszerek esetében az is elképzelhető, hogy az eredeti címzett meg sem kapja az adatokat.

**Hamisítás** (IP[13], ARP, DNS[14], blind spoofing[15]): IP spoofing esetében a támadó a forráscímet, míg ARP spoofing esetén a MAC[16] címet hamisítja az Ethernet csomagban. A DNS spoofingnak több megvalósítási módja létezik, de a cél minden esetben azonos, a célpont DNS kiszolgálójának manipulálása annak elérése céljából, hogy a támadó egy számára megfelelő IP cím - hostnév hozzárendeléshez hozzáférjen. A blind spoofing abban különbözik az előzőektől, hogy ezeknél a támadásoknál a támadó gépe nem kap közvetlen választ a hálózatról, hiszen a válasz a hamisított címre érkezik. Ezen eszközök segítségével a hálózati támadást indító számítógép elrejthető, megszemélyesíthető a rendszer egy másik számítógépe, ezáltal jogosultságok szerezhetők IP alapján kontrollált erőforrásokhoz (például adatbázisokhoz), vagy helytelenül beállított tűzfalak esetében kijátszhatók tűzfalszabályok azáltal, hogy a forrás IP a belső címtartományból való, így megbízhatónak tűnik a hálózat számára. Megvalósítható man-in-the-middle támadás[17] felépítése, zavarható a hamis IP cím eredeti tulajdonosának kommunikációja (IP ütközés - gyakori a kezelhetetlenül magas csomagvesztés, illetve a teljes forgalmazási képtelenség). Mindez azonban ma már lokális hálózaton belül valósítható meg könnyebben, mivel az interneten nem vehető át tetszőleges gép IP címe. Korábban előfordult, hogy a hamis feladóval elküldött IP adatcsomagok gond nélkül átmentek a hálózaton, de ma már sok helyen elvégzik a nem az adott hálózatba tartozó címekről érkező adatcsomagok szűrését (ingress filtering). Az ARP spoofing, mivel adatkapcsolati rétegbeli címeket használ, csak olyan eszközök ellen hajtható végre sikeresen, amelyek egy hálózaton vannak a támadóval, hiszen adatkapcsolat szin-

---

[13] IP (Internet Protocol): segítségével kommunikálnak egymással az internetre kötött csomópontok, meghatározza az egymásnak küldhető üzenetek felépítését, sorrendjét stb.

[14] DNS (Domain Name System): egy, a hálózaton elosztott adatbázis, mely az internetre kapcsolódó számítógépek Domain neveit tartalmazza és lehetővé teszi a nevek átfordítását IP címekre.

[15] Blind spoofing: Vak hamisítás, az IP-címhamisításnak az az esete, amikor a támadó gépe nem kap közvetlen választ a hálózatról, hiszen a válasz a hamisított címre érkezik.

[16] MAC (Media Access Control): a szabványügyi hivatal által a gyártónak kiadott, fizikailag a gyártó hálózati interfészeibe belesütött egyedi, 12 darab hexadecimális szánjegyből álló számsorozat, amellyel az interfész azonosítható. Az első hat hexadecimális számjegy az IEEE által felügyelt, a gyártót vagy az eladót azonosítják. A fennmaradó hat hexadecimális számjegyet a gyártó adminisztrálja.

[17] Man-in-the-middle támadás: két fél közötti kommunikáció kompromittálása úgy, hogy a kommunikációs csatornát (tipikusan valamilyen számítógépes hálózatot) eltérítve mindkét fél számára a másik félnek adja ki magát a közéjük ékelődött támadó. a kommunikáló felek számára a partnert személyesíti meg. Kevésbé súlyos esetben, csak a kommunikáció megfigyelésére képes, viszont súlyosabb esetben a kommunikáció tartalmát is módosíthatja anélkül, hogy a felek ezt észrevennék.

ten csak ezekkel lehet kommunikálni. Azaz ez a módszer hatékony eszköze lehet egy belső támadás kivitelezésének. A szerverek vagy hálózatok ellen irányuló támadások, behatolási kísérletek elég nagy százalékában használják ezeket a technikákat.

Egy ilyen típusú támadást lehetővé tevő sérülékenységre hívta fel a figyelmet a Nemzeti Hálózatbiztonsági Központ 2010.10.14-én. Az Oracle Open Office előző nap felfedezett olyan sérülékenységei váltak ismertté így, melyeket kihasználva a támadók spoofing támadásokat tudnak végrehajtani, megkerülhetnek bizonyos biztonsági szabályokat, módosíthatnak bizonyos adatokat és feltörhetik a felhasználó sérülékeny rendszerét. [46]

Ide tartozik egy még frissebb, sokakat érintő hír is, miszerint: *„több, igen súlyos hibát javított a Chrome böngészőben a Google, amelyek kihasználásával többek között spoofing támadás kezdeményezhető, kritikus adatokhoz lehet hozzáférni, és átvehető az ellenőrzés a rendszer felett. A 9.0.597.107-es változat már mentes a fenti sebezhetőségektől.*" [47]

**Kapcsolat lopás** (session hijacking): Ez egy manapság igencsak népszerű támadási módszer web alkalmazások sérülékenységeinek a kihasználása során. Mivel a közigazgatásban is jelentős mértékben megnövekedett a web alkalmazások üzemeltetése, így kiemelt figyelmet érdemel, ugyanis a munkamenet általában nem csak a felhasználók nyomon követésére szolgál, hanem azok azonosítására is. A felhasználó rendszerbe történő bejelentkezése során először egy authentikáció (a felhasználó azonosítása) zajlik le, általában úgy, hogy a munkamenetben elhelyezésre kerül egy a felhasználó kilétére utaló változó (például felhasználó azonosító). Ezt követően az authorizáció során történik annak ellenőrzése, hogy a felhasználó számára egy funkció elérhető-e jogosultságai alapján, melyek szintén a munkamenetben kerülnek tárolásra. Így, ha a támadónak sikerül egy bejelentkezett felhasználó munkamenetét megszerezni, akkor ezzel együtt megszerzi annak személyazonosságát is, az ő nevében lesz képes használni a rendszert. Belátható, hogy közigazgatási rendszer esetében hangsúlyozottan nem kívánatos, hogy az állampolgárok adataival a támadó visszaélhessen, módosíthassa, törölhesse, stb.

Ebből a szempontból sebezhető lehet számos igen széles körben használt alkalmazás, mint a Facebook, a Twitter, az Amazon, a Foursquare, a Github, a Flickr és a Windows Live (Hotmail) is. Annál is inkább, mivel a Firesheep nevű Firefox kiegészítő segítségével a támadónak nincs más dolga, mint titkosítatlan internetkapcsolaton keresztül az oldalsá-

von hálózati szkennelés kezdeményezését követően megjelent nyilvános Wi-Fi hálózathoz csatlakozó felhasználók által éppen igénybe vett fiókok kiválasztása, amelyekre kattintva átvehetővé válhat az azok feletti irányítás. [48] A közigazgatásban igaz eddig még csak próbálkozások voltak vezeték nélküli hálózaton történő szolgáltatások nyújtására, de ez a példa egyrészt elgondolkodásra késztet e téren, másrészt vezetékes hozzáférés esetén is számolni kell kapcsolat lopással végrehajtott támadásra.

A web alkalmazások térhódítása hangsúlyossá tette a **Fake login - Hamis bejelentkező felület** típusú támadásokat, melyek lényege, hogy bejelentkezés előtt elindul egy – az eredetihez megtévesztésig hasonlító – bejelentkező felület. Az áldozat azt hiszi, hogy ez az eredeti bejelentkező ablak és beírja a jelszavát, amit a program elment és valami hibaüzenet után a felhasználó megkapja az eredeti bejelentkező felületet. Közigazgatási web alkalmazásokkal kapcsolatban ugyan eddig még nem merült fel ez a típusú támadási forma, de pénzügyi szervezetek elleni támadás részeként már előfordult. 2006 novemberében phishing támadás érte a Raiffeisen Bank magyarországi ügyfeleit. Egy angol nyelvű adathalász levélben kérték a bank ügyfeleit, hogy adataik egyeztetése céljából keressék fel a bank oldalait, de a hamis linkek mögött egy magyar nyelvű raiffeisenhu.com hamisított weboldal várta az oda gyanútlanul ellátogatókat, ami megszólalásig hasonlított a bank online felületéhez. A fő cél ugyan adathalászat volt, de a kivitelezéshez szükség volt más támadási módszerek kombinálására is. A raiffeisenhu.com tartományt egy hamis japán címről jegyezték be, a leveleket pedig zombihálózat(ok) segítségével küldték szét. [49]

**Fragment támadás**: Ebben az esetben a csomagok nem egyben érkeznek meg a célponthoz, hanem apró fragmentek formájában – a célpont rakja össze őket –, ezáltal megnehezítve a csomagszűrő tűzfal dolgát, mert a csomag részeit külön-külön vizsgálva sokkal nehezebben azonosítható egy támadási kísérlet. Például az overlapping fragment támadás esetén a támadó az első csomag fejlécében olyan szolgáltatást ad meg, amit a tűzfal átenged, az utána következő csomagok viszont már egy szűrt szolgáltatás felé irányulnak, kártékony tartalommal.

**Elárasztásos támadás** (SYN flood[18], Smurf, Fraggle, ICMP flood[19]): SYN flood esetében a támadó SYN üzeneteket küld az áldozatnak, aki erre SYN-ACK[20] választ küld,

[18] SYN flood: SYN elárasztás. SYN: a TCP fejlécének 14. bitje jelzi, ha egy új kapcsolat felépítése kezdődik.
[19] ICMP flood: ICMP elárasztás. ICMP: az IP segédprotokollja.
[20] ACK: acknowledgement, nyugtázás.

és erőforrást foglal le. A támadó viszont nem küld ACK választ, így előbb-utóbb az áldozat leterhelődik. Smurf támadás során broadcast[21] ping üzenetet küldenek a hálózatra, forráscímként az áldozat IP címét megadva. Erre a hálózat összes bekapcsolt gépe válaszol, ezzel minden egyes csomagra akár több száz válaszcsomag érkezhet, ami elárasztja az áldozatot. A Fraggle támadás a smurf támadás továbbfejlesztése, ami UDP[22] echo csomagokat küld a hálózatra. ICMP flood támadás során pedig a támadó annyi ICMP echo csomagot küld az áldozatnak, hogy az már nem tudja azokat feldolgozni, és elérhetetlenné válik.

A The Register 2010. január 29-ei cikkében arról olvashatunk, hogy többek közt a CIA és a Paypal kezelésében lévő web szerverek ellen nagy mennyiségű flood-támadást észleltek, melynek köszönhetően a szerverek CPU-terhelése 40-50-szeresére ugrott fel, 1-2 perces üzemszünetet okozván. [50]

**Puffer túlcsordulás**: Oka, ha a kiszolgáló egyik szolgáltatása több adatot kap, mint amennyit fel tud dolgozni. Egy hálózati kiszolgáló pufferének túlcsordulásakor a kiszolgálón tárolt adatok megsérülhetnek vagy elveszhetnek, a szolgáltatások vagy maga a kiszolgáló is leállhat. Sok programban találkozhatunk ilyen hibákkal, amelyeket azonban a fejlesztők folyamatosan javítanak. A puffer túlcsordulásnak komolyabb következményei is lehetnek. Ha a túlcsorduló adatok által felülírt memóriaterület a számítógép utasításvermához tartozik, és a támadó tudja is ezt, akkor a pufferbe kerülő adatokat elő tudja úgy készíteni, hogy az utasításverembe csorduló rész új, értelmes utasításokat tartalmazzon, ily módon akár teljes körű hozzáférést kaphat az adott számítógéphez.

**Szolgálatmegtagadás típusú támadások**: az előbbi eszközök, vagy azok esetleges kombinálása segítségével meggátolható a hálózati szolgáltatások működése, vagy akár teljesen le is fagyaszthatják a rendszert. Az ilyen jellegű támadások zavart, anyagi kárt is okozhatnak a kérdéses hálózat üzemeltetőjének.

2007. áprilisban és májusban az úgynevezett „észt kiberháború" hívta fel a világ figyelmét arra, hogy az elektronikusan működő rendszerek bizonyos esetekben komoly sebezhetőséggel működnek. Az informatikailag különösen fejlett észt közigazgatás, kormányzat és a pénzügyi szektor komoly károkat szenvedett el DDoS-támadás következtében. Az orosz kormányzat támogatását élvező ifjúsági mozgalom vállalta magára a felelősséget és vezetőjük, Konsztantyin Goloszkokov véleménye szerint ez nem „kibertámadás",

[21] Broadcast: minden gépnek szóló üzenet.

[22] UDP: User Datagram Protocol, az internet egyik alapprotokollja, datagram alapú szolgáltatás biztosítása, azaz rövid, gyors üzenetek küldése esetén használatos.

hanem „kibervédekezés" volt, tiltakozásul a tallinni második világháborús szovjet emlékmű eltávolítása ellen. Úgy vélte, semmiféle illegális tevékenységet nem végeztek, mindössze annyit tettek, hogy bizonyos weboldalakat igen sűrűn látogattak meg, s az már az üzemeltetők hibája, hogy ezt a forgalmat nem bírta el a rendszerük. Katrin Pargmae, az Észt Informatikai Központ szóvivője elmondta, hogy a bankokat, közintézményeket érő, másodpercenként 100 megabájtos forgalmat generáló támadások összesen 178 országból érkeztek. [51]

A sikeres támadás végrehajtása érdekében a támadók a fenti módszereket kombinálják egymással és különböző eszközök (mint a kártékony kódok, port szkennerek, jelszó feltörő programok, stb.) segítségével hajtják végre. Például **hijack támadás** vihető véghez, ha mondjuk snifferrel összegyűjtik egy kapcsolat információit, behatolnak a TCP csatornába, és egyidejűleg egy Denial of Service támadással elnémítják az eredeti felhasználót. Ennek pontos időzítésű, hibátlan kivitelezésére nem sok esély van. Alesete a „**The man in the middle**" támadás, amikor a támadó két kommunikáló fél közé úgy épül be, hogy mindkettővel ő kommunikál, azaz minden forgalom áthalad rajta, s meg tudja hamisítani mind a parancsokat, mind pedig a választ.

Több okból is szükséges foglalkozni a **kártékony kódokkal**[23], egyrészt mert ez a leggyakoribb eszköz, amit a támadók alkalmaznak az egyes támadási módszerek végrehajtása során, másrészt pedig az előző fejezetben megállapított szabályozási hiányosságok növelik a kártékony kódok használatának lehetőségét.

Eleinte, a floppylemezek korszakában az egyetlen kártevőfajta a klasszikus vírus volt, azonban az azóta bekövetkezett fejlődés nem csak a technikai eszközöket érintette, a kártevők is haladtak a korral. Ahogy bővült a lehetőségek tárháza, úgy jelentek meg egyre másra az újfajta kártevők. A hálózatok elterjedése és az internet kiépülése alapjában változtatta meg a terjedés módját, és a vírusok körében is megfigyelhető konvergencia során olyan programkódok jelentek meg, amelyek több ártalmas funkciót egyszerre valósítanak meg. Mára a boot-vírusok szinte teljesen eltűntek, hiszen ezek akkor aktivizálódnak, amikor a BIOS rendszerbetöltést kísérel meg a fertőzött lemezről, viszont a cserélhető adathordozókról való rendszerindítás jelentősége igen visszaesett. Napjainkban a kártevők elsősorban a helyi hálózatokon és a világháló különböző csatornáin (levelezés, chat (pl.:

[23] Ang.: Malicious Softwares (malware) – rosszindulatú számítógépes programok, mint vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszer működését láthatatlanul ellenőrző rootkitek összefoglaló neve.

IRC[24], MSN[25]), fájlmegosztó rendszerek, stb.) terjednek. Ezeket a rosszindulatú programokat nem nevezhetjük minden esetben vírusnak, mert az eredeti definícióinkat már nem fedik le. Minden olyan szoftver rosszindulatúnak minősíthető, amely nem a számítógépes rendszer vagy hálózat rendeltetésszerű működését biztosítja. A trendeket vizsgálva kijelenthető, hogy amíg az elmúlt években a klasszikus számítógépvírusok és férgek száma csökkent vagy stagnált, addig az újonnan detektált malware szoftverek (trójai programok, keyloggerek, adware, spyware programok) száma egyre emelkedett.

A Nemzeti Hálózatbiztonsági Központ 2011. I. negyedéves jelentésében olvashattuk, hogy kiberbűnözők a februári – Franciaország által elnökölt – G20 csúcsra vonatkozó állományokra vadászva a francia pénzügyminisztérium több mint 150 gépébe törtek be, s állítólag más minisztériumokat is támadás ért. A tettesek e-mail csatolmányba bújtatott trójai kártevőt küldtek a kiszemelt címzetteknek – többségükben a G20 csúcson dolgozó minisztériumi munkatársaknak. [52: 41.p.]

Mindegyik malware-nek megvan a maga speciális funkciója, ami a hálózat forgalmának megzavarásától az adatlopásig vagy a rendszer feletti vezérlés átvételéig terjedhet, így a számítógép-hálózati támadások minden típusánál alkalmazhatók. A rosszindulatú szoftverek módosíthatják a programokat, erőforrásokat foglalhatnak le, veszélyeztethetik az adatok integritását, hardverhibát eredményezhetnek, eltávolításuk pedig egyre speciálisabb eszközöket, időt, energiát, egyes esetekben pedig különleges szakértelmet igényelhet. [42]

A felsorolt sérülékenységeket, eszközöket felhasználva kivitelezhető passzív (a hálózati forgalom lehallgatása) vagy aktív támadási forma, melynek célja általában a hálózat egy elemének kiiktatása, megszemélyesítése, esetleg az egész hálózat megbénítása.

„*A hálózatok támadására nagyon sokféle módszer létezik, így a támadóknak csak a megfelelő szakértelemre van szükségük, hogy a támadás eszközeit a megfelelő eljárásokkal kombinálják.*" [42]

Fentiek alapján kijelenthető, hogy a felsorolt támadási módszereket kombinálva és ötvözve a rendelkezésre álló eszközökkel, a megfelelő védelem hiányában lehetővé válik a **közigazgatási informatikai rendszerekbe történő sikeres behatolás**, melynek kapcsán a

[24] Internet Relay Chat sokkal elterjedtebb nevén IRC egy kliens–szerver alapú kommunikációt lehetővé tevő csevegőprotokoll

[25] A Microsoft ingyenes online kommunikációs szoftvere.

**támadó akadályozhatja, lehetetlenné teheti annak működését, illetve hozzáférhet adatokhoz.**

### 2.1.2. AZ OPERÁCIÓS RENDSZEREK BIZTONSÁGI KÉPESSÉGEI

Az operációs rendszerek sérülékenységének csökkentésére rendszeresen javítókódokat jelentetnek meg a gyártók, melyek alkalmazása, ezáltal a rések befoltozása már csak a felhasználón múlik. A rendszeres frissítések kikényszerítése már a szabályozási kérdéskörbe tartozik, melyről bővebben az előző fejezetben írtam.

Ma Magyarországon az állami-, közigazgatási rendszerekben túlnyomórészt Microsoft operációs rendszereket alkalmaznak mind szerver, mind kliens oldalon. Azonban nem hagyható figyelmen kívül az a tendencia, hogy **világszerte egyre gyakrabban állítják át az egyes országok közigazgatási, katonai, oktatási, stb. rendszereit, alkalmazásait – legfőképpen a költséghatékonyabb működtetés érdekében – nyílt forráskódú rendszerekre**. Mint például:

- 11 000 számítógépet migrál Linux-ra a német külügyminisztérium [53];
- az Egyesült Királyság kormánya felgyorsítaná a nyílt forráskódú szoftverek felhasználásának ütemét az állami kiszolgáló apparátusban [54];
- a Linux-ra váltáson dolgozik az amerikai hadsereg [55].

Így tehát az operációs rendszerekkel kapcsolatban azok sérülékenységei helyett elsősorban **arra a kérdésre kerestem választ, hogy a közigazgatásban nyílt vagy zárt forráskódú operációs rendszert használjunk-e.**

A munkaállomások tekintetében egyszerű a kérdés megválaszolása, mivel oktatásunkban, a háztartásokban olyan jelentős mértékben meghatározó a zárt forráskódú operációs rendszerek használata, hogy a közigazgatási humánerőforrás jelentős részének teljes átképzését igényelné egy platformváltás.

Figyelemmel kísérve a Puskás Tivadar Közalapítványon belül működő Nemzeti Hálózatbiztonsági Központ (CERT-Hungary) incidens jelentéseit, az operációs rendszer sérülékenységeit tekintve a két platform között lényeges eltérés nem fogalmazható meg. Ezért a kérdés megválaszolása érdekében, hogy nyílt vagy zárt forráskódú operációs rendszert használjunk-e, a **biztonsági képességek és teljesítmény szempontjából hasonlítottam össze** a legelterjedtebb **zárt forráskódú szerver** platform legfrissebb verziója (Microsoft Windows Server 2008), valamint az **egyik leggyakrabban használt GNU/Linux disztri-**

**búció szerver** változata (Ubuntu Linux Server Edition) által biztosított leggyakoribb szolgáltatásokat.

Az alkalmazottak hatékony munkavégzéséhez, az ügyfelekkel való kommunikációhoz a közigazgatásban is elengedhetetlen a saját levelező szerver nyújtotta szolgáltatás, így **fontosnak találtam megvizsgálni** a **biztonságos levelezéshez szükséges képességeket**. A levelezéshez hasonlóan ma már szinte az is elengedhetetlen feltétele egy szervezet sikeres működésének, hogy saját honlappal rendelkezzen, és amennyiben mindig friss adatokat kíván mutatni az ügyfeleknek, akkor dinamikusan frissülő oldalakat kell használnia, ami gyakran saját szerveren történik különböző alkalmazások összekapcsolásával. Ezért fontosnak találtam **megvizsgálni és összehasonlítani az operációs rendszerek webkiszolgáló képességének is a teljesítmény és biztonsági jellemzőit**. **Vizsgáltam továbbá a tanúsítványkezelés körülményeit** is a két kiválasztott platformon. A **biztonsági házirendben** megadható beállítások, azon belül is a **felhasználó- és a jelszókezeléssel** kapcsolatosak egy rendszer biztonságos üzemeltetésében kulcs szerepet játszanak, ezért elengedhetetlennek tartottam a **két platform képességeit ebből a szempontból is összehasonlítani**. Egy közigazgatási informatikai rendszer szervere esetén, de még otthoni felhasználóknak is ajánlott a **tűzfal** használata, mivel védelmet jelent főleg külső támadások ellen, de a belső adatkiszivárogtatást is megakadályozhatja, így ez sem maradhatott ki a tanulmányozott szolgáltatások köréből.

Az összehasonlítás alapját képező **teszteket azonos körülmények között** működő (memória-, háttértár kapacitás, alap-telepítés, **kizárólag a disztribúció csomagjai által biztosított képességeket felhasználva**) **virtuális gépeken végeztem** el. A Microsoft Windows Server 2008 esetében nem telepítettem további alkalmazásokat, amelyek nem érhetők el a telepítőlemezről, illetve a „Szolgáltatások hozzáadása" menüből. Az Ubuntu Linux Server Edition esetén pedig csak a gyári alap tárolókat használtam és nem adtam hozzá további szoftverforrást[26], valamint nem telepítettem a csomagkezelőn keresztül nem elérhető programot. A **teljesítmény méréséhez egy scriptet használtam**, mely **a gazda gépen mérve a virtuális gépek által használt processzor mennyiséget, mind a két platform terheltségét képes monitorozni**. A script azt a képességet használja ki, hogy a Linux rendszerekben a folyamatok adatai egy fájlban tárolódnak és mivel a virtuális gép is egy folyamat a gazdagép számára, ezért a fájlban megtalálható az eddigi használat processzor-

26 A Linux disztribúciók általában csomagokkal dolgoznak, melyekhez ún. tárolón keresztül juthatunk.

ideje jiffyben[27]. Bizonyos időközönként megvizsgálva a fájlt, százalékosan megkaphatjuk a jiffy különbségéből, hogy az adott időintervallumban milyen mértékben használta a folyamat a processzort.

A témakörben folytatott **kutatásom, illetve az elvégzett tesztek eredményeit** részletesen a „Nyílt és zárt forráskódú operációs rendszerek leggyakoribb szolgáltatásainak vizsgálata biztonság és teljesítmény szempontjából" [56] valamint a „Comparing the webservers of the opensource and the closed source operation systems" [57] című cikkeimben publikáltam. A fentiekben ismertetett **szolgáltatásonként elvégzett teszteket**, azok **eredményeit** és az azok alapján **levont következtetéseimet** az alábbiakban mutatom be.

**Levelező kiszolgáló** [56]

A biztonságos levelezéshez szükséges képességek vizsgálata során a levelező kiszolgálók vonatkozásában **a következőket állapítom meg**:

- a Windows Server 2008, ellentétben a Linux-szal, POP3[28] szolgáltatást nem nyújt;
- **mindkét rendszer SMTP[29] szolgáltatása teljesíti a** visszakövethetőség és a **titkosítás követelményeit**, mivel mindkét rendszer biztosít lehetőséget naplózás beállítására, valamint SSL[30] titkosításra, mellyel az üzenetek lehallgatás elleni védelme megoldható. **A titkosítás módja a szabványokhoz igazodik, így abban lényegi eltérés nem fedezhető fel**;
- **hozzáférés korlátozására** is ugyanúgy **nyújt lehetőséget mind a két rendszer**;
- a legnagyobb **lényegi különbség**, hogy **a Windows Server 2008 nem nyújt semmilyen vírus vagy kéretlen reklámlevél szűrési lehetőséget** (a Microsoft palettájáról az Exchange Server képes hasonló szolgáltatások biztosítására, de mivel a telepítő nem tartalmazza, további beszerzést igényel), míg ezzel szemben **a Linux** Postfix[31], Spamassasin[32] páros **képes hatékony védelmet nyújtani** Linux, de **akár Windows rendszereken is**. A hatékonyság tesztelése során

---

[27] Jiffy a Linux kernel 2.6.x.x verziókban 1/250 mp.

[28] POP3: Post Office Protocol version 3: egy alkalmazás szintű protokoll az elektronikus levelek lekéréséhez.

[29] SMTP: Simple Mail Transfer Protocol kommunikációs protokoll az elektronikus levelek interneten történő továbbítására

[30] Secure Socket Layer: A Netscape által kifejlesztett nyílt ajánlás (szabvány) biztonságos kommunikációs csatorna létrehozására.

[31] A Linux disztribúciók többségében a Postfix levelező szervert használják.

[32] Több különböző mechanizmust használó tartalom e-mail szűrő.

megállapítottam, hogy **a spamszűrés nem nagy erőforrás igényű** (2000 levél vizsgálata 16 percet igényelt, azaz 1 levelet átlagban 0,48 mp alatt vizsgált meg), valamint kellően nagy hatásfokú (0,3% nem felismert, 0,2% hamisan felismert).

**Webkiszolgáló** [57]

Elterjedtsége miatt tesztjeim során Linux esetében a LAMP (Linux, Apache, MySQL, PHP) összeállítást használtam és **az Apache webkiszolgáló beállítási lehetőségeit** vizsgáltam meg, míg a Microsoft Windows Server 2008 esetén az **IIS 7 web szervert vettem górcső alá.** A szolgáltatás teljesítmény- és biztonsági teszteléséhez egy egyszerű statikus HTML oldalt, egy dinamikus ASP.NET, és egy SQL Express-t használó ASP.NET alkalmazást használtam, és különböző teljesítmény valamint biztonsági teszteket futtattam le.

Megvizsgáltam, hogy lehetséges-e az alapértelmezett beállításoknál, egy biztonság szempontjából helytelenül megírt portal esetében SQL-injection és Cross Site Scripting (XSS) támadás végrehajtása.

1. táblázat: A web szerverek teljesítménytesztek eredményei

| | | **Apache** | | **IIS** | |
|---|---|---|---|---|---|
| | | 10 | 500 | 10 | 500 |
| **Statikus HTML** | Teljes teszt | 25,46 s | 26,63 s | 24,58 s | 18,53 s |
| | Teljes adatátvitel | 10,68 Mb | | 10,67 Mb | |
| | HTML forgalom | 3,72 Mb | | 3,72 Mb | |
| | Lekérdezések/mp | 981,88 | 938,23 | 1016,82 | 1350,32 |
| **Dinamikus oldal** | Teljes teszt | 61,68 s | 76,50 s | 80,72 s | 78,40 s |
| | Teljes adatátvitel | 173,04 Mb | | 181,27 Mb | |
| | HTML forgalom | 167,58 Mb | | 175,54 Mb | |
| | Lekérdezések/mp | 405,28 | 326,77 | 309,69 | 318,88 |
| **Dinamikus SQL** | Teljes teszt | 62,71 s | 78,24 s | 236,32 s | 238,78 s |
| | Teljes adatátvitel | 46,49 Mb | | 249 Mb | |
| | HTML forgalom | 41,03 Mb | | 243 Mb | |
| | Lekérdezések/mp | 398,65 | 313,27 | 105,92 | 014,7 |

A teljesítmény tesztekhez az ApacheBench programot használtam. Mind a két platformon három oldalt teszteltem, egy statikus, egy dinamikus, és egy SQL lekérdezéses dinamikus oldalt. Az oldalak tesztelésénél 25000 lekérdezést hajtottam végre, egyszerre 10, illetve egyszerre 500 lekéréssel. Az egyszerre elvégzett lekérdezések számát maximálni kellett (500), mert 1000 konkurens lekérdezés esetén a Windows Server már ASPX lekérdezés esetén megállt, és ráadásul csak a szolgáltatás újraindítása után lehetett a tesztet folytatni. Az Apache esetén pedig a MySQL szerver nem bírta az 1000 konkurens kapcsolatot. A tesztek eredményét az 1. táblázatban foglaltam össze.

A vizsgálatok és tesztek alapján **az alábbi megállapításokra jutottam:**

- az **Apache és az IIS 7 is moduláris szerver**, melynek köszönhetően kiválasztható az igényeknek megfelelően, hogy mely szolgáltatásokat kívánjuk használni. **Mindkét szerver esetén biztosítható az adatfolyam titkosítása a megfelelő modul alkalmazásával,** valamint **beállítható naplózás,** melynek elemzése lehetővé teszi egy esetleges incidens részleteinek felderítését;
- **megállapítottam, hogy a Windows Server 2008 operációs rendszer semmilyen védelmet nem nyújt** az alapbeállításokkal telepített ASP.NET-ben biztonság szempontjából rosszul megírt portál rendszerek esetében, melyeken **sikeresen végrehajtható SQL-injection**[33], azaz hozzáadható egy felhasználó az adatbázishoz, melynek segítségével a támadó a későbbiekben beléphet az oldalra. Ezzel szemben **az Ubuntu Server-nél telepített PHP alapértelmezés szerint** az aposztróf és idézőjel karakterek szűrése által **nem engedélyezi az ilyen jellegű támadásokat**;
- **az XSS**[34] **támadás ellen az ASP.NET**-ben egy olyan védelem van, ami **szűri a HTML kódokat, és figyelmeztetést ír ki támadás esetén, a PHP-ban** pedig szintén **az aposztróf és idézőjelek szűrése nyújt védelmet**, mely **azonban engedi beszúrni a külső rosszindulatú kódot, ha abban nem használják az említett karaktereket**;
- **mindkét szerver jól kezeli a konkurens kapcsolatokat**, mivel a hozzájuk intézett egyszerre 10, illetve 500 lekérdezés között nem tapasztaltam lényegi elté-

[33] Az SQL Injection-nek nevezzük azt a támadási módszert, amikor egy oldalra rosszindulatú SQL kód beékelésével végzi el a támadást a behatoló.

[34] Az XSS támadás a Cross Site Scripting, amikor egy Javascript, vagy egyéb szkriptet ültetnek be egy dinamikus oldalba.

rést. Az SQL tesztekből kiderült az is, hogy **az ASPX sokkal (kb. ötször) nagyobb adatforgalmat generál egy egyszerű tábla adat megjelenítésére**;

- a processzor használatának mértékében nem tudtam lényegi különbséget felfedezni, kivéve azt, hogy **a MySQL nagyjából 10-15 %-kal kevesebbet használja a kiszolgálót** ugyanazon parancs elvégzéséhez, mint az SQL Express.

**Tanúsítvány**

Egy elterjedt használati módja a publikus kulcs alapú kriptográfiának az alkalmazásréteg titkosítása SSL, vagy TLS[35] kapcsolat használatával. A HTTPS protokoll – azaz a HTTP TLS használatával, amely mindkét rendszer esetén létfontosságú – digitális tanúsítványt használ, melyet általában egy hitelesítő kiszolgálótól veszünk, de alternatív megoldásként a szervezet saját maga is aláírhatja a tanúsítványát. Az önaláírt tanúsítvány érzékeny adatokat tároló- feldolgozó rendszerek esetében, így a közigazgatási rendszerek esetén sem megfelelő megoldás. **Mivel a digitális aláírások, tanúsítványok kezelését szabványok írják le, így a böngészők számára platformtól függő különbség nem lehet.**

**Felhasználó- és jelszókezelés**

A biztonsági házirendben megadható beállítások, azon belül is a felhasználó- és a jelszókezeléssel kapcsolatban elvégzett összehasonlító teszt eredményeként az alábbi megállapításokat teszem:

- biztonsági szempontból jó megoldás az **Ubuntu Linux disztribúció esetén**, hogy **alapértelmezetten a root[36] felhasználói fiók tiltva van**, így egy esetleges behatolás esetén, ha megszerezte is egy támadó a root felhasználó jogait, nem tudja felhasználni. A root helyett az admin csoport tagjai, illetve az /etc/sudoers fájlban felsorolt felhasználók jogosultak átmeneti rendszergazdai tevékenység elvégzésére, de ellentétben a Windows-zal ilyenkor a felhasználónak a saját jelszavát kell használnia, nem kell tudnia a root fiókhoz tartozó jelszót, vagy akár a rendszergazdáétól és a felhasználóétól egyaránt különböző jelszóval is lehet használni, így biztonságosabb;

---

[35] Transport Layer Security: Az SSL továbbfejlesztése, 1999-ben az IETF (Internet Engineering Task Force) elfogadott szabvány szintre emelte (RFC 2246).

[36] A root a Linux rendszerekben a rendszergazda, akinek mindenható joga van, általában minden rendszert érintő módosításhoz ilyen szintű hozzáférés kell.

- **felhasználó törlésekor egyik platform esetén sem törlődik automatikusan a felhasználó könyvtára**. Ez veszélyes lehet, mert, ha egy felhasználót olyan UID[37]-vel adunk a rendszerhez, mint amelyikhez tartozó felhasználót töröltük, akkor az új felhasználónak a törölt felhasználó minden adatához lesz hozzáférési jogosultsága, illetve a vele azonos csoportban lévő felhasználóknak is lesz a beállított jogosultság szerint elérési lehetőségük;
- mindkét rendszerben **jelszókezelési házirend** segítségével előírható a felhasználó számára, hogy megfelelően hosszú és bonyolult jelszót válasszon, hogy le kelljen azt bizonyos időközönként cserélnie (bár alapértelmezés szerint ez a funkció általában tiltva van), hogy a korábban megadott jelszavak közül hányat jegyezzen meg a rendszer mielőtt ismételten megadható az eredeti jelszó. Tehát mind a két rendszeren részletesen beállítható a biztonsági házirend jelszókezelése, de **Windows Server esetén nem konfigurálható olyan részletességgel, mint Linux alatt.** Továbbá a biztonságos jelszó megalkotásához Linux választásakor lehetőség van szótár alapú támadások kivédésére, ellenőrzés által. [56]

**Tűzfal**

A tűzfal alapvető feladata a hálózati forgalom ellenőrzése, és különböző szabályok által tiltása, vagy engedélyezése. Vizsgálódásaim során megállapítottam, hogy **mindkét platform tűzfala hasonló képességekkel rendelkezik és hasonló részletességgel konfigurálható,** jelentős eltérést nem tapasztaltam. Véleményem szerint mind a két tűzfal esetében **a kiszolgáló biztonsága csak a megfelelő tűzfalszabályok megalkotásán, és beállításán múlik**.

A fentiek alapján **megállapítom**, hogy **teljesítménybeli különbség jelentős mértékben nem tapasztalható** a két vizsgált szerver platform tekintetében, azonban biztonsági szolgáltatások terén a Linux egy kicsit jobban vizsgázott (spam szűrés, SQL injection elleni védelem szemben az ASP.NET HTML kódok szűrésével). Azt is figyelembe véve, hogy a közigazgatás informatikai rendszereinek ma az egyik legjelentősebb sérülékenysége a web alkalmazások gyengeségei, állíthatnám, hogy Linux szerver üzemeltetése biztonságosabb és olcsóbb, mint egy Microsoft szerveré. Tehát igazolt a nemzetközi tendencia, mely szerint a közszféra egyre több rendszerét állítják át nyílt forráskódú operációs rend-

[37] UID -. User identifier – felhasználói azonosító.

szerekre. De hazánk sajátosságait is tekintve, mely szerint a nyílt forráskódú operációs rendszerek konfigurálásához, üzemeltetéséhez szükséges szaktudás még csak elvétve jelenik meg a közigazgatás humán erőforrás bázisában, valamint, hogy a korábbi saját fejlesztések is Microsoft platformra lettek optimalizálva, **az a véleményem**, hogy **nem olyan jelentős a különbség, mintsem indokolná a helytelen beüzemelés és működtetés kockázatát. A szakemberek képzésére, betanítására valamint az egyéb alkalmazások átállítására fordítandó összeget is figyelembe véve pedig már a költségek sem indokolják a nyílt forráskódú szoftverekre való átállást.**

### 2.1.3. AZ ALKALMAZÁSOK GYENGESÉGEI

Egy jól védett, megfelelően menedzselt hálózat rendelkezik azokkal a biztonsági eszközökkel (hálózati-, host alapú betörés detektáló, tűzfalak, stb.), melyek segítségével a hálózati réteget ért támadások viszonylag egyszerűen meghiúsíthatók. Az operációs rendszerek gyengeségeit kihasználó támadások pedig a gyártók által kiadott frissítések, javítócsomagok időben történő alkalmazásával kivédhetők. Ennek köszönhetően a támadások túlnyomó része ma már az igen csak sérülékeny alkalmazás réteget veszi célba. A statisztikai kimutatások is azt igazolják, hogy a támadók egyre nagyobb mértékben (a kisebb ellenállás irányában) az alkalmazás réteg sérülékenységeit kihasználva hajtják végre támadási tevékenységüket. Drasztikusan növekednek a web alkalmazások elleni támadások (Gartner: a hacker támadások 75 %-a az alkalmazás rétegből kerül ki). [58: 17.p.]

Az alkalmazás rétegen belül is a leggyengébb láncszem a web alkalmazások köre, melyet a Web Application Security Consortium (WASC) felmérése igazol is [59]:

- a vizsgált web alkalmazások több mint 7%-a automatikusan feltörhető;
- 7.72%-uk szenvedett magas besorolású sebezhetőségtől;
- a részletes, kézi módszerekkel történő sebezhetőség keresésnél a web alkalmazások 96,85%-ban találtak magas besorolású sérülékenységet.

Tekintve, hogy a közigazgatás jelentős mennyiségű szolgáltatása vehető igénybe web alkalmazásokon keresztül, így ebben a témakörben **vizsgálataim is a web alkalmazások problémakörére koncentrálódtak**.

Amikor még csak statikus weboldalak alkották az internetet, a védelem megfelelő szintje egyszerűen biztosítható volt. A támadások legrosszabb következménye az volt, hogy valaki illegális tartalmat jelenített meg egy statikus weblapon. Azonban az interneten

keresztül biztosított szolgáltatások térhódításának köszönhetően egyre jobban előtérbe kell, hogy kerüljenek a dinamikus weboldalakat kezelő web alkalmazások, ezért sebezhető pont keletkezik a rendszerben, ha nem biztosítunk alkalmazás szintű védelmet. **Az alkalmazás rétegre** viszont **ma még az jellemző, hogy nem alkalmaznak betörés megelőző mintázatokat**, amelyekkel hatékonyan lehetne detektálni, jelezni a behatolást és többnyire **nincsenek javító szoftverek sem**. Továbbá elég jelentős mértékben fordulnak elő házilag készített alkalmazások is, pl. számos önkormányzatnál költségkímélő megoldásként használnak **saját fejlesztésű alkalmazások**at, melyek elkészítésekor sok esetben a biztonságnak még a gondolata sem merült fel. Az egyetlen fő szempont a helyes működés. De a professzionális szoftvergyártók sem rendelkeznek a megfelelő szakemberbázissal, ezt a megállapításomat támasztja alá Bill Gates nyilatkozata is, miszerint a fejlesztők 64 %-a nem biztos benne, hogy képes biztonságos alkalmazást írni [60]. Ez nem is csoda, hiszen **egyetemen sem oktatják**, még alkalmazásfejlesztés szakirányon sem kellő mértékben kerül szóba, hogy hogyan kell biztonságos kódot fejleszteni.

Ezért fontosnak tartottam **megvizsgálni**, hogy **milyen fenyegetések okozzák a legnagyobb problémát az alkalmazás réteg** tekintetében. Vizsgálataim eredményeinek részleteit a „The security of Web Applications" című cikkemben publikáltam [61], mely alapján a fontosabb megállapításaim a következők:

- az interneten barangolva, az oldalakat böngészve gyakran találkozhatunk különböző **hibaüzenetek**kel (a legsúlyosabb, de előfordul, hogy az adatbázis hibaüzeneteit látjuk, különböző függvényhívásokat), melyek **rengeteg információt elárulnak magáról a rendszerről,** és amelyek segítségével egy hacker, aki kifejezetten ezeket az információkat keresi, lépésről lépésre egyre beljebb tud hatolni a rendszerbe. Így például az 5. ábrán látható hibaüzenetből megállapítható, hogy az alkalmazás nagy valószínűséggel Microsoft adatbázist használ és megtudhatja a támadó azt is, hogy az alkalmazás fájljai milyen könyvtárszerkezetben tárolódnak;
- a statisztikák szerint általában egy alkalmazás kódját tekintve 1000 sorban 15 kritikus biztonsági hiba van. Egy általános alkalmazás 150-200 ezer sorból áll. A kimutatás szerint egy biztonsági hibát 75 perc alatt lehet diagnosztizálni, 6 óra alatt megjavítani;

- a hibák kijavításának költségei igen magasak, de a helyreállítás, javítás költségei exponenciálisan növekednek, ha az éles beüzemelés után kerül csak rá sor;
- az Open Web Application Security Project (OWASP)[38] felmérése szerinti [62] **leggyakoribb sebezhetőségeket kihasználó támadási formákat megvizsgálva megállapítottam, hogy többségük tipikusan annak a sebezhetőségnek a kihasználásával történik, hogy valamilyen paraméter nem megfelelően van ellenőrizve**. Az alkalmazásba belefejlesztett úgynevezett nem kívánt funkcionalitást használják ki, pl. a felhasználó névnél nem csak felhasználó nevet fogad el egy alkalmazás, hanem mondjuk egy SQL lekérdezést is, és végre is hajtja. A támadók átadnak valamilyen scriptet, függvényhívást és utána hozzájutnak különböző információhoz, amellyel aztán akár a rendszerhez is hozzáférhetnek, admin/root jogosultságot szerezhetnek, vagy csak adatokat kérdeznek le;
- **hibásan beállított web szerverek** kihasználásával egy **támadó lefuttathat rosszindulatú kódokat a böngészőn**. De további fenyegetést jelent, hogy ilyenkor az esetek többségében a gyanútlan felhasználónak úgy tűnik, mintha a script a használt weboldaltól származna. A gondot még csak tetézi, ha ráadásul a látogató a weboldalt megbízhatónak tartja.

## 2.2. BELSŐ VESZÉLYFORRÁSOK

A belső biztonsági veszélyek a szervezeten belülről érkeznek. Belső veszélyt jelenthetnek az **adatlopás**t, **vírusok elterjesztésé**t vagy **hálózati támadások**at **szándékosan** megkísérlő alkalmazottak, de a külső, ideiglenesen a szervezeten belüli **szerződéses dolgozók** is, mint például takarítószolgálatot teljesítők, közművállalatok alkalmazottai, stb., akik fizikailag hozzáférhetnek a helyi hálózathoz kapcsolt számítógépekhez. **Számos belső veszély** azonban **véletlenül** lép fel. Előfordulhat az is, hogy saját kényelmük érdekében az alkalmazottak a saját szoftvereiket, hardvereiket telepítik vagy használják a gépükön, **anélkül, hogy tudatában lennének**, hogy ezzel a számítógépüket és a teljes hálózatot is biztonsági kockázatnak teszik ki. Az informatikai rendszerek esetében ez az egyik leggyakrabban előforduló és legnehezebben kiküszöbölhető sérülékenység.

[38] Több gyártót összefoglaló, nyitott fejlesztési rendszer, melynek keretében a web alapú szolgáltatások biztonságát vizsgálják, segédprogramokat, tudásbázist fejlesztenek, mely referenciaként szolgálhat rendszergazdák, fejlesztők, felhasználók számára.

**A legjelentősebb belső veszélyforrás tehát az emberi tényező**, mely szándékosan vagy akaratlanul idézheti elő a közigazgatási informatikai rendszer, vagy valamely elemének sérülését.

### 2.2.1. A SZERVEZET DOLGOZÓINAK SÉRÜLÉKENYSÉGET OKOZÓ SZÁNDÉKOS CSELEKEDETEI

Belső veszélyforrást elsősorban a szervezetek alkalmazottai jelentenek, azonban az állami, közigazgatási szervezetek esetében a humánerőforrással kapcsolatos kiválasztási, ellenőrzési folyamatoknak köszönhetően, szerencsére csekély mértékben jelentkezhet a dolgozók sérülékenységet okozó szándékos magatartása. **Véleményem szerint** ilyen **abban az esetben fordul elő**, amikor a szervezet alkalmazottja **vélt, vagy valós sérelmét kívánja megtorolni**, vagy **anyagi haszonszerzés** motiválja, esetleg csak **információt gyűjt** a későbbi hasznosíthatóság, pozíciójának kedvezőbb alakulásának reményében.

**Lehallgatás**

Ide sorolható az informatikai rendszeren továbbított digitális információ lehallgatásán túl a hagyományos audio alapú lehallgatás is, hiszen a technológia adott, egyszerű, kisméretű, hétköznapjainkban könnyen elérhető és elrejthető eszközök (diktafon, mobil telefon, felvételre is alkalmas MP3 lejátszó, stb.) állnak rendelkezésre. Azonban e címszó alatt az értekezés témáját tekintve mégis inkább a digitális információ lehallgatását kell érteni, mint arról már korábban a hálózat sérülékenységeit kihasználó módszerek esetében írtam.

**Adatlopás, adatszivárgás**

A hordozható adattároló eszközök paramétereinek (kapacitás, méret, ár) rohamos fejlődése következtében egy szervezet dolgozói könnyen kísértésbe eshetnek, hogy anyagi haszonszerzés vagy pusztán csak információszerzés céljából eltulajdonítsák a szervezet informatikai rendszerein tárolt, feldolgozott, továbbított bizonyos információit. Ezek az eszközök ma már igen nagy kapacitással egy hétköznapi alkalmazott számára is viszonylag olcsón beszerezhetők és könnyedén, méretüknek köszönhetően észrevétlenül csatlakoztathatók a szervezet számítógépeihez. Egy cég vagy intézmény szinte összes bizalmas adata ráfér.

Egy kutatás során Nagy-Britanniában a megkérdezett ezer alkalmazott 72 százaléka nyilatkozta azt, hogy tulajdonított már el munkahelyéről információkat USB-s memóriakártyán, laptopon, vagy más hordozható adattárolón, mobiltelefonon. Sokan vélik úgy,

hogy joguk van hozzá (59 %) – nyilatkozta a ComputerWeekly-nek Amichai Shulman, az Imperva technológiai vezetője. A felmérés azt is kimutatta, hogy a lopások ekkora mértékének a vállalati szabályozások hiánya a legfőbb oka. [63]

A megoldást nehezíti, hogy hiányoznak a megfelelő piackutatások, elemzések, illetve az adatvesztésről szóló híreket gyakran elhallgatják. Hiányosak a szabályozási folyamatok, illetve azok nem megfelelő betartása jellemző sok esetben. Az adatbiztonsági kultúra még gyerekcipőben jár hazánkban is.

**Az adatok megrongálása, szándékos törlése**

Előfordul az is, amikor a belső támadó célja nem az információ lehallgatása, eltulajdonítása, hanem épp ellenkezőleg, annak elérhetetlenné tétele, megsemmisítése. Az is jelentős problémát okozhat a szervezetnek, ha a felhasználó a jogosultsági körébe tartozó adatokat rongálja meg, de a nagyobb gondot az jelenti, ha a megfelelő szabályozás, konfigurálás hiányában a felhasználó hozzáférhet jogosulatlan adatokhoz és azokat is használhatatlanná teheti.

**Kémszoftverek, kártékony kódok**

Az előzőekben említett kisméretű, a szervezet dolgozói számára is elérhető árú, hordozható adattároló eszközök lehetőséget biztosítanak az ártó szándékú dolgozók számára, hogy segítségükkel vírusokat, kémprogramokat, akár jogsértő tartalmakat is bejuttassanak a vállalati hálózatba, lehallgatás, adatlopás, vagy annak megrongálása célzattal.

**Kapcsolók sérülékenységei**

A hálózat sérülékenységeit kihasználó eszközök tárgyalása során említettem, hogy a megbízhatóság, a rendelkezésre állás növelése érdekében egyre nagyobb számú kapcsolókat alkalmaznak a hálózati kapcsolatok kialakítása során. Azonban számos pozitív hatásuk mellett jelentős veszélyforrást is jelentenek a rendszerünkre nézve, de nem csak azért, mert a külső támadások ezeket a kapcsolódási pontokat érintik először, hanem azért is, mert a nem megfelelő konfigurálásuk a belső, rosszindulatú felhasználóknak is lehetőséget biztosít az adatok lehallgatására, eltulajdonítására, esetleg megrongálására. [44]

### 2.2.2. A SZERVEZET DOLGOZÓINAK SÉRÜLÉKENYSÉGET OKOZÓ AKARATLAN CSELEKEDETEI

Mint azt már korábban is írtam, ez az egyik leggyakrabban előforduló és egyben az egyik legnehezebben kiküszöbölhető sérülékenység. A szervezet dolgozóinak képzetlenségéből, hanyagságából, esetleg a szabályozók be nem tartásából fakad.

**Áramszünet előidézése**

A szervezet figyelmetlen alkalmazottja véletlenül kihúzhatja az informatikai rendszer valamely elemének (hálózati eszköz, munkaállomás, rosszabb esetben szerver, adattároló, stb.) áramellátását biztosító kábelét, mely cselekedet megfelelő biztonsági megelőző intézkedések hiányában adatvesztést, szolgáltatás kiesést, de akár az adott elem meghibásodását is okozhatja.

**Idegen eszközök, szoftverek használata**

A felhasználók saját kényelmük, esetleg szórakozásuk érdekében nagy előszeretettel használják munkahelyükön is saját szoftvereiket, hardvereiket, anélkül, hogy tudatában lennének, hogy ezzel a számítógépüket és a teljes hálózatot is biztonsági kockázatnak teszik ki.

**Vírusellenőrzés elmulasztása, ellenőrző szoftver kikapcsolása**

A végpontokon alkalmazott vírusvédelmi szoftverek általában valamilyen mértékben lassítják az adott gép működését és ezért igen gyakran előfordul, hogy a felhasználók kikapcsolják az aktív védelmet. Tovább növeli a biztonsági kockázatot, ha idegen eszközöket, szoftvereket telepítenek a munkaállomásra anélkül, hogy elvégezték volna az adathordozó vírusellenőrzését.

**Jelszókezelési problémák**

A felhasználók általában gyenge, megjegyezhető, esetleg a velük kapcsolatos, rájuk jellemző jelszavakat (családi dátumok, nevek, stb.) választanak, melyek megfejthetők, némi információval rendelkezve az adott felhasználóról könnyen kitalálhatóak, hacsak szabályzattal rá nem kényszerítik erős jelszó használatára. Abban az esetben azonban, ha túl szigorú a házirend, akkor a felhasználó biztosan megkísérli kijátszani azt. Például arra kényszerülhet, hogy feljegyezze a bonyolult, számára megjegyezhetetlen jelszavakat és azt a munkaállomás közelében tartsa, esetleg a monitorra ragassza, melyhez ezáltal a belső támadó

(akár a szervezet egy másik dolgozója, akár ideiglenesen a szervezeten belül tartózkodó szerződéses dolgozó) hozzájuthat. A másik probléma a jelszavakkal kapcsolatosan, hogy gyakran elárulják a munkatársak egymásnak a jelszavaikat, sőt használják is egymását.

**Munkaállomás felügyelet nélkül hagyása, hanyag tárolás**

A munkaállomás felügyelet nélkül hagyása – akár rövid időre is – támadási lehetőséget biztosíthat egy rosszindulatú alkalmazott számára, vagy akár a szervezetnél ideiglenesen szerződéssel foglalkoztatott külső alkalmazottak (mint például takarítószolgálatot teljesítők, közművállalatok alkalmazottai, stb.) számára, akik a nevükben, a jogosultságuknak megfelelően tevékenykedhetnek távollétükben. Arról sem szabad megfeledkezni, hogy a legrövidebb ismert víruskód mindössze 25 bájt, tehát nem kell sok idő a munkaállomásra juttatásához.

A rendszerbeli adatok archiválása, esetleg papíralapú előállítása esetenként szükséges lehet, de azok nem megfelelő tárolása (jogosulatlanok által is könnyen hozzáférhető helyen, titkosítás nélkül) újabb sérülékenységet jelent.

## 2.3. KÜLSŐ ÉS BELSŐ TÁMADÁS KOMBINÁCIÓJA

Mint azt már korábban is írtam, ez alatt a támadási forma alatt azt értem, amikor a támadás kezdeményezése a szervezeten kívülről történik ugyan, de belső (akaratlan vagy tudatos) segítséggel. Ide sorolom továbbá azt az esetet is, amikor a támadást egy esetleg nemrég elbocsájtott alkalmazott a szervezetről, a szervezetnél eltöltött ideje alatt megszerzett információinak segítségével kívülről hajtja végre.

### 2.3.1. KÜLSŐ TÁMADÁS BELSŐ AKARATLAN SEGÍTSÉGGEL

**Social Engeneering**

A szervezeten kívülről indított támadáshoz belső segítség legkönnyebben ennek a módszernek a segítségével szerezhető, mivel az emberi jóhiszeműség kihasználását célozza meg és sajnos ez ellen a legjobban felvértezett szervezetek sem tudnak kellő hatékonysággal védekezni. Számos formában kivitelezhető a támadó ötletességétől függően, a lényeg a szervezet valamely dolgozójának a bizalmába férkőzni. Például a behatoló munkatársnak álcázhatja magát, akinek hozzáférésre van szüksége a saját rendszere állítólagos leállása

miatt, és bizalmunkat úgy próbálja megnyerni, hogy beszélgetésbe elegyedik velünk, „belsős" kifejezéseket használ, megemlítheti egyik kollégánk (például főnökünk) nevét is. Hatósági személynek vagy hálózati hibaelhárítónak is álcázhatja magát, akinek egy azonosítóra és jelszóra van szüksége annak ellenőrzésére, hogy elhárult-e a hiba. De akár éjszakai takarítónak jelentkezve jelszavak után kutathatnak a papírkosarakban, a fiókokban vagy a monitorokra ragasztott cédulákon is, hogy bizalmas információkhoz jussanak. [64] Értékes adat lehet akár a belsős telefonkönyvek tartalma, vagy kidobott szervezeti felépítést mutató ábra is. Az így megszerzett információkat értékelve könnyebben hozzáférést szerezhetnek a szervezet informatikai rendszeréhez.

A probléma súlyosságának érzékeltetése érdekében ismertetek egy szimulációs példát, mely kiválóan tükrözi, hogy **hiába választjuk ki legkörültekintőbben a megfelelő operációs rendszert, hiába alkalmazzuk a legkorszerűbb védekezési formákat, biztonságunk akkor is labilissá válhat.**

Egyik hallgatóm évekkel ezelőtt azt a tesztelési feladatot kapta, hogy támadja meg valamilyen formában egy társa számítógépét és vegye át az irányítást felette. A feladat kivitelezéséhez egy kliens-szerver architektúrában működő programot használt fel, mely Windows alapú rendszerek távoli irányítását tette lehetővé. A támadás végrehajtásához szükséges volt a szerver rész célgépre juttatása és elindítása. A szerver rész célgépre juttatása céljából a hallgató írt egy egyszerű játékot, melynek indulásakor a szerver átmásolódik a Windows egyik rendszer-mappájába, átneveződik egy olyan exe fájlra, melynek neve hasonlít a Windows rendszerfájljainak nevéhez, és ezután elindul. A játékot egy zip fájlba csomagolva küldte el ismerősének, mondva, hogy egy játékot küld neki, amit nemrég talált az interneten. A társa kicsomagolta a játékot, teljesen megbízva ismerősében ellenőrzés és gyanakvás nélkül el is indította azt. [65]

A példa ugyan néhány évvel ezelőtti, de aktualitását nem vesztette el. Felmérést végeztem **informatikus** hallgatóim körében, és az eredmény még ma is siralmas. 76 % ma is mindenféle fenntartás nélkül elfogadta volna a küldött zip fájlt és ellenőrzés nélkül futtatná az ismerőstől származó játékot megbízva annak kilétében. Pedig manapság már első ránézésre egyáltalán nem lehetünk biztosak abban, hogy egy üzenet valóban attól a feladótól származik, mint aki fel van tüntetve és nem pedig egy támadó próbálja meg bizalmunkat elnyerni a feladót meghamisítva.

### Reverse Social Engineering

A Reverse Social Engineering szintén egy kiváló eszköz belső információkhoz való hozzáféréshez. Annyiban különbözik a Social Engineeringtől, hogy ez esetben az „áldozattal" azt is el kell hitetni, hogy ő a kezdeményező. Például előidéznek egy hibát, majd pedig kiadják magukat a szerelőnek, vagy esetleg véletlenszerűen felhívnak telefonszámokat, hogy „a bejelentett hiba ügyében telefonálok…", mert nagy valószínűséggel mindenhol akadnak megoldandó problémák, így kapva-kapnak a felkínált lehetőségen.

### Adathalászat

Korunk igen elterjedt, a támadók közkedvelt információgyűjtő eszköze, melynek segítségével érzékeny információkhoz tudnak hozzáférni. Ma még jellemzően banki adatok megszerzésére irányul, de ahogy szélesedik a különböző informatikai rendszereken – például a közigazgatási rendszereken is – a végrehajtható funkciók, valamint a tárolt adatok repertoárja úgy szélesedik az adathalászat által megcélzott rendszerek köre is.

### TEMPEST[39] típusú támadás

Ennek a támadástípusnak a jelentőségét nagymértékben csökkenti, hogy a katódsugárcsöves monitorokat lassan felváltják az alacsony kisugárzású monitorok, de ez a támadástípus nem csak az eszközök, hanem az átviteli utak, helyiségek kompromittáló kisugárzása alapján is eredményes lehet. Ez a támadási forma nem tartozik szorosan ebbe a csoportba, mivel a felhasználótól szinte egyáltalán nem függ, azonban nem hagyható figyelmen kívül. Ezért kutatásom is kiterjedt erre a támadástípusra is.

Sérülékenységnek tartom, hogy a probléma kezelése kormányzati szinten **csupán a „Bizalmas!" vagy magasabb minősítési szintű adatokat kezelő rendszerekre korlátozódik**, mint az kiderül a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendeletből is, mely a TEMPEST követelményeket csak ezekre a rendszerekre fogalmazza meg. [66] Ugyanis **ettől eltérő rendszereket is működtetnek** az általam vizsgált szervezetek, és **az átviteli utak és végberendezések által keltett kisugárzások illetéktelen detektálása és rögzítése veszélyes lehet azok esetében is**, mivel ez a támadási forma nem érzékelhető és megszerezhetők általa olyan rendszerinformációk,

[39] A TEMPEST egy kódnév, ami a nem szándékos, kompromittáló kisugárzások vizsgálatának, tanulmányozásának módszerére utal.

melyek további támadásokhoz támpontként szolgálhatnak.

Tempest típusú támadás esetén leginkább a monitor kisugárzásának vételére gondolunk, holott minden elektronikai eszköznek és alkatrésznek van nem szándékos rádiófrekvenciás kisugárzása. Így például a vezeték nélküli, sőt a vezetékes billentyűzetek, valamint a laptopok lehallgathatósága is ebbe a kategóriába tartozik. Ezt a módszert demonstrálta Martin Vuagnoux és Sylvain Pasini, amikor egy egyszerű huzalantennával, jelerősítővel és vevőberendezéssel akár 20 méter távolságból is le tudták hallgatni ezen eszközöket és a bevitt karakterek egy monitoron megjelentek. Így arra alkalmas eszközökkel akár banki jelszót is el lehet csípni, akár 2-3 téglafalon keresztül is. [67]

### 2.3.2. A SZERVEZET DOLGOZÓJÁNAK TUDATOS KÖZREMŰKÖDÉSE A TÁMADÁSBAN

Egy szervezet dolgozója foglakoztatása során számos érzékeny információhoz férhet hozzá. Az így megszerzett ismeretek felhasználása egy támadásban való közreműködés során általában akkor következhet be, ha a dolgozót vélt vagy valós komoly sérelem éri, alulmotivált, munkája nem kellő mértékben (anyagi és erkölcsi értelemben egyaránt) elismert, illetve, ha a dolgozót elbocsájtják és a kilépését nem kezelik megfelelően a rendszert illetően.

A szervezeti adatbiztonság helyzetét rontja már Magyarországon is az elbocsájtások egyre emelkedő száma. A Symantec és a Ponemon Institute tavaly közzétette egy közös felmérésük eredményét, miszerint a 2008-ban munkahelyet váltó vagy munkahelyét elvesztő megkérdezett közül 79 százalék vitt el vállalati adatot korábbi munkáltatójától annak engedélye nélkül. Ezek egy része pénzügyi adat és forráskód, de nagyobb része a dolgozói és a felhasználói információk, e-mail listák voltak. [68]

## 2.4. A TÁMADÓK KÖRE, MOTIVÁCIÓI, CÉLPONTJAIK, A TÁMADÁSOK HATÁSAI

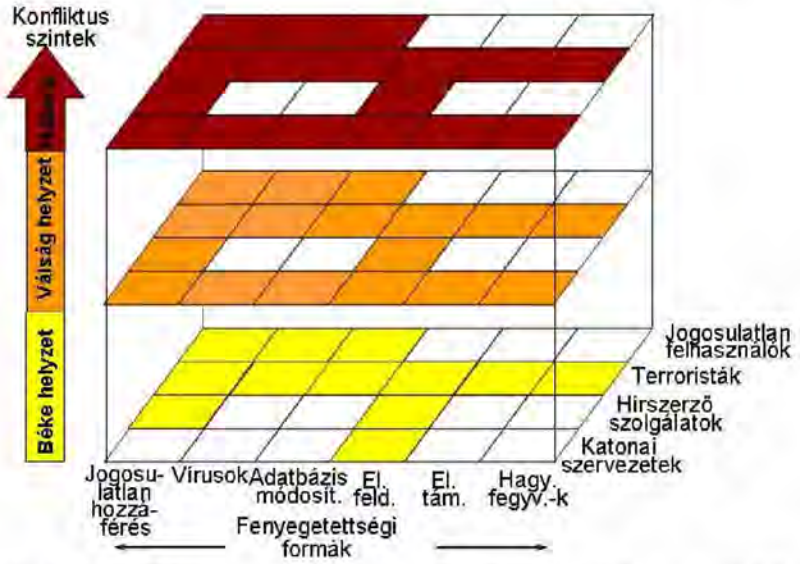
A megfelelő védelem kialakításához elengedhetetlennek tartottam a támadók körének, motivációinak, a támadások hatásainak megvizsgálását, valamint a technika fejlődésének hatását a célpontok alakulására.

### 2.4.1. A TÁMADÓK KÖRE

A külső támadásokat általában az információs technológiához kiválóan értők hajtják végre, míg ezzel szemben a belső támadások végrehajtói az esetek többségében a szervezet képzetlenebb, felelőtlenebb alkalmazottai közül kerülnek ki. Megállapítható az is, hogy a támadók köre az infokommunikációs rendszerek elterjedésével és fejlődésével, az ezzel járó sérülékenységek körének szélesedével egyre csak bővül.

Az infokommunikációs rendszerek elleni támadók köre a védelmi szervezetek szempontjából alapvetően négy kategóriába sorolhatók, melyet a 6. ábra is szemléltet:

1. jogosulatlan felhasználók;
2. terroristák;
3. hírszerző szolgálatok;
4. katonai szervezetek.




6. ábra: Védelmi célú infokommunikációs rendszerek elleni fenyegetési formák [69]

Az említett csoportok közül **az első két csoporttal** foglalkoztam részletesebben, hiszen a magyar közigazgatás informatikai rendszereire ők jelenthetnek jelentősebb fenyegetést.

**Jogosulatlan felhasználók**

A jogosulatlan felhasználó fogalma az elmúlt évtizedek alatt nagymértékű átalakuláson ment keresztül. A hackerek, crackerek fogalmai egyre inkább összefonódnak, összekapcsolódnak a köztudatban, köszönhetően elsősorban a médiának, valamint annak, hogy e fogalmak jelentése valóban megváltozott az évek folyamán.

A legelső ARPAnet kísérletek idejében kiváló programozók és alapos hálózati ismeretekkel rendelkező emberek honosították meg a „hacker" kifejezést. Hackerek tették például a Unix operációs rendszert azzá, ami. [70]

A hacker, cracker rokon értelmű kifejezések, azt jelentik, hogy betörő, kódfeltörő, titkosított hálózati rendszerekbe illegálisan behatoló. Az angolban a hack ige „betör, bezúz, becsákányoz" jelentésű, a crack pedig hangutánzó szó, és „tör, betör, feltör" az értelme. Szószerinti jelentésükben tehát nem sok különbség van, de valójában, eredetileg éles ellentét húzódott közöttük.

**A hacker** fogalom eredetileg olyan „számítógépgurut" jelentett, aki kihívásnak tekinti a különböző számítógépes problémák megoldását, az informatikai rendszerek biztonsági réseinek felderítését és megszüntetését. Az igazi hacker cselekedeteit jó szándék vezérli, komoly elvei vannak, melyekhez minden körülmények között tartja magát. Ha be is tör különböző rendszerekbe, semmiféle kárt nem okoz, csupán a kihívás kedvéért teszi, valamint azáltal, hogy betör valahova, felhívja a rendszergazda figyelmét a résre, hibára, még mielőtt egy cracker találná meg ugyanezt a bejáratot. Az információ megosztását szinte erkölcsi kötelességének érzi, melyek segítségével más hackerek új problémákkal hatékonyabban tudnak foglakozni. [69]

**A crackerek** azok, akik bűncselekményeket követnek el, adatbázisokba törnek be, információt rabolnak, jogvédett szoftverek védelmi rendszerét játsszák ki – a programkészítőknek, forgalmazóknak komoly károkat okozva –, szándékosan kárt okoznak különböző rendszerekben. [69]

Az alapvető különbség tehát: a hackerek építenek, míg a crackerek rombolnak. De tovább boncolgatva a jogosulatlan felhasználók körét, további csoportosítást alkothatunk. Az eredeti jelentésnek megfelelő **hackerekből** – akiket ma szokás etikus hackereknek is nevezni – lesznek a legjobb rendszergazdák, rendszerszervezők. A megbízó multicégek biztonsági rendszerét figyelik, ha rés keletkezik rajta, az ő feladatuk elhárítani a támadást, kijavítani a hibát, továbbfejleszteni a rendszert.

Meglátásom szerint az eredeti cracker fogalom pedig képességeiktől, céljaiktól, életkoruktól függően a következőképpen alakult:

- **Light hackerek:** Nagyságrenddel népesebb tábor mint a hackereké, különböző web helyeket törnek fel, ott illegális tartalmakat helyeznek el, vagy le is cserélik

azokat saját tartalmú honlapokra. Nekik már vajmi kevés közük van az igazi hacker fogalomhoz.

- **Dark hackerek**: Más néven evil, tetteiket nyereség- vagy bosszúvágy vezérli. Kémkednek, valamint mások által fizetett hitelrontásból élnek. Ők azok, akik közzétesznek különböző, illegális úton megszerzett adatokat, megcsapolják a bankszámlákat, internetes vírusokat készítenek, stb. Ők konkrétan bűnözők.
- **Phreak**: Telefonközpontok vezérlő-számítógépeinek, a távközlési vonalak ingyenes igénybevételének és általában a telekommunikációnak a szakértői. Rendelkeznek a központok átprogramozásához, illetve megfelelő eszközökkel a mobil telefonhálózat forgalmának, belső adatainak lehallgatásához szükséges tudással. Ők maguk, vagy akiknek az információkat továbbadták mások költségére telefonálnak. Szintén bűnözők.
- **Wannabe – hacker**: Mint a nevük is mutatja, csak szeretnének igazi hackerek lenni, mármint light vagy dark hackerek. Önállóan nem tudnak programot írni, ezért mások által készített hack-programokat használnak kisebb-nagyobb sikerrel.
- **Troll**: A legfiatalabb réteg, szaktudásuk nem sok van, de nagyon lelkesek. Sokban hasonlítanak a wannabe-hez, szintén mások – általában light hackerek – által készített programokat használnak, csak azzal a különbséggel, hogy nekik fogalmuk sincs róla, mit is csinálnak valójában. A legfiatalabb számítógépes generáció első szárnypróbálgatásai ezek.
- **Difter**: Csak keresgél és, ha talál valamit egy gépen, akkor azt lemásolja magának. Munkássága teljesen észrevétlen marad, csak az utal drifter tevékenységre, ha a modem transmit ledje ok nélkül villog.

Az Egyesült Államokban és Nyugat Európában 15 - 25 éves fiatalokból web-szerte ismert csoportok jöttek létre. A Legion of Doom (LoD), Masters of Deception (MoD), Cult of the Dead Cow (cDc), vagy a holland Hack-tic csak néhány, a legismertebbek közül. Tagjaik különböző dologra szakosodtak, közöttük munkamegosztás volt. Egyesek felderítéssel foglalkoztak: kukákban turkáltak, szervezetek papírhulladékai között login nevekre, jelszavakra vadászva keresgéltek. Mások, un. „WAR dialer"-t működtettek, ami éjszakánként több ezer számot is végigtárcsázott modemre bukkanás reményében. A talált számok listája, mint potenciális célpont felkerült a saját belső hálózatukra, hogy a többiek haszno-

sítsák. Mások a postai hálózatok működését tanulmányozták, pontos műszaki leírásokat adtak, hogyan lehet mindenféle „színes doboz"-t készíteni (blue box, red box .., stb.) a telefontársaságok kijátszására,. Minden információt közzétettek, megjelentettek, web szervereken, az általuk (is) látogatott NEWS group-ok listáin, és időszakos kiadványokban. [69]

**Terroristák**

Alvin Toffler világhírű társadalomtudós és kritikus az 1980-ban (2002-ben magyarul is) megjelent Harmadik hullám című könyvében már megjósolta, hogy az ipari korszakot felváltja egy új gazdasági, társadalmi korszak, amit ma információs társadalomnak hívunk. [71] A gyorsan bővülő nemzetközi számítógépes hálózatokon földrajzi és politikai-társadalmi korlátozás nélkül **egyre több ember számára válik lehetségessé** az otthoni, munkahelyi, vagy mobil számítógépen keresztül az óriási és naponta bővülő **információtömeghez való hozzáférés**, valamint a sokoldalú kommunikáció. Az információs társadalom kialakulásának számos pozitívuma mellett azonban negatív következményei is vannak, mint például bárki számára (felhasználási céltól függetlenül) elérhetővé vált egy hatalmas tudásbázis (akár bombák teljes kapcsolási rajzát is megtalálhatjuk az interneten). **Véleményem szerint** az előbbiek szükséges velejárója, hogy **megnő a bűnözés és a terrorizmus veszélye**, kialakulhat a **határok nélküli terrorizmus** („Digitális Pearl Harbor"), mivel a gazdasági és társadalmi élet a támadható információs rendszerekre épül. [72]

Már a 2001. szeptemberi terrorcselekményeket követően körvonalazódott az a félelem miszerint az al-Kaidához hasonló terrorcsoport számítógépes támadást indít az Egyesült Államok ellen. Ezt támasztja alá a CSO[40] felmérésének eredménye is, mely szerint **a megkérdezett szakértők 49%-a** már akkor **elképzelhetőnek tartotta egy számítógépes terrortámadás bekövetkezését**, **95 százalék** azon a véleményen volt, hogy **fokozni kell a számítógépes rendszerek biztonságát.** Az **amerikai biztonsági szakemberek jó része** is **óriási veszélyt lát** az egyre inkább elfajuló hackertámadásokban. Manapság már több nemzet hackerei is rendelkeznek olyan eszközökkel és képzettséggel, hogy akár az amerikai kormányzat számítógépes rendszereit is képesek lehetnek feltörni.

Az első cyberterrorista akcióként tartják nyílván az 1997-ben az LTTE (Tamil Eelam Felszabadító Tigrisei) nevéhez fűződő támadást, melynek során néhány tagjuk bebörtönzé-

[40] Chief Security Officer Magazine

se elleni tiltakozásul spamekkel árasztották el a világ különböző országaiban működő srí lankai követségek e-mail postaládáit. [73]

A cyberterrorizmus egyik legelső meghatározása az FBI cyber részlegének volt vezetőjétől – Keith Lourdeau-tól – származik: „*A cyberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy azok romboljak és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.*" [74]

A félelem pedig beigazolódni látszik, mert például 2009 júliusában feltételezhetően észak-koreai vagy velük szimpatizáló csoportok által dél-koreai magán- és kormányzati oldalakat ért DDoS-támadás. De célpont volt az elnök weblapja, a Koreában állomásozó amerikai csapatok honlapjai, bankok és hírportálok, stb. Ez többek közt azt bizonyítja, hogy „*néhány ember, különösebb hadászati tudás nélkül, akár egy informatikailag fejletlen államból is képes fennakadásokat okozni egy másik, informatikailag fejlett országban*". [75: 46.p.]

### 2.4.2. A TÁMADÓK MOTIVÁCIÓI

A kezdetek kezdetén a **legfőbb motiváció a kihívás** volt. Erre példa Kevin Mitnick is, a 80-as és a 90-es évek leghíresebb hackereinek egyike, aki öt évet töltött börtönben telefon- és számítógépes rendszerek feltöréséért. Számos rendszerbe betört, de nem anyagi haszonszerzés céljából (még saját ügyvédre sem tellett neki, kirendelt védő védte), hanem pusztán a kihívás végett.

A későbbiekben, mások esetében ez a motiváció megváltozott és már nem a képességek bizonyítása volt a legfőbb cél, hanem (személyes, üzleti, katonai, stb.) **információk megszerzése, szolgáltatásokhoz való illetéktelen hozzáférés** (például nyomtatni, filmeket letölteni) **haszonszerzés**, vagy **károkozás** céljából, esetleg **politikai okokból** és ennek elérése érdekében vagy pusztán csak szórakozás, versengés miatt szolgáltatások megbénítása, rosszindulatú program(ok) bejuttatása az egyes rendszerekbe.

Egyedi gépeket támadhatnak pusztán szórakozásból, de azzal a céllal is, hogy a későbbiekben felhasználják annak erőforrásait egy komolyabb rendszer ellen indított támadás során.

Kijelenthető tehát, hogy mára a támadások legfőbb motivációja a kihívás mellett, **anyagi- politikai-, gazdasági- vagy katonai előnyszerzés**. A közigazgatás informatikai rendszereire vonatkoztatva a katonai előnyszerzés jelenleg nem releváns.

### 2.4.3. A TÁMADÓK CÉLPONTJAI

A 21. században az **informatikailag fejlettebb országok egyre nagyobb veszélynek vannak kitéve**, hiszen a számítástechnika és az internet a világgazdaság civilszférájától egészen a kormányzatokig mára csaknem mindenhol jelen van. Célpontnak számíthatnak a bankok, a közlekedés, a pénzügyi rendszerek, a távközlés, a rendőrség, a katonai létesítmények, az energiaellátás, melyek esetleges támadása során az állami infrastruktúra is érzékenyen károsodhat, de célpont lehet akár az otthoni személyi számítógépünk is.

Az operációs rendszereket tekintve megállapítható, hogy 2004-ben **a Microsoft rendszerei voltak a támadások közkedveltebb célpontjai**. Ezt támasztotta alá az AvantGarde vállalat 2004 szeptemberében végzett vizsgálata is, miszerint (hat gépen interneteztek két héten keresztül, különböző operációs rendszereket használva, többségében vírusirtó és tűzfal nélkül) a legtöbb támadás (45 %) az 1-es javítócsomaggal ellátott Windows XP-t futtató PC-t érték, az első támadásra csupán négy percet kellett várni. A helyzeten csak rontott, hogy a Microsoft 2008 júniusában kivezette a terméket a piacról, és a tervek szerint csak 2014-ig nyújtanak hozzá támogatást, viszont valószínűleg az újabb verziókhoz képesti kisebb erőforrásigénye miatt még széles körben használják a közigazgatásban is. A vizsgálat adatait a 2. táblázat tartalmazza.

2. táblázat: A konfiguráció, a támadások száma és százalékos értéke [76]

| **Konfiguráció** | **Támadás** | **%** |
|---|---|---|
| Windows SBS 2003 | 25222 | 8,24% |
| Windows XP SP1 | 139024 | 45,44% |
| Windows XP SP1 with ZoneAlarm 5.1 (Free) | 848 | 0,28% |
| Windows XP SP2 | 1386 | 0,45% |
| Mac OS X 10.3.5 | 138647 | 45,32% |
| LinSpire (Linux) | 795 | 0,26% |

A legjobban a Linspire, az 1-es szervizcsomaggal és a Zone Alarm tűzfalprogram egy példányával ellátott Windows XP, illetve a 2-es javítócsomaggal kiegészített Windows XP teljesített. A számítógépes kártevők ezt a három PC-t, illetve operációs rendszert csu-

pán az esetek 0,3-0,4 százalékában támadták. A Mac OS X 10.3.5 operációs rendszert futtató számítógép esetében, bár a rosszindulatú akciók 45 százalékban ez ellen a gép ellen irányultak, gyakorlatilag semmilyen kár nem érte ezt a számítógépet. Ez az eredmény azzal magyarázható, hogy a kártevőket a Windows operációs rendszerekre, illetve azok biztonsági réseire „optimalizálták" és készítették a vírusírók. [65]

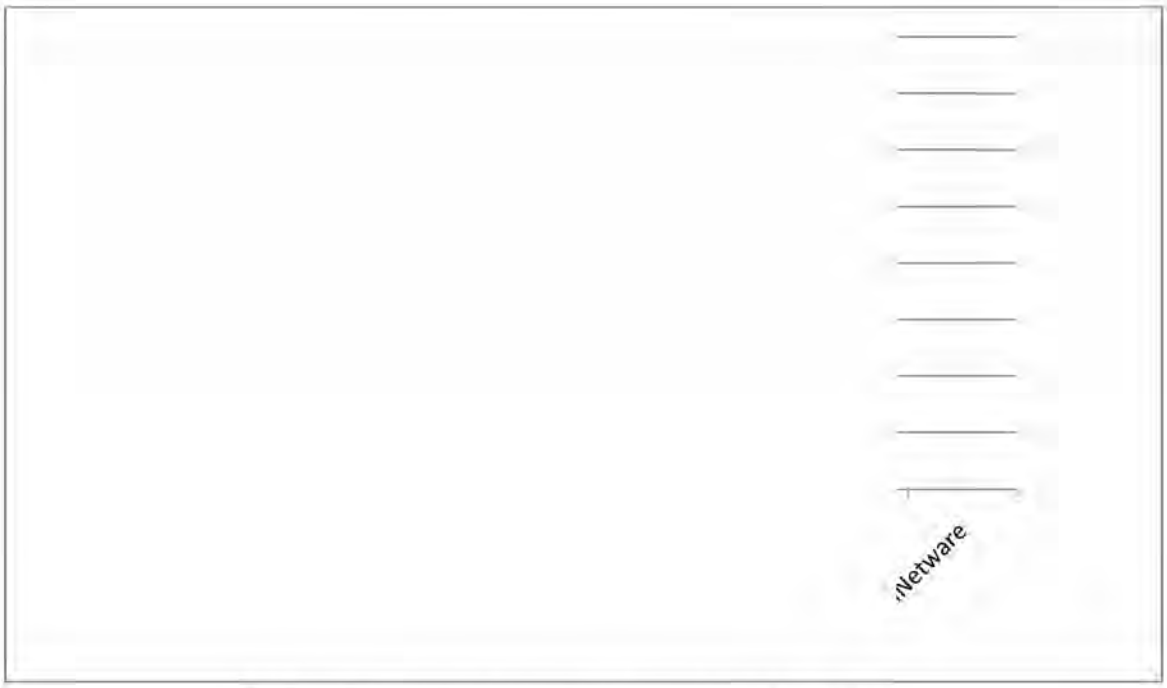
Sokan hitet tettek a **nyílt forráskódú rendszerek** biztonságossága mellett, ennek megfelelően sok helyen használják, legfőképpen szerver funkciók ellátására, azonban annak vitathatatlan előnyei mellett óriási hátrányai is kezdenek kibontakozni. Ennek legfőbb okát a **számtalan verzió** létezésében látom. Ezzel szemben a Microsoft termékek esetén nem kell annyi változatra koncentrálni, így azok biztonsági problémái is könnyebben javíthatók. Ez tükröződik a támadási kísérletek alakulásának vizsgálata során is, egyre inkább hátrányba kerül a Linux a Windows rendszerekkel szemben a biztonság területén.

Drasztikus mértékben nő a weboldal-feltörések száma. A zone-h.org honlap **szerverek biztonságáról**, illetve **sebezhetőségéről vezet listát**, az adatokat többnyire maguk a támadók szolgáltatják, de bárkinek lehetősége van hírt adni egy-egy támadásról, és annak körülményeiről. Az oldal lehetőséget biztosít **támadások archívumból történő, támadóra, dátumra, domainre vonatkozó szűrt listájának megjelenítésére**. Külön menüpontból érhető el a kitüntetett szerepű, pl. kormányzati szerverek elleni támadások archívuma.

**Megvizsgáltam a támadások alakulását a leggyakoribb** (Windows, Unix, Novell, Linux) **operációs rendszerek esetében, az elmúlt 3 évre** vonatkoztatva. Az eredményt a 3. táblázat, valamint a 7. ábrán látható diagram szemlélteti.

3. táblázat: Támadások operációs rendszerenként [77]

| | 2008 | 2009 | 2010 |
|---|---|---|---|
| **Win 2008** | 364 | 2977 | 3165 |
| **Win 2003** | 117978 | 127128 | 81785 |
| **Win 2000** | 21929 | 12529 | 2805 |
| **Win XP** | 329 | 270 | 72 |
| **Win NT9X** | 440 | 225 | 132 |
| **Linux** | 352468 | 378744 | 256648 |
| **Unix** | 3 | 29 | 43 |
| **NovellNetware** | 5 | 5 | 0 |
| **Összesen** | 495160 | 520939 | 343495 |




7. ábra: Támadások operációs rendszerenként [77]

Az elemzés eredményeként az alábbi **megállapításokat teszem**:

- az elmúlt években már – ellentétben a 2004-es állapottal – **a Linux sokkal kedveltebb célpont lett**, mint a Microsoft operációs rendszerei;
- a Windows operációs rendszerek esetében ugrásszerű változás nem tapasztalható. A **Windows 2008 támadásainak száma kismértékben növekszik**, ami betudható az operációs rendszer egyre szélesebb körű elterjedésének, **míg a Windows 2003, Windows 2000, XP, NT és 9X változatok** fokozatosan kiszorulnak a piacról, így érthető a **támadásuk számának kismértékű csökkenése**;
- Unix illetve NovellNetware rendszerek ellen a vizsgált időszakban csak néhány támadás történt, mely elhanyagolható, bár a Unix esetében folyamatos enyhe növekvő tendencia tapasztalható;
- a **Linux rendszerek elleni támadások száma lényegesen magasabb, mint a Windows rendszereké**, ami érthető is, hiszen a legnépszerűbb támadási forma web szerverek ellen irányul, és köztudott, hogy web szervereket leginkább Linux rendszerek alatt üzemeltetnek. Viszont a **Linux** rendszerek támadásában **csökkenés**, míg **Windows 2008** esetében **folyamatos emelkedés** tapasztalható.

Megfigyelhető továbbá az is, hogy a hackelések száma különböző politikailag érzékeny évfordulókon észrevehetően megszaporodik, különösen az Egyesült Államok és az

iszlám terroristák közötti konfliktusok évfordulóin. Egy vizsgálat azt is kimutatta, hogy a hosszabb munkaszüneti időszakok, például karácsony környéke is megemelik a támadások számát. [78]

### 2.4.4. A TÁMADÁSOK HATÁSAI

Egy vállalati és egy közigazgatási informatikai rendszer tekintetében az **alapvető különbség a tárolt-feldogozott információkban van.** A közigazgatási informatikai rendszerekben **lényegesen több személyes adattal dolgoznak**, melyet a szakági törvények eléggé kiterjesztetten engedélyezik is, ennek ellenére sokkal kevesebb informatikai biztonsági szabályt alkalmaznak, mint a vállalati szférában. Például katasztrófa-elhárítási terve az intézmények egytizedének, IT-szabályzata is csak 22 százalékának van és biztonsági auditot is csupán 4 százalékuk végeztetett 2010-ben. [79] Fontos még megemlíteni **a hivatalok közötti adatcserék**et, amik szintén **kiterjedtebbek**, mint a vállalatoknál.

Egy vállalati és egy közigazgatási informatikai rendszert ért támadást összehasonlítva megállapíthatjuk, hogy az alkalmazott **módszerek, eszközök** és a támadók **motivációja** tekintetében **lényeget érintő eltérés nem tapasztalható.**

**A lényegi eltérés a támadások hatásában jelentkezik**. Egyrészt a már említett **személyes adatokkal való visszaélés** messze nincs annyira jelen a vállalatoknál, mint a közigazgatásban. Senki sem örülne, ha bárki hozzáférne a személyes, vagyoni, pénzügyi, stb. adataihoz, vagy visszaélnének azokkal, esetleg meghamisítanák azokat. Mint azt már korábban is említettem, ha a rendszer sérülékenységéből adódóan egy támadó születési anyakönyvi kivonatot képes igényelni valakinek a nevében, azzal már a többi okmány beszerzésére is lehetősége nyílik és így képes lesz az illető identitását eltulajdonítani, az ő nevében esetleg törvénytelen dolgokat is elkövetni.

Az üzemeltetési hiányosságok miatt **a rendelkezésre állási fenyegetések komolyabbak a közigazgatásban,** mert – mint azt az első fejezetben megállapítottam, hogy a közigazgatási informatikai rendszerek kritikus információs infrastruktúrák, – működésük (működésfolytonosságuk) létfontosságú a társadalom számára. Különösen akkor, ha olyan az egész országot lefedő közigazgatási informatikai rendszerről van szó, mint az EKG, vagy az Ügyfélkapu, melyek működése nélkül ma már komoly kormányzási, igazgatási folyamatok sérülhetnek, ami nem megengedhető. Ha például egy támadás következtében

megbénul egy ügyiratot befogadó, feldolgozó rendszer, akkor az állampolgárok nem tudják az ügyeiket például adóbevallásukat időben elintézni, ami beadási határidő eltolódásához, sok elégedetlen bosszús állampolgárhoz, majd ezt követően a feldolgozási feltorlódásnak következtében túlterhelt ügyintézőkhöz vezet. Mindennek közvetett következménye lehet például a kormányzat (a kormányzó politikai erő) negatív politikai megítélése is.

Ilyen negatív hatások érvényesülhetnek az önkormányzatok szintjén is. 2007 decemberében egy Győr-Moson-Sopron megyei településen tolvajok elvitték az önkormányzat két számítógépét, mellyel szinte teljesen ellehetetlenítették az önkormányzat működését. A kár ugyan néhány százezer forintos volt, de a kis költségvetésű önkormányzat nem tudta azt pótolni és a számítógépen tárolt adatok egy része más formában nem létezett, így azok örökre elvesztek. Pályázati anyagok, elszámolások, temetői nyilvántartás, légi felvételek és fotók a falu életéből, mind pótolhatatlan dokumentumok. Az eszközök hiányában a lakosság jóval nehezebben tudta intézni ügyeit. [80]

Könnyen belátható az is, hogy **a vállalati szféra jobban érdekelt a biztonság kialakításában**, mivel ott egy támadásból, de akár még egy támadási kísérletsorozatból is konkrét anyagi veszteség keletkezhet (például piacvesztés). Ezzel szemben a közigazgatási rendszerben mivel ez egy nagy közös rendszer, – még ha esetleg nevesítik is a felelőst minisztériumok formájában – kevésbé érdekelt ebben. Nincs közvetlen anyagi kár, emiatt sokkal nehezebb a vezetőkkel és az alkalmazottakkal is elfogadtatni a biztonságtudatosság kérdését. A közvetett károkat (például a társadalom megítélése) tudatosítani pedig sokkal nehezebb.

Nem hagyható figyelmen kívül a **cyberhadviselési fenyegetés** sem, ami a kritikus információs infrastruktúrákon kívül nem jellemző a vállalati világban. Egy informatikai támadás során **az állami infrastruktúra is érzékenyen károsodhat**. De gondoljunk csak bele, hogy például egy komplex informatikai támadás eredményeként egy erőmű leállása csupán elektromos energia kieséssel járna, de ha mindez mondjuk egy forró nyári napon történne, akkor a légkondicionáló berendezések működés-kiesése következtében sokan lennének rosszul, és ha a támadás még a segélyhívószámok letiltásával is járna, akkor katasztrofális helyzet alakulhatna ki. A hatás akár nagyságrendekkel nagyobb lehet, ha az informatikai támadás kiegészül más, a teljes infokommunikációs rendszert érintő támadási formákkal például elektronikai zavarás, fizikai támadás. Ha egy ilyen komplex támadás áldozatává válik a kritikus információs infrastruktúra, akkor **a kormányzás, a közigazga-**

**tás működőképessége is veszélybe kerülhet,** ami jelentősen korlátozhatja az ország működését is.

Mindezek alapján teljesen egyet lehet érteni Kovács László és Krasznay Csaba értékelésével, miszerint: „*...informatikai eszközökkel végrehajtott támadásokkal már ma is komoly károk okozhatók, azonban ezek az ország egész lakosságára és gazdaságára vonatkoztatva feltételezhetően rövid ideig tartó, részleges fennakadásokat jelentenének csak. Akkor azonban, ha az informatikai támadásokat kiegészítik az információs rendszerek egyes – jól megválasztott – elemei ellen végrehajtott fizikai támadások, akkor a kár óriási lesz.*" [75: 47.p.]

# KÖVETKEZTETÉSEK

Az informatikai rendszerek elleni **támadások főbb lépéseinek tisztázása** után **újszerűen rendszereztem, csoportosítottam a közigazgatás informatikai rendszerei szempontjából** az egyes lépéseket támogató, leggyakrabban alkalmazott **veszélyforrást jelentő támadási formákat**. Ennek megfelelően **megvizsgáltam és elemeztem a külső támadások** lehetőségét a hálózat, az operációs rendszer és a telepített alkalmazások sérülékenységeinek kihasználása szempontjából, a **belső veszélyeztetések** különböző lehetőségeit, valamint a **kettő kombinációjában** végrehajtható támadási formákat.

Napjainkban egy igencsak aktuális kérdésre kívántam kutatásommal választ adni, hogy **nyílt vagy zárt forráskódú operációs rendszerek használata célszerűbb** a közigazgatási rendszerek számítógépein. Ennek megfelelően virtuális környezetben modelleztem, **teszteltem és elemeztem** több szerver-szolgáltatást – úgymint levelező-, webkiszolgáló, tanúsítványok alkalmazási lehetősége, felhasználó- és jelszókezelés, beépített tűzfalszolgáltatás – és azok biztonsági beállításait jellegzetes nyílt és zárt forráskódú rendszereken és **a következő összegzett megállapításokra jutattam:**

- a **nyílt forrású rendszerek** nagy előnye és egyben nagy hátránya is a zárt forrásúakéval szemben, hogy **bárki betekinthet a kódba**, így egy **biztonsági rés rövidebb időn belül javításra kerülhet**. Azonban felfogható ez úgy is, hogy **sokkal rövidebb időn belül válik sérülékennyé egy nyílt forráskódú operációs rendszer azáltal, hogy bárki betekinthet a kódba;**
- az elvégzett tesztek alapján **arra a következtetésre jutottam**, hogy **a vizsgált operációs rendszerek mind a beépített biztonsági képességek mind teljesítmény szempontjából nem mutatnak szignifikáns eltérést**. Egyes szempontokból az egyik, más szempontokból a másik bizonyult egy kicsivel előnyösebbnek. Bár az SQL injection elleni védelem és a spam szűrés lehetősége a **Linux felé billentené a mérleg nyelvét**, de figyelembe véve azt a speciális, magyarországi és egyben a magyar közigazgatásban is fennálló problémát, miszerint az esetek többségében **nincs meg a kellő szaktudás** a Linux rendszerek konfigurálásához és üzemeltetéséhez, valamint, hogy **a korábbi saját fejlesztésű Microsoft alapú alkalmazások átállítása is problémát jelent**, jelentősen megváltoztatja a helyzetet. A **szakemberképzésbe**, valamint a **saját fejlesztésű alkalmazások átállításába** invesztált tőke **és a nyílt és zárt forráskódú operációs**

**rendszerek költségbeli különbségeit** összevetve a különbség **már nem releváns**, ezért már nem éri meg a kellő szaktudás (részleges) hiányából fakadó **kockázatot** vállalva a kialakulóban levő nemzetközi trendet követni. **Véleményem szerint a döntő szempont a felhasználás szakszerű volta kell, hogy legyen**. Jelenleg a magyar informatikai szakemberek többsége inkább a Microsoft operációs rendszerek üzemeltetéséhez szükséges szaktudással rendelkezik.

**Megállapítottam** továbbá, hogy a közigazgatási szolgáltatások webes felületű alkalmazások területén történt térhódításából fakadóan **az egyik legnagyobb sérülékenységi** problémát az **alkalmazások gyengeségei** okozzák. Ugyanis a nem kellően biztonságos web alkalmazások üzemeltetése többek között a hátterükben működő adatbázisokban tárolt adatok kiszolgáltatását eredményezheti a támadók számára.

**Megvizsgáltam** a **támadók körét** és megállapítottam a magyar közigazgatási informatikai rendszerek támadásával kapcsolatba hozható csoportjait, a támadók **motivációinak átalakulását** a technológiai fejlődés következtében, valamint **a támadások lehetséges célpontjait**. **Elemeztem** a releváns operációs rendszereket ért támadási arányokat az elmúlt néhány évre vonatkozólag, mely alapján **megállapítottam**, hogy **a Linux elleni** támadások száma **drasztikusan magas** a többi operációs rendszerhez képest. Tehát ennek, és a fentebb tett megállapításaim fényében már könnyebb a döntés meghozatala, hogy **bár kisebb befektetést igényel** ugyan **a Linux használata**, **de a kellő szaktudással** rendelkező személyzet oktatása, ismereteinek frissen tartása, valamint a jelenleg működtetett Microsoft platformú alkalmazások átállítása jelentős költségeket von maga után, ráadásul, még **nagyobb valószínűséggel válik a támadások célpontjává**.

Vizsgálataim során **megállapítottam**, hogy egy vállalati és egy közigazgatási informatikai rendszert ért támadás során az alkalmazott **módszerek, eszközök** és a támadók **motivációja** tekintetében **lényeget érintő eltérés nem tapasztalható**. Az **alapvető különbséget** egyrészt a tárolt-feldogozott információk jellegének különbségéből fakadó **következményekben,** másrészt **a rendelkezésre állási fenyegetések kormányzásra gyakorolt negatív hatásában,** harmadrészt **a cyberhadviselési fenyegetéseknek a közigazgatás működőképességére gyakorolt negatív hatásában látom.**

# 3. FEJEZET
# A KÖZIGAZGATÁS INFORMATIKAI RENDSZEREIBEN ALKALMAZHATÓ VÉDELMI MEGOLDÁSOK

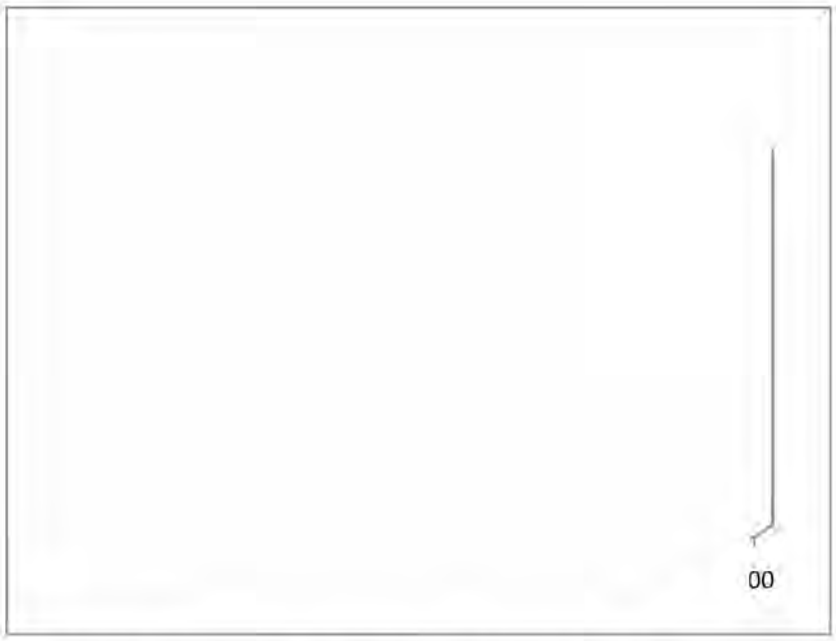
*„A támadás blokkolására, illetve bármilyen ellentámadásra ma még nincs hatékony infokommunikációs eszköz a kezünkben. Ugyanakkor – éppen e tényből következően – elengedhetetlenül fontos a megelőzés, a jogszabályoknak, szabványoknak, ajánlásoknak megfelelően felépített, megfelelő tartalékolással rendelkező biztonságos rendszerek kialakítása.*" [81: 51.p.]

A közelmúltban az informatikai rendszerek csaknem minden vállalat, illetve közigazgatási rendszer működésének alappillérévé váltak, nagyban segítik az eredményes munkavégzést, nagyobb szervezetek esetén elkerülhetetlen használatuk. Ugyanakkor az informatikai rendszerek kritikus fontossága nagymértékű kockázatot jelent, hiszen rengeteg veszélynek vannak kitéve, a működésük során fellépő hibák pedig komoly veszélyeket jelenthetnek egy szervezet működésére nézve. Ezen okokból kifolyólag az informatikai rendszerek kockázatkezelése egyre fontosabb szegmensévé válik egy szervezet irányításának.

A hibákat teljes mértékben kizárni nem lehet, és egzakt megoldás sincs a kockázatok kezelésére, hiszen a szervezet profiljától függően a kockázatok változnak. Ugyanúgy, ahogyan a kockázatok típusai, a mértékük is változó, az egészen apró működési problémáktól a teljes működés leállásáig terjedhetnek.

Muha Lajos „A Magyar Köztársaság kritikus információs infrastruktúráinak védelme" [81] című doktori értekezésében fentebb megfogalmazott gondolatsorát csak megerősíteni tudom, azzal egyetértve vizsgáltam meg, hogy milyen eszközök, módszerek, eljárások használhatók a közigazgatási informatikai rendszerek biztonságának magasabb szintre emelésének érdekében.

A Nemzeti Hálózatbiztonsági Központ 2010. éves jelentéséből [79] a Bellresearch kutatásai alapján készített, a költségvetési szektorban alkalmazott védelmi megoldásokkal kapcsolatos adatok a 8. ábrán láthatók.




8. ábra: Védelmi megoldások 2010-ben a költségvetési szektorban [79]

Az ábrán csak a korunk informatikai rendszereinek biztonsága érdekében **elvárt, alapvető védelmi megoldások kerültek ábrázolásra.** Ugyan pontos számadatok nem kerültek feltüntetésre, de hozzávetőlegesen leolvasható és jól látható, hogy még a legnagyobb arányban alkalmazott, **manapság már kötelezőnek mondható védelmi megoldások**, mint az antivírus-szoftverek és a tűzfalmegoldások **alkalmazása sem tapasztalható a teljes intézményi szektorban**. A jelentéséből az is kiderül, hogy a szervezetek egy része semmilyen informatikai biztonsági megoldást nem alkalmaz, azaz számítógépek ezrei minden védelmet nélkülöznek a közszférában. [79] Természetesen olyan munkaállomást tekintve, amely nem rendelkezik semmilyen hálózati kapcsolattal és nincs lehetőség külső adathordozó csatlakoztatására sem, valóban nincs szükség vírusellenőrzésre és tűzfalra sem. De a 21. században vajon milyen munkavégzésre használható fel egy ilyen munkaállomás?

A jelentésből kiderül az is, hogy **a kifinomultabb védelmi megoldások elterjedtsége valamelyest** ugyan **emelkedett**, azonban az olyan szofisztikáltabb védelmi megoldások, mint a rendszerhasználat és a hozzáférés naplózása vagy a behatolás-érzékelés, még az intézmények egyötödében sem került bevezetésre. [79]

Az **informatikai biztonsági stratégia hiányáról és a nem megfelelő szemléletmódról** az első fejezetben részletezett észrevételeimet is alátámasztja ez a felmérés, mely szerint a számos külföldi példa ellenére (Németország, USA, stb., ahol értékes – kormány-

zati – adatok kerültek illetéktelen kezekbe mulasztás, szándékos károkozás vagy véletlen hiba következtében) **az informatikai biztonságot stratégiai szintre emelő tudatos gondolkodás csak a hazai intézmények kis hányadára jellemző**. A magyarországi intézmények jó esetben jellemzően **csupán a védelem legalapvetőbb elemeit alkalmazzák**. Erre utal, hogy például „*... katasztrófa-elhárítási terve csak minden tizedik intézménynek van, de informatikai szabályzatot is csak az érintett döntéshozók egyötöde követelt meg, biztonsági auditnak pedig kevesebb, mint 3 százalék vetette alá magát.*" [79: 6.p.] Pedig a pontos, egyértelmű és a részletekre kiterjedő szabályozási keretek és a cselekvési tervek definiálása nélkül egyrészt nehezebb a számonkérés, másrészt nehezebb látni, hogy mi fog történni, ha bekövetkezik a baj. Az sem elhanyagolandó, hogy a szervezetek hiába védik adataikat például a külső támadásoktól, ha a jogosultságok hézagos szabályozása miatt bármely alkalmazott engedély nélkül is hozzáférhet az információkhoz, esetleg valamilyen adattárolón ki is viheti a szervezetből.

A veszély mértékét nem könnyű becsülni, de léte minden kétséget kizáróan belátható. A megfelelő, kockázattal arányos védelmi módszerek kiválasztásához **kockázatelemzés szükséges**.

## 3.1. KOCKÁZATELEMZÉS

### 3.1.1. KOCKÁZATELEMZÉS AZ INFORMATIKAI RENDSZEREKBEN

A teljes körű, és minden fenyegetést kezelő védelem kiépítéséhez szükséges **anyagi erőforrás nem minden szervezet esetében áll rendelkezésre**, különösen igaz ez a közigazgatás szervezeteire. Az egyes informatikai rendszereket fenyegető veszélyforrások által okozott kockázatok mértéke nagymértékben függ az adott szervezet tevékenység típusától, a szervezet által kezelt adatoktól, továbbá a szervezet elhelyezkedésétől, felépítésétől és méretétől is. **Ahány szervezet, annyiféle kockázat profil különböztethető meg**, ezért **nem lehet minden szervezetre érvényes, az informatikai kockázatok kezelésére vonatkozó konkrét útmutatót kidolgozni.** Például egy olyan kereskedelmi vállalatnak, amely honlapján csak statikus információt jelenít meg (reklám, elérhetőség, vállalati profil, vezetés, stb.), nem okoz nagy gondot, ha rövid ideig honlapjuk nem elérhető, de jelentős mértékben kell a kereskedelmi- és tervinformációit védeni. Egy nagy pénzügyi vagy egy közigazgatási szervezet esetében azonban jelentős károkat okozhat, ha sérül az elérhetőség és rendel-

kezésre állás követelménye. Így tehát nem adható minden szervezetre érvényes, a kockázatok kezelésére vonatkozó konkrét útmutató, de **általános iránymutatást meg lehet fogalmazni**, melyet a konkrét szervezet sajátosságainak figyelembevételével kell implementálni. Ilyen általános iránymutatást fogalmaztam meg a „IT kockázatok, elemzésük, kezelésük" [82] című cikkemben is melyben foglaltakat az alábbiak szerint felhasználtam a közigazgatási informatikai rendszerekre vonatkozó kockázatelemzés elkészítése során.

A **kockázat** egyrészt **valamilyen veszélyforrás által okozott nemkívánatos következmények lehetősége, valószínűsége**, másrészt **a következmények természete és súlyossága**. Az informatikai rendszereket érintő veszélyek kockázatai komoly hányadát, több mint 50%-át teszik ki a teljes szervezeti kockázathalmaznak.

**A kockázatmenedzsment feladata a rendszert fenyegető veszélyek felmérése, és a megfelelő védelmi stratégia kidolgozása**. A felmerülő kockázatok egyedi kezelése helyett **törekedni kell egy egyenszilárdságú rendszer kiépítésére**, mely minden pontján egyforma erősségű védelmet nyújt, így a teljes rendszer hatékonysága nagyban növelhető. Alapvető igény, hogy a védelem hatékony és optimális legyen, ehhez azonban szükséges **a kockázatok, és a lehetséges veszteségek** pontos ismerete. Ezen adatok **számszerűsítése, vagy pénzbeli kifejezése azonban nagyon nehézkes feladat**, legfőképp az informatikai rendszerek vizsgálatánál.

A védelemre fordítandó költség meghatározása hasonlóan nehéz feladat, de általában érvényes az a szabály, hogy **a védelemre fordított energia és tőkebefektetés ne haladja meg a lehetséges kár által okozott veszteséget**. Ezen stratégiai lépések meghozatalához **a vezetés, és a megfelelő szakemberek magas fokú együttműködése szükséges**, mivel a helyes döntések meghozatalához a problémakör megfelelő átlátására van szükség.

Több kockázatkezelési módszertant tanulmányozva és a fentiek figyelembevételével a kockázatmenedzsment általam is ajánlott szakaszai:

1. veszélyforrások felmérése;
2. kockázatelemzés, becslés;
3. a lehetséges védelmi intézkedések számbavétele;
4. kockázatok kezelése.

A **veszélyforrások felmérése** a jelenlegi rendszer elemzését, gyenge pontjainak feltárását, a lehetséges fenyegetettségek megismerését jelenti. A közigazgatási informatikai rendszerekre vonatkozólag ezt a lépést az előző fejezetben végeztem el.

A kockázatmenedzsment második szakasza a lehetséges **kockázatok felmérése** és a nemkívánatos események bekövetkezésekor **keletkező kár becslése**. Ez igen komoly feladatot jelent minden esetben, de az informatikai rendszereknél ezen adatok **számszerűsítése szinte lehetetlen feladat**. A legtöbb kockázatkezelési módszertan nem is vállalkozik a vagyoni ráfordításban való kifejezésre. Ennek legfőbb oka, hogy **az informatikai rendszereket ért károk** általában nem közvetlenül fejtik ki hatásukat, hanem a velük kapcsolatban álló rendszerelemeken keresztül **az egész szervezet működésére befolyással lehetnek**. Például egy adattároló meghibásodása, amelynek javítása vagy cseréje önmagában nem jelent nagy költséget, azonban az információvesztés, és az emiatt történő kiesés komoly kockázatokkal járhat. Az informatikai rendszerben bekövetkezett károsodás nem megfelelő védekezés mellett könnyen fennakadást okozhat a vele kapcsolatban álló munkafolyamatokban, ezzel áttételesen akár a szervezet alaptevékenységét is veszélyeztetheti.

Mivel a bekövetkezési valószínűségek, és az okozott veszteségek számszerűsítése nehéz feladat, ezért a legtöbb módszertan kategóriákat állít fel ezek becslésére. A kategóriákba sorolással lehetőség nyílik a becsült értékek nagyságrendbeli összehasonlítására.

A kockázatbecslés során három alapvető kategóriacsoport állítható fel, ezeket használtam én is az elemzés során:

- **kár kategóriák**: kis összegű elsődleges kártól, a szervezet létét fenyegető veszélyforrásokig. A kategóriákba sorolásnál figyelembe kell venni az okozott kár természetét, illetve, hogy a rendszer milyen tulajdonsága sérült. (Például bizalmasság, sértetlenség, rendelkezésre állás.);
- **a bekövetkezési valószínűségek kategóriái**: az évente többször előforduló, bármikor bekövetkezhető veszélyforrásoktól a minimális eséllyel rendelkező fenyegetettségekig. A kategóriákba sorolásnál a valószínűség meghatározása a tapasztalati tényezőkön vagy szimuláción alapulhat. Támadás elemzése esetén fontos szempontot játszik a rendszer gyengeségének kihasználásához szükséges támadási potenciál, szaktudás megállapítása;
- **kockázatok kategóriái**: a kockázatokra fordítandó relatív vagyon és energia befektetés kategóriái.

A kategóriák száma csoportonként erősen függ attól, hogy milyen és mekkora az elemzett rendszer, de általánosságban 4-7 kategória definiálása célszerű csoportonként.

Az előzetesen már felderített kockázati tényezők kategóriákhoz rendelése után megkezdődhet **az egyes fenyegetések kockázatának elemzése**. Ez általában az egyes fenyegetések előfordulási valószínűségének és az okozott kár nagyságának összevetésével, például az „Informatikai Rendszerek Biztonsági Követelményei" című MeH ITB ajánlása [83] alapján az alábbi matematikai módszer szerint történhet:

$$R=\sum p_t \times d_t \qquad \text{minden } t \in T \text{ –re}$$

ahol:

**R :** a kockázat (Risk);

**T :** a veszélyforrások halmaza (Threat);

$\mathbf{p_t}$ **:** egy adott veszélyforrás bekövetkezési valószínűsége (probability);

$\mathbf{d_t}$ **:** a keletkező kár (damage) mértéke.

A kockázatok bizonyos csoportjára külön figyelmet kell fordítani, mivel néhány, általában nagyon alacsony valószínűségű veszélyforrás a szervezet életére erős mértékben hathat, akár veszélyeztetheti is annak fennmaradását. Ezek az **elviselhetetlen vagy kiemelt kockázatok**, amelyek elleni védekezésre történő anyagi **ráfordítás** esetenként a valószínűség mértékéhez képest **indokolatlanul magas lehet**, azonban hosszútávon számolni kell velük, a felkészülés mindenképp szükséges.

A kockázatmenedzsment harmadik szakasza **a lehetséges védelmi intézkedések számbavétele**. A legfontosabb szempont természetesen az egyes veszélyforrások csökkentésére fordított anyagi ráfordítás és az elért hatás optimalizálása. Figyelembe kell venni azt is, hogy az egyes védelmi intézkedések hatással lehetnek egymásra, de hatásuk nem feltétlenül adódik össze. A cél, olyan kombinációt találni az adott lehetőségek közül, mely **a teljes rendszer védelmét a lehető legnagyobb mértékben lefedi, és minden elviselhetetlen mértékű kockázatot legalább elviselhető mértékűre csökkent, valamint lehetőség szerint költséghatékony is**.

A kockázatmenedzsment negyedik ajánlott lépése **a kockázatok kezelése,** amelynek alapvető módjai az alábbiak:

- a veszélyforrás megszüntetése;
- a bekövetkezési valószínűség csökkentése;
- az okozott kár csökkentése;
- a kockázat áthárítása, vagy
- tudatos kockázatvállalás útján.

A **veszélyforrás megszüntetése** lenne a leghatékonyabb stratégia, azonban a kockázat teljes kiküszöbölésére csak elméletben van lehetőség. Bizonyos kockázatokat körültekintő, alaposan átgondolt, teljes körű felmérésen, elemzésen alapuló intézkedésekkel, befektetésekkel ki tudunk ugyan küszöbölni, de tökéletesen biztonságosan üzemeltethető rendszer nincs. **A** gyakorlatban legtöbbször a **bekövetkezési valószínűség és az okozott kár csökkentése** valamely kombinációja jelenti az optimális megoldást a felmerülő kockázatok kezelésére. Bizonyos esetekben **lehetőség van egyes kockázati terhek átruházására** a partnerekkel, ügyfelekkel történő **szerződéskötés** során, vagy a kockázat áthárításának egy másik formája a **biztosítás**. Ez a módszer a legtöbb esetben nem tűnik kifizetődőnek, hiszen a biztosítási összeg rendszerint meghaladja az esetleg keletkező károk mértékét, azonban biztosítás kötésével elkerülhetők a hirtelen bekövetkező, nagyarányú anyagi veszteségek, így a kockázatkezelés kontrollálhatóvá válik. Egyes esetekben pedig **a védekezésre fordítandó összeg olyan mértékben meghaladja a lehetséges maximális veszteséget**, hogy megéri meghozni a döntést **a kockázat tudatos vállalásáról**. Ilyenkor azonban teljesen tisztában kell lenni a lehetséges következményekkel, a veszteség másodlagos és harmadlagos hatásmechanizmusaival.

### 3.1.2. KOCKÁZATELEMZÉSI MODELL EGY TIPIKUS KÖZIGAZGATÁSI INFORMATIKAI RENDSZERRE

Az e-Közigazgatási Keretrendszer Kialakítása projekt keretében létrehozott „Útmutató az IT biztonsági szintek meghatározásához" című [84] ajánlás szerint *„a közigazgatási szolgáltatásokat megalapozó információk és informatikai rendszerek biztonsági kategóriái három biztonsági cél, és az ezekkel kapcsolatos veszélyeztetettségi (kihatás) szinteken keresztül definiálhatók.*" [84] Az útmutató a **nemzetközi szakirodalom alapján** a **bizalmasság**, **sértetlenség**[41] és a **rendelkezésre állás** biztonsági célokra építve végzi el az informatikai rendszerek biztonsági kategorizálását, mely alapján **alacsony**[42], **fokozott**[43] és **kiemelt kihatású**[44] rendszereket különböztet meg.

---

[41] A sértetlenség fogalmába az útmutató beleérti az információk letagadhatatlanságát és hitelességét is.
[42] Mindhárom biztonsági cél szerinti kihatás alacsony szintű.
[43] Legalább az egyik biztonsági cél fokozott szintű, és nincs fokozottnál erősebb szintű biztonsági cél.
[44] Amelyben legalább az egyik biztonsági cél szerinti kihatás kiemelt szintű.

A biztonsági cél szerinti kihatás **alacsony,** „... *amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan korlátozott hátrányos hatást gyakorol a közigazgatási szervezet műveleteire vagy a szervezet eszközeire, illetve a szervezettel kapcsolatba kerülő egyénekre* ...", **fokozott, „...** *amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan komoly hátrányos hatást gyakorol a közigazgatási szervezet műveleteire, vagy a szervezet eszközeire, illetve a szervezettel kapcsolatba kerülő egyénekre* ...", és **k**iemelt, „... *amennyiben a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése várhatóan súlyos vagy katasztrofális hatást gyakorol a közigazgatási szervezet műveleteire, vagy a szervezet eszközeire, illetve a szervezettel kapcsolatba kerülő egyénekre.*" [84]

Az előbbieket és az előző részben ismertetett kockázatelemzési elveket felhasználva, elvégeztem egy **fokozott kihatású biztonsági osztályba** tartozó mintarendszer kockázatelemzését és hatáselemzését, melynek részletei a 2. melléklet táblázataiban találhatók. Megítélésem szerint – tekintettel a fenti kategorizálásra valamint a mintarendszer feladatrendszerére és szolgáltatásaira – ilyen például az 1. fejezetben bemutatott Ügyfélapu. Az elvégzett vizsgálat egy **általam javasolt, lehetséges kivitelezése** a kockázatelemzésnek. Nem terjedt ki egy informatikai rendszert fenyegető minden veszélyforrásra (a minden rendszerelemre vonatkozó gyengepont-elemzés nyilvánosságra hozása önmagában is veszélyforrás), csupán **célirányosan, az értekezés korábbi részeiben feltárt fenyegetésekkel kapcsolatos védelmi hiányosságokra koncentrálódott**.

Az előbbieket, valamint a 2. fejezetben ismertetett veszélyforrásokat is figyelembe véve a kockázatelemzés elvégzéséhez a következő kategóriákat állítottam fel:

4. táblázat: Bekövetkezési valószínűség kategóriák

| Megnevezés | Gyakoriság, illetve támadási potenciál | Jelölés |
|---|---|---|
| Nagyon ritka | 3 évente legfeljebb egyszer, vagy ritkábban bekövetkező esemény | **0** |
| Alacsony | Évente egyszer bekövetkező esemény, vagy csak profi támadó által kihasználható gyengeség | **1** |
| Közepes | Félévente egyszer bekövetkező esemény | **2** |
| Gyakori | Havonta bekövetkező esemény vagy átlagos szakember által végrehajtható visszaélés | **3** |
| Szinte folytonos | Heti gyakoriságú, vagy gyakrabban bekövetkező esemény vagy bárki által kihasználható gyengeség | **4** |

5. táblázat: Kár kategóriák

| Megnevezés | Magyarázat | Érték |
|---|---|---|
| Jelentéktelen | Az elsődleges kár kis összegű <100.000 Ft<br>Bizalomvesztés kockázata nem áll fenn.<br>Törvények, előírások megsértése nem áll fenn.<br>Nyilvános, máshol is elérhető adatok módosulnak, elvesznek.<br>Más számára értéktelen adatok kerülnek nyilvánosságra.<br>Helyreállítás időigénye legfeljebb 1 óra. | 1 |
| Csekély | Másodlagos, nagyobb összegű kár, 100.000 Ft-nál több, de 3 millió Ft-nál kevesebb<br>Bizalomvesztés kockázata nem áll fenn.<br>Törvények, előírások megsértése kis mértékben megtörténhet.<br>Alacsony bizalmasságú adatok, információk meghamisítása, nyilvánosságra kerülése előfordulhat.<br>Helyreállítás időigénye legfeljebb 1 nap. | 2 |
| Közepes | Fennakadás az alkalmazói rendszerben, az üzleti folyamatokban.<br>A bekövetkező pénzügyi veszteség 3 millió Ft-nál kevesebb.<br>Alacsony szintű bizalomvesztés kockázata fennáll.<br>Törvények, előírások megsértése megtörténhet.<br>Közepes bizalmasságú adatok, információk meghamisítása, nyilvánosságra kerülése bekövetkezhet.<br>Helyreállítás időigénye legfeljebb 1 hét. | 3 |
| Magas | Az üzletmenetben időleges fennakadás, ügyfélkörben is érezhető változás.<br>A bekövetkező pénzügyi veszteség 10 millió Ft-ig terjedhet.<br>Magas bizalmassági szintű adatok is nyilvánosságra kerülhetnek.<br>Törvények, előírások komoly megsértése megtörténhet.<br>Közepes szintű bizalomvesztés is megtörténhet.<br>Helyreállítás időigénye legfeljebb 2 hét. | 4 |
| Kritikus | Az üzletmenet hosszabb megszakadása, mely az egész szervezet csődjét okozhatja.<br>A bekövetkező pénzügyi veszteség 10 millió feletti.<br>Súlyos bizalomvesztés következik be.<br>Titkos adatok, információk meghamisítása, nyilvánosságra kerülése bekövetkezhet.<br>A helyreállítás időigénye 1 hónap, vagy több. | 5 |

Vagyonelemenként meghatároztam a fenyegetéseket és a hozzájuk tartozó sebezhetőségeket (a 2. melléklet táblázatainak 2. és 3. oszlopa).

Ezek alapján meghatároztam a kár értékeket a bizalmasság, sértetlenség és rendelkezésre állás szempontjából, szempontonként 5 fokozatú skálán megadva a kár várható értékét. A skála értékeket és annak magyarázatát az 5. táblázat tartalmazza. A teljes kárérték a három szempont esetén meghatározott számértékek összege lesz.

A kockázati tényező (6. táblázat zöld, sárga, piros mezői) a teljes okozott kár érték és a bekövetkezési valószínűség érték alapján határozható meg. Az elemzéshez úgy határoztam meg, hogy ha az így kapott érték kisebb, mint 5 (zölddel jelölve), akkor foglalkozni kell ugyan az adott fenyegetéssel, de nem igényel nagyobb intézkedéseket. Fokozott fi-

gyelmet igényel viszont és csökkenteni kell a kockázatot a megfelelő, kockázatokkal arányos anyagi befektetésekkel járó biztonsági intézkedések bevezetésével, ha 5 és 10 között van a kapott kockázati tényező (sárgával jelölve). Ha pedig a kockázat értéke eléri a 11 és 16 közötti kategóriát (pirossal jelölve), akkor az adott fenyegetés kiemelt intézkedést igényel függetlenül az anyagi befektetés értékétől.

6. táblázat: Kockázati tényező

| | | A teljes kárérték | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| Bekövetkezés valószínűsége | Nagyon ritka | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| | Alacsony | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| | Közepes | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| | Gyakori | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Szinte folytonos | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Az elemzés eredményéből a 7. táblázatban csak a kiemelt intézkedést igénylő sorokat jelenítettem meg, a részletes eredményeket a 2. sz. melléklet táblázatai tartalmazzák. A 7. táblázat és a 2. melléklet táblázatai is tartalmazzák egyrészt a kockázatelemzés eredményeit, másrész a javasolt biztonsági intézkedés bevezetésének hatáselemzés eredményeit is. A 7. táblázatból jól látható, hogy a fejezet elején, a Nemzeti Hálózatbiztonsági Központ 2010. éves jelentésében is tárgyalt védelmi megoldások – melyek alkalmazása jellemzően hiányos a közigazgatásban – a kiemelt intézkedést igénylő kockázatok szinte mindegyikét elviselhető szintre csökkentik.

7. táblázat: A kiemelt intézkedést igénylő veszélyforrások kockázatkezelése

| Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| A szoftver által okozott adatvesztések, károsodások, eltérések (hibás vagy manipulált alkalmazói, illetve rendszerprogramok által) | ismeretlen vagy nem megbízható eredetű programok használata | 3 | 4 | 4 | 11 | 4 | 12 | A munkaállomásokon a telepítési jogok, külső adathordozó csatlakoztatásának központi, automatizált szabályozása, szankcionálás | 1 | 1 | 1 | 3 | 1 | 1 |
| | rosszindulatú programok általi adatvesztés | 4 | 4 | 2 | 10 | 4 | 11 | Központosított vírus és e-mail szűrés, külső adatforgalom folyamatos ellenőrzése, jogosultságok megfelelő beállítása | 2 | 2 | 1 | 5 | 1 | 3 |
| Adathordozók (CD,DVD,pendrive,notebook , stb.) meghibásodása, elvesztése, vagy eltulajdonítása | az adatok nem biztonságos tárolása az adathordozón | 4 | 3 | 4 | 11 | 3 | 11 | Az adatok titkosítása, rendszeres mentése | 2 | 1 | 1 | 4 | 1 | 2 |
| Illetéktelen adathozzáférés | visszaélés hozzáférési joggal | 3 | 4 | 4 | 11 | 3 | 11 | A jogosultságok rendszeres, automatizált felülvizsgálata, csak a szükséges jogok megadása | 1 | 1 | 1 | 3 | 1 | 1 |
| | azonosítási, hitelesítési rendszer hiánya | 3 | 3 | 4 | 10 | 4 | 11 | Megfelelő szintű azonosítási és hitelesítési rendszer kialakítása | 2 | 2 | 2 | 6 | 2 | 5 |
| | kilépő dolgozó bosszúállása | 3 | 4 | 4 | 11 | 3 | 11 | Kilépés után a munkavállalói jogok automatikus visszavonása és eszközök visszaszolgáltatása | 1 | 2 | 2 | 5 | 2 | 4 |
| Információ szándékos kiszivárogtatása, megvesztegetés | megbecsülés hiánya | 3 | 3 | 5 | 11 | 3 | 11 | Csapat építő tréningek, jutalmazás és megfelelő juttatás rendszerének kidolgozása | 1 | 1 | 1 | 3 | 1 | 1 |
| Jogosulatlanok bejutása a hálózatba | nem megfelelő határvédelem | 3 | 3 | 4 | 10 | 4 | 11 | Központi és helyi tűzfalak, IDS-ek alkalmazása, forgalomszűrés, felhasználói jogok megfelelő beállítása, azonosítás és hitelesítés rendszerének kidolgozása | 2 | 2 | 2 | 6 | 3 | 6 |
| | azonosítási, hitelesítési rendszer hiánya | 3 | 3 | 5 | 11 | 3 | 11 | Hitelesítési rendszer kidolgozása | 2 | 2 | 3 | 7 | 1 | 5 |
| | védtelen publikus hálózathoz csatlakozó pontok | 4 | 4 | 4 | 12 | 3 | 12 | Komoly biztonsági intézkedésekkel védett kijárat az internetre | 2 | 1 | 2 | 5 | 0 | 2 |
| Távoli munkavégzés | a távoli gép sérülékenységei bekerülnek a rendszerbe | 3 | 3 | 4 | 10 | 4 | 11 | Hálózati hozzáférés vezérlés bevezetése | 1 | 2 | 2 | 5 | 2 | |

A **kockázatelemzés hatáselemzéséből megállapítható**, hogy a közigazgatási informatikai rendszerekben az általam vizsgált, kiemelt védelmi intézkedést igénylő veszélyforrások kockázatainak kezelésére a következő védelmi intézkedések a legalkalmasabbak:

- kártékony kódok elleni védelem;
- tűzfalak alkalmazása;
- behatolás detektálás, megelőzés;
- hálózati hozzáférés vezérlés;
- felhasználó- és hozzáférés-menedzsment;
- titkosítás, adatmentés;
- naplózás, naplóelemzés.

A fentieknek megfelelően ezért ezeket a védelmi megoldásokat vizsgáltam meg részletesebben.

## 3.2. A KÖZIGAZGATÁSI INFORMATIKAI RENDSZEREKBEN ALKALMAZHATÓ VÉDELMI MEGOLDÁSOK ÉRTÉKELÉSE

### 3.2.1. KÁRTÉKONY KÓDOK ELLENI VÉDELEM

Mint azt az előző fejezetben is kifejtettem a malware a támadók alapeszköze, a legtöbb esetben alkalmazzák az egyes támadási módszerek végrehajtása során. Így kiemelt fontosságú az ellene történő hatékony védelem kialakítása.

Az informatikai biztonsági „etikett" szerint ezt a kérdést le lehetne zárni azzal, hogy víruskereső programokat kell alkalmazni a munkaállomásokon, a szervereken és biztosítani kell a rendszeres frissítésüket, de ennél jóval komplexebb a probléma. Ugyanis a **kártékony programok rendszerbe kerülése** az esetek döntő többségében valamilyen **felhasználói interakciót igényel**, így tehát a védelemben is elég **meghatározó szerepe van a rendszer humán elemének**. Ezt a véleményemet támasztja alá például a DTI és Pricewaterhouse Coopers által „Az Információ Biztonság Megsértései" címmel készített 2006-os felmérés is, mely szerint például a trójai támadások 32%-áért belső alkalmazottakat terhel a felelősség. Megsértik a biztonsági előírásokat, naivitásból, tudatlanságból, kíváncsiságból rákattintanak bármilyen felugró ablakra, e-mailben érkezett linkre, vagy esetleg hivatalosan nem engedélyezett alkalmazásokat telepítenek a munkahelyi hálózatra. [85] Az európai és amerikai törvényhozási szakértők pedig több mint 50 százalékban tartják az

alkalmazottakat felelősnek.

Az előbbieket is figyelembe véve a védelem kialakítása során szem előtt tartandó szempontok:

- a legtöbb kártékony program magának a **felhasználónak a viselkedése miatt képes bejutni a rendszerbe**;
- **az átjáró szintű szűrés** nem helyettesítheti a helyi gépen alkalmazandó biztonsági szoftvereket (antivirus, firewall) és **nem is képes megállítani a kártevőt, ha már a host belsejében található**;
- fontos a **helyi gépek biztonsági konfigurációinak megerősítése** és a felhasználók jogosultságainak helyes beállítása;
- **szűrni kell** a webes tartalmakat, illetve a levelezési forgalmat;
- a kártékony kód **nem csak és kizárólag kívülről jöhet**, ezért a fizikai védelmet is érdemes szem előtt tartani;
- még a naprakész víruskeresők sem képesek lépést tartani minden esetben az új vírusokkal, ezért olyan általános szabályokat kell elfogadni, amelyek jelentősen korlátoznák az e-mailen keresztül terjedő vírusok és férgek terjedését. **A levelezőszerveren nem szabad átengedni semmilyen futtatható állományt** (.COM, .EXE, .VXD, .SCR, .VBS) mellékletként. Ugyanígy blokkolni kell minden, az ugyancsak e-mail férgek által használt, kettős kiterjesztésű (.TXT, .VBS, .BMP, .PIF) levélmellékletet. Továbbá maximáljuk a percenként fogadható, és beérkező üzenetek számát és a csatolt állományok méretét;
- célszerű **vírusvédelemmel kombinált levélszűrő** programokat alkalmazni. Ezek egy vagy több, illesztett víruskereső motort használnak, és a be- valamint kimenő levelek vírusellenőrzését biztosítják. Figyelni kell arra, hogy a **legfrissebb adatbázissal** fussanak, ezt akár naponta történő ellenőrzéssel is biztosítani kell. [86]
- a **kártékony programok** elemzése során megállapíthatjuk, hogy egy – már a rendszerbe bejuttatott – kémprogramot a különböző adatrejtési és rootkit technikák alkalmazása miatt sokszor igen nehéz detektálni. Azonban **a hálózati forgalom és a hálózati események folyamatos monitorozás**a mellett ezek a kártevők is **kiszűrhetők**.

Fentiekből következően **megállapítom**, hogy **a kártékony kódok elleni védelem** is

**komplex**, több módszert, alkalmazást, eszközt magába foglaló eljárás. A kártékony kódok elleni védelem hatásfokát a **vírus- és kémprogram kereső alkalmazások használata mellett** jelentős mértékben **növeli** a megfelelően megválasztott és beszabályozott **tűzfalak alkalmazása**, az informatikai biztonságra vonatkozó **szervezeti szabályozások**, előírások betartatása, valamint az **alkalmazottak ez irányú képzése**. Ez a közigazgatásban fokozott figyelmet igényel mivel, mint azt már az 1. fejezetben megállapítottam, hiányosak az ez irányú szabályozások. **Véleményem szerint minden szerveren és** minimálisan minden olyan **munkaállomáson**, ahol külső adattároló eszköz csatlakoztatására lehetőség van vagy hálózaton keresztül bármilyen adatforgalom kivitelezhető, **működnie kell naprakész vírusadatbázissal rendelkező, központilag menedzselt és szabályozott vírusirtó alkalmazásnak**, mely működésének letiltására ne legyen a helyi felhasználónak lehetősége.

### 3.2.2. TŰZFALAK

A külső védelem már régóta elsődleges szempont, mégis még mindig találkozni nem egy olyan implementációval, ahol ez a védelem alapjaiban hibázik. Gyakran megelégednek annyival, hogy csak vírusvédelemmel látják el a számítógépeket, és a hálózatot egyáltalán nem védik, pedig akár egy egyszerű csomagszűrő tűzfal is rengeteg behatolást tud megakadályozni. Ezen kívül egy tűzfal alkalmas a hálózat egyes részeinek szegmentálására is, így az egyes, különösen védendő alhálózatokat is képes megvédeni a többi szegmens elemeitől, illetve azt is megakadályozza, ha a hálózat valamely részébe sikerül is a támadónak betörnie, akkor sem tudja elérni közvetlenül a különösen védett részt.

Az előző fejezetben ismertetett, közigazgatási informatikai rendszereket is érintő **hálózati sérülékenységeket kihasználó módszerek ellen** alapvetően szükséges **tűzfalak** elhelyezése és megfelelő beállítása (legalább a hálózat határán és a különösen védett szegmensek elkülönítésére), ezért **megvizsgáltam és elemeztem** a különböző tűzfaltípusok tulajdonságait működési elvük szerint.

A **statikus csomagszűrő tűzfalak** az ISO/OSI réteg hálózati rétegében működnek. Ezek a tűzfalak alapvetően csak forrás és cél IP címre tudnak szűrni. Egy átlagos útvonalválasztó rendelkezik ilyen opcióval, melyet érdemes bekapcsolni. Mivel a védett hálózat határán helyezkedik el ezért előnye hogy **gyors, és olcsó**. Hátránya viszont, hogy mivel csak a 3. rétegben működik **nem szűri az adattartalmat**, így nem nyújt elegendő védelmet, a magas szintű támadások ellen. További hátránya még hogy **nem kezeli a kapcsola-**

**tokat**, ezáltal nem tudja, hogy éppen egy kapcsolatot épít ki valaki kívülről, vagy csak egy belülről jövő kérésre küldtek választ. Erre a problémára megoldás a **dinamikus csomagszűrő tűzfal**, ami már a 4. rétegben is működik.

Az **állapottartó (stateful) tűzfalak** az engedélyezett **belső hálózatról induló forgalmat vizsgálják** (IP-cím, port, TCP/UDP fejlécek), **a kapcsolat állapotát figyelik** és az erre érkező választ beengedik. Egészen az 5. rétegig képes szűrni. Hátrányuk, hogy a "Denial of Service" (DoS) típusú támadásokkal szemben sokkal sérülékenyebbek olyan helyzetekben, amikor az új kapcsolatok nagyon gyorsan jönnek létre.

Az **alkalmazás szintű tűzfalak**, – mint azt a neve is sugallja – az ISO/OSI modell legfelső, 7. rétegében működnek. Ez a típus már **képes a csomagok tartalmát is vizsgálni**, és **megkülönbözteti a már kiépített, és a kiépíteni kívánt kapcsolatokat**. Előnye, hogy magas szintű biztonságot nyújt a támadások ellen, és **egyszerűen konfigurálható**. Hátránya, hogy **nem transzparens**[45], ugyanis a belső hálózatbeli gép vele építi fel a kapcsolatot, és a tűzfal építi ki a kapcsolatot a célállomással. További hátrány még az erőforrásigény, **nagy hálózati forgalom esetén a tűzfal túlságosan leterhelt** lehet. Ebbe a csoportba tartoznak az XML[46] tűzfalak is. [87] Az előző fejezetben **a web alkalmazásoknál említett problémákra az alkalmazás szintű tűzfalak nyújthatnak megoldást**.

Megemlítendő még a **proxy** eszköz, egy kitüntetett hardware vagy software, ami **úgy viselkedik, mint egy tűzfal**, és így szűri a hálózaton nem engedélyezett forgalmat. Működése ugyanaz, mint az alkalmazás szintű tűzfalaknak. Minden protokollra külön proxy-t kell beállítani, ami alapján el tudja dönteni, hogy engedélyezett-e az adott csomag.

A különböző tűzfal komponensek összeillesztésével többféle architektúrát meg lehet valósítani. Többek között Dual-Homed Host architektúrát, Screened Host architektúrát és Screened Subnet architektúrát is.

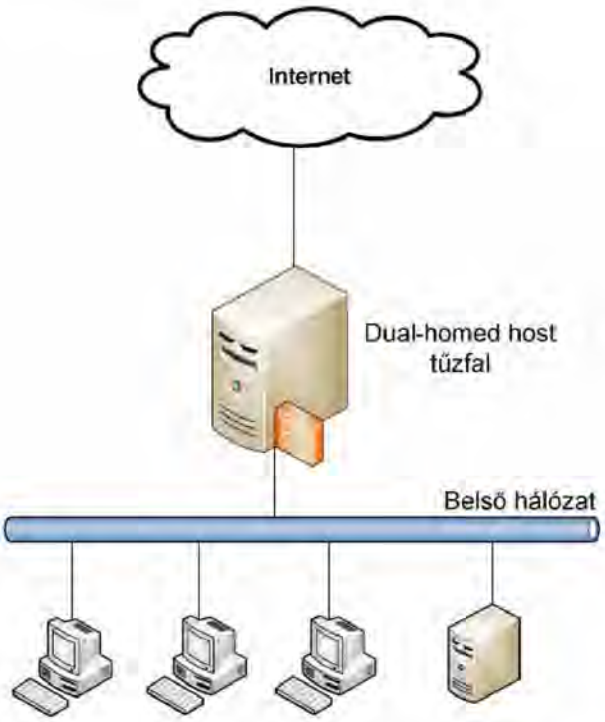
A **Dual-Homed Host architektúra** (9. ábra) a tűzfal köré épül, amely minimum két interfésszel rendelkezik.

---

[45] A kliens a tűzfallal kommunikál (eltérő protokoll használat lehetséges).

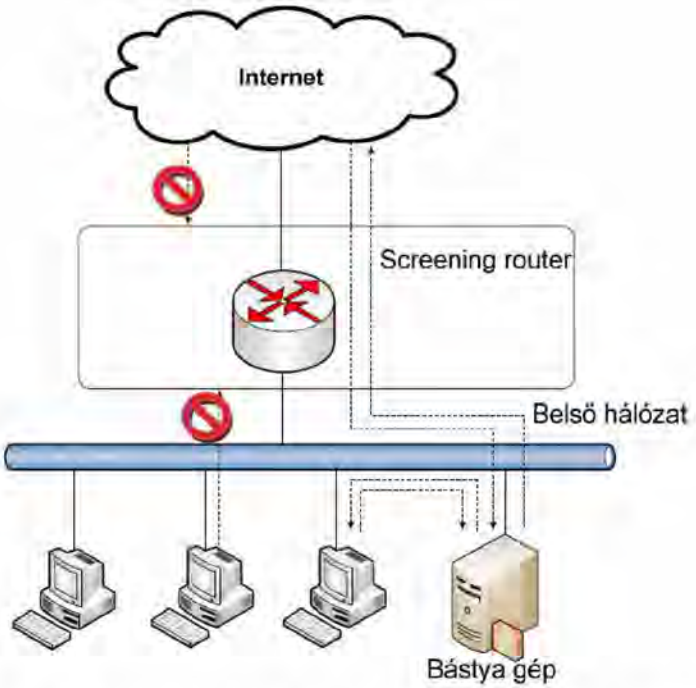
[46] Extensible Markup Language - kiterjeszthető jelölő nyelv a W3C által ajánlott általános célú leíró nyelv, speciális célú leíró nyelvek létrehozására.

Az egyik hálózati interfész többnyire egy külső nem megbízható hálózathoz, míg a másik interfész a belső vagy megbízható hálózathoz kapcsolódik. Ebben az esetben a tűzfalnak közvetítőként kell működnie, nem szabad engednie a külső hálózatról közvetlenül a megbízható hálózatra való kapcsolatépítést.




9. ábra: Dual-Homed Host architektúra [szerkesztette a szerző]

A **Screened Host architektúra** (10. ábra) a szolgáltatásait úgy biztosítja, hogy a kiszolgáló gép csak a belső hálózatra csatlakozik. Az elsődleges biztonságot a forgalomirányító (tűzfal) nyújtja. Ez a router megakadályozza azt, hogy a felhasználók közvetlenül hozzáférhessenek az internethez. A bástya gép a belső hálózaton található, a forgalomirányítón olyan szabályokat kell konfigurálni, hogy az internet felől érkező kapcsolatok csak a bástya géphez mehessenek. Ennek a gépnek a biztonsága elsőrendű. A bástya gép proxyként működik. A screening router akár úgy is konfigurálható, hogy bizonyos szolgáltatások közvetlenül is elérhetőek legyenek, míg mások csak a szerveren keresztül működhessenek.




10. ábra: Screened Host architektúra [szerkesztette a szerző]

Ez az architektúra nagyobb biztonságot nyújt, mint a dual-homed host felépítés. Viszont ennek is vannak hátrányai, például, ha egy támadónak sikerül betörnie a bástya gépre, akkor a belső hálózatot teljes egészében elérheti.

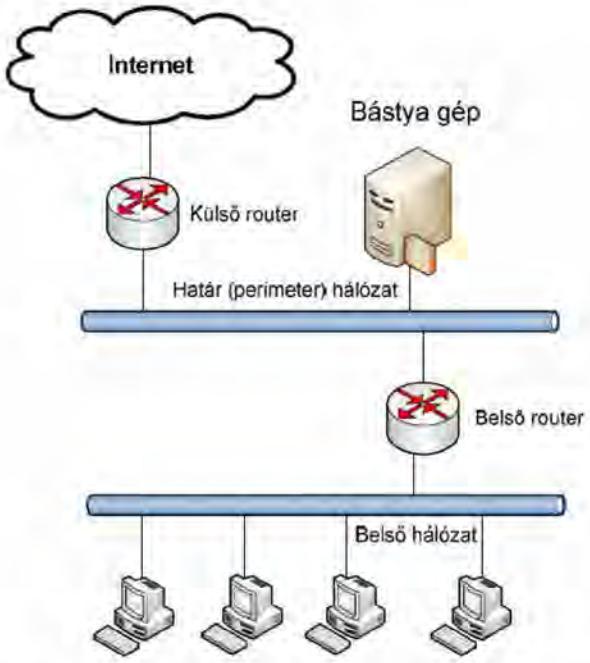
Erre a hátrányra kínál megoldást a **Screened subnet architektúra** (11. ábra), mely egy újabb biztonsági réteget helyez el az internet és a belső hálózat közé. Ezt nevezik perimeter hálózatnak (DMZ[47]). Az itt található bástya gép sebezhető, ezt támadják leginkább, de ha a támadó be is jut ide, akkor is még mindig útját állja a belső forgalomirányító. Ez biztonságosabbnak tekinthető az előző két architektúránál.

Tehát, ha egy támadó bejut a bástya gépre, akkor csak a perimeter hálózat forgalmát tudja lehallgatni, a belső hálózat forgalmát nem láthatja. A bástya gép rendszerint a bejövő forgalom kezelésének a helye. Ezek a forgalmak többek közt a bejövő e-mail (SMTP), FTP[48] forgalom, a bejövő DNS kérések.

[47] DMZ - Demilitarizált Zóna: olyan fizikai vagy logikai alhálózat, ami egy szervezet belső szolgáltatásait tartalmazza és tárja fel egy nagyobb, nem megbízható hálózatnak, általában az internetnek.

[48] File Transfer Protokol

A kifelé irányuló forgalmak kezelhetőek a belső és külső routerek csomagszűrő szabályainak beállításával, vagy proxy szerverek futtatásával a bástya gépen.




11. ábra: Screened Subnet architektúra [szerkesztette a szerző]

A belső router szabályozza azt, hogy a belső hálózatról mely szolgáltatások érhetőek el közvetlenül (pl. telnet, HTTP[49], FTP stb.). Szabályozza a belső hálózat és a bástya gép közötti forgalmat. Ezeket a forgalmakat minél kevesebb protokollra (SMTP, DNS) és hosztra kell csökkenteni, hogy minél kevesebb gép legyen elérhető a bástya gépről.

A külső router védi a perimeter és a belső hálózatot az internet felől. A perimeter hálózatról általában minden forgalmat kienged. Ugyanolyan szabályokat tartalmaz, mint a belső router kiegészítve a bástya gépet védő szabályokkal.

**Ezeknek az architektúráknak a komponensei variálhatóak**. Például több bástya gépet is lehet használni, a belső és külső forgalomirányító összevonható, több külső router is alkalmazható stb. Nem ajánlott azonban a bástya gép és a belső forgalomirányító összevonása, valamint több belső router alkalmazása.

Fentiekből következik, hogy nincs éles határ az egyes architektúrák, típusok között. A minél magasabb szintű biztonság eléréséhez ötvözni kell a különböző típusokat, aminek segítségével az erősségeket megfelelően kihasználva el lehet érni a kívánt mértékű védelmet. A legfontosabb a kialakításkor, hogy a védendő hálózattal összhangba legyen a tűzfal-

[49] HTTP - **H**yper**T**ext **T**ransfer **P**rotocol - információátviteli protokoll

architektúra, és igényeinek megfelelően kell választani.

A kiválasztáskor figyelembe kell venni, a védendő hálózat jelenlegi biztonsági megoldásait és eszközeit, milyen funkciókat kell ellátni a tűzfalnak és mekkora a szükséges védelmi igény.

A **közigazgatás informatikai rendszereiben** – tekintettel a tömeges mennyiségű érzékeny adatok jelenlétére és figyelembe véve a számos web alkalmazáson keresztül nyújtott szolgáltatásokat is – a **Screened Subnet architektúra alkalmazását javaslom**, **alkalmazás szintű tűzfal** üzemeltetésével. A tűzfal legyen képes **VPN kapcsolatok kezelésére** a biztonságos távoli munkavégzés megvalósíthatósága érdekében. Az **ügyfelek számára** szolgáltatásokat nyújtó **szerverek** elhelyezése **DMZ-be** javasolt. Ezen kívül, minden szerver és munkaállomás **központilag menedzselt tűzfallal** rendelkezzen. Ezen túlmenően időnként felül kell vizsgálni és az új fajta támadásoknak megfelelően módosítani kell.

Nem szabad azonban megfeledkezni arról, hogy egy **tűzfal nem véd** a rosszindulatú **belső felhasználók ellen**, és nem véd olyan kapcsolatoktól sem, **amelyek nem mennek rajta keresztül** (pl. telefonos kapcsolat a belső hálózat és az internet között). Az ilyen jellegű sérülékenységekre a behatolás detektáló rendszerek adnak megoldást.

### 3.2.3. BEHATOLÁS DETEKTÁLÁS, MEGELŐZÉS

A külső támadások egy része ellen tűzfalakkal lehet védekezni, de a **belső hálózaton történő támadások**, illetve **illetéktelen hozzáférési kísérletek** érzékelésére és elhárítására mindenképpen szükség van behatolás érzékelő, illetve -megelőző (IDS[50]/IPS[51]) eszközökre.

Az ilyen rendszerek biztonsági szempontból nélkülözhetetlen információt biztosítanak a DDoS támadásokról, a hálózaton kommunikálni próbáló trójai falovakról, a jogosulatlan belépési kísérletekről és egyéb, az alkalmazások vagy az operációs rendszer sérülékenységének kihasználására irányuló tevékenységről.

Az eszközök gyanús tevékenység érzékelése esetén **képesek automatikusan beavatkozni** a folyamatba (pl. adatkapcsolat megszakításával vagy a felhasználói fiók felfüggesztésével), a hálózatnak valós idejű védelmet biztosítva.

---

[50] Intrusion Detection System
[51] Intrusion Prevention System

#### 3.2.3.1 IDS rendszerek működése, típusai

Az IDS alapú rendszereknek az a célja, hogy segítséget nyújtson az alkalmazóiknak, azzal, hogy tudomásuk lesz az őket ért támadásokról, még akkor is, ha azok csak kísérletek voltak.

Többféle behatolás detektáló rendszer létezik, viszont céljukat tekintve mind közösek: észleljék a támadást. Ehhez különböző eszközöket vesznek igénybe. Léteznek **tudásbázis alapú érzékelők**, amelyek a bennük eltárolt támadási minták alapján észlelik a támadást, vagy napló állományok elemzésével próbálják feladataikat ellátni. [88, 89] Ezen detektáló rendszereknek előnye, hogy egyszerűbb kialakításúak, de hátrányuk, hogy csak olyan mintákat ismernek fel, amelyek tudásbázisukban megtalálhatók. Nagyon hasonlítanak a korai antivírus rendszerekre, amelyek még nem rendelkeztek proaktív védelemmel, így csak azon vírusokat érzékelték, amelyek a vírus definíciós adatbázisukban fellelhetők voltak.

Egy fejlettebb változatuk az **„intelligencián" alapuló érzékelő rendszerek**, amelyek megtanulják a rendszer használata során, hogy normális körülmények között az alkalmazás milyen viselkedést mutat. Majd ezt veszik a későbbi elemzéshez alapértékként. Ha a megtanult viselkedési mintáktól szignifikánsan eltérő forgalmat tapasztalnak, akkor riasztanak. Vagy egy másik, hasonló elv, hogy a betanulás után az egyes kérésekhez küszöbszámokat rendelnek, majd ennek az elérését esetleg átlépését veszik incidensnek. Azonban nagy tapasztalat szükséges a megfelelő beállításukhoz, hiszen egy rossz taníttatás következményeképpen sok fals pozitív, de még nagyobb baj, hogy akár fals negatív eredményt is adhatnak. Nagy előnyük viszont, hogy képesek felvenni a versenyt a nem várt, esetleg nem ismert – „0 day" – támadásokkal szemben.

Egy harmadik típusként említhető egy elég speciális megoldás, de véleményem szerint ugyancsak alkalmazható behatolás detektálásra. Az említett megoldás a mézes bödön – **honeypot**[52] – alapú rendszerek. Elvük lényege, hogy olyan adatokat, részegységeket hoznak létre a hálózaton vagy az adatbázisban, amelyeket sohasem használna normál körülmények között, de felkeltheti egy támadó érdeklődését. Ha a támadó rátalál, azonnal riaszt. A honeypot alapú rendszerek előnye az egyszerűsége, azaz akár teljesen független is lehet az alkalmazástól, vagy akár a rendszerbe is implementálható. Hátránya viszont, hogy rossz

[52] Egy alaposan ellenőrzött erőforrás, melyet szeretnénk, hogy mások megvizsgáljanak, megtámadjanak, és végül feltörjenek.

csalikat alkalmazva előfordulhat, hogy semmit sem sikerül lépre csalni. Tehát jól meg kell gondolni, hogy hol és hogyan használható egy „mézes bödön". [88, 89]

Tekintve, hogy **a közigazgatás egyre több szolgáltatását lehet webes felületen igénybe venni**, – amivel azonban egyre nő a sérülékenységek száma is –, így ezen a területen is hatékonyan alkalmazható a webes alkalmazásoknál a honeypot következő implementációja, mely nagy segítséget nyújthat például az SQL befecskendezés észlelésében. Ha az alkalmazás hátterében működő adatbázis minden táblájába beszúrunk egy nullás indexel ellátott rekordot, majd az alkalmazás összes lekérdezését úgy alakítjuk ki, hogy ezt a nullás indexű elemet sohase adja eredményül. Viszont olyan adatbázis burkolót használunk, amely minden lekérdezés után megvizsgálja, hogy nullás indexű elemet kapott-e eredményül. Ha igen, akkor módosításra került az eredeti lekérdezés, tehát egy támadási kísérletről van szó. Így belátható, hogy **a honeypot-okat** nem csak önállóan, külön rendszerként, hanem akár **az alkalmazás szerves részeként is lehet értelmezni és használni**, amely a fentieknek megfelelően, **mint behatolás detektáló eszköz** segít a biztonsági szint növelésében.

A belső hálózat viselkedésének elemzésére alkalmas más, hálózat-monitorozó megoldás is, mint például a Cisco Netflow. A Netflow-rekordok csak az átvitt csomagok fejléceit tartalmazzák, így ennél az IDS-ek mélyebben képesek elemezni az adatcsomagokat, viszont éppen ezért lassabb és erőforrás-igényesebb, mint a Cisco megoldása.

#### 3.2.3.2. IPS rendszerek működése

A behatolást megelőző rendszerek **jóval bonyolultabbak és összetettebbek, mint a detektáló rendszerek**, hisz nem csak érzékelni tudják a támadásokat, hanem valós időben, akár emberi beavatkozás nélkül is különböző intézkedéseket tudnak eszközölni a támadással, vagy akár magával a támadóval szemben. Az adott alkalmazáshoz, esetleg a kiszolgáló rendszerhez is hozzáféréssel kell, hogy rendelkezzenek, így érhető el, hogy a fenyegetést jelentő csomagokat egyszerűen eltávolíthassák a hálózati forgalomból, vagy akár a tűzfal ACL[53] tábláját átkonfigurálva kitiltsák a támadó hálózati címét. [88, 89]

A tevékenységeikről értesíthetik a rendszer adminisztrátorát, hogy ellenőrizhesse az IPS rendszer működését. Így csak akkor szükséges az emberi beavatkozás, ha hibás érzéke-

[53] Access Control List

lés miatt rossz intézkedést alkalmazott a behatolás megelőző rendszer. Tehát az IPS rendszerek nagyobb fokú automatizmussal rendelkeznek és az adminisztrátorra inkább ellenőrző feladat hárul, szemben az IDS rendszerekkel, ahol az érzékelést követően a döntés és a cselekvés az adminisztrátor feladata.

Léteznek olyan integrált megoldások, melyek megoldást kínálnak a kártékony kódok ellen, valamint tartalmaznak IDS/IPS funkciókat is. Minimálisan ilyen **integrált szoftvercsomag alkalmazása a közigazgatás hálózati kapcsolattal rendelkező munkaállomásain javasolt.**

### 3.2.4. HÁLÓZATI HOZZÁFÉRÉS VEZÉRLÉS

A Hálózati Hozzáférés Vezérlés[54], egy olyan hálózatbiztonsági megközelítés, mely megkísérli egyesíteni a végponti biztonsági technológiák, a felhasználó- és rendszerszintű hitelesítés és a hálózat-biztonság egyes elemeit. A hálózati hozzáférést **biztonsági politikák alkalmazásával** szabályozza, beleértve csatlakozáskor az **előzetes végpont-biztonsági ellenőrzéseket**, valamint a **csatlakozás utáni felügyelet** lehetőségét is. Segítségével egy olyan szabályrendszer állítható fel, amely megadja, hogy **milyen biztonsági beállítások** (például bekapcsolt tűzfal, naprakész vírusadatbázissal frissített víruskereső, megfelelően frissített alkalmazások, esetleg behatolás detektáló szoftver, stb.) teljesülése mellett **milyen számítógépek**, illetve **milyen felhasználók férhetnek hozzá a hálózat adott területeihez**. Továbbá **képes** olyan **automatikus helyreállítási folyamatot indítani,** amely a hálózati erőforrások és az erre a célra előkészített háttér-szerverek segítségével **képes a csatlakozó eszközt a biztonsági követelményeknek megfelelően módosítani**.

**Működésének lényege**, hogy amikor a számítógép csatlakozik a hálózathoz, addig nem tud hozzáférni a hálózati erőforrásokhoz, amíg az általunk felállított házirend követelményeinek meg nem felel. Beleértve, azt hogy a vírusirtó, a rendszerfrissítések és az esetleges tűzfal telepítve van-e, fut-e és megfelelően frissítve van-e. Azt eldönthetjük, hogy biztosítunk-e a végpont részére részleges hálózati hozzáférést, amíg a gép át nem megy az ellenőrzésen. Ha egy gép nem felel meg a követelményeknek tovább lehet irányítani az automatikus helyreállítást végző szerverekhez, vagy áthelyezhető egy vendégek számára

[54] Network Access Control – NAC

fenntartott VLAN-ba[55]. VPN kapcsolódás esetén ezt szokás VPN karanténnak is nevezni. [90]

Amint a végponti eszköz megfelel az előírt követelményeknek, onnantól teljes egészében hozzáfér a hálózathoz. A hozzáférés szinkronizálható a felhasználó profiljával is, azaz akár ugyanolyan hozzáféréssel használhatja a megszokott erőforrásokat, mintha a belső hálózatban végezné a munkáját.

A **közigazgatási feladatok ellátásához** is szükséges lehet időnként bizonyos felhasználók számára biztosítani a rendszerhez való **távoli hozzáférés** lehetőségét. Egy természetes igény például a parlamenti munka kapcsán is, hogy a képviselők megfelelő biztonsági szabályok betartása mellett otthonról, illetve távoli munkahelyről is be tudjanak kapcsolódni a parlamenti munkafolyamatokba. A **biztonságos távoli munkavégzés** lehetőségeit ezért alaposabban **megvizsgáltam és vizsgálataim eredményeit** „A távoli munkavégzés biztonsági kérdései, megoldási lehetőségek Windows szerverek esetén" [90] című cikkemben publikáltam, melynek **fontosabb megállapításai** a következők:

- távoli munkavégzés biztonságos megvalósítására **VPN** kialakítása lenne célszerű, de tekintve a megvalósítás **nehézségeit** (szakértelem hiány, operációs rendszer nem teszi lehetővé, nyilvános helyek problémái, stb.) és **kockázatait** (kellő körültekintés nélkül könnyen bekábelezhető a szervezeti hálózatba nem biztonságos számítógép is), érdemes alaposan megfontolni, hogy milyen célok elérésére is van szüksége a távoli felhasználónak és annak megfelelően kell kiválasztani az anyagi lehetőségektől is függő megfelelő technológiát;
- hordozható eszköz, notebook segítségével történő távoli munkavégzés esetén számos kártékony program kerülhet be a szervezeti rendszerekbe, illetve onnan bizalmas adatok szivároghatnak ki;
- ha mindenképpen elkerülhetetlen a VPN kapcsolat kialakítása, akkor van lehetőség a felhasználó, ügyfél, partner számára a megfelelő beállításokkal előre preparálni azt, melynek eredményeként előállított, a kapcsolat kiépítéséhez szükséges fájlokat megfelelő titkosítással a rendelkezésükre lehet bocsátani. Így biztosítható, hogy a VPN kliens **kötelezően** azokkal a beállításokkal tudjon belépni a szervezet hálózatába, amit a csomagban előre előírtunk számára.

[55] VLAN: virtuális (logikai) felosztása a hálózatnak. Különböző VLAN-ban lévő gépek nem látják egymást.

Az első két pontban felsorolt problémára megfelelő megoldást biztosít a hálózati hozzáférés vezérlés bevezetése a közigazgatási rendszerekbe.

### 3.2.5. FELHASZNÁLÓ- ÉS HOZZÁFÉRÉS-MENEDZSMENT

A felhasználó életciklus kezelés alatt – amelyre angolszász nyelvterületen a „user provisioning"[56] kifejezést használják –, a felhasználó menedzsment szoftver piacon az egyik jelentősebb gyártó, a Courion cég megfogalmazása alapján az alábbit értjük: *„A felhasználó-kezelés megvalósítja a biztonsági politikát, oly módon, hogy létrehozza, kezeli, és eltávolítja a felhasználói fiókokat és jogosultságokat az informatikai rendszerekben és erőforrásoknál mind a belső mind a külső felhasználók tekintetében".* [91] A meghatározás pontosan bemutatja az életciklus egyes fázisait, és kihangsúlyozza, hogy nemcsak a szervezet dolgozóira vonatkozhat, hanem a külső felhasználók (partnerek, vásárlók) adatainak kezelésére is. Annyiban **módosítanám a definíciót**, hogy véleményem szerint **a jogosultság létrehozása** – amely elvi síkon a szerepkör felhasználóhoz rendelésekor jön létre – **a szerepkör menedzsment hatókörébe tartozik**, a felhasználó-kezelés csak a létrehozott felhasználói fiókokhoz állítja be a megfelelő hozzáférési engedélyeket. Gyakorlatilag a felhasználó-kezelő rendszer gondoskodik arról, hogy az általa felügyelt alkalmazásokban létrehozza a felhasználó fiókokat, és beállítsa az érvényes jogosultságokat. [92]

Az informatikai rendszerek felhasználói adatainak a menedzselése napjainkban egyre nehezebb és összetettebb feladat lett. A szervezetben **a munkavállalók felvétele és elbocsátása gyors ütemben történik**, és a dolgozók is – a szervezetben betöltött szerepük változása során – **újabb munkaköri feladatokat kapnak**, melyekhez más és **más hozzáférési jogosultság tartozik**. Már egy közepes létszámú szervezetnél is alkalmazások tucatjait használják, melyek mindegyikéhez külön jogosultságrendszer tartozik. [93] Használhatják a szervezet adatait és erőforrásait külső partnerek is, vagy tanácsadók, akiknek szintén szükséges kezelni a jogosultságaikat. A felhasználók adatainak és jogosultságainak adminisztrációja is jelentős élőmunkát és időt igényel, és nagyobb az emberi figyelmetlenségből (például elgépelés, vagy papíralapú információk hibás értelmezése) vagy szándékosságból (többlet jogok biztosítása) fakadó hibalehetőség is.

Látható, hogy **a felhasználói adatok kezelésének informatikai támogatása fontos a szervezet hatékony és biztonságos működése szempontjából**, és a folyamat automati-

[56] A provisioning szó magyar jelentése: ellátás, gondoskodás,

zálása jelentős gazdasági előnnyel jár. A felhasználó életciklus- és jogosultságkezelés[57] az informatikai biztonság területének egyik legdinamikusabban fejlődő ága.

Fentiek ellenére **a központi integrált felhasználó- és hozzáférés-menedzsment még egy igencsak gyerekcipőben járó terület a közigazgatás rendszereit illetően**. Felhasználó- és hozzáférés kezelés terén a közigazgatási rendszerek számos területén megelégednek az operációs rendszerek és némely alkalmazás szolgáltatásaival, esetleg még azok kihasználása sem történik, annak ellenére sem, hogy ez szerepel az ISO 27001 szabványban is.

Pedig **a felhasználó menedzsment rendszerek** (IDM) használata jelentős mértékben növelheti a szervezet informatikai biztonsági szintjét, mivel **a felhasználó teljes rendszerbeli életciklusa alatt automatizálható annak és jogosultságainak kezelése**, azaz nem fordulhat például olyan elő, hogy egy dolgozó már elment a szervezettől, de még mindig él a rendszerhez való hozzáférése. Vagy ez fordítva is igaz, mert könnyen összekapcsolható például a Humán Erőforrás Osztály rendszerével, és ahogy ott felvették a dolgozót, esetleg áthelyezték, azonnal életbe lépnek az informatikai rendszerhez való hozzáférési beállításai, jogosultságai, vagy azok változásai is (esetleg engedélyezési folyamattól függően, amiről az engedélyező, akár automatikus e-mailértesítést is kaphat). **Előbbiek alapján feltétlenül javaslom a bevezetését a közigazgatási rendszerekben is.**

Fontos megjegyezni azonban, hogy még így sem védhető ki a dolgozók felelőtlen viselkedése, és az iratokkal történő visszaélés sem. **Az IDM rendszernek összhangban kell lennie a közigazgatás szervezeti biztonsági szabályozással**. Irányítási és szabályozási eljárások kialakításával kell megteremteni az informatikai rendszerek biztonságát, és folyamatos ellenőrzés és felülvizsgálat segítségével biztosítani a fejlődést.

### 3.2.6. TITKOSÍTÁS, ADATMENTÉS

Akár az otthoni felhasználóknak, akár kisebb vállalkozásoknak, de a közigazgatás keretein belül is egyaránt szükséges az elektronikus adatok biztonságának biztosítása. A titkosítás jó eszköz arra, hogy akár az archivált adatainkat, akár a napi szinten, például notebookunkon használt adatokat biztonságban tudhassuk.

2010-ben az Intel és a Ponemon Institute végzett egy átfogó felmérést (8. táblázat),

[57] Identity Management – IDM A szakmaterület szóhasználata igen változatos, de általában az „Identity Management" kifejezés kiterjesztett értelmezésébe beleveszik a felhasználók kezelésével kapcsolatos összes folyamatot, mint például a jogosultság-kezelés, jelszókezelés, egyszeri bejelentkezés.

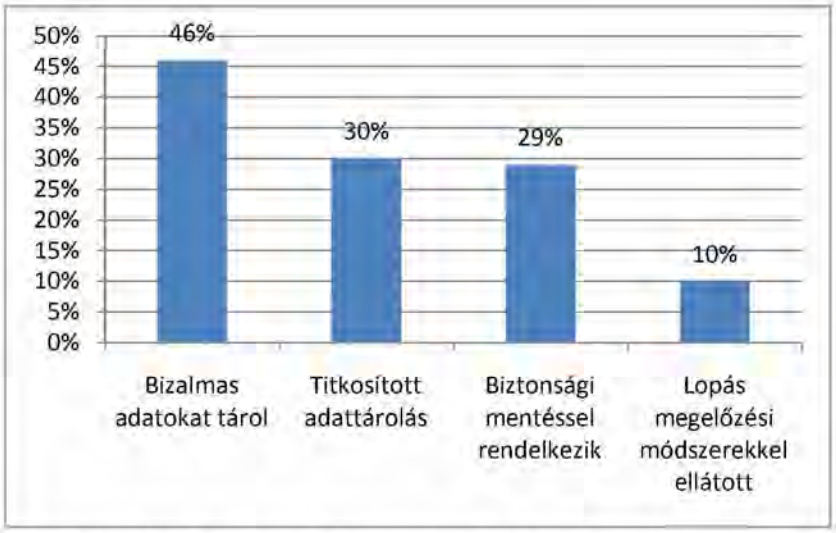
több mint 300 amerikai szervezet körében a hordozható számítógép eszközök biztonságával kapcsolatban. [94] A vizsgálat során kiderült, hogy a megkérdezett vállalatokon belül **az elmúlt egy évben több mint 86 ezer notebooknak veszett nyoma**, ami **komoly** 2,1 milliárd dolláros **veszteséget okozott a szervezeteknek**. Így vállalatonként átlagosan 6,4 millió dolláros vesztességgel kell számolni. Ez **a kár** nem csak az eltűnt hardvereszközöknek köszönhető, hanem **főként az illetéktelen kezekbe került bizalmas adatoknak** is, ami adatbiztonsági incidensekre vezethető vissza. Az eltűnt számítógépek 46%-án voltak bizalmas adatok, és csak 30 százalékuk volt védve valamilyen titkosítással. A laptopok alig 10 százaléka támogatta az olyan megoldásokat, amelyek révén a lopások megelőzése, felderítése megoldható lett volna.

8. táblázat: Ponemon Institute felmérése a hordozható eszközök biztonságáról [94]

| Gazdasági kihatások elemzése | Összeg ($) vagy Darab (db) |
|---|---|
| Elveszett laptop | 86 455 db |
| | |
| Elveszett titkosítatlan laptop | 60 518 db |
| Bizalmas adatokat tároló titkosítatlan laptop | 27 838 db |
| Elveszett titkosítatlan laptopok átlagköltsége* | 56 165 $ |
| Mérési minta gazdasági értéke | 1 563 521 270 $ |
| | |
| Elveszett titkosított laptop | 25 937 db |
| Bizalmas adatokat tároló titkosított laptop | 11 931 db |
| Elveszett titkosított laptopok átlagköltsége* | 37 443 $ |
| Mérési minta gazdasági értéke | 446 732 433 $ |
| | |
| Bizalmas adatokat nem tároló laptop | 46 686 db |
| Bizalmas adatokat nem tároló laptopok átlagköltsége* | 4 078 $ |
| Mérési minta gazdasági értéke | 190 385 508 $ |
| | |
| Mérési minta összesített gazdasági értéke | 2 200 639 211 $ |
| Egy elveszett laptop átlagköltsége | 25 454 $ |
| Levonandó a megtalált laptopok értéke | 100 187 565 $ |
| Mérési minta korrigált, összesített gazdasági értéke | 2 100 451 646 $ |
| Átlagos érték a vizsgált cégekre vetítve | 6 384 352 $ |

* Korábbi kutatások átlagköltsége elveszett vagy ellopott laptopoknál

A biztonsági mentések tekintetében sem lettek jók az eredmények. A kutatás szerint megállapítható, hogy **az elvesztett hordozható számítógépek közel 71%-áról soha nem készült biztonsági mentés** (12. ábra).




12. ábra: Az eltűnt laptopok biztonsági szintjei %-os lebontásban [94]

Úgy gondolom, hogy a közigazgatás sem kivétel ez alól, így a fentiekből következik, hogy **lényeges kérdés** az említet probléma olyan irányú megoldása, hogy, ha már egy adathordozó nem áll rendelkezésre – akár azért, mert eltulajdonították, megrongálták vagy egyszerűen csak meghibásodott –, a kockázatok bekövetkezéséből származó kár jelentős mértékben csökkenthető **az adatok titkosításá**val (illetéktelen kezekbe kerülve a bizalmassága ne sérüljön), illetve a rendszeresen végrehajtott **mentések** alkalmazásával.

### 3.2.6.1. Titkosítás

*„A titkosítás olyan, mintha valami értékeset egy erős dobozba kulcsra zárnánk. A bizalmas adatok titkosítása kulcsként felfogható algoritmus segítségével történik. A titkosított adatok a kulcs ismerete nélkül olvashatatlanok.*" [95]

A fenti definícióban említett kulcs az egyik legfontosabb része a kriptográfiának. A kulcs mérete és algoritmusa határozza meg, hogy milyen gyorsan törhető fel a titkosítás. Lehet alkalmazni szimmetrikus[58] és aszimmetrikus[59] kulcsú titkosítást valamint ezek kombinációját. A **szimmetrikus** titkosítás előnye, hogy a titkosítás művelete **gyors**an végrehajtható, viszont a **kulcs csere nehézkes**, mivel mindkét félnek rendelkeznie kell ugyanazzal a kulccsal, melyet csak biztonságos úton oszthatnak meg egymással. További problémát jelent, ha kettőnél több résztvevő kommunikál egymással. Ilyenkor minden egyes fel-

[58] Ugyanaz a kulcs használandó a titkosításhoz és a visszafejtéshez egyaránt.
[59] A titkosítás a címzett publikus kulcsával történik, melyet a privát kulcsa segítségével tud visszafejteni.

adónak minden egyes címzettel meg kell egyeznie. Ha pedig többen ugyanazt a kulcsot használják, akkor nem azonosítható egyértelműen a feladó. Ezzel szemben az **aszimmetrikus** titkosítás **lassabb** ugyan, de **nem okoz gondot a kulcs csere**, mivel minden, a titkosításban résztvevő fél rendelkezik egy saját kulcspárral (publikus-privát), melynek a publikus részét szabadon terjesztheti (közzé teheti akár a honlapján is), mivel a vele titkosított állományt csak a privát kulcsával lehet visszafejteni, valamint a publikus kulcsból semmilyen módon nem következtethető ki a privát kulcs. Ennél a titkosítási módszernél lehetőség nyílik a feladó azonosítására is. A feladó a saját titkos kulcsával kódolja az üzenetet (digitálisan aláírja), amely műveletet csak ő tud elvégezni (feltéve, hogy nem szerezte meg valaki a privát kulcsát). A címzett pedig a feltételezett küldő nyilvános kulcsával ellenőrizheti a küldő és a küldemény valódiságát. [96]

Talán a legjobb megoldás a kettő kombinációja, az un. hibrid tikosítás, amikor a titkosítás szimmetrikus kulccsal történik, tehát a titkosítás művelete gyors és a szimmetrikus kulcs titkosítása történik aszimmetrikus tikosítással (páncélba zárjuk a gyengébb kulcsot), tehát nehezebb biztonságosabb.

Ha két számítógép kommunikál egymással nem biztonságos csatornákon, a támadók lehallgathatják, módosíthatják az üzenetet, vagy meggátolhatják annak továbbítását. A küldött adatok információtartalmának védelme mellett azonban elvárt az is, hogy tudjuk, kitől származik az üzenet. Ehhez figyelnünk kell az üzenet digitális aláírását, érvényességét, tanúsítványát, a szerző által elkülönülő harmadik fél igazolását és a visszaigazolásokat. [97]

Azért, hogy védjük hálózatunk adatforgalmát, egyéb titkosnak szánt adatunkat az illetéktelen megismerés, torzítás vagy módosítás ellen, biztosítanunk kell azok bizalmasságát, sértetlenségét és hitelességét. Egyik nagyon jó módszere, hogy ezen követelményeknek eleget tegyünk, a tikosítás.

„*Az adattitkosítási kulcsok meghatározása a csatlakozáskor történik az összeköttetésbe kerülő számítógépeken. Az adattitkosítás használatát kezdeményezheti a felhasználó számítógépe, vagy a kiszolgáló, amelyhez kapcsolódik.*" [95]

Megállapítottam, hogy **a titkosítás a közigazgatásban** is **jól hasznosítható** egyrészről **az adathordozókon tárolt adatok titkosítására**, de használható a **kommunikáció titkosítására** is.

#### 3.2.6.2. Adatmentés

Adatvesztés számos ok miatt következhet be, például lehet az ok mechanikai (por, karcolás, túlfeszültség, fizikai sérülés, stb.), logikai, elektronikai és ezek kombinációja. Bármi is az ok a megoldás a helyreállítási próbálkozások helyett a megelőzés, vagyis az adatmentés a megoldás.

Több féle mentési technika létezik, de a leglényegesebb a rendszeres ütemezett mentési struktúra kialakítása, azaz először készítünk egy teljes mentést, majd például naponta inkrementális mentést[60] és például hetente, hétvégére ütemezve teljes mentést.

Az 1. fejezetben vizsgált 223/2009. (X. 14.) Korm. rendelet [35] részletesen foglalkozik a mentés és archiválás rendjével

### 3.2.7. NAPLÓZÁS, NAPLÓELEMZÉS

Napjainkban nem csak az informatikai rendszerek válnak egyre összetettebbé, korszerűbbé, hanem az azok működését felügyelő biztonsági komponensek is. Az informatikai rendszereket fenyegető veszélyek megelőzésének és elhárításának számos eszközét használhatjuk, mint **tűzfal, víruskereső, IDS vagy IPS, melyek megfelelő konfigurálás esetén képesek akár bőséges naplózásra** is. Az így keletkezett naplók a későbbi auditok vagy más vizsgálatok lehetőségét teremtik meg. A kimondottan biztonsági berendezések pedig alkalmasak riasztások küldésére is egyes biztonsági esemény bekövetkezése esetén. [98]

**A nagyméretű naplóállományok humán átvizsgálása ma már nehézkes, szinte lehetetlen**, főleg, ha nincs meg hozzá a megfelelő létszámú humánerőforrás.

A **közigazgatásban** is problémát jelent, hogy **nincs a rendszerek monitorozására, a naplók elemzésére kialakított munkakör és nem használnak erre a feladatra alkalmas szoftvereket sem**. Amennyiben történik naplózás, akkor is általában egy **másik munkakört ellátó dolgozóra** (általában rendszergazdára) ruházzák rá ezt a feladatkört is. Ilyen esetben gyakran még a saját munkakörének ellátása is nehézkes és előfordulhat az is, hogy **nem is tudja**, valójában **mit figyeljen**, mit keressen a nagy mennyiségű naplóállományokban. A figyelmeztető értesítések magas számától való félelem miatt, a **riasztások beállítása sokszor elmarad**, vagy ha meg is történik, a sok vaklárma-riasztás (például elgépelt jelszó miatti sikertelen bejelentkezés) között elsikkadnak az igazán fontos üzene-

[60] Az előző mentés óta történt változásokat menti.

tek. **Több**, esetleg **eltérő típusú** vagy **különböző forrásból** származó üzenet egyidejű bekövetkezése viszont jelenthet **sérülékenység**et, vagy biztonsági rést kihasználó **támadás**t.

A napló fájlok lehetővé teszik a rendszer üzemeltetéséért felelős alkalmazottnak, hogy észlelje a támadásokat és mielőbb reagáljon rájuk.

A weben nyújtott egyre szélesebb körű szolgáltatások miatt **kiemelten fontos a közigazgatásban** például a **web alkalmazások üzemeltetése során keletkező naplóállományok átvizsgálása**, mivel hasznos **információkkal szolgálhat behatolási kísérletekkel kapcsolatban**. Ha a naplózás engedélyezve van, az átvizsgálással fény derülhet arra, hogy egy támadás alkalmával **a támadó milyen adatokhoz fért hozzá**, **milyen sérülékenységeket használt ki** és esetleg **bizonyítékot is szolgáltathat** a támadó személyazonosságáról.

A közigazgatás esetében egy **web alkalmazás hozzáférési naplónak** (log) minimum a következő adatokat **kell tartalmaznia**:

- **autentikációval kapcsolatos információk**, mint például a sikeres és sikertelen bejelentkezések és a jelszó megváltozása;
- a hozzáférés kezelés által **blokkolt adathozzáférési próbálkozások**;
- minden **kérés**, mely **ismert támadásokra használható karakterláncot tartalmaz**.

A legtöbb esetben a figyelmeztető mechanizmusnak döntést kell hoznia, hogy valóban támadás történt-e, és ne generáljon téves riasztásokat. Egy jól megtervezett riasztó mechanizmus képes a különböző tényezők kombinációja alapján döntéseket hozni.

A **rendellenes események**, melyeket a riasztó mechanizmus figyel, a következők lehetnek:

- felhasználói anomáliák, mint például, ha nagyszámú kérés érkezik egyetlen IP címről, vagy felhasználótól, amit például egy scripttámadás idézheti elő;
- a szokásosnál eltérő forgalom;
- a kérések ismert támadási karaktersorozatokat tartalmaznak;
- a kérésekben a felhasználó elől rejtett adatokat megváltoztatták.

**A napló fájlokat erős védelemmel kell ellátni** a jogosulatlan hozzáférések ellen. Egy tipikus megvalósítása a log fájlok tárolásának, hogy egy teljesen különálló rendszert hozunk létre, mely csak a fő alkalmazástól érkező frissítő üzeneteket engedi be.

A fentebb említett problémák megoldására a közigazgatásban **javaslom** külön **monitorozó munkakör létrehozását**, valamint **automatizált napló- vagy esemény-feldolgozó rendszerek alkalmazását**. Ezek a rendszerek képesek az információ centralizált gyűjtésére, összefüggések figyelésére, az események szelektálására, a biztonsági incidensek jelzésére. Segítségükkel lehetővé válik a naplóállományok biztonsági szempontú szisztematikus feldolgozása, és megoldás adható a szabályzatokban, biztonsági irányelvekben, törvényekben is megjelenő napló-feldolgozási követelményre.

## 3.3. JAVASLATOK A KÖZIGAZGATÁSI INFORMATIKAI RENDSZEREKBEN ALKALMAZANDÓ VÉDELMI MEGOLDÁSOKRA

A fejezetben megfogalmazottak és megállapítások alapján, valamint az elvégzett kockázatelemzés és hatáselemzés eredményei alapján a következő **védelmi intézkedések** alkalmazását **javaslom** a közigazgatás **minden szervezetének** informatikai rendszereiben:

1. a **szerverek** és a hálózati kapcsolattal vagy a nélkül ugyan, de külső adathordozó csatlakozási lehetőséggel rendelkező **munkaállomások** esetében **integrált** (vírusvédelem, tűzfal, IDS/IPS) **végpont védelem bevezetését.** Ennek segítségével **a hibás vagy manipulált alkalmazói, illetve rendszerprogramok hibáiból eredő adatvesztések, károsodások**, valamint a távoli munkavégzés lehetőségének biztosításával **a távoli gépről rendszerbe kerülő sérülékenységek kockázata elviselhető szintre redukálható**. Ez a védelmi forma az említett kockázatokra egyrészt a szerverek és munkaállomások használatára vonatkozó megfelelő **központi szabályozással** (telepítési jogokra, jogosultságokra, külső adathordozó csatlakoztatására, stb.), másrészt **központosított vírus és e-mail szűréssel** és a **külső adatforgalom folyamatos ellenőrzésének** lehetőségével biztosít megoldást. Ezen funkciók **automatizált** megvalósítására alkalmasak a mai korszerű **integrált végpontvédelmi megoldások**, melyek a **víruskeresés és irtás** lehetőségein túl **tűzfal, behatolás érzékelés és megelőzés**, sőt még **hálózati hozzáférés vezérlési** szolgáltatásokat is nyújtanak;
2. a végpontok (szerverek, munkaállomások) szoftvereinek (felhasználói, operációs rendszer és a végpontok védelmét ellátó is) **rendszeres frissítésére** szolgáló **architektúra kialakítását**, mely a frissítési szolgáltatást egy, a rendszer méretétől és elhelyezkedésétől függően esetleg több **Update szerver segítségével** szerve-

zeti szinten **központi csoportházirend terjesztési elv alapján** biztosítja;

3. a **határvédelem megerősítését** Screened Subnet tűzfal architektúra kialakításával, a web alkalmazások biztonsága érdekében megfelelően konfigurált **alkalmazás szintű tűzfal alkalmazásával,** melynek segítségével a hálózatba történő jogosulatlan bejutás kockázata csökkenthető;
4. azoknak a szervereknek a DMZ-be való elhelyezését, amelyeket a hálózaton kívülről és a védett hálózaton belülről is el kell érni;
5. a **levelező szerveren vírusvédelemmel kombinált levélszűrés** és általános korlátozó szűrési **szabályok** alkalmazását;
6. napló-házirend készítését és legalább az „Alkalmazás", a „Biztonság" és a „Rendszer" **naplózását**, valamint a naplófájlok **folyamatos**, **automatizált elemzésére** szolgáló **napló- vagy esemény-feldolgozó rendszerek alkalmazását,** továbbá **a felügyelet ellátására külön munkakör létrehozását**;
7. a naplófájlokhoz csak **megfelelő jogkörrel** való hozzáférést;
8. **integrált központi felhasználó- és hozzáférés-vezérlés bevezetését**, mely az illetéktelen adathozzáférés kockázatát jelentős mértékben csökkenti, mivel segítségével **a humánerőforrás gyengeségei a felhasználói életciklus tejes egészében minimálisra csökkenthető a felhasználók és a jogosultságok kezelésének automatizálási lehetőségével**;
9. **üzenetek, fájlok titkosítását**, **automatizált mentési rendszer bevezetését**, melynek segítségével a **nyílt csatornákon történő levélforgalom védelme megoldható**, illetve az **adathordozók** (CD, DVD, pendrive, notebook, stb.) **elvesztése, sérülése, vagy eltulajdonítása kapcsán keletkező kockázat** az információhoz történő illetéktelen hozzáférés meggátolásával és a mentésből történő visszaállításával **elfogadható szintre csökkenthető**;
10. a képzés, felkészítés hatékonyabbá tétele, a biztonságtudatosság növelése mind felhasználó, mind üzemeltetői oldalon.

A fenti védelmi intézkedések – a már meglévő jogszabályokkal és ajánlásokkal – és az általam az első fejezetben tett jogszabályi (törvényi) és szervezeti javaslatokkal, jelentősen növelheti a közigazgatási szervezetek informatikai biztonságának megteremtése terén tett erőfeszítéseink sikerét.

A fenti védelmi intézkedések többsége külön díjazás mellett igénybe vehető az Elektronikus Kormányzati Gerinchálózathoz és az Informatikai Közhálóhoz csatlakozott szervezetek részére az EKG-n keresztül. Ebben az esetben az igénybevett szolgáltatások esetében a kockázatokért az üzemeltető a felelős, azaz kockázat áthárításról beszélünk.

Áttekintve az elemzett és javasolt védelmi megoldásokat, megállapíthatjuk, hogy a vállalkozásokban (vállalati szférában) és a közigazgatási informatikai rendszerekben alkalmazható megoldások között nincsenek lényegi eltérések, de, mint ahogy a korábbi CERT jelentés és a statisztikai elemzés is mutatja, ezeknek az alkalmazása a közigazgatási informatikai rendszerekben kevésbé elterjedt. Ennek okait a szabályozás, finanszírozás, szaktudás, biztonsági igényesség, motiváltság területeken meglévő hiányosságokban látom.

# KÖVETKEZTETÉSEK

A **közigazgatásban** üzemeltetett informatikai rendszerek esetében, **mint egyfajta kritikus információs infrastruktúra**, **kiemelt fontosságú**, hogy **az alkalmazottak tisztában legyenek a rendszert esetlegesen fenyegető veszélyforrásokkal, kezelésükkel**. Az 1. fejezetben is rámutattam, hogy alsóbb szinteken nem, vagy csak részben valósulnak meg a felsőbb szintű rendeletek implementációi, ami nagymértékben nehezíti, szinte lehetetlenné teszi egy megfelelő informatikai biztonsági védelmi rendszer kialakítását. Ebben a fejezetben is alátámasztottam, hogy **a megfelelő szabályzatok megalkotása, betartatása és a biztonságtudatosság fejlesztése számos kockázati tényező kezelését szolgálja**.

**Megvizsgáltam** a ma rendelkezésre álló, **korszerű védelmi megoldásokat** és statisztikai adatok alapján **megállapítottam**, hogy nem, vagy csak **részben alkalmazzák** őket a közigazgatás informatikai rendszereiben.

Ennek megfelelően **elvégeztem** egy, az értekezés korábbi részeiben feltárt fenyegetésekre és védelmi hiányosságokra koncentrálódott célzott, részleges **kockázatelemzést**, melynek **eredményei alapján javaslatot tettem a közigazgatás minden szervezetének** informatikai rendszereiben az alábbi **védelmi megoldások bevezetésére, erősítésére:**

- **megvizsgálva** a **kártékony kódok** elleni védelem kialakításának lehetőségeit, megállapítottam, hogy a malware incidensek megelőzésére **elengedhetetlen, de nem elégséges a vírusvédelmi eszközök telepítése** és azok megfelelő konfigurációja, valamint a **naprakész vírusadatbázis biztosítása**. Mivel némely kártevőt gyakran igen nehéz detektálni, ezért a vírusvédelem mellett szükséges **a hálózati forgalom és a hálózati események folyamatos monitorozás**a is. Így tehát komplex megoldás alkalmazása szükséges annak érdekében, hogy a rosszindulatú programokat észlelni tudja, még akkor is, ha azok az „antivírus" szoftverek adatbázisaiban sem szerepelnek. Fentiekből, valamint a kockázatelemzés eredményeiből **arra a következtetésre jutottam**, hogy ma már ennek a veszélyforrásnak a kezelése leghatékonyabban **központilag vezérelt, integrált** alkalmazások segítségével oldható meg. Ezek alkalmasak **a hibás vagy manipulált alkalmazói, illetve rendszerprogramok hibáiból eredő adatvesztések, károsodások**, valamint a távoli munkavégzés lehetőségének biztosításával **a távoli gépről rendszerbe kerülő sérülékenységek által okozott kockázatok elviselhető szintre redukálására**. Ennek megfelelően javaslatot tettem a közigazgatási

informatikai rendszerekben **integrált végpontvédelmi megoldások bevezetésére** valamint a szerverek és munkaállomások szoftvereinek **rendszeres frissítésére** szolgáló **architektúra kialakítására;**

- **elemeztem** a **tűzfal** rendszer kialakításának lehetőségeit, a különböző típusú tűzfalak képességeit és **arra a következtetésre jutottam**, hogy a közigazgatási informatikai rendszerek és szolgáltatások sajátosságai **Screened subnet architektúra** kialakítását, **alkalmazás szintű tűzfallal történő üzemeltetését igényli,** melynek segítségével a hálózatba történő jogosulatlan bejutás kockázata csökkenthető. Ez az architektúra lehetőséget biztosít azoknak a szervereknek a DMZ-be való elhelyezésre, amelyeket a hálózaton kívülről és a belső védett hálózatból is el kell érni;
- megvizsgáltam a **behatolás érzékelő, illetve -megelőző eszközök** képességeit és megállapítottam, hogy a **belső hálózaton történő támadások**, illetve **illetéktelen hozzáférési kísérletek érzékelésére és elhárítására** ezek az eszközök **nyújtanak megnyugtató megoldást**;
- a **felhasználó- és hozzáférés-menedzsment rendszerek vizsgálata során arra a megállapításra jutottam**, hogy a szervezetekben végbemenő felhasználói szerepkörökkel kapcsolatos **gyors ütemű változások**, mint a humánerőforrás felvétele, elbocsátása, átcsoportosítása során lezajló **felhasználói adatok**, **hozzáférési jogosultság változások hatékony kezelése** már egy közepes létszámú szervezetnél sem képzelhető el az alkalmazásuk nélkül. Különösen igaz ez **a közigazgatásban** manapság is **végbemenő jelentős mértékű átszervezések kapcsán**. Ezért javasoltam **integrált központi felhasználó- és hozzáférés-vezérlés bevezetését**, mellyel az illetéktelen adathozzáférés kockázatát jelentős mértékben csökkenteni lehet;
- a titkosítás és adatmentés lehetőségeit vizsgálva **megállapítottam**, hogy a **titkosítás jól alkalmazható** többek között a nyílt csatornákon történő kommunikáció védelme mellett a levélforgalom védelmére is, valamint **automatizált mentési rendszer bevezetésével kombinálva** hatékony megoldást nyújt a közigazgatásban jelentős mértékben jelen levő **adathordozók elvesztése, sérülése, vagy eltulajdonítása kapcsán keletkező kockázatok elfogadható szintre történő csökkentésére;**

- **a naplóelemzés** kérdéskörében történt vizsgálódásaim során arra a következtetésre jutottam, hogy a közigazgatás informatikai rendszerei esetében is elengedhetetlen napló-házirend készítése, az események naplózása, a naplók elemzése, mely csupán humánerőforrás alkalmazásával elvégezhetetlen, ennek megfelelően **javaslatot tettem a naplófájlok folyamatos, automatizált elemzésére** szolgáló **napló- vagy esemény-feldolgozó rendszerek alkalmazására,** továbbá **a felügyelet ellátására külön munkakör létrehozására.** A naplóelemző rendszer bevezetése a kockázatelemzésem eredménye alapján ugyan nem a kiemelt intézkedéseket igénylő sérülékenységek kezelésére szolgáló eszköz, de jelentős szerepet tölthet be például egy, a rendszerbe történő illetéktelen behatolás felderítésében.

Megállapítottam, hogy a vállalkozásokban (vállalati szférában) és a közigazgatási informatikai rendszerekben nincsenek lényegi eltérések az alkalmazható védelmi megoldásokban, de, mint ahogy a korábbi CERT jelentés és a statisztikai elemzés is mutatja, ezeknek az alkalmazása a közigazgatási informatikai rendszerekben kevésbé elterjedt. Megítélésem szerint az általam javasolt védelmi megoldások bevezetésével a **közigazgatási informatikai rendszerek biztonsága jelentősen fokozható**.

# ÖSSZEGZETT KÖVETKEZTETÉSEK

A szükséges alapvető fogalmak tisztázását, valamint a közigazgatási informatikai rendszer **meghatározását** követően **megalkottam** a **közigazgatási informatikai rendszerek funkcionális és strukturális modelljét.**

Bemutattam az elektronikus kormányzás alapinfrastruktúráját alkotó Elektronikus Kormányzati Gerinchálózatot és **elemeztem** az Ügyfélkaput.

**Megvizsgáltam** az informatikai rendszerek alapvető folyamatait és **megállapítottam**, hogy **a legkritikusabb az adatok rendszerbe kerülési, kivételi folyamata, valamint a tárolás**. Ezeknek a folyamatoknak **a megfelelő szabályozása** jelentős mértékben **növelheti** az informatikai biztonság szintjét.

Tanulmányoztam az e-közigazgatási keretrendszer informatikai biztonsági követelményrendszerét, **elemeztem** a szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételeit és **megfogalmaztam az informatikai biztonsági stratégia célkitűzéseit, követelményeit** és bemutattam egy **lehetséges felépítését**.

A célkitűzések alapján **megállapítottam** az informatikai biztonság kialakítása során a legfontosabb végrehajtandó **feladatokat,** azok rendszeres felülvizsgálatának kérdéseit.

**Megvizsgáltam** a közigazgatás informatikai rendszereire informatikai biztonság szempontjából jelenleg érvényben levő és **irányadó kormányrendeletet** és elődeinek tartalmát, és **megállapítottam**, hogy még mindig **vannak hiányosságok,** továbbá a megfelelő implementációk **az alsóbb szinteken nem, vagy csak részben jönnek létre,** melynek okát legfőképpen a megfelelő szakember és a finanszírozás hiányában látom.

Fentiek alapján **javaslatot tettem** egy nemzetközi szabványon és jó gyakorlatokon alapuló, a közigazgatási szervezetek informatikai biztonságát széleskörűen szabályozó **információbiztonsági törvény kidolgozására**, továbbá egy szakértőkből álló **belső auditori** és **tanácsadói** feladatokat ellátó **információbiztonsági szervezet létrehozására**.

**Megvizsgáltam** a közigazgatási informatikai rendszerek kialakításában, szabályozásában, működtetésében, felhasználásában részt vevő humán oldal **biztonságtudatosságának fejlettségi szintjét** és **megállapítottam**, hogy a közigazgatási szervezetekben **szemléletmódbeli problémák is akadályozzák** a megfelelő informatikai biztonság kialakítását, fenntartását, ezért **javaslatot tettem** annak megváltoztatását célzó **módszerek**, úgymint tréningek, szituációs gyakorlatok, tesztvizsgák szervezésére, **bevezetésére**.

Az informatikai rendszerek elleni **támadások főbb lépéseinek tisztázását** követően **elemeztem, rendszereztem, csoportosítottam** a közigazgatási informatikai rendszerek biztonságát fenyegető **veszélyforrásokat**, a támadók körét, célpontjait, és a támadások módszereit. **Megvizsgáltam és elemeztem a külső támadások** lehetőségét a hálózat, az operációs rendszer és a telepített alkalmazások sérülékenységeinek kihasználása szempontjából, valamint a **belső veszélyeztetések** különböző lehetőségeit, továbbá a **kettő kombinációjában** végrehajtható támadási formákat.

Ezt követően egy aktuális kérdésre kívántam választ adni, hogy nyílt vagy zárt forráskódú operációs rendszerek használata a célszerűbb a közigazgatási rendszerek számítógépein. Ezért **teszteltem, megvizsgáltam és összehasonlítottam** a közigazgatási informatikai rendszerekben **leggyakrabban alkalmazott szerver operációs rendszerek több szolgáltatását a biztonságos alkalmazás szempontjából**, és **megállapítottam**, hogy **a nyílt forráskódú operációs rendszerek alkalmazása** a szoftverek beszerzésének költségei terén ugyan **költségcsökkentő tényezőként szolgálhatna**, képességeit tekintve nem rosszabb, mint a zárt forráskódú operációs rendszerek biztonsági szolgáltatásai. Azonban a biztonságos működtetés humánerőforrás háttere, **a kellő szaktudás hiányzik**, valamint jelentős idő-, energia- és anyagi ráfordítást igényelne a közigazgatás **saját fejlesztésű**, tipikusan Microsoft alapú alkalmazásainak átállítása. Továbbá a nyílt forráskódú operációs rendszerek alkalmazásával **jelentős sérülékenység kerülne a rendszerbe**, mert statisztikai adatokkal **bizonyítottam**, hogy azok **sokkal kedveltebb célpontjai a támadásoknak**.

**Megállapítottam**, hogy egy vállalati és egy közigazgatási informatikai rendszert ért támadást tekintve az alkalmazott **módszerekben, eszközökben és** a támadók **motivációjában lényeget érintő eltérés nem tapasztalható**. Az **alapvető különbséget** egyrészt a tárolt-feldogozott információk jellegének különbségéből fakadó **következményekben,** másrészt **a rendelkezésre állási fenyegetések kormányzásra gyakorolt negatív hatásában,** harmadrészt **a cyberhadviselési fenyegetéseknek a közigazgatás működőképességére gyakorolt negatív hatásában látom.**

**Megvizsgáltam és értékeltem a korszerű informatikai védelmi megoldásokat,** statisztikai adatok alapján **megállapítottam**, hogy a közigazgatás informatikai rendszereiben azokat nem, vagy **csak egy részét alkalmazzák.**

**Elvégeztem** egy, az értekezés korábbi részeiben feltárt fenyegetésekre és védelmi hiányosságokra koncentrálódó célzott, részleges **kockázatelemzést és hatáselemzést**, mely-

nek **eredményei alapján javaslatot tettem a közigazgatás minden szervezetének** informatikai rendszereiben történő következő **védelmi megoldások bevezetésére, erősítésére:**

- **központilag vezérelt, integrált végpontvédelmi megoldások** bevezetése valamint központilag vezérelt **szoftver frissítési architektúra kialakítása** a hibás vagy manipulált alkalmazói, illetve rendszerprogramok, valamint a távoli munkavégzés során a távoli gépről rendszerbe kerülő sérülékenységek által okozott kockázatok elviselhető szintre redukálására;
- **Screened subnet tűzfal architektúra** kialakítása, **alkalmazás szintű tűzfallal történő üzemeltetése** a hálózatba történő jogosulatlan bejutás kockázatának csökkentése érdekében;
- **behatolás érzékelő, illetve -megelőző eszközök** alkalmazása a belső hálózaton történő támadások, illetve illetéktelen hozzáférési kísérletek érzékelésére és elhárítására;
- **integrált központi felhasználó- és hozzáférés-menedzsment rendszerek** bevezetése az illetéktelen adathozzáférés kockázatának csökkentése érdekében;
- **titkosítás** és **automatizált mentési rendszer** bevezetése a nyílt csatornákon történő kommunikáció védelme mellett a levélforgalom védelmére, valamint az adathordozók elvesztése, sérülése, vagy eltulajdonítása kapcsán keletkező kockázatok elfogadható szintre történő csökkentésére;
- **napló- vagy esemény-feldolgozó rendszerek alkalmazása,** továbbá **a felügyelet ellátására külön munkakör létrehozása** a rendszer problémáinak, illetve az esetleges illetéktelen behatolás vagy kísérlet felderítésére.

**Megállapítottam**, hogy a vállalati szférában és a közigazgatási informatikai rendszerekben az **alkalmazható védelmi megoldásokban nincsenek lényegi eltérések**, de azok alkalmazása a közigazgatási informatikai rendszerekben **kevésbé elterjedt.** Ezért a fent javasolt megoldások bevezetése szükségszerű, alkalmazásukkal a **közigazgatási informatikai rendszerek biztonsága jelentősen fokozható**.

# ÚJ TUDOMÁNYOS EREDMÉNYEK

1. **Megalkotva** a közigazgatási informatikai rendszerek **funkcionális és strukturális modelljét**, és **elemezve** a működési folyamatait, biztonsági szabályzóit, **feltártam azok hiányosságait, felvázoltam a fejlesztés irányait, és meghatároztam** az e szervezetekben kialakítandó **informatikai biztonsági stratégiával szemben támasztott követelményeket, a stratégia lehetséges felépítését** és a hozzá kapcsolódó **informatikai biztonsági politikában foglalt feladatokat**.

2. A közigazgatási informatikai rendszerek **strukturális modelljére alapozva elemeztem** az azok elleni támadók körét és a támadások fajtáit, majd ennek eredményeként **megalkottam az e rendszerek elleni veszélyforrások (támadások) újszerű csoportosítását**.

3. A támadók körének és a támadási fajtáknak a **vizsgálata** valamint a támadási célpontok arányának **statisztikai elemzése**, továbbá **saját tesztelési eredményeim alapján összehasonlítottam** a közigazgatási informatikai rendszerekben leggyakrabban alkalmazott operációs rendszereket a biztonságos alkalmazás szempontjából, és **igazoltam, hogy a zárt forráskódú operációs rendszerek további alkalmazása nem hátrányosabb, mint áttérni a** lényegesen nagyobb mértékben célpontnak számító **nyílt forráskódú operációs rendszerekre**.

4. A feltárt fenyegetésekre és védelmi hiányosságokra koncentrálódó célzott, részleges **kockázatelemzés és hatáselemzés alapján** megvizsgáltam és értékeltem a korszerű informatikai védelmi megoldásokat, és ezek eredményeként **javaslatokat tettem azoknak a közigazgatási informatikai rendszerekben való alkalmazhatóságára**, melyekkel eredményesen **növelhető** a közigazgatási szervek **informatikai biztonsága**.

# AJÁNLÁSOK

1. Javaslom a doktori (PhD) értekezésem közigazgatási szervezetek informatikai rendszerei biztonságának szabályozási kérdéseivel foglalkozó fejezetének felhasználását egy új, a közigazgatási informatikai rendszerek magasabb biztonsági szintre emelését megcélzó rendelet megalkotásában, illetőleg a benne foglalt ajánlások figyelembevételét az egyes szervezetek informatikai biztonsági stratégiájának kialakítása során.

2. Javaslom az értekezésem felhasználását az államigazgatás informatikai irányultságú területére szakembereket képző felsőoktatási intézmények alap, mester és doktori képzésében tananyagként.

3. Javaslom továbbá az informatikai rendszerek elleni támadási formákról, valamint az alkalmazható védelmi megoldásokról szóló fejezeteit felhasználni az informatikai biztonság irányultságú alap, mester és doktori képzésben tananyagként.

# TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM

## Lektorált folyóiratban megjelent cikkek

1. V. Póserné Oláh: Security and performance of the webservers, the open source and the closed source operation systems, in Scientific Bulletin of "Politechnika" University of Timisoara, Romania, Vol. 55(69), No. 1 / March 2010, pp. 43-48., ISSN 1224-600X
2. V. O. Póserné - Zs. Haig: The Forms and Defence Possibilities of the Threats Against Computer Networks, Hadmérnök, 2006. I. évf. 1. sz., Budapest, 2006, p. 13, ISSN 1788-1919, http://hadmernok.hu/archivum/2006/1/2006_1_haig.pdf
3. V. O. Póserné: The security of Web Applications, AARMS Vol. 8, No. 1, 2009, pp. 173-178., ISSN 1788-0017 (Online), ISSN 1588-8789 (Print)
4. Póserné O. V.: Az információs társadalom és a terrorizmus kapcsolata, Bolyai Szemle, 2006. 1. sz., Budapest, 2006, pp. 145-159., ISSN 1416-1443.
5. Póserné O. V.: IT kockázatok elemzésük, kezelésük, Hadmérnök, 2007. II. évf. 3. sz., Budapest, 2007, p. 9, ISSN 1788-1919, http://hadmernok.hu/archivum/2007/3/2007_3_poserne.pdf
6. Póserné O. V.: A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei, Hadmérnök, 2007. II. évf. 4. sz., Budapest, 2007, p. 10, ISSN 1788-1919, http://hadmernok.hu/archivum/2007/4/2007_4_poserne.pdf
7. Póserné O. V.: Rejtjelző módszerek vizsgálata, Hadtudományi Szemle, 2008. 1. évf. 1. sz., Budapest, 2008, p. 14, HU ISSN 2060-0437, http://hadtudomanyiszemle.zmne.hu/files/2008/1/pov.pdf
8. Póserné O. V.: Nyílt és zárt forráskódú operációs rendszerek leggyakoribb szolgáltatásainak vizsgálata biztonság és teljesítmény szempontjából, Bolyai Szemle, 2009. XVIII. évf. 4. sz., Budapest, 2009, pp. 103-117, ISSN 1416-1443

## Konferencia kiadványban megjelent előadások

1. V. O. Póserné: Comparing the webservers of the opensource and the closed source

operation systems, Proc of the 5th International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, May 28-29, 2009, pp. 169-172., IEEE Catalog Number CFP0945C-CDR, ISBN 978-1-4244-4478-6, Library of Congress 2009903350,

2. Póserné O. V.: Az Internet adta hadászati lehetőségek és veszélyek, Robothadviselés 4. nemzetközi tudományos konferencia kiadványa, Budapest, 2005, pp. 136-148., ISBN 963 7060 08 1

3. Póserné O. V.: Informatikai biztonság gyakorlatban, Matematika-, fizika, számítástechnika főiskolai oktatók XXX. konferencia publikációs kiadvány-CD, Pécs, 2006., p. 5, ISBN-13: 978-963-7298-12-7

4. Póserné O. V. - Katona K. - Szénási S.: A Delphi haladó eszközeinek alkalmazása, Matematika-, fizika, számítástechnika főiskolai oktatók XXX. konferencia publikációs kiadvány-CD, Pécs, 2006., p. 6, ISBN-13: 978-963-7298-12-7

5. Póserné O. V.: Számítógép-hálózati támadások, Hadmérnök, Robothadviselés 6. tudományos szakmai konferencia Különszám, Budapest, 2006, p. 9, ISSN 1788-1919, http://hadmernok.hu/kulonszamok/robothadviseles6/poserne_rw6.pdf

6. Póserné O. V.: A távoli munkavégzés biztonsági kérdései, Hadmérnök, Robothadviselés 7. tudományos szakmai konferencia Különszám, Budapest, 2007, p. 9, ISSN 1788-1919, http://hadmernok.hu/kulonszamok/robothadviseles7/poserne_rw7.pdf

7. Póserné O. V.: A kapcsolók hatása a hálózati biztonságra, Informatika Korszerű Technikái Konferencia 2008, Dunaújváros, 2008, pp. 102-109., ISBN 978-963-87780-2-4

8. Póserné O. V. – Schubert T.: Informatikai biztonság – szakirányú képzés a Budapesti Műszaki Főiskolán, Informatika a felsőoktatásban 2008 konferencia publikációs kiadvány-CD, Debrecen, 2008, p. 8, ISBN 978-963-473-129-0

9. Póserné O. V.: A magyar közigazgatás az informatikai biztonság szemszögéből, Bolyai Szemle, 2008. XVII. évf. 4. sz., A Robothadviselés 8. Tudományos konferencia előadásainak szerkesztett változata, Budapest, 2008, pp. 157-166., ISSN 1416-1443

# FELHASZNÁLT IRODALOM


1. Chikán Attila: Vállalatgazdaságtan, Aula Kiadó, Budapest, 2001., ISBN: 9789639478749
2. Detrekői Ákos, Szabó György: Térinformatika, Nemzeti Tankönyvkiadó, Budapest, 2002., ISBN 963 19 266 5
3. Dr. Munk Sándor: Katonai informatika II. Katonai informatikai rendszerek, alkalmazások egyetemi jegyzet, ZMNE, Budapest, 2006.
4. Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, Bolyai Szemle XVII. évf. 4.sz., 2008., pp. 137-154., ISSN: 1416-1443
5. Dr. Haig Zsolt: Az információbiztonság komplex értelmezése, Robothadviselés 6. tudományos konferencia kiadványa, Hadmérnök különszám, 2006. nov. 22., ISSN 1788-1919., http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.htm, 2009.05.20.
6. Munk Sándor: Információbiztonság vs. informatikai biztonság, Robothadviselés 7. tudományos konferencia kiadványa, Hadmérnök különszám 2007. nov. 27., ISSN 1788-1919., http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf, 2009.05.20.
7. Haig Zsolt: Az információs társadalom információbiztonsága, Robothadviselés 8. tudományos konferencia kiadványa, Bolyai Szemle, 2008. 4. sz., Budapest, pp. 167-180., ISSN 1416-1443., http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/12_Haig_Zsolt.pdf, 2009.05.23.
8. Mezey Gy. szerk., Karap G.: Központi államigazgatási információs rendszerek, Bp. HEFOP 2006.
9. Lőrincz Lajos: A hatékony állam, Magyar közigazgatás 2005. augusztus 8. sz., 452.p.
10. IT Biztonsági követelményrendszer érvényesítésének módja a közigazgatási informatikai rendszerek fejlesztések során, MEH EKK, 2008.07.10.

11. 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. Határozatok tára 31. szám. Budapest, 2008. június 30. 217-231p.
12. Communication from the Commission to the Council and the European Parliament. Critical Infrastructure Protection in the Fight Against Terrorism. Brussels, 20.10.2004 COM(2004) 702 final.
13. Seres György: Fenntartható fejlődés – fenntartható nemzetvédelem, Hadmérnök, 2010. V. évf. 4. sz., Budapest, 2010, pp. 322-339., ISSN 1788-1919, http://hadmernok.hu/2010_4_seres.pdf, 2011.03.23.
14. Dr. Kovács László: Kritikus információs infrastruktúrák Egyetemi jegyzet, ZMNE, 2007.
15. Elektronikus Kormányzati Gerinchálózat. http://www.ekk.gov.hu/hu/emo/ekg/ekg, 2011.04.25.
16. Általános Ügyfélkapu leírás. http://www.ekk.gov.hu/hu/emo/csatlakozaskr/ugyfelkapu/uk?keresett_kifejezes=ügyfélkapu, 2011.04.14.
17. Ügyfélkapu. https://ugyfelkapu.magyarorszag.hu/, 2011.05.15.
18. dr. Dedinszky Ferenc Miniszterelnöki Hivatal Informatikai Biztonsági Felügyelő: Vezetői összefoglaló a Központi Rendszer egyes szolgáltatásainak üzemzavarairól, http://www.ekk.gov.hu/hu/ekk/letoltheto/osszesitett_jelentes_KR.pdf, 2009.03.04.
19. Póserné Oláh Valéria: A szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételei, Hadmérnök, 2007. II. évf. 4. sz., Budapest, 2007, pp. 84-93., ISSN 1788-1919, http://hadmernok.hu/archivum/2007/4/2007_4_poserne.pdf, 2010.10.22.
20. e-Közigazgatási Keretrendszer Kialakítása projekt: Közigazgatási Operatív Programok IT Biztonsági környezete, a biztonsági követelményrendszer struktúrája, Miniszterelnöki Hivatal, 2008 http://www.ekk.gov.hu/.../EKK_ekozig_KOP_ITBizt_kornyezete_080529_V1. docx, 2011.03.21.

21. Muha Lajos: Infokommunikációs biztonsági stratégia, Hadmérnök, 2009. IV. évf. 1. sz., Budapest, 2009, pp. 214-224., ISSN 1788-1919, http://hadmernok.hu/2009_1_muha.pdf, 2010.05.23.

22. Póserné Oláh Valéria: A magyar közigazgatás az informatikai biztonság szemszögéből, Bolyai Szemle, 2008. XVII. évf. 4. sz., A Robothadviselés 8. Tudományos konferencia előadásainak szerkesztett változata, Budapest, 2008, pp. 157-166., ISSN 1416-1443

23. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

24. Informatikai biztonsági módszertani kézikönyv (ITB 8. sz. ajánlása). - Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Budapest, 1994. http://www.itb.hu/ajanlasok/a8/, 2010.05.22.

25. Informatikai biztonsági módszertani kézikönyv (ITB 12. sz. ajánlása). - Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Budapest, 1994., http://www.itb.hu/ajanlasok/a12/, 2010.05.22.

26. Muha Lajos: Magyar Informatikai Biztonsági Keretrendszer (MIBIK), Budapest: Miniszterelnöki Hivatal, 2008.

27. Fleiner Rita; Muha Lajos: Adatbázisok biztonságának kezelése a közigazgatásban, Hadmérnök, 2010. V. évf. 4. sz., Budapest, 2010, pp. 235-247., ISSN 1788-1919, http://hadmernok.hu/2010_4_muha_fleiner.pdf, 2011.04.17.

28. Berkes Zoltán; Déri Zoltán; Krasznay Csaba; Muha Lajos: Informatikai Biztonsági Irányítási Rendszer (IBIR), Budapest: Miniszterelnöki Hivatal, 2008.

29. Déri Zoltán; Lobogós Katalin; Muha Lajos; Sneé Péter; Váncsa Julianna: Informatikai Biztonság Irányítási Követelmények (IBIK), Budapest: Miniszterelnöki Hivatal, 2008.

30. Balázs István; Déri Zoltán; Lobogós Katalin; Muha Lajos; Nyíri Géza; Sneé Péter; Váncsa Julianna: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Budapest:

31. Balázs István; Szabó István: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS), Budapest: Miniszterelnöki Hivatal, 2008.

32. Krasznay Csaba; Muha Lajos; Rigó Ernő; Szigeti Szabolcs: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX), Budapest: Miniszterelnöki Hivatal, 2008.

33. 195/2005. (IX. 22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról, www.ekk.gov.hu/hu/ekk/letoltheto/195_2005.pdf, 2008.11.15.

34. A Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről szóló 84/2007 (IV.25.) Korm. rendelet, 3. melléklet, Magyar Közlöny 52. szám, Budapest, 2007.04.25., p. 3401.

35. 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról

36. Magyar cégek előadása Brüsszelben ,Computerworld, 2007. május 11. http://computerworld.hu/magyar-cegek-eloadasa-brusszelben.html, 2008.11.15.

37. Krasznay Csaba; Szigeti Szabolcs: A magyar elektronikus közigazgatási rendszer biztonsági analízise, Networkshop 2006., Miskolc

38. Parlamenti ülés, http://www.parlament.hu/internet/plsql/ogy_naplo.naplo_fadat_aktus?p_ckl=38&p_uln= 103&p_felsz=163&p_felszig=166&p_aktus=29

39. Csillag Imre: A Baranya Megyei Rendőr-főkapitányság informatikai biztonsági átvilágításának tapasztalatai, Belügyi szemle, 2004. (52. évf.) 11-12. sz. pp. 124-135.

40. Kovács László; Sipos Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala, Hadmérnök, 2010. V. évf. 4. sz., Budapest, 2010, pp. 163-172., ISSN 1788-1919, http://hadmernok.hu/2010_4_kovacs_sipos.pdf, 2011.02.15.

41. Muha Lajos: Fogalmak és definíciók, 2004., Az informatikai biztonság kézikönyve (szerk.: Muha Lajos), Budapest, Verlag Dashöfer Szakkiadó, ISBN 963 9313 12 2

42. Dr. Haig Zsolt: Az információs társadalmat fenyegető információalapú veszélyforrások, Hadtudomány, 2007. XVII. évf. 3. sz., Budapest, 2007.

43. Támadási információk, http://www.zone-h.org/archive/special=1, 2010.10.14.

44. Póserné Oláh Valéria: A kapcsolók hatása a hálózati biztonságra, Informatika Korszerű Technikái Konferencia 2008., Dunaújváros, 2008, pp. 102-109.

45. Tipton, Harold F.;, Krause, Micki, editors: Information security management

handbook 5th ed., Auerbach Publications, A CRC Press Company, Boca Raton London New York Washington, D.C., 2005.

46. Nemzeti Hálózatbiztonsági Központ: Oracle Open Office sérülékenységek, http://tech.cert-hungary.hu/vulnerabilities/CH-3773, 2010.10.14.
47. itB online: Fő a biztonság, http://www.itbusiness.hu/print/rss_3/itst110302.html, 2011.03.02.
48. Kristóf Csaba: Mit is tud valójában a Firesheep kiegészítő?, http://computerworld.hu/mit-is-tud-valojaban-a-firesheep-kiegeszito.html, 2010.10.29.
49. Leitold Ferenc: Horgászni jó - de hogy pont a mi zsebünkből..., http://computerworld.hu/horgaszni-hogy-pont-zsebunkbol.html, 2006.11.29.
50. Dan Goodin: CIA, PayPal under bizarre SSL assault, http://www.theregister.co.uk/2010/01/29/strange_ssl_web_attack/, 2010.01.29.
51. Dajkó Pál: Ifjúoroszok hajtották végre az észtek elleni internetes támadást, http://itcafe.hu/hir/kibertamadas_esztorszag_oroszorszag.html, 2009-03-12
52. PTA CERT-Hungary Nemzeti HálózatbiztonságiKözpont: 2011. I. negyedéves jelentés, http://www.cert-hungary.hu/node/134, 2011.05.10.
53. Hillenius, Gijs: Cost of Open Source desktop maintenance is by far the lowest, http://www.osor.eu/news/de-foreign-ministry-cost-of-open-source-desktop-maintenance-is-by-far-the-lowest, 2009.01.20.
54. BBS NEWS: UK government backs open source, http://news.bbc.co.uk/2/hi/technology/7910110.stm, 2009.02.25.
55. Modine, Austin: US Army struggles with Windows to Linux overhaul, http://www.theregister.co.uk/2008/02/05/us_army_linux_integration, 2008.02.28
56. Póserné O. V.: Nyílt és zárt forráskódú operációs rendszerek leggyakoribb szolgáltatásainak vizsgálata biztonság és teljesítmény szempontjából, Bolyai Szemle, 2009. XVIII. évf. 4. sz., Budapest, 2009, pp. 103-117, ISSN 1416-1443
57. V. O. Póserné: Comparing the webservers of the opensource and the closed source operation systems, in Proc of the 5th International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, 2009, pp. 169-172.

58. Ng, David: Our Vision for Application Security, http://www-07.ibm.com/th/events/ rsdc2008/downloads/ rsdc_vision_for_application_scurity.pdf, p. 16., 2008.12.12.

59. Web Application Security Consortium: Web Application Security Statistics, http://www.webappsec.org/projects/statistics/, 2008.12.12.

60. Bill Gates szerint lényeges a biztonság, http://www.sg.hu/cikk.php?cid=35643, 2005.02.17.

61. V. O. Póserné: The security of Web Applications, AARMS, ISSN 1788-0017, Vol. 8, No. 1, 2009, pp. 173-178.

62. Muha L.; Bodlaki Á.; Csikely J.; Endrédi G.: Az informatikai biztonság kézikönyve 5.9.4.4.4., Verlag Dashöfer Ltd., 2005.

63. Dajkó Pál: Napi statisztika: mindennapos a munkahelyi adatlopás, http://itcafe.hu/hir/imperva_felmeres_munkahelyi_adatlopas.html, 2010.11.23.

64. Mitnick, Kevin: Art of Deception: Controlling the Human Element of Security, Wiley, John & Sons, Incorporated, 2003., ISBN-13: 9780764542800

65. Póserné Oláh Valéria: Számítógép-hálózati támadások, Hadmérnök, Robothadviselés 6. tudományos szakmai konferencia Különszám, Budapest, 2006., http://hadmernok.hu/kulonszamok/robothadviseles6/poserne_rw6.pdf, 2008.12.12.

66. 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=A1000161.KOR, 2010.07.07.

67. Martin Vuagnoux and Sylvain Pasini: COMPROMISING ELECTROMAGNETIC EMANATIONS OF WIRED AND WIRELESS KEYBOARDS, http://lasecwww.epfl.ch/keyboard/, 2009.10.01.

68. Symantec: More Than Half of Ex-Employees Admit to Stealing Company Data According to New Study, http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01, 2010.05.06.

69. V. O. Póserné - Zs. Haig: The Forms and Defence Possibilities of the Threats Against Computer Networks, Hadmérnök, 2006. I. évf. 1. sz., Budapest, 2006, pp. 12-24., ISSN 1788-1919, http://hadmernok.hu/archivum/2006/1/2006_1_haig.pdf, 2008.11.23.

70. Raymond, Eric S. : How To Become A Hacker? http ://www.catb.org/~esr/ faqs/hacker-howto.html, 2005.05.24.

71. Toffler, Alvin : A harmadik hullám. Információs Társadalom A-tól -Z-ig sorozat, Typotex Kiadó, 2002, ISBN: 963 9326 21 6

72. Póserné Oláh Valéria: Az információs társadalom és a terrorizmus kapcsolata, Bolyai Szemle, 2006. 1. szám, pp. 145-159., ISSN 1416-1443.

73. Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai, Hadmérnök, 2008. III. évf. 2. szám, Budapest, 2008, pp. 138-148., ISSN 1788-1919, http://hadmernok.hu/archivum/2008/2/2008_2_kovacsl.pdf, 2009.06.23.

74. Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004, http://www.fbi.gov/congress/congress04/lourdeau022404.htm, 2008.06.10.

75. Kovács László – Krasznay Csaba: Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen, Nemzet és Biztonság 2010/1. szám 2010. február pp. 44-56, ZMNE, HU ISSN 1789-5286

76. Avantgarde: Time to live on the network, http://www.avantgarde.com/xxxxttln.pdf, 2006.03.23.

77. Defacements Statistics 2008 - 2009 - 2010, http://www.zone-h.org/news/id/4735, 2011.01.25.

78. Felmérték, hogy miért hackelnek a hackerek http://www.hvg.hu/Tudomany/20050425hacker.aspx, 2005.04.25.

79. A Nemzeti Hálózatbiztonsági Központ 2010. éves jelentése, http://www.cert-hungary.hu/node/125, 2011.03.12.

80. Pák Eszter: Kifosztották a polgármesteri hivatalt, RTL Klub Híradó, 2007.12.14.

81. Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, doktori (Phd) értekezés, ZMNE, Budapest, 2007.

82. Póserné O. V.: IT kockázatok elemzésük, kezelésük, Hadmérnök, 2007. II. évf. 3. sz., Budapest, 2007, p. 9, ISSN 1788-1919, http://hadmernok.hu/archivum/2007/3/2007_3_poserne.pdf, 2008.11.26.

83. Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei – Budapest, 1996.

84. e-Közigazgatási Keretrendszer Kialakítása projekt: Útmutató az IT biztonsági szintek meghatározásához, MEH, 2008.08.22.

85. Csizmazia István: Mitől keletkeznek a biztonsági rések?, http://computerworld.hu/mitol-keletkeznek-biztonsagi-resek.html, 2007.11.23.

86. Becz Tamás; Kincses Zoltán; Tiszai Tamás; Lakatos György; Pásztor Szilárd; Rigó Ernő; Tóth Beatrix: Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai. MTA SZTAKI, 2005.

87. Cheswick, William; Bellovin, Steven M.; Rubin, Aviel D. Firewalls and Internet Security: Repelling the Wily Hacker, 2nd Edition. Boston, MA: Addison-Wesley, 2003.

88. Scarfone, Karen; Mell, Peter: Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, February 2007

89. Ristic, Ivan: Web Intrusion Detection with ModSecurity, http://www.slideshare.net/abhishek_singh/web-intrusion-detection, 2011.03.18.

90. Póserné Oláh Valéria: A távoli munkavégzés biztonsági kérdései, megoldási lehetőségek Windows szerverek esetén, Hadmérnök, Robothadviselés 7. tudományos szakmai konferencia Különszám, Budapest, 2007, p. 9, ISSN 1788-1919, http://hadmernok.hu/kulonszamok/robothadviseles7/poserne_rw7.pdf, 2009.05.12.

91. Courion: User Provision, http://www.courion.com/solutions/user-access-provisioning.html, 2010.03.15.

92. Windley, Phillip J.: Digital Identity, O'Reilly Media, 2005., Print ISBN: 978-0-596-00878-9 | ISBN 10: 0-596-00878-3

93. Josang A.; Zomai M. Al; Suriadi S.: Usability and privacy in identity management architectures. In ACSW '07: Proceedings of the 5th Australasian symposium on ACSW frontiers, 143-152.p

94. Ponemon Institute: The Billion Dollar Lost Laptop Problem, http://newsroom.intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf, 2011.02.22.

95. Microsoft TechNet Library: Adattitkosítás, http://technet.microsoft.com/hu-hu/library/cc785633%28WS.10%29.aspx, 2011.02.23.

96. Stinson, D. R.: Cryptography Theory and Practice, Third Edition, Chapman & Hall/CRC, 2005.

97. Póserné Oláh Valéria: Rejtjelző módszerek vizsgálata, Hadtudományi Szemle, 2008. I. évf. 1. sz., Budapest, 2008, pp. 38-47., HU ISSN 2060-0437, http://hadtudomanyiszemle.zmne.hu/ files/2008/1/pov.pdf, 2009.06.23.

98. Dr. Szenes Katalin: Adatfeldolgozási és biztonsági események naplózása - Az Informatikai biztonság kézikönyve, 34. aktualizálás - Verlag Dashöfer, Budapest, 2009. szeptember

# MELLÉKLETEK

1. sz. melléklet

## Az interjúk

**Interjú alanyok:**

- Kenézy Csaba, Miniszterelnöki Hivatal Elektronikuskormányzat-Központ, Védelemszervezési Irodavezető
- Dr. Kassai Károly mk. ezredes, Honvédelmi Minisztérium Informatikai és Információvédelmi Főosztály, kiemelt főtiszt
- Takács Attila, Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala Távbeszélő Szolgáltatási Osztály, osztályvezető
- Máté József pv. alezredes, Országos Katasztrófavédelmi Főigazgatóság Informatikai és Távközlési Főosztály, főosztályvezető
- Draskóczi József r. alezredes, Országos Rendőr-főkapitányság Híradástechnikai Osztály, osztályvezető
- Csillag Imre, Budapesti Rendőr-főkapitányság Informatikai Osztály, osztályvezető

Az **interjúk** kötetlen beszélgetés formájában történtek, melyek fontosabb **témakörei** az alábbiak voltak:

- a szervezet felépítése, feladatköre;
- a szervezet számítógép-hálózati felépítése, elemei;
- nyílt hálózattal való kapcsolat megoldása;
- a szervezet informatikai rendszerei (funkciók, hardver elemek, operációs rendszerek, alkalmazások);
- a kezelt adatok;
- az informatikai rendszerek üzemeltetése;
- az alkalmazott védelmi megoldások;
- támadások támadási kísérletek kezelése;
- a szervezet informatikai rendszerei és az Elektronikus Kormányzati Gerinchálózat viszonya;
- szabályozók.

2. sz. melléklet

## A magyar közigazgatás informatikai rendszereinek informatikai biztonságára vonatkozó kockázatelemzés eredményei

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Adatvagyon | Külső partnerek által, vagy felé közölt adatok | | | | | | | | | | | | | | |
| | Hardver hibák által keletkező adatvesztések, károsodások, eltérések | szakszerűtlen használat | 3 | 3 | 1 | 7 | 3 | 7 | A felvételi eljárás szabályozása, rendszeres archiválás, folyamatos oktatás, redundáns tárolás | 1 | 2 | 1 | 4 | 2 | 3 |
| | | szándékos rongálás | 3 | 4 | 1 | 8 | 1 | 6 | Biztonsági rendszer kiépítése, számonkérhetőség, nyomon követhetőség megléte, felvételi eljárás szabályozása, rendszeres archiválás, redundáns tárolás | 2 | 2 | 1 | 5 | 2 | 4 |
| | | rendszeres mentés hiánya | 4 | 3 | 1 | 8 | 4 | 9 | Rendszeres archiválás rendszerének kialakítása, redundáns tárolás | 1 | 2 | 1 | 4 | 1 | 2 |
| | | személyi felelősség hiánya | 2 | 2 | 1 | 5 | 2 | 4 | Felelősségi körök körültekintő kialakítása, rendszeres felülvizsgálata | 2 | 2 | 1 | 5 | 1 | 3 |
| | | üzemeltetési napló hiánya | 2 | 2 | 1 | 5 | 2 | 4 | Napló állományok naprakészen tartása | 2 | 2 | 1 | 5 | 1 | 3 |
| | A szoftver által okozott adatvesztések, károsodások, eltérések (hibás vagy manipulált alkalmazói, illetve rendszerprogramok által) | ismeretlen vagy nem megbízható eredetű programok használata | 3 | 4 | 4 | 11 | 4 | 12 | A munkaállomásokon a telepítési jogok, külső adathordozó csatlakoztatásának központi, automatizált szabályozása szankcionálás | 1 | 1 | 1 | 3 | 1 | 1 |
| | | szoftver illetéktelen módosítása | 3 | 3 | 4 | 10 | 2 | 9 | A szoftverekhez történő hozzáférés megfelelő jogosultságokhoz kötése, rendszeres ellenőrzés | 1 | 1 | 2 | 4 | 2 | 3 |
| | | rosszindulatú programok általi adatvesztés | 4 | 4 | 2 | 10 | 4 | 11 | Központosított vírus és e-mail szűrés, külső adatforgalom folyamatos ellenőrzése, jogosultságok megfelelő beállítása | 2 | 2 | 1 | 5 | 1 | 3 |
| | Adathordozók (CD,DVD,pendrive,notebook, stb.) meghibásodása, elvesztése, vagy eltulajdonítása | adathordozó használhatóságának rendszeres vizsgálata elmarad | 2 | 2 | 1 | 5 | 3 | 5 | Szabályozás a rendszeres állapotfelmérésre | 1 | 2 | 1 | 4 | 1 | 2 |
| | | az adatok nem biztonságos tárolása az adathordozón | 4 | 3 | 4 | 11 | 3 | 11 | Az adatok titkosítása, rendszeres mentése | 2 | 1 | 1 | 4 | 1 | 2 |
| | | személyi felelősség hiánya | 2 | 2 | 2 | 6 | 3 | 6 | Felelősségi körök körültekintő kialakítása | 1 | 1 | 1 | 3 | 2 | 2 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Adatvagyon | Adat megváltozás | hibás adatrögzítés, futtatásvezérlés, adattörlés/változtatás, | 3 | 4 | 1 | 8 | 3 | 8 | Redundáns tárolás, változtatás előtti megerősítés kérése, rendszeres archiválás | 1 | 2 | 1 | 4 | 2 | 3 |
| | | bonyolult felhasználói felület | 3 | 3 | 1 | 7 | 3 | 7 | A könnyű felhasználhatóság szempontjait figyelembe vevő szoftver fejlesztése, beszerzése | 3 | 2 | 1 | 6 | 1 | 4 |
| | Illetéktelen adathozzáférés | visszaélés hozzáférési joggal | 3 | 4 | 4 | 11 | 3 | 11 | A jogosultságok rendszeres, automatizált felülvizsgálata, csak a szükséges jogok megadása | 1 | 1 | 1 | 3 | 1 | 1 |
| | | biztonsági rendszer elégtelensége | 3 | 3 | 3 | 9 | 2 | 8 | Szegmentált, azonosítást és hitelesítést, nyomonkövetést lehetővé tevő hálózat kialakítása | 2 | 2 | 2 | 6 | 1 | 4 |
| | | azonosítási, hitelesítési rendszer hiánya | 3 | 3 | 4 | 10 | 4 | 11 | Megfelelő szintű azonosítási és hitelesítési rendszer kialakítása | 2 | 2 | 2 | 6 | 2 | 5 |
| | | elégtelen jelszó menedzsment | 2 | 2 | 3 | 7 | 3 | 7 | Jelszó alkotási szabályok lefektetése, biztonság tudatosság növelése | 2 | 2 | 1 | 5 | 2 | 4 |
| | | információbiztonsági oktatás hiánya | 3 | 3 | 3 | 9 | 3 | 9 | Folyamatos, új kihívásokat figyelembe vevő oktatási rendszer kialakítása | 2 | 2 | 1 | 5 | 1 | 3 |
| | | kilépő dolgozó bosszúállása | 3 | 4 | 4 | 11 | 3 | 11 | Kilépés után a munkavállalói jogok automatikus visszavonása és eszközök visszaszolgáltatása | 1 | 2 | 2 | 5 | 2 | 4 |
| | | kompromittáló kisugárzás | 1 | 1 | 4 | 6 | 1 | 4 | Árérték arányos árnyékolás biztosítása | 1 | 1 | 2 | 4 | 1 | 2 |
| | | személyi felelősség hiánya | 2 | 2 | 3 | 7 | 2 | 6 | Felelősségi körök körültekintő kialakítása | 1 | 1 | 2 | 4 | 1 | 2 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Szoftver | Felhasználói szoftverek | | | | | | | | | | | | | | |
| | Hiba a szoftverekben | nem jogtiszta szoftver telepítése | 2 | 2 | 2 | 6 | 3 | 6 | Központi szabályozás, rendszeres ellenőrzés, szankcionálás | 1 | 2 | 1 | 4 | 1 | 2 |
| | | nem jól tesztelt (web) alkalmazások használata | 3 | 3 | 4 | 10 | 3 | 10 | Tesztelési, telepítési eljárások rendszerének kialakítása | 1 | 2 | 1 | 4 | 1 | 2 |
| | | program írás során keletkező, később felfedezett hibák | 3 | 3 | 3 | 9 | 3 | 9 | Központilag vezérelt szoftverfrissítés, javítások készítése saját szoftverhez, olyan szoftver vásárlása, melynek komoly felhasználó támogatása van | 1 | 1 | 2 | 4 | 1 | 2 |
| | Szoftver ellenőrizetlen bevitele | személyi felelősség hiánya | 1 | 1 | 2 | 4 | 3 | 4 | Szankcionálási rendszer kialakítása | 1 | 1 | 2 | 4 | 1 | 2 |
| | | ellenőrizetlen letöltések, telepítések | 3 | 3 | 4 | 10 | 3 | 10 | A hálózati forgalom szűrése, figyelése, a telepítési jogok korlátozása, szankcionálás rendszerének kialakítása | 1 | 1 | 2 | 4 | 1 | 2 |
| | Jogosulatlan bejutás az informatikai rendszerbe a kezelői helyről vagy hálózatról | betörésvédelmi eszközök hiánya | 3 | 3 | 3 | 9 | 4 | 10 | Központi és helyi tűzfalak, víruskeresők és irtók, IDS-ek, IPS-ek alkalmazása, forgalomszűrés, felhasználói jogok megfelelő beállítása, azonosítás és hitelesítés rendszerének kidolgozása | 1 | 1 | 2 | 4 | 1 | 2 |
| | | tűzfal hibája | 3 | 3 | 3 | 9 | 2 | 8 | A tűzfalak megfelelő konfigurációja, redundáns és többszintű tűzfalrendszer | 2 | 1 | 1 | 4 | 1 | 2 |
| | | jelszavak kezelési hibája | 1 | 2 | 3 | 6 | 3 | 6 | Jelszóalkotási és jelszó kezelési szabályok kidolgozása | 1 | 2 | 1 | 4 | 1 | 2 |
| | | azonosítási és hitelesítési rendszer hiánya | 2 | 3 | 4 | 9 | 2 | 8 | Központi felhasználó- és hozzáférés kezelés, azonosítás és hitelesítés rendszerének kidolgozása, a hálózati események és felhasználók mozgásának naplózása | 1 | 1 | 2 | 4 | 1 | 2 |
| | Rosszindulató szoftver | ismeretlen vagy nem megbízható eredetű programok használata | 3 | 3 | 4 | 10 | 3 | 10 | Telepítési jogok korlátozása, csak a munkavégzéshez lényeges szoftverek használatának engedélyezése | 1 | 2 | 1 | 4 | 1 | 2 |
| | | a vírusvédelmi adatbázis frissítése nem történik meg | 4 | 3 | 3 | 10 | 3 | 10 | Központilag vezérelt frissítési rendszer | 1 | 1 | 1 | 3 | 1 | 1 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Hardver | Hálózati aktív eszközök: | | | | | | | | | | | | | | |
| | Műszaki hibák, meghibásodás | nincs tartalékberendezés | 4 | 1 | 1 | 6 | 3 | 6 | Redundáns eszközelhelyezés, hálózat kialakítás | 1 | 1 | 1 | 3 | 2 | 2 |
| | | személyi felelősség hiánya | 2 | 1 | 1 | 4 | 3 | 4 | szankcionálás rendszere | 2 | 1 | 1 | 4 | 1 | 2 |
| | | karbantartás hiánya | 3 | 2 | 1 | 6 | 2 | 5 | Rendszeres időközönkénti felülvizsgálat, tesztelés és karbantartás, valamint ezek dokumentálása | 2 | 1 | 1 | 4 | 1 | 2 |
| | | karbantartási, üzemeltetési napló hiánya | 2 | 3 | 1 | 6 | 2 | 5 | Naplók meglétének ellenőrzése | 2 | 1 | 1 | 4 | 1 | 2 |
| | Személyekkel összefüggő fenyegetés, szakértelem hiánya | oktatás nem rendszeres | 3 | 3 | 3 | 9 | 2 | 8 | A munkahelyi követelményeknek megfelelő rendszeres oktatás | 2 | 2 | 2 | 6 | 1 | 4 |
| | | nem megfelelő dokumentáció | 3 | 2 | 1 | 6 | 3 | 6 | A dokumentációk meglétének és tartalmának rendszeres ellenőrzése | 2 | 1 | 1 | 4 | 1 | 2 |
| | | illetéktelen konfiguráció módosítás | 3 | 3 | 4 | 10 | 2 | 9 | Központi felhasználó- és jogosultság kezelés | 2 | 1 | 2 | 5 | 1 | 3 |
| | | hozzánemértésből fakadó hiba | 3 | 2 | 1 | 6 | 2 | 5 | Rendszeres oktatás | 1 | 1 | 1 | 3 | 1 | 1 |
| | | ki-, bekapcsolás | 3 | 1 | 3 | 7 | 1 | 5 | Szankcionálás rendszere | 2 | 1 | 2 | 5 | 1 | 3 |
| | | eltulajdonítás | 3 | 1 | 3 | 7 | 2 | 6 | Központi szabályozás, rendszeres ellenőrzés, szankcionálás | 2 | 1 | 1 | 4 | 1 | 2 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Humán erőforrás | Felhasználók, ügyintézők | | | | | | | | | | | | | | |
| | Időszakos kiesés (betegség, szabadság) | nincs kidolgozott helyettesítési rend | 1 | 1 | 1 | 3 | 0 | 0 | | 1 | 1 | 1 | 3 | 0 | 0 |
| | | más hozzáférési fiókjának használata | 2 | 2 | 4 | 8 | 2 | 7 | Központi szabályozás, rendszeres ellenőrzés, szankcionálás | 2 | 1 | 1 | 4 | 1 | 2 |
| | | dokumentálás hiánya | 2 | 1 | 1 | 4 | 1 | 2 | | 2 | 1 | 1 | 4 | 1 | 2 |
| | Információ véletlen kiszivárogtatása | konferenciákon részvétel | 1 | 1 | 2 | 4 | 1 | 2 | Biztonságtudatosság oktatása, az céges információk bizalmasság szerinti osztályozásának kidolgozása | 1 | 1 | 1 | 3 | 1 | 1 |
| | | rendszeres információbiztonsági képzés hiánya | 1 | 1 | 3 | 5 | 2 | 4 | Biztonságtudatosság és alapvető információ biztonsági ismeretek oktatása rendszeres szemináriumok szervezésével | 1 | 1 | 2 | 4 | 1 | 2 |
| | Információ kiszivárogtatása - szándékos, megvesztegetés | fegyelmi eljárás hiánya | 1 | 2 | 3 | 6 | 2 | 5 | Szankcionálás rendszerének kidolgozása | 1 | 1 | 2 | 4 | 1 | 2 |
| | | megbecsülés hiánya | 1 | 2 | 3 | 6 | 2 | 5 | Csapat építő tréningek, jutalmazás és megfelelő juttatás rendszerének kidolgozása | 1 | 1 | 2 | 4 | 1 | 2 |
| | | biztonsági átvilágítás hiánya | 1 | 2 | 3 | 6 | 2 | 5 | Cégen kívüli munkák, állások, kapcsolatok vizsgálata a belépéskor, összeférhetetlenség esetén jelölt módosítás | 1 | 1 | 2 | 4 | 1 | 2 |
| | Felügyeleti személyzet | | | | | | | | | | | | | | |
| | Időszakos kiesés (betegség, szabadság) | nincs kidolgozott helyettesítési rend | 4 | 1 | 3 | 8 | 2 | 7 | Létszám növelése, vagy külső cég megbízása meghibásodás időszakos javítására | 2 | 1 | 1 | 4 | 1 | 2 |
| | | más jogosultságainak használata | 3 | 1 | 3 | 7 | 2 | 6 | Létszám növelése, vagy külső cég megbízása meghibásodás időszakos javítására | 2 | 1 | 1 | 4 | 1 | 2 |
| | | dokumentálás hiánya | 3 | 2 | 2 | 7 | 2 | 6 | Kiesés esetén a felettesek felé kommunikálni kell a számonkérhetőség érdekében | 2 | 1 | 1 | 4 | 1 | 2 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Humán erőf. | Információ véletlen kiszivárogtatása | konferenciákon részvétel | 1 | 1 | 4 | 6 | 2 | 5 | Biztonságtudatosság oktatása, a céges információk bizalmasság szerinti osztályozásának kidolgozása | 1 | 1 | 3 | 5 | 1 | 3 |
| | | rendszeres információbiztonsági képzés hiánya | 1 | 1 | 4 | 6 | 2 | 5 | Biztonságtudatosság és alapvető információ biztonsági ismeretek oktatása rendszeres tréningek szervezésével | 1 | 1 | 2 | 4 | 1 | 2 |
| | | biztonságtudatosság hiánya | 1 | 1 | 4 | 6 | 2 | 5 | Biztonságtudatosság oktatása rendszeres tréningek szervezésével | 1 | 1 | 2 | 4 | 1 | 2 |
| | Információ szándékos kiszivárogtatása, megvesztegetés | fegyelmi eljárás hiánya | 1 | 1 | 5 | 7 | 2 | 6 | Szankcionálás rendszerének kidolgozása | 1 | 1 | 3 | 5 | 1 | 3 |
| | | megbecsülés hiánya | 3 | 3 | 5 | 11 | 3 | 11 | Csapat építő tréningek, jutalmazás és megfelelő juttatás rendszerének kidolgozása | 1 | 1 | 1 | 3 | 1 | 1 |
| | | nem figyelemmel kísért cégen kívüli munka, vagy nem ismert személyzet | 3 | 2 | 5 | 10 | 3 | 10 | Cégen kívüli munkák, állások, kapcsolatok rendszeres vizsgálata (legalább félévente), összeférhetetlenség esetén pozició, vagy munkavállaló megváltoztatása | 2 | 1 | 3 | 6 | 1 | 4 |
| | | biztonsági átvilágítás hiánya | 3 | 1 | 5 | 9 | 1 | 7 | Cégen kívüli munkák, állások, kapcsolatok vizsgálata a belépéskor, összeférhetetlenség esetén jelölt módosítás | 2 | 1 | 3 | 6 | 1 | 4 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Hálózat | Hálózati kapcsolatok | | | | | | | | | | | | | | |
| | Jogosulatlanok bejutása a hálózatba | jelszó nem megfelelő tárolása | 2 | 2 | 4 | 8 | 4 | 9 | Központi szabályozás, titkosítás, biztonság tudatosság | 2 | 1 | 2 | 5 | 1 | 3 |
| | | jelszó kompromittálódása | 1 | 3 | 5 | 9 | 3 | 9 | Megfelelő jelszóházirend kialakítása | 1 | 2 | 3 | 6 | 1 | 4 |
| | | nem megfelelő jelszó alkotási szabályok | 2 | 2 | 3 | 7 | 3 | 7 | Megfelelő jelszóházirend kialakítása | 2 | 2 | 1 | 5 | 1 | 3 |
| | | nem megfelelő határvédelem | 3 | 3 | 4 | 10 | 4 | 11 | Központi és helyi tűzfalak, IDS-ek alkalmazása, forgalomszűrés, felhasználói jogok megfelelő beállítása, azonosítás és bitelesítés rendszerének kidolgozása | 2 | 2 | 2 | 6 | 3 | 6 |
| | | azonosítási, hitelesítési rendszer hiánya | 3 | 3 | 5 | 11 | 3 | 11 | Hitelesítési rendszer kidolgozása | 2 | 2 | 3 | 7 | 1 | 5 |
| | | védtelen publikus hálózathoz csatlakozó pontok | 4 | 4 | 4 | 12 | 3 | 12 | Komoly biztonsági intézkedésekkel védett kijárat az internetre | 2 | 1 | 2 | 5 | 0 | 2 |
| | | nyomonkövetési, bizonyítási folyamatok hiánya | 1 | 1 | 4 | 6 | 3 | 6 | A felhasználók tevékenységének nyomon követése, naplózása és központi automatikus kiértékelése. Incidenskezelés | 1 | 1 | 2 | 4 | 2 | 3 |
| | | biztonsági felelősségi körök tisztázatlansága incidensek esetén | 4 | 2 | 3 | 9 | 2 | 8 | Szerepkörök pontos meghatározása, katasztrófaelhárítási terv készítése | 1 | 1 | 3 | 5 | 2 | 4 |

| | Fenyegető tényező leírása | Sebezhetőség | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke | Külön intézkedés | Okozott kár | | | Okozott kár ∑ (Bizalmasság + Sértetlenség + Rendelkezésre állás) | Bekövetkezés valószínűsége | Kockázat mértéke |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | | | Rendelkezésre állás | Sértetlenség | Bizalmasság | | | |
| Hálózat | Hálózati hardverek/szoftverek manipulálása | jogosultsági rendszer nem megfelelősége | 3 | 4 | 4 | 11 | 1 | 9 | A rendszer folyamatos felülvizsgálása, aktualizálása, naplózása, az incidenseknek megfelelő továbbfejlesztése | 2 | 2 | 1 | 5 | 1 | 3 |
| | | biztonsági rendszer elégtelensége | 2 | 3 | 4 | 9 | 1 | 7 | A szükséges biztonsági rendszer kialakítása | 2 | 1 | 2 | 5 | 1 | 3 |
| | Távoli munkavégzés | a távoli gép sérülékenységei bekerülnek a rendszerbe | 3 | 3 | 4 | 10 | 4 | 11 | Hálózati hozzáférés vezérlés bevezetése | 1 | 2 | 2 | 5 | 2 | |
| | Túlterhelés | célzott terhelési támadások | 4 | 1 | 1 | 6 | 4 | 7 | Tűzfal, redundáns külső csatlakozási pont kialakítása a nagyobb terhelhetőség érdekében | 2 | 1 | 1 | 4 | 3 | 4 |
| | | rosszul tervezett forgalmazási csúcsok | 4 | 1 | 1 | 6 | 2 | 5 | A forgalmazás folyamatos felülvizsgálása, mérése, indokolt esetben a hálózat módosítása, fejlesztése | 2 | 1 | 1 | 4 | 1 | 2 |
| | Üzenetek eltérítése, meghamisítása, | személyi felelősség hiánya, hozzánemértés | 3 | 1 | 4 | 8 | 2 | 7 | Rendszeres biztonsági oktatás | 3 | 1 | 2 | 6 | 1 | 4 |
| | Üzenetek helytelen sorrendje a fogadónál | a hálózati eszközök nem megfelelő beállítása | 3 | 1 | 2 | 6 | 2 | 5 | Rendszeres felülvizsgálat | 2 | 1 | 1 | 4 | 1 | 2 |
| | Kommunikációs kapcsolatok felderítése | biztonsági rendszer elégtelensége, jogosultsági rendszer nem megfelelősége | 1 | 1 | 4 | 6 | 2 | 5 | Központi és helyi tűzfalak, víruskeresők és irtók, IDS-ek, IPS-ek alkalmazása, forgalomszűrés, felhasználói jogok megfelelő beállítása, azonosítás és hitelesítés rendszerének kidolgozása, a jogosultsági rendszer rendszeres felülvizsgálata | 1 | 1 | 3 | 5 | 1 | 3 |

3. sz. melléklet

# RÖVIDÍTÉSEK JEGYZÉKE

| Rövidítés | Angol | Magyar/Jelentés |
|---|---|---|
| ACK | Acknowledgement | Nyugtázás. |
| ACL | Access Control List | Hozzáférés-vezérlési lista. |
| ARP | Address Resolution Protocol | Címfeloldási protokoll. |
| ASP | Active Server Pages | A Microsoft dinamikus weboldalak generálására alkalmas szerveroldali keretrendszere. |
| BM | | Belügyminisztérium. |
| CERT | Computer Emergency Response Team | Számítástechnikai Sürgősségi Reagáló Egység. |
| CSO | Chief Security Officer Magazine | Chief Security Officer Magazine. |
| DDoS | Distributed Denial of Service | Terjesztett szolgáltatásmegtagadás. |
| DMZ | Demilitarized Zone | Határhálózat. |
| DNS | Domain Name System | Tartománynév-szolgáltatás. |
| EKG | | Elektronikus Kormányzati Gerinchálózat. |
| EU | European Union | Európai Unió. |
| FIN | Final data from sender | Adatküldés vége. |
| FTP | File Transfer Protocol | Állományátvitelre szolgáló szabvány. |
| GNU | | Egy kizárólag szabad szoftverből álló Unix-szerű operációs rendszer „a GNU Nem Unix" rekurzív rövidítése. |
| HTML | HyperText Markup Language | Leíró nyelv, melyet weboldalak készítéséhez fejlesztettek ki. |
| HTTP | HyperText Transfer Protocol | Információátviteli protokoll. |
| HTTPS | Hypertext Transfer Protocol Secure | Egy URI séma, amely biztonságos http kapcsolatot jelöl. |
| IBIK | | Informatikai Biztonság Irányítási Követelmények. |
| IBIR | | Informatikai Biztonsági Irányítási Rendszer. |
| IBIV | | Informatikai Biztonsági Irányítás Vizsgálata. |
| IBIX | | Informatikai Biztonsági Iránymutató Kis Szervezetek Számára. |
| IBSZ | | Informatikai biztonsági szabályzat. |
| ICMP | Internet Control Message Protocol | Internet vezérlőüzenet protokoll. |
| IDM | Identity Management | Felhasználók kezelése. |
| IDS | Intrusion Detection System | Behatolás detektáló rendszer. |
| IEC | International Electrotechnical Commission | Nemzetközi Szabványügyi Szervezet. |

| Rövidítés | Angol | Magyar/Jelentés |
|---|---|---|
| IIS | Internet Information Services | Microsoft Windows-platformon futó internet-alapú szolgáltatásokat összefogó termék. |
| IP | Internet Protocol | Az internet alapvető szabványa. |
| IPS | Intrusion Prevention System | Behatolás megelőző rendszer. |
| IRC | Internet Relay Chat | Kliens-szerver alapú kommunikációt lehetővé tevő csevegő protokoll. |
| IS | Information system | Informatikai rendszer. |
| ISO | International Organization for Standardization | Nemzetközi Szabványügyi Szervezet. |
| ITB | | Informatikai Tárcaközi Bizottság. |
| KIB | | Közigazgatási Informatikai Bizottság. |
| LAMP | Linux, Apache, MySQL, PHP | |
| MAC | Media Access Control | A szabványügyi hivatal által a gyártónak kiadott, fizikailag a gyártó hálózati interfészeibe belesütött egyedi azonosító. |
| MeH EKK | | Miniszterelnöki Hivatal Elektronikus Kormányzat Központ. |
| MIBA | | Magyar Informatika Biztonsági Ajánlások. |
| MIBÉTS | | Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma. |
| MIBIK | | Magyar Informatikai Biztonsági Keretrendszer. |
| NATO | North Atlantic Treaty Organization | Észak-Atlanti Szövetség. |
| ORFK | | Országos Rendőrfőkapitányság. |
| OWASP | Open Web Application Security Project | Több gyártót összefoglaló, nyitott fejlesztési rendszer. |
| POP3 | Post Office Protocol version 3 | Egy alkalmazás szintű protokoll az elektronikus levelek lekéréséhez. |
| SMTP | Simple Mail Transfer Protocol | Kommunikációs protokoll az elektronikus levelek interneten történő továbbítására. |
| SQL | Structured Query Language | Strukturált lekérdező nyelv. |
| SSL | Secure Socket Layer | A Netscape által kifejlesztett nyílt ajánlás (szabvány) biztonságos kommunikációs csatorna létrehozására. |
| TCP | Transmission Control Protocol | Átvitel-vezérlési Protokoll |
| TESTA | Trans European Services for Telematics between Administrations | Zárt, internettől független gerinchálózat, amely az Európai Unió adminisztrációja és a tagországok kormányzatai közötti információcserét teszi lehetővé. |
| TLS | Transport Layer Security | Az SSL továbbfejlesztése |

| Rövidítés | Angol | Magyar/Jelentés |
|---|---|---|
| UDP | User Datagram Protocol | Az internet egyik alapprotokollja, datagram alapú szolgáltatás biztosítása, azaz rövid, gyors üzenetek küldése esetén használatos. |
| UID | User identifier | Felhasználói azonosító. |
| VLAN | Virtual Local Area Network | Virtuális (logikai) felosztása a hálózatnak. |
| VPN | Virtual Private Network | Virtuális magánhálózat. |
| WASC | Web Application Security Consortium | |
| XML | Extensible Markup Language | Kiterjeszthető jelölő nyelv a W3C által ajánlott általános célú leíró nyelv, speciális célú leíró nyelvek létrehozására. |
| XSS | Cross Site Scripting | Oldalközi szkriptelés. |

4. sz. melléklet

# TÁBLÁZATOK JEGYZÉKE



# ÁBRÁK JEGYZÉKE



Budapest, 2011. június 21. .....

Póserné Oláh Valéria