10.17625/NKE.2012.013

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
HADTUDOMÁNYI KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

KRASZNAY CSABA

A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSI ALKALMAZÁSOK INFORMÁCIÓBIZTONSÁGI MEGOLDÁSAI

Doktori (PhD) értekezés

Témavezető: Prof. Dr. Kovács László mk. alezredes

2011. Budapest

TARTALOMJEGYZÉK

BEVEZETÉS

A modern hadviselés egyik legfontosabb színtere a kibertér[1]. [1] Ezek támadása, informatikai vagy más módon, fontossá tette azt, hogy az informatikai rendszerek a lehető leginkább biztonságos módon kerüljenek kifejlesztésre. Az elektronikus közigazgatási rendszerek kiemelt szerepet töltenek be, hiszen ezek nélkül a közigazgatás része vagy egésze működésképtelenné, de legalábbis jelentősen akadályozottá válik. Emiatt válik szükségessé az e-közigazgatási rendszerek biztonságos alkalmazásfejlesztésének tanulmányozása és tudományos eredményekkel – közvetve – a nemzet biztonságának fokozása.

A tudományos probléma megfogalmazása

A Magyar Köztársaság közigazgatásának működésében egyre hangsúlyosabb szerep jut az elektronikus szolgáltatásoknak, melyek a közigazgatáson belüli (G2G – Government-to-Government), a közigazgatás és a vállalkozások közötti (G2B – Government-to-Business) és a közigazgatás-állampolgár relációban (G2C – Government-to-Citizen) is kikerülhetetlen megoldások. Mind a központi intézményeknek, mind az önkormányzatoknak kötelessége az elektronizált működés további terjesztése az Európai Unió elveivel összhangban. Ezen szolgáltatások biztonságos működése **nemzetbiztonsági szempontból kritikus kérdés**, hiszen ezek nélkül az ország gazdasági és társadalmi működése jelentős akadályokba ütközne. A szolgáltatások biztonságát a jogalkotók jogszabályokkal próbálják garantálni, azonban bizonyos területeken **jelenleg nincsenek olyan egységes műszaki ajánlások**, melyek a szolgáltatások bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit meghatároznák.

A nemzetközi trendek és a hazai tapasztalatok is azt mutatják, hogy az elektronikus közigazgatási szolgáltatások állandó célpontjai a szervezett bűnözésnek, a hackereknek és más államok hivatalos szerveinek. Tökéletes védelmet nyújtani aránytalanul magas költséget jelentene, azonban az elvárható gondosság elve alapján szükséges a nyilvánosan elérhető szolgáltatásokat biztonságosan kifejleszteni. Ez azt jelenti, hogy a biztonsági gondolkodásnak már az új alkalmazások tervezésénél meg kell jelennie. Az elektronikus közigazgatási szolgáltatásokba biztonsági megoldásokat fejleszteni több szinten lehet. Adminisztratív

[1] Kibertér fogalma az idézett forrás szerint: „egy olyan tartomány, ahol hálózatos rendszerekben működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására, kiterjesztve azon hálózatokra is, melyek elemei nem rádiócsatornán, hanem vezetéken (rézvezeték, optikai kábel stb.) vannak egymáshoz kapcsolva” A cybertéri védelem (továbbiakban kibervédelem) „arra irányul, hogy fenntartsa a saját hálózatos információs rendszereinkben a hozzáférhetőséget az információkhoz, információalapú folyamatokhoz, és biztosítsa ezen rendszerek hatékony használatát békeidőben, válság vagy konfliktus idején egyaránt.”

módon, szabályokat hozva, biztonságos fizikai környezet kialakításával, megfelelő logikai intézkedések meghozatalával, pl. tűzfalak telepítésével. Emellett azonban nagyon fontos az alkalmazás teljes életciklusa során a **biztonsági követelmények megállapítása** is. A szoftverfejlesztési életciklusban a megfelelő védelmi intézkedések meghozatala azonban a gyakorlatban gyakran elmarad, mert sem a megrendelők, sem a fejlesztők számára nem ismertek a kritériumok. Emiatt az alkalmazások olyan **biztonsági hibákkal üzemelnek**, mely végső soron a szolgáltatások, így a teljes elektronikus közigazgatás működésére is hatással lehetnek.

Kutatási célkitűzések

Kutatásom célja, hogy az elektronikus közigazgatás területére olyan **alkalmazásfejlesztési keretet és követelményrendszert alkossak**, melynek felhasználásával az ilyen szolgáltatások biztonsági szintje jelentősen növelhető. Mindezek alapján a felmerült **nemzetbiztonsági kockázatok nagymértékben csökkenthetők**. A terület tudományos jelentősége, hogy az alkalmazásfejlesztés biztonsági aspektusának számos területe kevéssé kidolgozott, sem a megrendelők, sem a fejlesztők számára nem áll rendelkezésre olyan, a gyakorlatban is hasznosítható eljárásrend, melynek felhasználásával mérhető módon is javítható az alkalmazások biztonsága. Célomat az iparági szabványok és jógyakorlatok (best practice, azaz széles körű tapasztalaton alapuló, több szervezetnél is sikeresen bevált gyakorlat) felhasználásával és továbbfejlesztésével, valamint az elektronikus közigazgatás védelmi igényeihez történő hozzáigazításával kívánom elérni. Az elektronikus közigazgatási szolgáltatások biztonsági szintje számos módon növelhető, értekezésemben azonban **egyetlen specifikus területre koncentrálok**, ez pedig **a szolgáltatások mögött álló alkalmazások biztonsági kérdése**. **A kutatási területek kiválasztásánál azokra a részfeladatokra koncentrálok, melyek világszerte kidolgozatlan és megoldatlan problémaként jelentkeznek a közigazgatási szektorban.**

Az alábbi részcélokat határoztam meg:

1. Védelmi Profil eszköztár meghatározása az elektronikus közigazgatási alkalmazásokhoz

Célom a Common Criteria (illetve ennek feldolgozásai, mint az ISO/IEC 15408 és a Magyar Informatikai Értékelési és Tanúsítási Séma[2]) ajánlás alapján olyan **Védelmi Profil eszköztár kidolgozása**, mely a Magyar Köztársaság elektronikus közigazgatási szolgáltatásaiban

[2] Az ISO/IEC 15408 szabvány jelenleg szövegszerűen megegyezik a Common Criteria ajánlással, a MIBÉTS pedig a CC egy korábbi változatának magyar feldolgozása és értelmezése a hazai viszonyokra. Az értekezésben a CC legfrissebb változatát használom.

használt alkalmazások minimálisan elvárt funkcionális és garanciális követelményeit határozza meg, az elvárt működési környezet leírásával. A Common Criteria választását az indokolja, hogy a magyar műszaki ajánlások is erre építenek, több magyar e-közigazgatási rendszer fejlesztésénél is követelmény volt ennek használata, valamint véleményem szerint ez a szabvány adja a legteljesebb keretet a biztonságos alkalmazásfejlesztéshez. A dokumentum tartalmazza azokat a fenyegetéseket, feltételezéseket és szabályokat is, melyek az ilyen alkalmazásokra vonatkoznak. Jelenleg nyilvánosan nem érhető el olyan Common Criteria szerinti Védelmi Profil, ami erre a felhasználási területre vonatkozna. Az e-közigazgatási rendszerek közötti jelentős különbségek miatt egy Védelmi Profil nem is lenne elégséges, de a dolgozatomban levezetett biztonsági funkciók minimális elvárásként kell, hogy megjelenjenek az érintett Védelmi Profilokban és Biztonsági Előirányzatokban.

2. Common Criteria által megkövetelt, fejlesztői környezetre vonatkozó garanciális követelmények rendszerének kidolgozása a magyar szabályozási környezetben

Az alkalmazásfejlesztés során a gyakorlatban a legnagyobb gondot a biztonsági garanciális követelmények kielégítése okozza. Ebbe a körbe tartozik a megfelelő funkcionális specifikáció megalkotásától kezdve, a fejlesztői környezet biztonságán át, a helyes biztonsági tesztelésig több terület is. Ezek közül a fejlesztői környezet biztonsági kérdései a leginkább kidolgozatlanok. A kutatási **cél** olyan, **gyakorlatban is használható követelményrendszer meghatározása**, mely az elektronikus közigazgatásban dolgozó fejlesztők számára egyértelművé teszi a tőlük elvárt, biztonsággal kapcsolatos tevékenységeket, és segítséget nyújt ezek elkészítésében, mindezt a magyar jogi és műszaki szabályozási környezetben. A feladat tudományos értékét az adja, hogy a szabvány csak magas szinten határozza meg a követelményeket, ennek értelmezése és gyakorlati használata kevéssé körüljárt terület.

3. Sérülékenységi tesztelési eljárások kidolgozása az elektronikus közigazgatási alkalmazások területére

A Common Criteria szabvány egyik sarkalatos pontja a biztonsági értékelést végző által készített sérülékenység-elemzés. Ezért **célom** olyan **sérülékenység-tesztelési eljárás kidolgozása**, mely speciálisan az elektronikus közigazgatási alkalmazásokra használható. A sérülékenység-elemzés átfogó képet nyújt a fejlesztő által felhasznált biztonsági kontrollok hatékonyságáról. Az elektronikus közigazgatás területén végzett sérülékenység-elemzésekre jelenleg nem létezik módszertan, így a több más terület tapasztalatát felhasználó eljárások kidolgozása hiánypótló munka lehet. A kutatási cél megalapozása érdekében bemutatok egy lehetséges kibertámadási forgatókönyvet, mely rámutat a sebezhetőség-vizsgálat fontosságára,

valamint meghatározok néhány olyan követelményt, mely hazánk kibervédelmének kidolgozásához szükséges. Bemutatom továbbá azt a felmérést, mely a hackerközösség tagjainak kibervédelemhez való viszonyát taglalja.

Kutatási hipotézisek

Kutatómunkám megkezdésekor abból indultam ki, hogy az általam választott területeken nem, vagy csak egyes részterületein folyt olyan kutatás Magyarországon, melyre támaszkodhattam volna. Feltételeztem, hogy a magas szintű ajánlásokon túl semmilyen konkrét követelményt nem határoztak meg a magyar szabályozási környezetben. Az 1. célkitűzéshez kapcsolódóan feltételeztem, hogy nem létezik olyan Védelmi Profil, mely a Common Criteria elvei alapján meghatározná a magyar közigazgatási rendszerek biztonsági funkcióit. Feltételeztem továbbá, hogy az egyes rendszerek ajánlásokban leírt biztonsági besorolási rendszere továbbgondolásra szorul. Hipotézisem szerint kidolgozható olyan Védelmi Profil eszköztár és besorolási rendszer, mely érdemben használható a magyar közigazgatási rendszerek fejlesztésénél.

A második célkitűzésemhez kapcsolódóan a feltételezésem az volt, hogy a magyar közigazgatási környezetben dolgozó alkalmazásfejlesztők munkáját semmilyen biztonsági előírás nem szorítja keretek közé. Feltételeztem továbbá, hogy az összes megkötés jellemzően a fizikai biztonságra korlátozódik, így szükségessé válik egy teljes szabályzati keretrendszer kialakítása. Hipotézisem szerint létre lehet hozni olyan biztonsági keretrendszert, mely a meglévő ajánlások bázisán érdemben szabályozza a fejlesztőkkel kapcsolatos biztonsági kérdéseket.

A harmadik célkitűzésem abból az előfeltételezésből eredt, hogy nincsen semmilyen konkrét eljárásrend az alkalmazások biztonsági tesztelésére, annak ellenére, hogy ilyen vizsgálatot a Nemzeti Hálózatbiztonsági Központ és a Nemzeti Biztonsági Felügyelet is jogosult végezni. Az egységes eljárásrend pedig mind a fejlesztőnek, mind a megrendelőnek fontos útmutató, egyben segíti az elektronikus közigazgatás területén az egyenszilárdságú biztonság elérését. A hipotézisem az, hogy meg lehet határozni azokat a szabályokat, melyek mentén az alkalmazások biztonsági vizsgálata elvégezhető.

Kutatási módszerek

Munkám során széleskörű nemzetközi és hazai irodalomkutatásra, valamint a gyakorlati tapasztalatra támaszkodtam. Tapasztalataimat tájékoztatási céllal írtam le, tudományos következtetések meghozatalára azokat nem használtam. Feltérképeztem azokat a

szakkönyveket, szabványokat és ajánlásokat, melyek valamilyen módon segítik a munkámat. Alaposan áttekintettem a hazai jogszabályi és műszaki szabályozási hátteret. Ezek egy részén a dolgozatban részletezett módon másodelemzést végeztem, illetve a kritikai adaptáció módszerével próbáltam meggyőződni több forrás megfelelőségéről. Emellett részt vettem több e-közigazgatási rendszer fejlesztésében, ahol az általam felállított hipotézisekről próbáltam meggyőződni, illetve tudományos munkám eredményeit igyekeztem beilleszteni.

A kutatás során az indukció és a dedukció módszerével egyaránt éltem. A gyakorlati tapasztalatomat, mely csak egyes rendszerekre terjed ki, induktív módon általánosítottam, és győződtem meg arról, hogy saját tapasztalatom helytálló-e. Mindeközben az információbiztonság általános érvényű elveit deduktív módon alkalmaztam ezekre az egyedi esetekre, azaz a gyakorlatban használhatók-e az általánosan elfogadott elvek.

Részt vettem továbbá a témával foglalkozó hazai és nemzetközi konferenciákon, gyakran előadóként is, valamint ezeken a rendezvényeken lehetőség szerint próbáltam információt gyűjteni a terület kormányzati és szállító oldali szakembereitől. Kidolgoztam továbbá egy olyan kérdőívet, mely reprezentatívnak tekinthető módon ad képet a hackerközösség kibervédelemről alkotott véleményéről.

1. FEJEZET

A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁS ALKALMAZÁSRÉTEGÉNEK BIZTONSÁGI ELEMZÉSE ÉS JAVASOLT VÉDELMI PROFIL ESZKÖZTÁRA

Napjaink trendje szerint, mely a jelentősebb információbiztonsági cégek negyedéves jelentéseiből is kiderül, egy informatikai rendszerbe bejutni két úton a legegyszerűbb: emberi hibát kihasználva, illetve valamilyen alkalmazás nem megfelelő programozására építve. [2] Az emberi hiszékenység vagy rosszakarat ellen nehéz közvetlenül védekezni, de megfelelő műszaki környezettel csökkenthetők a hatásai. A nem biztonságos programok jelentette fenyegetés viszont egyértelműen töredékére eshet, ha megfelelő tervezést, kivitelezést és tesztelést alkalmaz a fejlesztő.

A tervezés első lépése az, hogy tisztában kell lenni azzal, mit is csinál valójában az alkalmazás, és mindezt milyen biztonsági környezetben teszi. Az elektronikus közigazgatási rendszereket szignifikánsan egymáshoz hasonló fenyegetések érik, így felvázolható egy (vagy több) „tipikus” e-közigazgatási alkalmazás profilja. Ezekben hasonló biztonsági funkciókat kell megvalósítani, így biztosítható a teljes kormányzati informatikai tér egyenszilárdságú védelme. Természetesen a részletek ismeretében a funkcionális követelmények bővülhetnek, de a biztos és egységes alapok rendkívül fontosak, hiszen az egyik legfontosabb információbiztonsági alapelv az egyenszilárdságú védelem elve, azaz egy informatikai rendszer minden elemének azonos biztonsági fokot kell elérnie. A magyar közigazgatási rendszereket pedig azok összetettsége és egymástól való függése miatt mindenképpen egységes rendszernek kell tekinteni. Itt kell megjegyezni, hogy az értekezésben az információbiztonság szó az információ bármilyen adathordozójának (pl. papír, gondolat) védelmét jelenti, az informatikai biztonság kizárólag az informatikai rendszerekben megjelenő adat védelmére vonatkozik. Az 1. fejezetben tipikusan informatikai biztonságról, a másodikban pedig információbiztonságról esik szó.

Jelen fejezetben áttekintem a magyar e-kormányzati teret, megjelölve ezen belül a legfontosabb védendő rendszereket. Megvizsgálom azokat a jogszabályokat, melyek hatással lehetnek ezekre a rendszerekre. Kitérek a valós e-közigazgatási fenyegetések felsorolására, melyek ugyan folyamatosan változhatnak, de az értekezés írásának időpontjában a fő trendeket jelölik. Bemutatom az e-közigazgatás típusalkalmazásait, melyekre a biztonsági követelmények megfogalmazhatók. Nem foglalkozom azonban az informatikai környezet más

elemeivel, kizárólag az egyedi fejlesztésű alkalmazásokra terjed ki dolgozatom. Végül előterjesztek egy olyan Common Criteria szerinti Védelmi Profil eszköztárat, melynek segítségével az egyenszilárdságú védelem elérhető.

1.1 A magyar közigazgatás informatikai rendszereinek logikai architektúrája

Egy ország társadalmi és gazdasági működésének szempontjából meghatározó fontosságúak bizonyos területek, iparágak informatikai rendszerei. Ezeken belül kiemelkedő fontosságúak a közigazgatás működését támogató, annak működését segítő rendszerek. Ezek biztonságos működése nélkül nem képzelhető el egy modern ország, függetlenül attól, hogy a fejlett vagy a fejlődő államokról beszélünk. Kevés kivételtől eltekintve minden ország közigazgatása valamilyen mértékben függ az informatikától.

Torma András meghatározása szerint „… a közigazgatási informatika a jogi informatikának, mint szakinformatikának az az ága, amely a közigazgatási szervnek a különböző eszközökkel és módszerekkel, de különösen a számítógéppel megvalósított információkezelésével foglalkozik.” [3] A magyar és általában a nemzetközi jogrend a közigazgatást központi és helyi szintekre bontja, így a közigazgatási informatikát is ezen a két szinten kell vizsgálni. Jelen értekezésben a közigazgatási és e-közigazgatási alkalmazások szinonimaként szerepelnek, hiszen az újonnan fejlesztett közigazgatási rendszerek közvetve vagy közvetlenül az elektronikus közigazgatást erősítik. Az értekezésben a központi közigazgatás informatikai rendszerei kerülnek elemzésre, mivel a tapasztalatom szerint helyi szinten nem reális a követelmények elvárása, ezeket a központi rendszerek szempontjából olyan megbízhatatlannak kell kezelni, mint bármelyik másik külső felhasználó számítógépét. Ettől függetlenül törekedni kell a szabályok átvételére ezen a szinten is.

Magyarországon évtizedekre visszamenőleg van hagyománya a számítógépes rendszerek használatának ezeken a területeken. A Központi Statisztikai Hivatal vagy a Pénzügyminisztérium számítógépközpontja már az informatikai hőskorában is kiszolgálta a közigazgatás igényeit. [4]

A mai magyar központi közigazgatási rendszer alapjai már a ’70-es években léteztek, amikor az Államigazgatási Számítógépes Szolgálat (ÁSzSz) keretein belül elérhető volt az Állami Népesség-nyilvántartás Rendszere, egyes egészségügyi rendszerek, a szociálpolitika rendszerei, a természeti környezet rendszerei és különféle anyagi és szellemi javak nyilvántartó rendszerei. [5] Ezek ma is meghatározó fontosságúak, továbbélnek a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEKKH), a Magyar

Államkincstár (MÁK), az Országos Egészségpénztár (OEP) és a Földmérési és Távérzékelési Intézet (FÖMI) keretein belül, egyben a közigazgatási informatika gerincét adják, kiegészítve a már említett KSH és az Adóhivatalban és a MÁK-ban továbbélő PM rendszerekkel.

A helyi közigazgatás informatikai infrastruktúrája a rendszerváltás előtt elsősorban a központi közigazgatás helyi szintre helyezett rendszereit jelentette. A legfontosabb szereplő a KSH cége, a Számítástechnikai és Ügyvitel-szervezési Vállalat (SZÜV) volt, mely a helyi igazgatástól származó statisztikai adatokat szolgáltatta a központi rendszerekbe. A SZÜV komoly hálózattal rendelkezett az országban, megkerülhetetlen tényezője volt a helyi igazgatási informatikának. Kiemelt szerepet kaptak még a megyei tanácsok és a Tanácsi Költségvetési Elszámoló Hivatalok. A rendszerváltás után a helyi közigazgatási informatika hirtelen légüres térbe került, újonnan kialakuló feladataihoz lassan kapcsolódtak a számítógépes rendszerek. Informatikai tevékenységük saját hatáskörben jelenleg is elsősorban a helyi adók, a vagyonkataszter, a gyámügy és a szociális igazgatás területeire terjed ki, IT rendszereket elsősorban a központi közigazgatás igényeinek kiszolgálására használnak. [6]

A központi közigazgatásban egyetlen komoly új bázis jelent meg a rendszerváltás óta, ez pedig a Központi Rendszer (KR). Ez azonban egyrészt nem is új, hiszen a Nemzeti Infokommunikációs Szolgáltató Zrt., korábban Kopint-Datorg keretein belül működik, mely cég szintén fajsúlyos szereplő volt a rendszerváltás előtt, másrészt a filozófia sem új, hiszen az ÁSzSz által korábban már megvalósított erős centralizációt volt hivatott visszaállítani. A KR-en belül az Elektronikus Kormányzati Gerinchálózat (EKG) és a magyarorszag.hu portál, azon belül is az Ügyfélkapu megkerülhetetlenné vált. A helyi közigazgatásban a KEKKH alá tartozó Okmányirodák és a 2011-ben felállt kormányhivatalok ún. kormányablakai jelentik a modern informatikát, ám ezek is központi szervekhez kapcsolódnak.

A közigazgatási informatika Magyarországon erősen centralizált, helyi szinten nincsen jelentős informatikai rendszer. Az igazgatási informatika struktúrája évtizedek óta szinte változatlan, ami annak köszönhető, hogy az állam nagy számítási és tárolási igényű feladatai is változatlanok. A megoldandó célok tehát adottak, de a megvalósító technikák jelentősen változnak, ahogy az informatikai fenyegetések természete is. Ezért a közigazgatási rendszerek fejlesztésének és üzemeltetésének **biztonsági filozófiája** és ebből következő szabályozása **véleményem szerint jelentős újragondolásra szorul**.

A centralizáltságot, illetve a kiemelt fontosságú közigazgatási rendszerek körét két adathalmaz támasztja alá. Egyrészt érdemes megvizsgálni, hogy a Magyar Köztársaság kormánya mely szervezetek rendszereit tartotta érdemesnek Európai Uniós forrásból

fejleszteni az Új Magyarország Fejlesztési Terv Elektronikus Kormányzat Operatív Programján (EKOP) belül, másrészt érdekes, hogy a kormány mit tekint a nemzeti adatvagyon körébe tartozó adatbázisnak, rendszernek. Az EKOP források elosztása az alábbiak szerint alakul: [7]

Szervezet megnevezése	Elnyert pályázatok száma
Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala	10
Pénzügyminisztérium Informatikai Szolgáltató Központ	6 (ide tartozik a MÁK és az Adóhivatal)
Nemzeti Fejlesztési Ügynökség	6 (elsősorban az EU-s források elosztását lehetővé tevő fejlesztések, valós szerepe nincs a központi közigazgatási informatikában)
Közigazgatási és Igazságügyi Minisztérium	3
Belügyminisztérium	2
Nemzeti Infokommunikációs Szolgáltató Zrt.	2
Miniszterelnöki Hivatal	2
Külügyminisztérium	1
Földmérési és Távérzékelési Intézet	1
Központi Statisztikai Hivatal	1 (érdekes, hogy a rendszerváltás előtt egyértelműen vezető szerepet játszott a közigazgatási informatikában, jelentősége azóta csökkent)
Kulturális Örökségvédelmi Hivatal	1
Legfőbb Ügyészség	1
Magyar Szabadalmi Hivatal	1
Mezőgazdasági és Vidékfejlesztési Hivatal	1
Nemzetbiztonsági Szakszolgálat	1
Oktatási Hivatal	1
Országgyűlés Hivatala	1

Országgyűlési Biztos Hivatala	1
Országos Egészségbiztosítási Pénztár	1
Országos Igazságszolgáltatási Tanács Hivatala	1
Országos Katasztrófavédelmi Főigazgatóság	1
Országos Nyugdíjbiztosítási Főigazgatóság	1
Országos Tisztifőorvosi Hivatal	1

1. táblázat: Államigazgatási szervez által elnyert EKOP pályázatok száma

A 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról melléklete sorolja fel tételesen azokat az adatbázisokat, melyek kiemelt fontosságúak: [8]

- Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala: A polgárok személyi adatainak és lakcímének nyilvántartása, Központi útiokmány-nyilvántartás, Központi szabálysértési nyilvántartás, Közúti közlekedési nyilvántartás, A Magyar igazolvány és a Magyar hozzátartozói igazolvány tulajdonosainak nyilvántartása, Kötvénynyilvántartás, Az egyéni vállalkozók nyilvántartása, Bűnügyi nyilvántartási rendszer, N.SIS;
- Nemzeti Foglalkoztatási Hivatal: Foglalkoztatási és Szociális Adatbázis;
- Magyar Államkincstár: Egységes szociális nyilvántartás;
- Nemzeti Fejlesztési Ügynökség: Az Áht. 124. § (2) bekezdés l) pontjában foglalt felhatalmazás alapján kiadott kormányrendeletben meghatározott nyilvántartások, ide nem értve a Magyar Államkincstár által működtetett kincstári monitoring rendszert;
- Földmérési és Távérzékelési Intézet: Földhasználati nyilvántartás, Az állami földmérési alaptérképek, nagyméretarányú állami topográfiai térképek, alapponthálózatok, az államhatár földmérési munkarészei, valamint a magyarországi hivatalos földrajzi nevek nyilvántartása;
- HM Geoinformációs Szolgálat: Közepes és kisméretarányú állami topográfiai térképek;
- Országos Nyugdíjbiztosítási Főigazgatóság: Nyugdíj-biztosítási nyilvántartás;
- Országos Egészségbiztosítási Pénztár: Egészségbiztosítási nyilvántartás;

- Kulturális Örökségvédelmi Hivatal: Kulturális örökségvédelmi nyilvántartás;
- Nemzeti Adó és Vámhivatal: A Nemzeti Adó- és Vámhivatal által kezelt adóhatósági és vámhatósági adatok nyilvántartása, A Nemzeti Adó- és Vámhivatal által kezelt, a 15. pont alá nem tartozó adatok nyilvántartása;
- Közigazgatási és Igazságügyi Minisztérium: Cégnyilvántartás;
- Mezőgazdasági és Vidékfejlesztési Hivatal: A mezőgazdasági és vidékfejlesztési támogatási szerv által kezelt nyilvántartási rendszerek;
- Bevándorlási és Állampolgársági Hivatal: Központi idegenrendészeti nyilvántartás.

A két felsorolás meghatározza azokat az intézményeket, melyek az elektronikus közigazgatás szempontjából kiemelt jelentőségűek. Ezen intézmények esetén, valamint az ezekkel informatikai kapcsolatban álló minden egyéb központi közigazgatási rendszerre olyan biztonsági követelményeket kell meghatározni, melyek garantálják a központi rendszerek ellenálló képességét az informatikai támadásokkal szemben. **Álláspontom szerint a védendő intézmények köre** tehát a következő, szigorúan az e-közigazgatásra koncentrálva:

- Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala;
- Nemzeti Foglalkoztatási Hivatal;
- Magyar Államkincstár;
- Nemzeti Fejlesztési Ügynökség;
- Földmérési és Távérzékelési Intézet;
- Országos Nyugdíjbiztosítási Főigazgatóság;
- Országos Egészségbiztosítási Pénztár;
- Kulturális Örökségvédelmi Hivatal;
- Nemzeti Adó és Vámhivatal;
- Közigazgatási és Igazságügyi Minisztérium;
- Mezőgazdasági és Vidékfejlesztési Hivatal;
- Bevándorlási és Állampolgársági Hivatal;
- Belügyminisztérium;

- Nemzeti Infokommunikációs Szolgáltató Zrt.;
- Központi Statisztikai Hivatal;
- Oktatási Hivatal;
- Országos Tisztifőorvosi Hivatal.

A Magyar Köztársaság kormánya, alkalmazkodva az ipari trendekhez és az EU e-közigazgatási ajánlásaihoz, a szolgáltatásorientált architektúrát (SOA – Service Oriented Architecture) választotta fejlesztési iránynak. Ez a törekvés mind az írott stratégiákban, mind az eddigi központi fejlesztéseknél tetten érhető. A Közigazgatási Informatikai Bizottság 28. számú ajánlásából (továbbiakban KIB 28. ajánlás vagy követelménytár) azonban részletesen megismerhetjük azt a fejlesztési elképzelést, melyet a következő évek kiemelt közigazgatási informatikai rendszereinél meg kell valósítani, egyben láthatóvá válik az az irány, ahol a felsorolt szervek informatikai kapcsolatait elsősorban védeni kell. [9]

A SOA megoldást kínálhat a közigazgatási informatika alapvető problémáira. Segítségével szabványos módon kapcsolhatók össze a döntően szigetszerűen működő rendszerek, kvázi online kapcsolatok építhetők ki az eddig sok helyen használt offline adatátvitel helyett, összehangolhatóvá válnak a közigazgatási szervezetek folyamatai, valamint olyan preventív, detektív és korrektív védelmi intézkedések határozhatók meg, melyek ezeket a komplex, több szervezetet is érintő folyamatokat biztonságossá tehetik. Megjegyzendő, hogy a felsorolt szervek közötti adatkapcsolatok teljes köre jelenleg feltáratlan, ezért indokolt lenne egy teljeskörű felmérést elvégezni a közigazgatáson belül.

A követelménytár e-közigazgatási architektúráról szóló részében leírt modell szerint a magyar e-közigazgatás központi eleme az ún. e-közigazgatási sín lesz, mely szolgáltatási szinten köti össze a különböző szakrendszereket. [10] Ennek előfeltétele az, hogy a szakrendszerek képesek legyenek csatlakozni ehhez a sínhez, azaz olyan szolgáltatásokat, szakszóval web service-eket tudjanak kiajánlani, melyet más szakrendszerek a megfelelő jogosultság után el tudnak érni. Természetesen a szolgáltatást nyújtó és szolgáltatást igénybe vevő szakrendszereknek a sínen keresztül valamilyen szabványos nyelven kell kommunikálniuk annak érdekében, hogy a kért szolgáltatás végrehajtódjon.

A sín a szakrendszer-specifikus szolgáltatások mellett alapszolgáltatásokat is nyújt. Az eredeti tervek szerint hat olyan alapszolgáltatás valósul meg, mely a központi rendszer része. Ezek a következők:

- szolgáltatáskatalógus, mely az összes elérhető szolgáltatás adatait tartalmazza;
- tokenszolgáltató, mely az adatvédelmi szabályok szerint, a célhoz kötöttség elvét nem sértő módon segít megteremteni a kapcsolatot két elszigetelt adatbázis között;
- hitelesítés-szolgáltató, mely nem részletezett módon OCSP (Online Certificate Status Protocol) szolgáltatást nyújt a nem részletezett tanúsítványok állapotának ellenőrzésére;
- e-tár, mely adott ideig tárol központilag egy beadott dokumentumot, amihez hozzáférési jogosultságot lehet meghatározni, feltehetően a már működő Hivatali Kapu alapjait felhasználva;
- ügyfélkapu, mely számos elektronikus szolgáltatást nyújt az állampolgár és a közigazgatás között, többek között az adóbevallás, valamint a szociális és egészségügyi ügyintézés területén (C2G és G2C irányban);
- naplózási szolgáltatás, mely a szolgáltatók működéssel kapcsolatos információit hivatott nyilvánosan elérhető formában tárolni.

Az e-közigazgatási sín koncepció legnagyobb előnye az, hogy a szolgáltatáskatalógus központi vezetésével megkönnyíti a várhatóan továbbra is szigetszerűen kifejlesztésre kerülő rendszerek közötti interoperabilitást. Komoly kockázat van viszont abban, hogy a szolgáltatások interfészének meghatározását a dokumentum szerint teljes mértékben a szolgáltatás fejlesztőjére bízzák. Bár a borítékok formátuma kötött, a szolgáltatáshoz kapcsolódó adatok köre és formátuma nem. A koncepció szerint bár egy e-közigazgatást ellenőrző felügyelet engedélye kell a sínhez való csatlakozáshoz, nem lehet tudni, milyen egyeztetési folyamat során fog valóban minőségi, biztonsági és együttműködési szempontokat is figyelembe vevő szolgáltatásdefiníció keletkezni. Ezek a kérdések, kételyek az ajánlások 2008-2009-es megjelenése óta nem kerültek megválaszolásra, és várhatóan 2011-ben sem fognak. Magát az e-közigazgatási sín koncepciót azonban eddig nyilvánosan nem kérdőjelezték meg.

A biztonsági kérdéseket az ajánlás három részbe sorolja.

- foglalkozni kell az állampolgárok személyiségi és adatvédelmi jogaival, melyek garantálására a dokumentum a megfelelő authentikációs védelmet, valamint a tokenszolgáltató segítségével egyfajta feljogosításon alapuló authorizációs védelmet javasol;

- a szolgáltatások biztonságával foglalkozó rész az üzenet-titkosítást, valamint a tanúsítvány alapú azonosítást és hitelesítést említi. Várhatóan ezek a követelmények egy központilag működtetett hitelesítés-szolgáltatóval oldhatók majd meg;
- az e-közigazgatási közmű biztonságának garantálására a jogosultságmenedzsment és a naplózás jelenik meg javaslatként.

Ez a felsorolás arra enged következtetni, hogy a csatlakozó szolgáltatásoknak minimálisan fel kell készülniük az erős authentikáció megvalósítására (amennyiben a kockázatelemzés szerint erre szükség van), a tokenszolgáltatóhoz való integrációra, a nyílt kulcsú infrastruktúra (PKI – Public Key Infrastructure) alapú működésre, a központi jogosultságmenedzsment rendszerbe való belépésre, valamint bizonyos naplóadatok automatikus vagy manuális kiadására.

A dokumentum nevesíti azokat a keretrendszereket is, amikben a közigazgatási fejlesztések nagy valószínűséggel el fognak készülni. Biztonsági szempontból az elterjedt rendszerek használata folyamatosan vitákat vált ki, hiszen a jól ismert alkalmazások jól ismert sebezhetőséggel rendelkezhetnek, ám a gyakorlat mégis azt mutatja, hogy sokkal jobban kezelhetők ezek a sokak által ismert sebezhetőségek, mint egy nem ismert rendszerben levő nem ismert, vagy csak kevesek által felderített sérülékenység. A megfelelő biztonsági szint eléréséhez azonban szükséges lefektetni, hogy milyen biztonsági környezet és beállítás mellett tekinthetők ezek a keretrendszerek elfogadhatónak.

1.2 Az elektronikus közigazgatás biztonsággal kapcsolatos jogi és műszaki szabályozási kerete

A magyar jogszabályi környezet az élet számos területén szab olyan követelményt, mely az információbiztonsággal kapcsolatos. Ebből is kiemelkedik az elektronikus közigazgatás és a pénzügyi szektor. Az alábbi felsorolásban **áttekintem** azokat a jogszabályokat, melyek valamilyen módon érintik az információbiztonság szabályozását az értekezés írásának időpontjában. Ezek közül számos jogszabály nem az elektronikus közigazgatással foglalkozik, de tartalmából ötletet lehet meríteni a biztonsági követelmények meghatározásához. Az e-közigazgatás szempontjából legfontosabb szabályozásokat külön kiemelem.

- 1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről
- 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
- 2000. évi C. törvény a számvitelről

- 34/2004. (XI. 19.) IM rendelet az elektronikus dokumentumok közjegyzői archiválásának szabályairól és az elektronikus levéltárról
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- **2009. évi CLV. Törvény a minősített adat védelméről**
- **2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről**
- 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
- 284/2001. (XII. 26.) Korm. rendelet a dematerializált értékpapír előállításának és továbbításának módjáról és biztonsági szabályairól, valamint az értékpapírszámla, központi értékpapírszámla és az ügyfélszámla megnyitásának és vezetésének szabályairól
- 2003. évi LX. törvény a biztosítókról és a biztosítási tevékenységről
- 1997. évi LXXXII. törvény a magánnyugdíjról és a magánnyugdíjpénztárakról
- 1993. évi XCVI. törvény az Önkéntes Kölcsönös Biztosító Pénztárakról
- **2009. évi LX. törvény az elektronikus közszolgáltatásról**
- **222/2009. (X. 14.) Korm.rendelet Az elektronikus közszolgáltatás működtetéséről**
- **223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról**
- **224/2009. (X. 14.) Korm.rendelet A központi elektronikus szolgáltató rendszer igénybevevőinek azonosításáról és az azonosítási szolgáltatásról**
- **225/2009. (X. 14.) Korm.rendelet Az elektronikus közszolgáltatásról és annak igénybevételéről**
- 78/2010. (III. 25.) Korm. Rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól
- 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

- 24/2006. (IV. 29.) BM-IHM-NKÖM együttes rendelet a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről
- 305/2005. (XII. 25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról

Az elektronikus közigazgatás biztonságát elsősorban a 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról határozza meg, támogatva a Közigazgatási Informatikai Bizottság 25. (továbbiakban KIB 25.) és 28. számú ajánlásával. [11] [12]

A kormányrendelet hatálya kiterjed az elektronikus közszolgáltatásokra, azok működtetőire, üzemeltetőire, az elektronikus közszolgáltatások nyújtásában részt vevő szervezetekre és személyekre, valamint az elektronikus közszolgáltatások igénybe vevőire, azaz szinte teljeskörűen lefedi az e-közigazgatás szereplőit.

A 223/2009. Korm. rendelet 7 fejezetbe és 43 szakaszba sűríti mindazon személyi, szervezeti és műszaki követelményeket, melyek betartása kötelező. A két KIB ajánlás ezen követelmények részletes kifejtését tartalmazza. A fő előírások a következők:

- Az elektronikus közszolgáltatásoknak meg kell valósítaniuk a bizalmasság, sértetlenség, törvényes adatkezelés és kockázatarányos védelem elveit.
- Az elektronikus közigazgatási rendszerek biztonsági felügyeletét a kormány informatikai biztonsági felügyelője látja el.
- A magyar kritikus információs infrastruktúra védelméért a Nemzeti Hálózatbiztonsági Központ a felelős.
- Az érintett szervezeteknek információbiztonsági irányítási rendszert kell létrehozniuk. Ezen belül meg kell valósítani a minőségbiztosítást és szabályzati rendszert kell létrehozni.
- A kritikus rendszereket naplózni, menteni és archiválni kell.
- Meg kell oldani az ügyféltámogatást.
- Speciális esetekben az üzemeltetés kiszervezhető, de ilyenkor is be kell tartani a biztonsági előírásokat.
- Vírusvédelmet kell megvalósítani.

- Adattovábbítás során kriptográfiai megoldásokat kell használni az üzenetek titkosítására.
- A hozzáférés-védelmet mind logikai, mind fizikai szinten gondosan meg kell tervezni és valósítani.
- Az üzemeltetés biztonsági elveinek kialakítása során a legjobb gyakorlatokra kell alapozni.
- Az elektronikus közszolgáltatásokat biztonsági auditnak kell alávetni az erre felhatalmazott szervezet által.

Ezek mellett még a szolgáltató központok és a központi rendszer biztonsági szabályozása található meg a jogszabályban.

A magyar jogszabályi környezet tehát régóta tartalmazza az információbiztonsági elveket, a közigazgatáson belül azonban kérdéses ezek megvalósulása. A jogalkotó korábban tett már kísérletet a követelmények kötelezővé tételére, szabott határidőket az ellenőrzések bevezetésére, de olyan egységes IT biztonsági környezet még nem alakult ki, amit a szabályozási háttér egyébként lehetővé tenne. Ennek oka elsősorban a forráshiány, illetve a kötelezettek körének pontatlan meghatározása.

A 2009-ben alkotott törvények és rendeletek már jó irányba mutatnak, elsősorban az elektronikus közszolgáltatásokat próbálják megrendszabályozni. Ez azonban még kevés, hiszen az intézmények közötti adatkapcsolatok kérdése nem rendezett. Emellett a jogszabályok túlságosan a Központi Rendszerhez kapcsolódó szolgáltatásokra vannak kihegyezve, mely koncepció számos vitát váltott ki, és nem valószínű, hogy ez a kizárólagosság hosszú távon fennmarad.

A jogalkotónak a következő évek szabályozási munkája során figyelembe kell vennie azt a tényt, hogy az e-közigazgatás néhány nagy rendszer köré csoportosul, melyekhez gyakorlatilag minden költségvetési szerv csatlakozik valamilyen módon, sőt nem egy esetben költségvetésen kívüli entitások kapcsolatával is számolni kell. **Véleményem szerint**, okulva az elmúlt évtized tapasztalataiból, **az alábbi biztonsági elvek törvénybe vagy rendeletbe iktatása látszik indokoltnak**:

- A kiemelt központi rendszerek valós kockázatokkal arányos informatikai védelme az üzemeltetés helyén. Ez jelenti mind az alkalmazásfejlesztés, mind az üzemeltetés folyamatának biztosítását.

- A kiemelt központi rendszerekhez közvetlenül hozzáférő személyekre, intézményekre kiemelt információbiztonsági követelmények meghatározása. Ez tipikusan az intézményen belüli felhasználók köre, de elképzelhető, hogy a rendszer rendeltetése szerint elsődlegesen egy másik intézmény a felhasználó, nem az, amely az üzemeltetést ellátja.
- A csatlakozó költségvetési szervekre információbiztonsági ajánlásokat kell kidolgozni, melyeket széles körben oktatni kell. Bizonyos alapelvek be nem tartása esetén legyen lehetőség valamilyen szankció kirovására, hiszen a felelőtlen felhasználás veszélyezteti a közigazgatás folyamatos működését.
- Az e-ügyintézést végző, költségvetésen kívüli szervezetek esetében olyan felületet kell használni, mely az éles rendszerektől megfelelően leválasztott. Ezen szervezeteknél indokolt esetben elvárható olyan biztonsági megoldás használata, mely számukra akár költséggel is járhat (pl. elektronikus aláírás használata).
- Az e-ügyintézést végző állampolgárok esetén az ügyintézési felületeket olyan módon kell megvalósítani, hogy azok a teljes rendszer biztonságát ne veszélyeztessék. Nagy kockázatú tranzakciók során elvárható az állampolgároktól valamilyen erős authentikációs megoldás (pl. SMS-ben érkező one-time password) használata, de ezen kívül nincs realitása más biztonsági követelmény kikényszerítésének, közvetlen költséget nem lehet rájuk hárítani.
- A központi rendszerek egymás között adatokat cserélnek, illetve a körön kívüli intézmények rendszerei is adatkapcsolatban állnak velük. Ezeket az automatikus adatcsere interfészeket megfelelően kell szabályozni. A SOA irány a szinkron adatkapcsolatokat preferálja, ezt különös körültekintéssel kell megvalósítani.
- Létre kell hozni egy olyan műszaki bizottságot, mely többek között az e-közigazgatás biztonsági követelményeit meghatározza, az előírásokat karbantartja, jógyakorlatokat dolgoz ki, vitás esetekben dönt, kérdésekre pedig érdemi választ ad. Optimális esetben a bizottság olyan személyekből áll, akik kellő műszaki tájékozottsággal rendelkeznek a területen és képesek külső befolyástól mentes döntéseket hozni, függetlenül attól, hogy a közigazgatásban, a piacon vagy a tudományban dolgoznak.
- Fel kell állítani egy olyan felügyelő hatóságot, mely az információbiztonsági felügyelő hatáskörét átvéve, azt kiterjesztve engedélyezni és ellenőrizni tudja az e-közigazgatási szolgáltatásokat. Ideális esetben eljárhatna bármelyik költségvetési szerv

információbiztonságát érintő esetben. Működési modelljét tekintve a Pénzügyi Szervezetek Állami Felügyeletének informatikai auditori rendszerét lenne érdemes átvenni.

- Az e-közigazgatáson belül és kívül meg kell határozni és szabályozni kell a kritikus információs infrastruktúrákat. A közigazgatási körön kívüli kritikus információs infrastruktúrák döntően magánkézben levő szervezetek, ezért egy ilyen szabályozás jelentős érdeksérelmet jelent számukra, de ebben az esetben a nemzetvédelmi érdekek felül kell, hogy írják ezt a szempontot. A kritikus információs infrastruktúrák ellenőrzését a felügyelet szintén elláthatja.

Újra le kell szögeznem, hogy **a legfontosabb közigazgatási rendszerek köre**, amelyekre kiemelt védelmet kell biztosítani, a következő évtizedekben jelentősen **nem fog változni**. Ezen a területen a mindenkori kormánynak van jogszabályi lehetősége, és egyben kötelessége is a modern információbiztonsági fenyegetések kivédésére. Más, ebből a szempontból nem fontos központi költségvetési szerveknél olyan előírásokat fogalmazhat meg, melyek jelentős költségek nélkül megvalósíthatók. A helyi szerveknél és a közigazgatáson kívüli világban azonban értelmetlen nagy elvárásokat táplálni, ezeket az entitásokat informatikai szempontból megbízhatatlannak kell kezelni.

1.3 Informatikai fenyegetések és feltételezések a központi rendszerekben

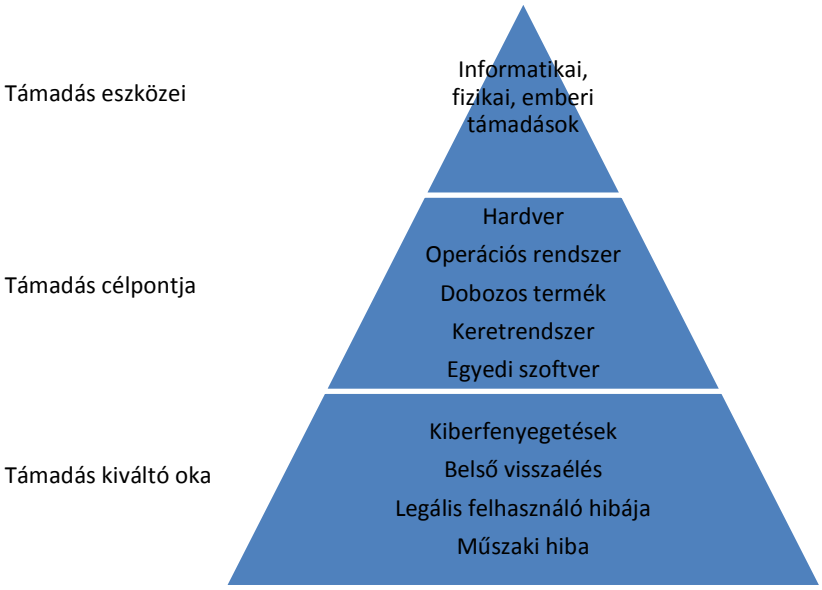
Az e-közigazgatási stratégia és a már működő rendszerek alapján **kiemelem a komplex magyar e-kormányzati infrastruktúra néhány jellegzetességét**. A létrejövő megoldások centralizáltak, internetes felületen, de az Elektronikus Kormányzati Gerinchálózaton (EKG) keresztül elérhetővé válnak, alapvetően szolgáltatásorientált architektúra (SOA) alapon fogják tervezni, valamint webes technológiákra fognak épülni. Ezek a tervezési elvek olyan tipikus fenyegetéshalmazt jelentenek, melyekkel minden rendszernek számolnia kell.

A magyar szakirodalom eddig kevéssé foglalkozott a speciális e-közigazgatási fenyegetésekkel, de korábban már jelent meg olyan tanulmány, mely az Ügyfélkapu néhány sebezhetőségére hívta fel a figyelmet. [13] A szerzők ebben arra figyelmeztettek, hogy egyrészt az alkalmazott hitelesítési megoldás (jelszó) tömeges használat esetén adathalász támadásoknak lesz kitéve, így tömegesen szivároghatnak ki jelszavak, másrészt arra hívták fel a figyelmet, hogy az Ügyfélkapun beadott iratok, például adóbevallások műszaki értelemben nem garantálják a sértetlenséget és a letagadhatatlanságot. A tervezett programok legalább az

első fenyegetésre opcionális választ adnak, ám a második fenyegetés továbbra is érvényes marad.

A tervezett technológia ismeretében azonban további, **releváns fenyegetéseket állapítok meg**. Ez a fenyegetéshalmaz kiindulópont lehet az e-közigazgatás Common Criteria (CC) szerinti Védelmi Profilok és Biztonsági Előirányzatok előállításához, ezért a CC formalizmus szerint is meghatározásra kerülnek.

Jelen értekezésben kifejezetten az e-közigazgatásban használt, döntően egyedi fejlesztésű szakigazgatási rendszerek biztonsági problémáira koncentrálok. Nem célom meghatározni ezen kívül más informatikai elemek biztonsági követelményeit, ezeket környezeti elemnek tekintem, legyen az fizikai, logikai vagy adminisztratív biztonsági intézkedés. De az összkép érdekében fontos leírni, hogy milyen fenyegetésekkel kell számolni a kockázatelemzésnél, és az ezekből eredő kockázatokra milyen, a szakigazgatási rendszerben megjelenő programozott védelmi intézkedés hozható. **A fenyegetéseket az alábbi ábrán mutatom be, mely az általam kidolgozott szisztéma szerint épül fel**.



1. ábra: E-közigazgatási rendszerek fenyegetései

Először is meg kell vizsgálni az elektronikus közigazgatási rendszereket fenyegető tényezők motivációit, kiváltó okait, amelyek a következőek lehetnek:

- Műszaki hiba: az informatikai rendszerek biztonságos működésére vonatkozó legnagyobb veszélyt a műszaki hibák jelentik. Ezek adódhatnak a hibás programozásból vagy a nem megfelelő üzemeltetésből. A hiba bekövetkezése a

gyakorlatban elkerülhetetlen, de megfelelő üzemszervezéssel, azaz üzletmenet-folytonossági (BCP – Business Continuity Plan) és katasztrófa tervekkel (DRP – Disaster Recovery Plan) hatása csökkenthető vagy kiiktatható.

- Legális felhasználó hibája: egy olyan személy hibázik, aki jogosult felhasználója a rendszernek, és ezzel aláássa a rendszer megbízható működését. A felhasználó tevékenységének korlátozásával, a kliensoldal megfelelő biztonsági szintjének kiépítésével, a biztonságtudatossági oktatással a kockázat csökkenthető, de teljes egészében nem iktatható ki.
- Belső visszaélés: a rendszer jogosult felhasználója valamilyen okból szándékosan okoz kárt, követ el visszaélést. Mivel felhasználóként jól ismeri a rendszert, esetleg annak védelmi intézkedéseivel is tisztában van, a kockázat ebben az esetben a legnagyobb. Általában fejlett preventív védelmi intézkedésekkel jó eséllyel megakadályozható a támadás, de nem szabad elfeledkezni a detektív kontrollokról sem. Abból kell kiindulni, hogy a támadás sikerrel fog járni, kiterjedése azonban elsősorban az érintett szervezetre korlátozódik.
- Kiberfenyegetések: ebbe a körbe sorolunk minden olyan támadást, amit a rendszerhez jogosultsággal nem rendelkező, külső támadó hajt végre. A motivációk különbözőek, de a felhasznált eszközök általában azonosak.
    - Kémkedés: egy idegen állam észrevétlenül információkat szerez a közigazgatási rendszerekből. Kiterjedése általában jelentős, az okozott kár is, de az ország működését közvetlenül nem fenyegeti, hiszen nem jár a rendszerek kiesésével.
    - Kiberterrorizmus/hacktivizmus: célja valamilyen ideológia vagy csak a bizonyítás miatt egyes rendszerek működésének leállítása, a felhasználói felület megváltoztatása (deface) vagy adatok ellopása, és később nyilvánosságra hozása. Általában egy vagy csekély számú rendszerre terjed ki, az okozott kár többnyire nem jelentős, az ország működését nem fenyegeti, de jelentős imázsvesztéssel jár. A szakirodalom a két fogalmat külön kezeli, de mivel a technika és a célpont többnyire azonos és a védelem szempontjából is hasonló a két támadási fajta, én összekötöm a két területet.

- Kiberbűnözés: a kémkedéshez hasonló tulajdonságokkal rendelkezik, a különbség az, hogy általában egy szervezetet érint, célja bizonyos információk megszerzése, majd továbbértékesítése.
- Kiberhadviselés: egy ország által a másik ország ellen indított támadás, melynek célja az adott ország társadalmi és gazdasági működésének akadályozása vagy ellehetetlenítése. Lehet egy fegyveres konfliktus kísérőjelensége is. Kiterjedése és az okozott kár mértéke hatalmas, az egész ország működését veszélyezteti.

A műszaki hibák ellen megfelelő alkalmazásfejlesztéssel és üzemeltetéssel tudunk védekezni. A Common Criteria terminológia szerint ez azt jelenti, hogy megfelelő garanciális szintet kell felmutatni, illetve feltételeznünk kell, hogy hibatűrő informatikai környezetet hoztak létre az alkalmazás köré, amit megfelelően üzemeltetnek. **Az alábbi felsorolásban bemutatom az általam kidolgozott, a magyar e-közigazgatási alkalmazásokra vonatkozó Common Criteria szerinti Védelmi Profil eszköztár első részét.** A felsorolásban a CC szerinti jelölést használom. Ebben az A az Assumption, azaz Feltételezés, a T a Threat, azaz Fenyegetés, a P a Policy, azaz Szabályzat rövidítése. A Feltételezések az informatikai környezetre vonatkozó előzetes elvárásokra vonatkoznak, a Fenyegetések a rendszerre vonatkozó fenyegetések halmaza, a Szabályzatok pedig a rendszerre vonatkozó jogszabályi, szabványból eredő vagy belső szabályozási követelményeket foglalja össze.

- **A.FAILSAFE**: az alkalmazás hibatűrő informatikai infrastruktúrán üzemel.
- **A.OPERATION**: az üzemeltetés során betartják a jogszabályokban, szabványokban és belső utasításokban foglaltakat.

A jogosult felhasználó hibái tevékenységéből és a nem megbízható kliensoldalból erednek.

- **T.USER_ERROR**: a jogosult felhasználó olyan hibát vét, ami veszélyezteti a rendszer biztonságát
- **T.INSECURE_CLIENT**: a jogosult felhasználó kliense a felhasználó tudta nélkül veszélyezteti a rendszer biztonságát.

A belső felhasználó és általában a kiberfenyegetések is elsősorban adatszivárgással kapcsolatos fenyegetést jelentenek, amit észrevétlenül hajtanak végre.

- **T.DATA_LEAKAGE**: a rendszerben tárolt védett információ jogosulatlanul kikerül a rendszer hatóköréből.

- **T.UNDETECTED_INCIDENT**: az alkalmazásban észrevétlen marad egy biztonsági incidens.

A kiberfenyegetések további jellemzője, hogy bizonyos esetekben a szolgáltatás leállítása a cél oly módon, hogy azt a hibatűrő környezet nem képes kezelni.

- **T.AVAILABILITY**: az alkalmazás valamilyen külső informatikai támadás következtében nem működik.

A támadások célja után át kell tekinteni a megcélzott informatikai elemeket. A támadások az informatikai környezet bármely elemét érhetik, így a hardvert, a hálózati kapcsolatokat, az operációs rendszert, a kereskedelmi forgalomban kapható ún. dobozos szoftvereket (COTS – Commercial off-the-shelf), a keretrendszereket és az egyedi alkalmazásokat is. A dobozos szoftver és a keretrendszer között azért kell különbséget tenni, mert míg a dobozos szoftverben (pl. egy víruskeresőben) a felhasználó csak konfigurációt hajt végre és univerzálisan egy adott biztonsági funkciót szolgál, a keretrendszerek lehetőséget adnak speciális, személyre szabott folyamatok megvalósítására oly módon, hogy az alapvető biztonsági funkciók csak konfigurációs beavatkozást igényelnek. Egyedi fejlesztésű szoftvereknél a biztonsági funkciók is az adott szoftverhez kerülnek kifejlesztésre.

A **centralizálásból** eredő elsődleges fenyegetés az, hogy a korábban szétosztott információk néhány jól meghatározható földrajzi helyen, akár egy belső hálózaton, sőt, a virtualizációt figyelembe véve akár egy számítógépen is találhatók. Programozott védelmi intézkedéseket a hardver, hálózat, operációs rendszer és dobozos alkalmazás szinten nem lehet megfogalmazni, így környezeti biztonsági célokat lehet kialakítani. Feltételezhetjük, hogy a géptermek fizikailag védettek, a hálózatokat tűzfalak védik, a személyzet megbízható, de a virtualizáció reális fenyegetés. **A Common Criteria formalizmusa szerint ezt a következőképp fogalmazom meg.**

- **A.PHYSICAL**: A szervertermek az elvárható fizikai védelemmel vannak ellátva.
- **A.SEGMENTATION**: A belső hálózat tűzfallal van elválasztva az internetes kapcsolattól, valamint a virtuális LAN-okat is tűzfalas védelem választja el egymástól.
- **A.PERSONNEL**: A rendszer üzemeltetését végző személyzet megbízható.
- **T.VIRTUALIZATION**: A virtualizációs megoldás hibájából nem kontrollált hozzáférés jöhet létre.

Az internetes vagy EKG-n keresztüli hozzáférés nyílt hálózatú hozzáférésnek minősül, hagyományos TCP/IP protokollon keresztül érhetők el a szolgáltatások. Nem szabad elhanyagolni a megfelelő hálózatvédelmet, mely az előző pontban említett tűzfalas védelmen kívül az operációs rendszerek és a hálózati elemek védelmét jelenti. A gyakorlatban ugyanis egy nem megfelelően beállított eszköz komoly fenyegetést jelenthet. Feltételezésként tehát elvárhatjuk tanúsított hálózati eszközök, operációs rendszerek és dobozos termékek használatát, valamint azt, hogy az alkalmazás olyan környezetben fut, mely megfelel a korábban már elemzett 223/2009 Korm. rendelet előírásainak.

- **A.CERTIFIED**: Az Értékelés Tárgyát futtató operációs rendszer, valamint a vele közvetlen kapcsolatban levő hálózati elemek és biztonsági funkciókat megvalósító dobozos termékek rendelkeznek Common Criteria vagy azzal egyenértékű tanúsítással.
- **P.EKG**: Az Értékelés Tárgyát futtató infrastruktúra eleget tesz a 223/2009. Korm. rendeletnek.

A szolgáltatásorientált architektúrák használatával új, eddig még nem tapasztalt fenyegetésekkel kell megbirkózni. A SOA, vagy kicsit kibővítve, a Web 2.0 elterjedésével megjelenő fenyegetések széles listáját írja le a szakirodalom. A hivatkozott forrás négy speciális támadási pontot, és ezen belül számos fenyegetést azonosít. [14] Mivel ezek részletes ismertetése meghaladja jelen értekezés kereteit, a fenyegetéseket a támadási pontok, vektorok alapján lehet csoportosítani. Ezek a valós fenyegetések a keretrendszerekre és az egyedi alkalmazásokra.

Az első támadási pont a **kliensoldal**, azaz tipikusan a böngésző. A Web 2.0 által meghonosított technológiák közül itt az Ajax komponensek, a RIA és Flash komponensek, a sérülékeny böngészők, a Javascript és DOM objektumok, a HTML tag-ek, az intranetes node-ok és a widget-ek képviselnek különleges sebezhetőségeket. Ezek közvetlenül a felhasználóra nézve veszélyesek, közvetve azonban a közigazgatási rendszer biztonságát is aláássák. A második támadási pontot a **struktúra szintű támadások** jelentik, hiszen a korábbi, kizárólag HTML alapú struktúrák kétirányú, pl. XML formátumban leírt struktúrákra változtak. Ennél a támadási pontnál ki kell emelni az XML, valamint speciálisan az RSS és Atom node-okat, valamint a név-érték párokat, mint sebezhető elemeket. A harmadik támadási pontot a **protokoll szinten** lehet azonosítani. Az olyan protokollok, mint az XML-RPC vagy a SOAP a fejlécben, valamint a tartalmi részben hordozhatnak sebezhetőségeket. Végül az utolsó,

negyedik támadási pontot a **szerver oldalán** találhatjuk meg, ahol a hagyományos alkalmazási erőforrások, a web service erőforrások és a hálózati erőforrások válhatnak támadási célpontokká. **A Common Criteria szerint tehát a következő fenyegetéseket határozom meg.**

- **T.CLIENT_SIDE**: A támadó egy áldozat kliens oldali alkalmazásán vagy böngészőjén keresztül nem jogosult műveletet hajthat végre.
- **T.STRUCTURE**: A támadó az adatcsere üzenet formátumának módosításával nem jogosult műveletet hajthat végre.
- **T.PROTOCOL**: A támadó a kommunikációs protokoll manipulálásával nem jogosult műveletet hajthat végre.
- **T.SERVER_SIDE**: A támadó a szerveroldali erőforrások manipulálásával nem jogosult műveletet hajthat végre.

A motivációk és a célok után az eszközöket kell megvizsgálni. Az informatikai erőforrásokkal tárolt, feldolgozott és továbbított információkat informatikai, fizikai és emberi támadásokkal lehet megszerezni. A fizikai támadás célszerűen a rendszert futtató infrastruktúrára vonatkozik, erre korábban már létrehoztunk egy feltételezést. Emberi támadás alatt az ún. social engineering (SE) támadást értjük, melyet fel kell venni a valós fenyegetések listájára.

- **T.SOCIAL_ENGINEERING**: Jogosulatlan felhasználó egy jogosult felhasználó nevében visszaélést követ el.

Az informatikai támadásokat elsősorban az alkalmazási szinten értelmezzük, mert az egyéb, pl. hálózati támadások elemzése nem célja a tanulmánynak, másrészt nem részletezve már felsoroltuk őket a korábbi fenyegetések között. A webes technológiákra vonatkozó számtalan fenyegetés közül az OWASP (Open Web Application Security Project) Top 10 2010 tartalmazza azokat, melyek ellen mindenképpen programozott védelmet kell nyújtani. [15] Az itt felsorolt fenyegetések azonban nem csak webes, hanem más programozási környezetre is igazak. Ezek sorrendben:

- Beszúrásos támadások (Injection);
- Cross-Site Scripting (XSS);
- Hibás hitelesítés és sessionkezelés (Broken Authentication and Session Management);
- Nem biztonságos direkt objektumhivatkozás (Insecure Direct Object References);

- Cross-Site Request Forgery (CSRF);
- Helytelen biztonsági beállítások (Security Misconfiguration);
- Nem megfelelő kriptográfiai tárolás (Insecure Cryptographic Storage);
- URL hozzáférés korlátozásának hibája (Failure to Restrict URL Access);
- Nem megfelelő szállítási réteg védelem (Insufficient Transport Layer Protection);
- Nem ellenőrzött átirányítások és továbbítások (Unvalidated Redirects and Forwards).

A Common Criteria terminológia szerint így fogalmazom meg ezeket.

- **T.INJECTION**: Egy támadó injektálásos támadást hajthat végre a nem megfelelő inputvalidálás miatt.
- **T.XSS**: Egy támadó Cross Site Scripting támadást hajthat végre a nem megfelelő inputvalidálás miatt.
- **T.SESSION**: A nem megfelelő sessionkezelés miatt a támadó hozzáférhet egy legális felhasználó jogosultságaihoz.
- **T.DIRECT_REFERENCE**: Egy támadó olyan objektumhoz férhet hozzá a nem megfelelő URL kezelés miatt, melyhez nincs jogosultsága.
- **T.CSRF**: Egy támadó Cross Site Request Forgery támadást hajthat végre a nem megfelelő inputvalidálás miatt.
- **T.INFO_LEAKAGE**: A nem megfelelő beállítások és hibakezelési hibák miatt az Értékelés Tárgyából konfigurációs információk szivárognak ki.
- **T.CRYPTO**: A nem megfelelő kriptográfia használata miatt a felhasználói adatok dekódolhatóvá válnak.
- **T.URL**: Egy támadó olyan URL-hez férhet hozzá a nem megfelelő szerverbeállítás miatt, melyhez nincs jogosultsága.
- **T.INSECURE_COMMUNICATION**: A nem titkosított adatátvitel miatt a hálózati forgalom lehallgathatóvá válik.
- **T.REDIRECT**: Egy támadó a nem megfelelő átirányítások miatt nem jogosult hozzáférést szerez.

A fentiekben felsorolt fenyegetések, feltételezések és szervezetbiztonsági szabályok minden e-közigazgatási Védelmi Profil és Biztonsági Előirányzat részeivé kell, hogy váljanak, hiszen az ezekből következő biztonsági célok képesek a tipikus fenyegetésekre adekvát választ adni.

1.4 Az alkalmazások biztonsági besorolási rendszere

Az előző pontban felsorolt fenyegetések univerzálisan érvényesek a központi e-közigazgatási rendszerekre, ám a sebezhetőségek, és ennek következtében a kockázatok is különbözőek. Ezért célszerű az e-közigazgatási rendszereket valamilyen elv szerint besorolni, és ezekhez kötelező védelmi intézkedéseket előírni. Ezt a célszerűséget a kormány is felismerte, a KIB 25. és a KIB 28. ajánlásban is három jól elkülöníthető biztonsági szint került leírásra.

A gyakorlatban azonban az ajánlások szintjei nehézkesen használhatók. Hiába írják le pontosan a kockázatelemzés lépéseit, és ez alapján a kitettség számításának mértékét, hiába van külön szint-meghatározási minta is, a közigazgatási döntéshozókat ez sokszor félrevezeti, a besorolás nem objektív módon történik meg. A következő felsorolás tehát a **meglévő ajánlás egyszerűsítése**, nem az információbiztonsági szabványokban megszokott sértetlenség, bizalmasság, rendelkezésre állás szerinti kockázatok alapján, hanem funkcionalitás szerint határoz meg szabályokat.

Az értekezésben mindezeknek megfelelően három védelmi szintet határozok meg, melyek megfelelnek az ajánlásokban leírt három szintnek: a minősített adatot kezelő rendszerekre (kiemelt), a belső használatú, nem nyilvános információkat kezelő rendszerekre (fokozott), valamint a széles körben, interneten keresztüli hozzáférést biztosító rendszerekre (alap) határozok meg követelményeket. Mindezt összhangban az ajánlásokkal. Meg kell jegyezni, hogy a kiemelt rendszerek esetén lehetnek olyan nem nyilvános szabályok, melyek befolyásolják az értekezésben javasolt szabályozási javaslatokat, de olyan nem nyilvános szabályozásra való utalást, mely a komplex informatikai rendszere vonatkozik, a kutatásom során nem találtam. Emellett azt is érdemes feljegyezni, hogy az elektronikus közigazgatási rendszerek többnyire nem tartalmaznak minősített adatot, de pl. a titkosszolgálatok személyi állományával kapcsolatos pénzügyi, szociális információkat kezelő rendszerekben előfordulhat ilyen modul, mely az értekezésben részletezett műszaki megoldásokat használja. **A kiemelt szint tehát olyan esetekre szab követelményeket, amikor egy komplex államigazgatási rendszer bizonyos modulja minősített adatokat is kezel, de nem ez az elsődleges funkciója.**

A KIB 28. ajánlás „Útmutató az IT biztonsági szintek meghatározásához” című dokumentuma a következő kihatási szinteket definiálja. [16]

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.

A korlátozott hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése:

a) a szolgáltatási képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani ugyan elsődleges funkcióit, de a funkciók hatásossága észrevehetően csökken; vagy

b) a szervezeti eszközök kisebb mértékű károsulását eredményezi; vagy

c) kisebb mértékű pénzügyi veszteséget okoz; vagy

d) a jogbiztonságot kisebb mértékben veszélyezteti.

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.

A komoly hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése:

a) a szolgáltatási képességet oly mértékben és olyan időtartamra csökkentheti, hogy a szervezet képes végrehajtani elsődleges funkcióit, de a funkciók hatásossága jelentős mértékben csökken; vagy

b) a szervezeti eszközök jelentős károsulását eredményezi; vagy

c) jelentős pénzügyi veszteséget okoz; vagy

d) a jogbiztonságot jelentős mértékben veszélyezteti.

Kiemelt: 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.

A súlyos vagy katasztrofális hátrányos hatás azt jelenti, hogy a bizalmasság, sértetlenség vagy rendelkezésre állás elvesztése:

a) a szolgáltatási képességet olyan mértékben és olyan időtartamra csökkentheti, illetve akár meg is szüntetheti, hogy a szervezet nem képes végrehajtani egy vagy több elsődleges funkcióját; vagy

b) a szervezeti eszközök lényegi károsulását eredményezi; vagy

c) lényegi pénzügyi veszteséget okoz; vagy

d) a jogbiztonságot alapvető mértékben veszélyezteti.

Összhangba hozva a dolgozat és az ajánlás szóhasználatát, a tanulmány alap biztonsági szintje az *alacsony kitettségnek*, a fokozott a *fokozottnak*, a kiemelt pedig a *kiemeltnek* felel meg. Bár nem tökéletes az egyezés, de tapasztalatból elmondható, hogy a széles körben, állampolgárok által használt szolgáltatásokkal kapcsolatos incidensek kihatása megfelel az alacsony szint definíciójának. Az már vitatható, hogy a szakigazgatási rendszerekkel kapcsolatos biztonsági incidensek a fokozott vagy kiemelt kihatású csoportba tartoznak, de mivel a KIB 28. ajánlás nem kezeli a minősített adatokat kezelő alkalmazások követelményeit, így indokoltnak látszik az értekezés által javasolt felosztás. Külön ki kell emelni, hogy a minősített adatokat kezelő alkalmazások biztonsági funkcióira semmilyen nyilvános előírás nem létezik, csupán a 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól tesz említést néhány követelményről, de ez közel sem kielégítő. [17]

Az előző alfejezetben felsorolásra kerültek a biztonsági incidensek kiváltó okai, motivációi. A három típusalkalmazás mindegyikére vonatkoznak azok a fenyegetések, melyek említésre kerültek. **Azonban a hangsúlyok mások, ezért meghatározom a tipikus támadási motivációkat**. Az alap biztonsági szintű rendszerek webes interfészen, direkt módon elérhetők, ezért gyakran, sokan próbálják azt megtámadni – annak ellenére, hogy érdemi kárt nagyon ritkán lehet ezzel okozni. Viszont helytelen szeparáció esetén a sikeres támadás ugrópontot ad a belső szakrendszerek felé, amit mindenképpen el kell kerülni. A kiberfenyegetések közül ennél az alkalmazástípusnál elsősorban a kiberterrorizmust/hacktivizmust és a kiberhadviselést kell figyelembe venni.

A belső szakrendszerek rejtettebben működnek, de sokszor olyan adatokkal dolgoznak, melyek informatikai értelemben megbízhatatlan forrásból származnak. Elsősorban a legális felhasználók hibája okozhat gondot, de a belső visszaéléseknek is ez az elsődleges területe. Általában ez utóbbiból ered a kémkedés és a kiberbűnözés megjelenése is, hiszen sokszor egyszerűbb egy jogosult felhasználót megvesztegetni, mint direkt informatikai módon

behatolni egy rendszerbe. Ettől függetlenül nem tekinthetünk el ezen motivációk direkt megjelenésétől sem. A kiberhadviselésnek természetszerűleg elsődleges célpontjai kell, hogy legyenek a belső közigazgatási rendszerek, hiszen az állam ügyvitelére ezeken keresztül lehet a legnagyobb csapást mérni, de a kisszámú példából még nem lehetett látni ilyen rendszer támadását. Ettől függetlenül a közigazgatás informatikai rendszerei a jövőben egy kiberhadviselési tevékenység elsődleges célpontjaivá válhatnak.

A kiemelt biztonsági szintű, minősített adatokat kezelő közigazgatási rendszereknél speciális, célzott támadásokkal kell számolni, hiszen sokszor ezek léte is csak kevés személy számára ismert. Elsősorban a belső visszaéléssel kell számolni, de több példa szerint a kémkedést szolgáló direkt informatikai támadások elsődleges célpontjai ezek a rendszerek. Mindezt ráadásul olyan eszközökkel teszik meg, mely ellen preventív módon igen nehéz védekezni. A szakirodalom az ilyen támadásokat Advanced Persistent Threat (APT – Összetett Állandó Fenyegetés) néven ismeri. [18]

Az APT támadások néhány jellemzője rávilágít, hogy miért kell kiemelt biztonsági szintet megfogalmazni a minősített adatokat kezelő rendszerekre: [19]

- Advanced, azaz összetett, hiszen a támadók az információszerzés teljes tárházát bevetik. Ide tartoznak az informatikai támadások eszközei mellett a hagyományos információszerzési eszközök, mint a telefonlehallgatás vagy akár a műholdas megfigyelés. Az informatikai támadás során tipikusan olyan kártékony kódokat használnak fel, melyekre a vírusvédelmi rendszerek és a tartalomszűrő megoldások nem készültek fel. Ezek lehetnek valamilyen kártékony kódot generáló eszközzel előállított trójaiak és hátsókapuk, de lehetnek egyedileg írt, korábban nem ismert szoftverhibákat kihasználó kódok is. Általában jól felépített, célzott támadásokról beszélhetünk, amit speciálisan a célpontra dolgoztak ki, akár komoly hírszerzési információk felhasználásával.
- Persistent, azaz állandó, hiszen a támadó kimondottan egy célponttal foglalkozik ahelyett, hogy egyszerre több helyen, próba-szerencse alapon dolgozna. A támadók mögött gyakran állami szervek állnak, de ez a legtöbbször csak sejthető, de nem bizonyítható. A támadás során felhasznált információk köre azonban többnyire olyan, amit például hacktivista csoportok nem tudnak megszerezni. A folyamat hosszú ideig tart, a támadó folyamatos, de nehezen észlelhető adatkapcsolatban van a célponttal,

ezzel tesztelve annak védelmi képességeit. Amennyiben a kapcsolat megszakad, a támadó később tovább próbálkozik.

- Threat, azaz fenyegetés, hiszen mind a képesség, mint a cél adott. Mindig valamilyen humán intelligencia áll mögötte, nem egy automatikus kód kerül lefuttatásra. Stratégiai cél áll a támadás mögött, a támadónak meghatározott céljai vannak, amihez tudás, motiváció, szervezettség és megfelelő anyagi háttér társul.

Egy-egy példával még jobban alátámasztom azt, hogy a három típusrendszert miért érdemes külön kezelni, miért különböző egy biztonsági incidens hatása a teljes közigazgatásra nézve akkor, amikor az incidens műszaki háttere egyébként azonos. Egyben jelzésértékű az is, hogy a felsorolt példák alkalmazáshibák miatt következtek be.

2009. február 7-én terjedt el az interneten az információ, mely szerint néhány órára használhatatlanná vált a Miniszterelnöki Hivatal (MEH) alá tartozó kormányzati informatikai rendszer, az Ügyfélkapu, mely tipikusan a széles körben használt, interneten keresztül elérhető kategóriába tartozik. Az üzemzavar következtében az oldalra belépő ügyfelek más személyek és cégek adatait, APEH-től érkező leveleit látták a sajátjuk helyett. Ez rövid időn belül a második incidens volt, egy hónappal korábban a rendszer jelentősen lelassult. [20]

Az eseményeket értékelő végleges vizsgálati jelentés egy korábbi, az év januári lassulás kapcsán az informatikusok személyes felelőssége mellett kiemeli: „A helyzetet súlyosbította, hogy a felhasználók tájékoztatására szolgáló kommunikációs rendszer sem működött, így a lassulásról szóló üzenetet sem tudták a képernyőn megjeleníteni.” Ez a komoly fennakadásokat okozó lassulás azonban sem adatvesztéssel, sem illetéktelenek hozzáférési lehetőségével nem járt, de a probléma miatt az informatikai kormánybiztos levélben fordult az üzemeltető Kopint-Datorg Zrt. vezérigazgatójához. A vizsgálatot vezető információbiztonsági felügyelő megállapította, hogy a rendszer teherbíró képességét növelni kell, emellett megengedhetetlen, hogy a vészforgatókönyvek nem működnek, így szoftveres okok miatt nem volt lehetőség a felhasználók tájékoztatására.

A 2009. februári esetben komolyan fennállt az adatvesztés kockázata, hiszen a hiba következtében a bejelentkezők mások fiókjaiba érkeztek meg. E hiba a kapcsolódó rendszerek egy részét (pl. az APEH) is érintette, de a feltárt eredmények alapján nem találtak kárt okozó, illetéktelen adatkezelésre utaló nyomot (a mások fiókjába érkezők szinte azonnal ki is léptek).

A hibát belső tevékenység okozta, újra csak az történt, hogy az üzemeltetők megsértették az eljárásrendet, s az előzőekhez hasonlóan a rugalmatlan és hierarchikus döntési protokoll súlyosbította a helyzetet.

A vizsgálat megállapította, hogy külső támadás nem történt, feltehetően újra csak egy tesztelés nélkül végrehajtott frissítés okozta az üzemzavart. A biztonsági incidensek kezelésére előírt protokoll, illetve annak alkalmazása azonban katasztrofálisan vizsgázott, a jelentés szerint: az alkalmazottak „a hibabejelentés fogadásától annak elhárításáig a szakmai tevékenységük során az üzemeltetési szabályzat szerint jártak el. Ugyanakkor az is megállapítható, hogy a módosítás éles rendszerbe töltése előtt, valamint annak megvalósítása során eljárásrendi szabályokat sértettek meg, illetve megsértették az üzemeltetési szerződés azon pontját, amely szerint a változásról a Megrendelő (Miniszterelnöki Hivatal) képviselőjét/kapcsolattartót tájékoztatni szükséges.” Emellett nem tájékoztatták a MeH-et a hiba okáról sem, illetve egy megadott lista alapján az érintetteket is értesíteniük kellett volna SMS-ben.

A felügyelő a teljes jelentés lezárásaként újra megállapítja: „A működési zavarok mindhárom esetben ugyanarra az okra vezethetők vissza: emberi mulasztásra, a programok módosítását követő, nem az erre vonatkozó hatályos szabályzatok előírásainak megfelelő és nem körültekintően végzett tesztelésre. Az esetek – az érintett felhasználóknak okozott kellemetlenségen kívül, amelyért mind az OEP, mind a MeH az érintettektől elnézést kért – adatvesztést, visszaállíthatatlan adatmódosulást, anyagi kárt nem okoztak. A rendszerek biztonságát, az adatok közhitelességét az üzemzavarok nem veszélyeztették. A hibás működés okai és a felelősök mindhárom esetben egyértelműen megállapítást nyertek, a felelősségre vonások folyamatban vannak.” [21]

Hasonlóképpen vélekedett a közigazgatási informatikát felügyelő államtitkár is, aki a sajtótájékoztatóján elmondta, hogy a technikai hiba mellett igen nagy gondot okozott az is, hogy a szervezet eljárásrendje és szervezettsége nem volt megfelelő, ennek köszönhető a probléma eszkalálódása, melyet egy időben történő rendszerleállítás meggátolt volna, ám ez a rossz hierarchia miatt nehézkes, ezért feltétlenül szükséges újraalkotni a struktúrát, s új, egyszerűbb eljárási rendet fognak kialakítani. Megemlítette azt is, hogy nem csak a belső információáramlás volt elégtelen, hanem a felhasználók sem kaptak tájékoztatást, s ez megengedhetetlen. [22]

Az ígért biztonsági intézkedések ellenére az Ügyfélkapu május 29-én újra összeomlott. A közigazgatás működése azonban nem forgott veszélyben, az eset imázsvesztésnek tekinthető. [23]

2009 januárjában egy súlyos üzemzavar következett be az egészségbiztosítás jogviszony-nyilvántartási adatállományában, nevezetesen: hiba miatt a rendezett jogviszonyú biztosítottak is piros lámpát, azaz helytelen igazolást kaphattak, amikor háziorvosuknál, patikákban vagy más egészségügyi ellátónál jelentkeztek. Ez tehát egy szakigazgatási rendszer, mely belső felhasználású, hibája azonban jelentős fennakadásokat okozott az egészségügyben.

A hivatalos közlemény szerint: „Az OEP munkatársai hétfőn délben észlelték, hogy az egészségbiztosító jogosultság-ellenőrzés lekérdezéseket kiszolgáló informatikai rendszerei (OJOTE, VIREP) számára jogosultsági információkat szolgáltató belső adatbázisban, ill. informatikai rendszerben olyan jellegű probléma következett be, mely bizonyos esetekben tévesen »piros lámpát« jelez, egyébként jogosultsággal rendelkező állampolgár esetében is.

A probléma egy, az alkalmazói rendszerrel kapcsolatos szoftverfejlesztés során lépett fel, melyet ugyan néhány óra alatt sikerült elhárítani, de a program módosította az OEP jogviszony-nyilvántartási adatbázisában lévő adatokat is. Az egészségbiztosító a hiba felfedezését követően tájékoztatta az egészségügyi szolgáltatókat, valamint a lakosságot.

A meghibásodása százezreket érinthetett, de kizárólag azok a betegek tapasztalhatták a hibás működést, akik az adott időben orvosnál jártak, illetve ki akarták váltani például a gyógyszereiket. A hatályos jogszabályok alapján a jogviszony-ellenőrzés eredményétől függetlenül a beteget ugyanúgy el kell látni, a pácienssel az ellátás költségét kifizettetni nem lehet, a támogatott gyógyszer, gyógyászati segédeszközt ártámogatással kell kiadni.”

Ez ügyben már viszonylag hamar – ez nem meglepő, hiszen az üzemzavar okozta gondok szinte azonnal jelentkeztek a rendelőkben – kommentálta az illetékes hivatal, ám mint kiderült, valószínűleg ismét emberi hanyagság okozta a gondot, de a történet szerencsésen végződött: „Mint minden módosítás előtt, úgy e program fejlesztését megelőzően sor került tesztelésre, ám annak során a szoftver megfelelő eredményeket produkált. Ugyanakkor a hiba végleges adatvesztést nem okozott, okozhatott, hiszen az adatbázisról folyamatos biztonsági mentés készül.” [24]

A végleges vizsgálati jelentés szerint (ld. Ügyfélkapuról szóló vizsgálati jelentés): „…közvetlen felelősség terheli az OEP és a Fejlesztő által delegált mindkét projektvezetőt, és közvetett felelősség terheli a Projektben részt vevő valamennyi munkatársat”. A jövőt

érintően megállapítja a jelentés, hogy: „létrejött a programrendszer fejlesztéséhez elengedhetetlen OEP-en belüli tesztkörnyezet, ám a valóban elvárható teljes funkcionalitású, minden külső kapcsolattal is rendelkező, »éles« tesztrendszer a mai napig nem került kiépítésre”, s az évek során felhalmozódott komoly lemaradásokra figyelmeztet.

Minősített adatokat kezelő rendszerrel kapcsolatos incidens mindeddig nem került napvilágra Magyarországon.

1.5 Elvárt védelmi intézkedések a kritikus alkalmazásokban

A különböző biztonsági szintekre vonatkozó műszaki követelményeket a KIB 28. ajánlás „IT biztonsági műszaki követelmények a különböző biztonsági szintekre” című dokumentuma írja le. [25] Ebben a KIB 25. ajánlás alapjául is szolgáló ISO 27002 és ISO 15408 (Common Criteria) szabványok bizonyos elemeit rendelik az egyes biztonsági szintekhez. [26]

Az ISO 27002 elsősorban szervezeti biztonsági szabályokkal, illetve üzemeltetési követelményekkel foglalkozik, közvetlenül az alkalmazásokra nincs olyan funkcionális követelmény, ami a Common Criteria-ból ne lenne levezethető. A CC két részre tagolódik, egyrészt garanciális követelményeket szab a fejlesztés menetére vonatkozóan, másrészt funkcionális követelmények olvashatók ki belőle. [27] Jelen értekezés tárgya a közigazgatási rendszerek biztonsága, ezen belül jelen fejezet a funkcionális biztonsággal foglalkozik. **Ezért a következőkben a KIB 28. ajánlás alkalmazásokra vonatkozó funkcionális követelményeit elemzem**.

Az ajánlás az alábbi funkcionális osztályokkal foglalkozik, az alábbi meghatározásokkal:

Biztonsági naplózás FAU

A biztonsági naplózás velejárója a biztonsági tevékenységekhez kapcsolódó információk észlelése, rögzítése, tárolása és vizsgálata. Az ilyen tevékenységek napló rekordokat állítanak elő, amelyeket át lehet vizsgálni biztonsági szempontból. Az osztály olyan családokból áll, amelyek egyebek között követelményeket definiálnak a naplózható események kiválasztására, a napló rekordok vizsgálatára, azok védelmére és tárolására.

Kriptográfiai támogatás FCS

Ezt az osztályt akkor lehet alkalmazni, ha az értékelés tárgya kriptográfiai funkciókat is megvalósít. Ezek a funkciók felhasználhatók például kommunikáció támogatására, azonosításra és hitelesítésre, adatok elkülönítésére. Az osztály két családja a kriptográfiai kulcsok működtetés közbeni használatát, illetve menedzselését fedi le.

Felhasználói adatok védelme FDP

Ez az osztály olyan családokat tartalmaz, amelyek a felhasználói adatok védelmével kapcsolatos követelményeket határoznak meg. A családok az értékelés tárgyán belüli adatokkal foglalkoznak azok importálása, exportálás és tárolása során, valamint a felhasználói adatokhoz tartozó biztonsági jellemzőkkel kapcsolatosak

Azonosítás és hitelesítés FIA

Az azonosításra és hitelesítésre vonatkozó követelmények a jogosult felhasználók egyértelmű azonosítását és a biztonsági jellemzőknek a felhasználókkal és alanyokkal való pontos összekapcsolását biztosítják. Ezen osztályban a családok a felhasználói azonosítók meghatározásával és ellenőrzésével, az értékelés tárgyával való kölcsönhatás jogosultságának meghatározásával, valamint a biztonsági jellemzőknek a jogosult felhasználókkal való pontos összekapcsolásával foglalkoznak.

Biztonságkezelés FMT

Ez az osztály arra szolgál, hogy meghatározza az értékelés tárgyának biztonsági funkcióira vonatkozó biztonsági jellemzők, adatok és funkciók menedzsmentjét. Különböző menedzsment szerepkörök és ezek kölcsönhatása definiálható, mint pl. a képességek szétválasztása. Ez az osztály szolgál a többi funkcionális osztály menedzselési szempontjainak lefedésére is.

Az értékelés tárgya biztonsági funkcióinak védelme FPT

Ez az osztály az értékelés tárgyának biztonsági funkciói adatainak a védelmére koncentrál elsősorban, s nem a felhasználói adatokéra. Az osztály az értékelés tárgyának biztonsági funkcióira vonatkozó mechanizmusok és adatok sértetlenségére és menedzselésére vonatkozik.

Erőforrás-felhasználás FRU

Az erőforrás-felhasználás három családot tartalmaz, melyek az igényelt erőforrások rendelkezésre állását biztosítják, (pl. feldolgozó kapacitás, tároló kapacitás). A családok a hibatűrésre, a szolgáltatások prioritására, illetve az erőforrások lefoglalására nézve részletezik a követelményeket.

Az értékelés tárgyához való hozzáférés FTA

Ez az osztály az azonosításra és hitelesítésre megadottakon kívül további funkcionális követelményeket határoz meg egy felhasználói aktív munkaszakasz létrehozásának szabályozására. Az értékelés tárgyához való hozzáférési követelmények olyanokat szabályoznak, mint a felhasználói aktív szakaszok számának és hatókörének korlátozása, a korábbi hozzáférések megjelenítése, a hozzáférési paraméterek módosítása.

Bizalmi elérési út/csatornák FTP

Ez az osztály megbízható kommunikációs útvonalakkal foglalkozik a felhasználók és a biztonsági funkciók között, illetve különböző, az értékelés tárgyában megvalósított biztonsági funkciók között. A megbízható útvonalak eszközt biztosítanak a felhasználónak ahhoz, hogy a biztonsági funkciókat közvetlenül aktivizálják. A felhasználó vagy a biztonsági funkció kezdeményezheti az adatcserét, s ez a csere garantáltan védett a nem megbízható alkalmazások módosításaival szemben

A KIB 28. ajánlás ezen részének egyik vitatható pontja, hogy a követelmények előírása jógyakorlat alapján történt, azaz nem bizonyítható, hogy valóban releváns kockázatokra jelentenek védelmi intézkedéseket. Nem követhető benne továbbá a Common Criteria logikája, mely a fenyegetések, feltételezések és szervezetbiztonsági szabályokból vezet le ún. biztonsági célokat, melyekből a funkcionális követelmények következnek. Az értekezés korábbi szakaszában kidolgozásra kerültek azok a fenyegetések, feltételezések és szervezetbiztonsági szabályok, melyek a közigazgatási alkalmazások esetén valósak lehetnek. **A következőkben felsorolom az ezekhez tartozó biztonsági célokat, amelyekkel ellenőrizni lehet, hogy a KIB 28. ajánlás valóban a megfelelő funkcionális követelmény-halmazt rendelte-e a különböző biztonsági szintekhez.** A Common Criteria szabályai szerint a feltételezések környezeti biztonsági célokkal oldhatók meg, a fenyegetések és a szervezetbiztonsági szabályok környezeti és alkalmazásban implementált megoldásokkal is. A környezeti biztonsági célok OE (Objective of Environment) rövidítéssel kezdődnek, és nem az alkalmazásban kerülnek implementálásra. Az alkalmazásra vonatkozó biztonsági célok O (Objective) rövidítéssel kezdődnek, és az alkalmazásban meg kell ezeket valósítani.

A műszaki hibák során két feltételezés került leírásra, mely a hibatűrő működést és a megfelelő üzemeltetést írta elő. **Ezekből két környezeti biztonsági célt fogalmazok meg**.

- **OE.FAILSAFE**: Az alkalmazást hibatűrő infrastruktúrán kell futtatni.

- **OE.OPERATION**: Olyan informatikai infrastruktúrát kell kialakítani, mely kikényszeríti a jogszabályokban, szabványokban és belső utasításokban foglalt üzemeltetési eljárásokat.

A jogosult felhasználót érintő incidenseknél két kockázatot találtunk. Egyrészt az alkalmazás helytelen használatából eredő hibákat, másrészt a nem biztonságos felhasználói oldalt lehetett megemlíteni. **Erre több környezeti és alkalmazásra vonatkozó biztonsági célt is meg tudok fogalmazni**.

- **O.LEAST_PRIVILAGE**: A felhasználói tevékenységnél érvényesülnie kell a legkisebb jogosultság elvének.
- **O.IDENTITY:** A felhasználóknak egyedi azonosítóval kell rendelkezniük.
- **O.AUTHENTICATION**: A felhasználóknak hitelesíteniük kell magukat az alkalmazásban.
- **O.ROLE**: A felhasználókhoz szerepköröket kell rendelni a legkisebb jogosultság elvének kikényszerítéséhez.
- **O.FOUR_EYE**: Bizonyos biztonsági értelemben vett kritikus információkkal való folyamatok esetén a négy szem elvet kell érvényesíteni.
- **OE.MALWARE**: A kártékony kódok kiszűrése érdekében vírusvédelmi rendszert kell üzemeltetni.
- **OE.BOUNDARY_PROTECTION**: Az alkalmazás környezetében határvédelmi rendszert kell üzemeltetni.

A belső felhasználók és egyes kibertámadások az érzékeny információk kiszivárgására figyelmeztetnek. **Erre a problémára az előző biztonsági célok mellett a következő célokat tudom megfogalmazni**.

- **O.RBAC**: Az adatokhoz szerepkör alapon kell hozzáférést biztosítani.
- **O.LOG**: Naplózni kell a biztonságilag kritikus adathozzáféréseket.
- **OE.LOG_MANAGEMENT**: A keletkezett naplóadatokat biztonságos körülmények között kell kezelni.
- **OE.DLP**: Adatszivárgást meggátló megoldást kell alkalmazni az informatikai környezetben.

A kiberfenyegetések sajátja még az, hogy megpróbálják elérhetetlenné tenni a szolgáltatást. Ezt a problémát nem az alkalmazásnak kell kezelnie, megoldást a hibatűrésre vonatkozó korábbi biztonsági cél jelent. Szintén a korábbiakban javasolt környezeti biztonsági célok adnak választ a hardverekkel és a hálózattal kapcsolatos feltételezésekre, kiegészítve egy újjal. **A virtualizáció jelentette kockázatra, valamint a tanúsított rendszerekre vonatkozó feltételezésre a következő környezeti biztonsági célokat vonatkoztatom.**

- **OE.PHYSICAL:** Megfelelően biztonságos fizikai környezetet kell létrehozni az alkalmazás üzemeltetésére.
- **OE.SECURE_CONFIG**: A rendszer elemeit a Common Criteria vagy más gyártói biztonsági ajánlás szerint kell konfigurálni.

A 223/2009 Korm. rendelet behoz néhány funkcionális követelményt, amelyet a korábbi célok nem kezeltek. **Ezért a következő célokkal egészítem ki a felsorolást**.

- **OE.SSL**: Nyilvános hálózaton történő adatcsere esetén titkosított adatkapcsolatot kell felépíteni.
- **O.ENCRYPT**: Amennyiben a rendszer határain kívül kerülő adatok nem titkosított adatcsatornán jutnak el a célhoz, a nyílt hálózatokon közlekedő adatokat titkosítani kell.
- **OE.KEY**: A titkosításra használt kulcsokat biztonságosan kell kezelni.
- **OE.BACKUP**: Az alkalmazásban tárolt adatokat rendszeresen menteni kell.

A web service technológiából eredő fenyegetéseket egy korábban említett környezeti (alkalmazástűzfal) és egy alkalmazás-biztonsági céllal lehet ideálisan kezelni. Ezek megoldást nyújtanak több alkalmazás szintű támadási móddal szemben is.

- **O.INPUT_VALIDATION**: Az alkalmazás interfészeinek bejövő adatait biztonsági szempontból szűrni kell.

A social engineering támadás ellen kritikus információkhoz való hozzáférés esetében az erős authentikáció jelent kielégítő megoldást.

- **O.STRONG_AUTHENTICATION**: Bizonyos adatkörök elérésénél legyen erős authentikáció.

Az OWASP Top 10-ben felsorolt támadási módok közül az előzőekben felsorol biztonsági célok védelmet nyújtanak, kivéve a session kezeléssel kapcsolatos hibát.

OE.SESSION: Megfelelő session kezelést kell megvalósítani.

Az 1. számú mellékletben található táblázatokban bemutatom a fenyegetések, feltételezések és szervezetbiztonsági szabályok összerendelését a biztonsági célokkal, a Common Criteria által elvárt formában.

Ha megvizsgáljuk, hogy a KIB 28. ajánlás előírásaiból mit kell az alkalmazásban megvalósítani, akkor a következő osztályok maradtak:

- Biztonsági naplózás FAU;
- Kriptográfiai támogatás FCS;
- Felhasználói adatok védelme FDP;
- Azonosítás és hitelesítés FIA.

Valamint a függőségek miatt környezeti célként valósul meg:

- Biztonságkezelés FMT;
- Az értékelés tárgya biztonsági funkcióinak védelme FPT;
- Az Erőforrás felhasználás FRU;
- Az értékelés tárgyához való hozzáférés FTA;
- és a Bizalmi elérési út/csatornák FTP.

1.6 A magyar e-közigazgatási alkalmazások javasolt Védelmi Profil eszköztára

Az előző alfejezetekben bemutattam a közigazgatási alkalmazásokra vonatkozó fenyegetéseket, feltételezéseket és szervezetbiztonsági szabályokat, valamint az ezekből következő biztonsági célokat. **Meghatároztam** továbbá három biztonsági szintet, amelyeken belül a biztonsági célokhoz tartozó minimális funkcionális követelményeket kell kijelölni a Common Criteria 2. kötetéből. [28] **Ezzel elkészítettem az elektronikus közigazgatási szolgáltatások Védelmi Profiljának alapelemeit, amire a specifikus alkalmazások Biztonsági Előirányzatait alapozni lehet**.

Ezek a funkcionális követelmények kiolvashatók a KIB 28. már többször hivatkozott részéből, ám az ott vázolt előírásokat a gyakorlati tapasztalat alapján felül kell vizsgálni, továbbá szükséges a Common Criteria terminológiára átfordítani. **Az előző alfejezetben szétválogattam a környezeti infrastruktúra és az alkalmazás által megoldandó**

feladatokat. Ezzel a KIB 28. előírásainak nagyobb részét környezeti előírásként sikerült azonosítanom.

Ennek oka az, hogy a modern, Magyarországon elterjedt közigazgatási rendszerfejlesztés elsősorban keretrendszerekre épül. Ezeknek sajátossága, hogy a legtöbb biztonsági funkciót nem kell külön lefejleszteni, csak valamilyen konfiguráció során a fejlesztő felhasználja ezeket. Ezek a funkciók alkotják a Common Criteria szerinti Értékelés Tárgyát, hiszen felhasználásuk egyedi. Tipikusan ide tartoznak az azonosítás és hitelesítés, a jogosultságkezelés és a naplózás területei. Más biztonsági funkciók a fejlesztők számára láthatatlanok, sem fejlesztés, sem konfigurálás nem szükséges. Pl. a biztonságos adatutak kérdését vagy a session kezelést lehet ide sorolni. Ezekben az esetekben a keretrendszerek Common Criteria szerinti, a gyártó által létrehozott útmutatói írják le a biztonságos használat módját. **A továbbiakban tehát definícióm szerint azokat a biztonsági funkciókat kell az Értékelés Tárgya alatt érteni, melyek egyedi fejlesztésűek vagy egy keretrendszer biztonsági funkcióinak egyedi testre szabása után jöttek létre.**

A Common Criteria a magyar közigazgatási ajánlások között a KIB 25. ajánlásban jelenik meg. Ez azonban még csak a CC 2.3 verziót foglalja össze, miközben a hivatalos változat már a 3.1 Release 3 verziónál tart. Jelen értekezésben ez utóbbit használom, mert több funkcionális követelmény esetén életszerűbb megfogalmazást található benne.

Elsőként a naplózásra vonatkozó FAU osztály követelményeit veszem sorra. A KIB 28. számos naplózást szabályozó követelményt támaszt, ezek nagy része azonban a naplóbejegyzések menedzsmentjére, megőrzésére vonatkoznak. A modern közigazgatási rendszerek a naplómenedzsmentet külső célalkalmazással, ún. központi naplózóval oldják meg. Ez dobozos termékként nem része az Értékelés Tárgyának, így a Védelmi Profilba sem kerülnek be a funkciói. A közigazgatási alkalmazás naplózással kapcsolatos feladata mindössze annyi, hogy a naplóbejegyzéseket a kívánt tartalommal létrehozza.

FAU_GEN.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak naplóbejegyzéseket kell tudnia előállítani a következő átvilágítási eseményekből:

a) A naplózási funkciók inicializációja és leállítása;

b) Minden naplózandó esemény (*minimális, alap, részletes)* naplózási szinten;

A három biztonsági szint három különböző naplózási szintet kíván meg. **Meghatározásom szerint** alap biztonsági szinten minimális, fokozott szinten alap, kiemelt szinten részletes naplózás szükséges, ami az adatszivárgási kockázatból, illetve annak esetleges

észrevétlenségéből ered. A naplózandó események köre egyenesen következik a Common Criteria szabványból, hiszen a biztonsági funkcionális követelmények mindegyikéhez hozzá vannak rendelve a szintek naplózási követelményei.

FAU_GEN.1.2 Az Értékelés Tárgya Biztonsági Funkcióinak minden egyes naplóbejegyzésen belül legalább a következő információkat szükséges rögzítenie:

a) Az esemény időpontját és dátumát, az esemény fajtáját, a szubjektum azonosítóját (ha ez lehetséges), valamint az esemény kimenetelét (sikeres vagy sikertelen), és

b) Mindenegyes naplóbejegyzés esetében, amely a Védelmi Profilban található funkcionális összetevők naplóbejegyzéseinek meghatározásain alapszik, *naplózni kell az esemény forrásának azonosítóját és a bejegyzés súlyát.*

Ez az általam kiegészített előírás a naplóbejegyzés tartalmát határozza meg oly módon, hogy egy naplóelemző rendszerben egyszerűen feldolgozható legyen.

FCS_CKM.4.1 Az Értékelés Tárgya Biztonsági Funkcióinak meg kell semmisítenie a kriptográfiai kulcsot azzal a kulcsmegsemmisítési eljárással, *melyet a Nemzeti Média és Hírközlési Hatóság, minősített adatok esetén a Nemzeti Biztonsági Felügyelet előír.*

FCS_COP.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak *végre kell hajtania a kiküldött adat titkosítását, amennyiben az nyilvános hálózaton, nem titkosított csatornában közlekedik. Mindezt a Nemzeti Média és Hírközlési Hatóság, minősített adatok esetén a Nemzeti Biztonsági Felügyelet által előírt kriptográfiai algoritmussal kell végrehajtania.*

Az általam meghatározott két utóbbi követelményt akkor kell használni, ha egy adatot titkosítva kell a rendszer határain kívülre küldeni. Kiemelt fokozatnál a Nemzeti Biztonsági Felügyelet előírásai szerint kell cselekedni.

FDP_ACC.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak érvényesítenie kell a *rendszer* hozzáférés-ellenőrzési szabályzatát *az ott leírt* szubjektumok és objektumok listáján *és minden műveletet a hozzáférés-ellenőrzési politika által tartalmazott szubjektumok és objektumok között*.

Alap és fokozott esetben a dőlt betűk nélküli részt, kiemelt esetben a dőlt betűkkel együttes szöveget **tartom fontosnak használni**, FDP_ACC.2.1 megnevezéssel.

FDP_ACC.2.2 Az Értékelés Tárgya Biztonsági Funkcióinak biztosítania kell, hogy az Értékelés Tárgya Biztonsági Funkciói által ellenőrzött bármely szubjektum és bármely objektum közötti valamennyi műveletre legyen egy hozzáférés-vezérlési politika.

E két előírás rendelkezik arról, hogy legyen valamilyen hozzáférési szabályzat implementálva a rendszerben. A közigazgatáson belüli bonyolult hozzáférések miatt ez tipikusan valamilyen szerepkör alapú hozzáférés (role base access control) egy hozzáférési mátrixban ábrázolva. Jellemzően a keretrendszerek ezt a funkciót nem tudják megvalósítani, így ez döntően egyedi fejlesztésű szokott lenni. Alap és fokozott esetben csak az első előírást kell figyelembe venni, kiemelt esetben azonban mindkettőt. Ezzel kontrollálható az adatszivárgás. Amennyiben kiemelt esetben a szerepkör alapú hozzáférés nem lenne elégséges, lehetséges a Bell-LaPadula modell alapján leírt kötelező hozzáférési modell (Mandatory Access Control) használata is.

FDP_ACF.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak a *hozzáférési szabályokban leírt* objektumok és szubjektumok biztonsági attribútumai alapján kell megvalósítaniuk a hozzáférés-vezérlést.

FDP_ACF.1.2 Az Értékelés Tárgya Biztonsági Funkcióinak a *hozzáférési szabályokban leírt* szabályrendszer felhasználásával kell dönteniük, hogy az ellenőrzése alatt lévő objektumok és szubjektumok közötti művelet megengedett.

FDP_ACF.1.3 Az Értékelés Tárgya Biztonsági Funkcióinak a *hozzáférési szabályokban* meghatározott szabályok alapján kell explicit engedélyeznie a hozzáférést a szubjektumoknak az objektumokon.

FDP_ACF.1.4 Az Értékelés Tárgya Biztonsági Funkcióinak a *hozzáférési szabályokban* meghatározott szabályok alapján kell explicit tiltania a hozzáférést a szubjektumoknak az objektumokon.

Az előző négy előírással a szerepkör alapú hozzáférés folyamatát írtam le, melynek segítségével a rendszer egy felhasználóhoz rendelt szerepkör alapján dönt arról, hogy a hozzáférés engedélyezett vagy nem.

FDP_ETC.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak érvényesíteni kell a *hozzáférési szabályokban leírtakat*, amikor a felhasználói adatok exportja a Biztonsági Funkcionális Szabályzat ellenőrzése alatt, az Értékelés Tárgya Biztonsági Hatókörén kívülre történik.

FDP_ETC.1.2 Az Értékelés Tárgya Biztonsági Funkcióinak a felhasználói adatokat a felhasználói adatokhoz kapcsolódó biztonsági attribútumok nélkül/*attribútumokkal együtt* kell exportálnia.

FDP_ETC.2.3 Az Értékelés Tárgya Biztonsági Funkcióinak biztosítania kell, hogy a biztonsági attribútumok, az Értékelés Tárgya Biztonsági Funkcióin kívülre történő exportálásánál, egyértelműen kapcsolódjanak az exportált felhasználói adatokhoz.

FDP_ETC.2.4 Az Értékelés Tárgya Biztonsági Funkcióinak *nem kell további szabályokat* érvényesíteni, amikor felhasználói adatok kerülnek exportálásra az Értékelés Tárgya Biztonsági Hatóköréből.

Alap és fokozott biztonsági szinten az első két követelmény, kiemelt szinten mind a négy követelmény, a másodikban levő dőlt betűs résszel teljesítendő. Az első két követelmény FDP_ETC.2.1 és FDP_ETC.2.2 néven található meg. **Ezekben határoztam meg** az adatexportálás folyamatát, kiemelt szinten az adatszivárgás megelőzése érdekében úgy, hogy az adathoz az exportáló felhasználói azonosítója elválaszthatatlanul kapcsolódik.

FDP_ITC.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak érvényre kell juttatnia a *hozzáférési szabályokban leírtakat* a felhasználói adatok Értékelés Tárgya Biztonsági Hatókörén kívülről, a Biztonsági Funkcionális Szabályzat ellenőrzése mellett történő importálásakor.

FDP_ITC.1.2 Az Értékelés Tárgya Biztonsági Funkcióinak figyelmen kívül kell hagynia bármely olyan biztonsági attribútumot, amely kapcsolatban áll a felhasználói adatokkal az Értékelés Tárgya Biztonsági Hatókörén kívülről való importáláskor.

FDP_ITC.1.3 Az Értékelés Tárgya Biztonsági Funkcióinak *a felhasználói felületen keresztül történő adatbevitel és a gépi interfészen történő adatbevitel során inputvalidálást kell végrehajtania a gyakori, felhasználói felületen keresztül elkövetett támadások elkerülésének érdekében.*

Biztonsági szempontból az egyik legfontosabb előírás, hiszen napjaink modern, alkalmazásszintű támadástípusait hivatott kivédeni **ez az általam előírt követelményhalmaz.** Mindhárom biztonsági szinten alapvető elvárás, de a környezetben egy alkalmazástűzfal használatával FDP_ITC.1.3 gyengíthető.

FIA_AFL.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak észlelnie kell, amikor *a rendszer belépési felületén 3* sikertelen hitelesítési próbálkozás fordul elő.

FIA_AFL.1.2 Amikor a sikertelen hitelesítési próbálkozások száma eléri vagy meghaladja ezt a számot, az Értékelés Tárgya Biztonsági Funkcióinak *alap biztonsági esetben*

fel kell függesztenie a felhasználói hozzáférést, fokozott és kiemelt esetben nagy prioritású naplóbejegyzést kell előállítania és fel kell függesztenie a felhasználói hozzáférést.

Bár a felhasználói fiókok felfüggesztése kockázatos döntés, alap esetben a felhasználónak komoly érdeksérelme nem származik belőle, így **álláspontom szerint** elfogadható. Fokozott és kiemelt esetben a három elrontott authentikációs kísérlet mindenképpen jelzésértékű, így azonnal értesíteni kell a biztonsági adminisztrátort, és kivizsgálásig fel kell függeszteni a hozzáférést.

FIA_ATD.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak karban kell tartania a *hozzáférési szabályokban leírt* biztonsági attribútumlistát, amely különálló felhasználókhoz tartozik.

Ezzel a követelménnyel lehetővé válik az, hogy a felhasználókhoz pl. jelszavakat lehessen rendelni. Minden biztonsági szinten azonos.

FIA_SOS.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak ellenőrizni kell, hogy az objektumokhoz való kapcsolódáshoz szükséges hitelesítési adatok megfelelnek-e a mindenkori jelszópolitika követelményeinek: *legalább 8 karakter hosszú, kis és nagybetűt, számot tartalmazó jelszavak, olyanok, amik nem kapcsolhatóak a felhasználóhoz, nincsenek benne egy szótárban sem. Amennyiben a szervezet szabályaiból további követelmények adódnak, azokat is alkalmazni kell.*

FIA_SOS.2.1 Az Értékelés Tárgya Biztonsági Funkciói lehetőséget biztosítanak titkok generálására, amelyek megfelelnek a mindenkori jelszópolitika követelményeinek: *legalább 8 karakter hosszú, kis és nagybetűt, számot tartalmazó jelszavak, olyanok, amik nem kapcsolhatóak a felhasználóhoz, nincsenek benne egy szótárban sem. Amennyiben a szervezet szabályaiból további követelmények adódnak, azokat is alkalmazni kell.*

FIA_SOS.2.2 Az Értékelés Tárgya Biztonsági Funkcióinak ki kell kényszerítenie a hitelesítési adatok használatát *az anonim felületeken kívül minden* egyes objektumhoz való kapcsolódás során.

A szerepkörök hozzárendelése és a jelszavak kezelése gyakran külső, ún. identitásmenedzsment rendszerben történik, de szemben a naplózással, még mindig gyakori, hogy a felhasználók és azok authentikációs adatainak kezelése az alkalmazás felületén történik, ezért ezeket a követelményeket **szerepeltetem a Védelmi Profil eszköztárban**. Központi identitásmenedzsment rendszer használata esetén elhagyható. A jelszóhossz

meghatározása minden biztonsági szint esetén azonos, a különbséget a később meghatározandó erős authentikáció jelenti.

FIA_UAU.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak a sikeres hitelesítés előtt lehetővé kell tennie *a rendszer esetlegesen anonim módon használható felületeinek* elérését a felhasználók számára.

FIA_UAU.1.2 Az Értékelés Tárgya Biztonsági Funkcióinak ellenőriznie kell, hogy minden egyes felhasználó sikeresen hitelesítve lett, mielőtt hitelesítéshez kötött funkciót engedélyeznének a felhasználónak.

Ezzel a követelménnyel válik engedélyezetté az, hogy bizonyos funkciókhoz, mint például nyilvános információk elérése, űrlapok letöltése, stb. ne kelljen a felhasználónak hitelesítenie magát. **Ezt csak az alap biztonsági szinten tartom megengedhetőnek**. Fokozott és kiemelt szinten csak a második követelmény érvényes FIA_UAU.2.1 néven.

FIA_UAU.5.1 Az Értékelés Tárgya Biztonsági Funkcióinak biztosítania kell *az SMS-ben érkező egyszeri jelszó alapú / tanúsítvány alapú erős authentikációt* a felhasználói hitelesítés támogatásához.

FIA_UAU.5.2 Az Értékelés Tárgya Biztonsági Funkcióinak *erős authentikációt* kell alkalmaznia minden olyan esetben, amikor *az adat elérése valamilyen értelemben kockázatot jelent.*

Az erős authentikáció követelményét mindhárom biztonsági szinten indokoltnak tartom. Az alap szint esetében tipikusan egy SMS alapú megoldás jöhet szóba, hiszen az elv az, hogy ez a megoldás az állampolgárok számára plusz költséget nem jelenthet. Más esetekben a tanúsítvány alapú authentikáció lehet jó megoldás, kiemelt szinten ez kötelező előírás.

FIA_UAU.7.1 Az Értékelés Tárgya Biztonsági Funkcióinak csak a *felhasználói bejelentkezési képernyőt szabad* biztosítania a felhasználó számára, mialatt a hitelesítés folyamatban van, *oly módon, hogy hibás bejelentkezési kísérletekről csak egyszerű hibajelzést szabad visszaadni*.

Ezzel a követelménnyel közvetve T.INFO_LEAKAGE fenyegetésre adok választ.

FIA_UID.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak lehetővé kell tennie a *rendszer anonim felhasználói felületeihez való hozzáférést* a felhasználó nevében, mielőtt a felhasználó azonosítása megtörténik.

FIA_UID.1.2 Az Értékelés Tárgya Biztonsági Funkcióinak meg kell követelni minden egyes felhasználó sikeres azonosítását, mielőtt bármelyik másik, az Értékelés Tárgya Biztonsági Funkciói által közvetített tevékenységet engedélyez annak a felhasználónak a nevében.

Alapértelmezésben minden olyan felhasználó azonosításra kerül, aki interakciót kezdeményez a közigazgatási rendszerekkel, hiszen IP címe naplózásra kerül, így visszakövethetővé válik. Elképzelhető azonban olyan eset, amikor még ezt az azonosítást sem lehet megtenni a felhasználó anonimitása érdekében (pl. bűnügyi bejelentő rendszer). Ez csak az alap szint esetében képzelhető el, fokozott és kiemelt esetben a második követelmény FIA_UID.2.1 néven érvényes.

FMT_MOF.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak korlátoznia kell a *jelen Védelmi Profilban megjelölt Biztonsági Funkciókat megvalósító funkciók* kikapcsolásának, bekapcsolásának és viselkedésének módosítási képességét *a szervezet által kijelölt biztonsági szerepköröket betöltő felhasználók számára, az ott meghatározott módon.*

Az alkalmazás biztonsági üzemeltetésének a szervezet szabályait kell leképeznie.

FMT_MSA.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak érvényre kell juttatnia a *hozzáférési szabályzatban leírt szabályokat*, hogy korlátozzák a *lekérdezési, módosítási, törlési* képességet a biztonsági attribútumok *hozzáférési szabályzatban leírt szerepkörökre*.

FMT_MSA.2.1 Az Értékelés Tárgya Biztonsági Funkcióinak biztosítania kell, hogy csak biztonságos értékek kerüljenek elfogadásra a biztonsági attribútumok esetén.

FMT_MSA.3.1 Az Értékelés Tárgya Biztonsági Funkcióinak ki kell kényszerítenie a *hozzáférési szabályzatban leírtakat* azért, hogy biztosítva legyenek azon *engedélyező* alapértelmezett értékek a biztonsági attribútumok számára, amelyek a hozzáférési szabályzat végrehajtásakor használatosak.

FMT_MSA.3.2 Az Értékelés Tárgya Biztonsági Funkcióinak lehetővé kell tennie a *szervezet szabályzataiban leírt szerepkörök* számára azt, hogy az alapértelmezett értékeket felülírják egy másik kezdeti értékkel, amikor egy objektumot vagy információt hoznak létre.

Ezekkel a követelményekkel azt várom el, hogy az e-közigazgatási alkalmazás biztonsági funkciói esetén legyenek meghatározva biztonságos alapértelmezett értékek. A

keretrendszerben történő fejlesztés során a gyártó általában segíti a fejlesztőt ilyenekkel, de amennyiben ez nem áll rendelkezésre, a fejlesztőnek kell meghatároznia. A követelmények arról is rendelkeznek, hogy ezeket az értékeket csak indokolt esetben és csak az arra jogosultak változtathatják meg. Egy példa lehet erre például a jogosultsági szabályok átállítása.

FMT_MTD.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak korlátoznia kell az *alapértelmezés változtatási, lekérdezési, módosítási, törlési, megtisztítási* képességet a *szervezet szabályzataiban leírtaknak megfelelően*.

Ezzel a követelménnyel az előzőekben leírt alapértelmezett értékek után minden más, biztonsági funkciót befolyásoló érték beállítási lehetőségét jogosultsághoz kötöttem.

FMT_SMF.1.1 Az Értékelés Tárgya Biztonsági Funkciói a következő menedzsment funkciók végrehajtására képesek: *az alkalmazás kiválasztott biztonsági funkcióinak Common Criteria-ból eredő menedzsment funkciói.*

Ez a követelmény – hasonlóan a naplózáshoz – automatikusan adódik a Védelmi Profilba beválasztott biztonsági funkcionális követelményekből. Az FMT követelmények eddig a pontig bezárólag minden biztonsági szinten azonosak.

FMT_SMR.2.1 Az Értékelés Tárgya Biztonsági Funkcióinak karban kell tartania a *szervezet szabályzataiban szereplő* szerepeket.

FMT_SMR.2.2 Az Értékelés Tárgya Biztonsági Funkciói legyenek képesek összekapcsolni a felhasználókat szerepekkel.

FMT_SMR.2.3 Az Értékelés Tárgya Biztonsági Funkcióinak biztosítania kell, hogy a *szervezet szabályzataiban leírt kizárási* feltételek ki legyenek elégítve.

Az SMR család segítségével válik lehetővé a felhasználók szerepkörökhöz rendelése.

FPT_STM.1.1 Az Értékelés Tárgya Biztonsági Funkcióinak képesnek kell lenni megbízható időbélyegeket biztosítani saját felhasználás számára.

Ez az igény a megbízható naplózásból ered, így biztosítható, hogy minden rendszerelem azonos időinformációval rendelkezik, így egy incidens időbelisége követhetővé válik.

A biztonsági célok és a funkcionális biztonsági követelmények összerendelését a 2. mellékletben mutatom be. Szintén itt mutatom be azt, hogy az értekezésben javasolt

biztonsági szintek, valamint a KIB 28. előírásai hogyan és mennyire kapcsolódnak egymáshoz.

1.7 Következtetések

A fejezetben elvégzett vizsgálatok alapján megállapítottam, hogy az elmúlt 40 évben **a központi közigazgatás bázisa lényegében változatlan**, a nagyméretű adatbázisok és nyilvántartások jelentik a legfontosabb elemeket. Megállapítottam továbbá azt, hogy **a közigazgatási informatika Magyarországon erősen centralizált, helyi szinten nincsen jelentős informatikai rendszer**. A technikai környezet azonban folyamatosan változik, így az új kihívások miatt a közigazgatási rendszerek fejlesztésének és üzemeltetésének biztonsági filozófiája és ebből következő szabályozása jelentős újragondolásra szorul. Több forrás összevetésével **meghatároztam a védendő intézmények körét**, szigorúan az e-közigazgatásra koncentrálva.

A fejezetben áttekintettem azokat a jogszabályokat, melyek valamilyen módon érintik az információbiztonság szabályozását az értekezés írásának időpontjában, valamint ezek hiányosságaiból kiindulva **javaslatot tettem bizonyos biztonsági elvek törvénybe vagy rendeletbe iktatására**. Álláspontom szerint a legfontosabb közigazgatás rendszerek köre, amikre kiemelt védelmet kell biztosítani, a következő évtizedekben jelentősen nem fog változni.

Az e-közigazgatási stratégia és a már működő rendszerek alapján **kiemeltem a komplex magyar e-kormányzati infrastruktúra néhány műszaki jellegzetességét**. A tervezett technológia ismeretében **felsoroltam a releváns fenyegetéseket**, melyeket egy általam kidolgozott szisztéma szerint építettem fel. Ezekből kiindulva **javaslatot tettem egy Common Criteria szerinti Védelmi Profil eszköztárra**, annak felépítését és formalizmusát követve.

Az értekezésben ezt segítendő **három védelmi szintet határoztam meg**, melyek összehangolhatók a magyar ajánlásokban leírt biztonsági szintekkel. A védelmi szintek esetében a hangsúlyok eltérnek, ezért **meghatároztam a tipikus támadási motivációkat**, valamint ebből kiindulva egy-egy példával alátámasztottam azt, hogy a három típusrendszert miért érdemes külön kezelni. **Felsoroltam a szintekhez tartozó biztonsági célokat**, mellyel ellenőriztem, hogy a KIB 28. ajánlás valóban a megfelelő funkcionális követelmény-halmazt rendelte a különböző biztonsági szintekhez.

Az első fejezetben **szétválogattam a környezeti infrastruktúra és az alkalmazás által megoldandó feladatok**. Ezzel a KIB 28. előírásainak nagyobb részét környezeti előírásként sikerült azonosítanom. Ajánlásom szerint azokat a biztonsági funkciókat kell az Értékelés Tárgya alatt érteni a magyar e-közigazgatási környezetben, melyek egyedi fejlesztésűek vagy egy keretrendszer biztonsági funkcióinak egyedi testre szabása után jöttek létre.

2. FEJEZET

ELEKTRONIKUS KÖZIGAZGATÁSI ALKALMAZÁSOK FEJLESZTÉSÉNEK SZERVEZETI ÉS SZABÁLYZATI KÖVETELMÉNYEI

Az előző fejezet arról szólt, hogyan lehet magát az alkalmazást biztonságosabbá tenni. Ebben a fejezetben a már korábban említett emberi faktorból eredő hibák valószínűségének csökkentésére teszek javaslatot. A gyakorlatban a már működő alkalmazásokat több helyen is védik a külső és belső támadókkal szemben. Kevés figyelem összpontosul azonban a fejlesztés alatt lévő programokra, ahol tulajdonképpen bármi bekerülhet a kódba, illetve minden olyan információ összegyűlik az alkalmazásról, mely akár egy működő rendszer biztonságát is alááshatja. Ennek ellenére nagyon ritkán foglalkoznak a fejlesztői környezet információbiztonsági vonatkozásaival.

A minősített adatokat kezelő rendszerek fejlesztőivel szemben ugyan vannak elvárások, de ez közel sem teljes, nem fed le minden biztonsági területet. A minősített adatot nem kezelő, de az állam működése szempontjából mégis kritikus informatikai rendszerekre viszont semmilyen előírás nincsen. Így nehezen lehet számon kérni a fejlesztőt is a saját környezetére vonatkozó biztonsági előírásokkal kapcsolatban.

Jelen fejezetben áttekintem a fejlesztési folyamat legfontosabb biztonsággal kapcsolatos tevékenységeit, valamint számos előírást javaslok az egyes biztonsági szinteken dolgozó fejlesztők adminisztratív, logikai és fizikai védelmi kontrolljaira. Külön kitérek a személyi követelményekre, a szerepkörökre és ezek felelősségeire.

2.1 A szoftverfejlesztés életciklusának biztonsági vonatkozásai

A szoftverfejlesztés biztonságát nagyon sokan – véleményem szerint tévesen – kizárólag azzal azonosítják, hogy az adott alkalmazás milyen biztonsági funkciókat valósít meg. A valóság azonban az, hogy emellett legalább annyira fontos, ha nem fontosabb, az a biztonságos alkalmazásfejlesztési folyamat, aminek mentén a szoftver elkészül. Az előző fejezetben példaként hozott e-közigazgatási rendszerhibák mind valamilyen kódban rejlő problémára voltak közvetlenül visszavezethetők, közvetve azonban a rendszer fejlesztőinek nem megfelelő eljárásai okozták ezeket. Ezért nagyon fontos, hogy egységes, számonkérhető fejlesztési folyamatok alakuljanak ki a közigazgatási rendszerek fejlesztésénél.

A KIB 25. ajánlásban foglalt Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma (MIBÉTS), illetve az alapjául szolgáló Common Criteria szabvány 3. kötete részletesen, különböző követelményszintek mellett leírja, hogy mi várható el a fejlesztőtől biztonsági szempontból. [29] [30] Ez azonban kizárólag a tervezési, fejlesztési és tesztelési fázisra terjed ki. A későbbiekben jelen értekezés erre koncentrál, de előtte látni kell egy szoftver életciklusának egészét, és benne az információbiztonság helyét is!

Az információbiztonságra már az alkalmazás első tervezéséi lépéseinél gondolni kell. Ezért bármilyen fejlesztési életciklus-modellt is használ a fejlesztő, a biztonsággal kapcsolatos lépéseket be kell építenie a modelljébe. Az egyes fejlesztési életciklus-modellek eltérő elnevezéssel ugyan, de általában az alábbi lépéseket tartalmazzák: Projektindítás és tervezés, Funkcionális követelmények meghatározása, Rendszertervezés, Fejlesztés és dokumentálás, Átvétel, Telepítés, Üzemeltetés és fenntartás, Átvizsgálás és kivonás. [31]

Projektindítás és tervezés

- A biztonsági igények felderítése:
    - Az alkalmazásban tárolt információk kritikusságának meghatározása
    - Alapvető biztonsági célok meghatározása
- Kezdeti kockázatelemzés
    - Fenyegetések/sérülékenységek/kockázatok
    - A védelmi intézkedések megvalósíthatóságának elemzése
    - A biztonsággal kapcsolatos költség/haszon elemzés elvégzése
- Biztonsági keretrendszer meghatározása

- Lényeges biztonsági kérdések és kockázatok
- A szolgáltatás-szint megállapodás (SLA) meghatározása

Funkcionális követelmények meghatározása

- Biztonsági feladatok a projekttervben
  - Konfigurációkezelés és hozzáférés-védelem a projekt végrehajtása során
  - Nyomonkövethetőség
- Biztonsági követelmények meghatározása
  - A kockázatelemzés alapján védelmi intézkedések meghatározása
- Előzetes biztonsági tesztelési terv
  - Tesztelési eljárások és erőforrások
  - Értékelési követelményrendszer meghatározása
- Biztonsági követelmények beépítése a pályázatokba és szerződésekbe
  - Az SLA szerződések tartalmazzák a biztonságot
  - Hardver- és szoftver-mentések, letétek
- A funkcionális alapkövetelmények tartalmazzák a biztonságot

Rendszertervezés

- Biztonsági specifikációk meghatározása
  - Rendszer/alrendszer/interfész
  - Alkalmazás/adatbázis/hardver és firmware/hálózat
- A biztonsági tesztelési terv finomítása
  - Biztonsági tesztelési eljárások kidolgozása
  - Biztonsági tesztelés abnormális és illegális körülmények között
- A biztonsági terület beillesztése a formális dokumentációba és a minőségbiztosításba

Fejlesztés és dokumentálás

- A biztonsággal kapcsolatos kód megírása és beillesztése
  - Hozzáférés-védelem a kódhoz

    - A kód dokumentálása
- A biztonsággal kapcsolatos kódok tesztelése és értékelése
- Annak ellenőrzése, hogy a jóváhagyott biztonsági komponensek megvalósultak-e

Elfogadás

- Biztonsági komponensek tesztelése
- Biztonsági tesztelés az integrált környezetben
    - A funkcionális működés és teljesítmény felmérése
    - A tesztelési hibák azonosítása
    - A teszteredmények összevetése a biztonsági követelményekkel
- A biztonsági kód telepítése a szükséges módosításokkal
- A biztonsági intézkedések dokumentálása
    - A felhasználói útmutatóknak tartalmaznia kell a biztonságos működés feltételeit
- Elfogadási tesztelés
    - Az utolsó lehetőség a sérülékenységek azonosítására
- A projekt biztonságosságának elfogadása/megerősítése

Telepítés

- Biztonsági minősítés megszerzése
- Felhasználók oktatása
- A rendszer élesüzemű telepítése

Üzemeltetés és fenntartás

- Mentési és visszaállítási tesztelések
- Biztonsági eljárások megfelelőségének ellenőrzése
- Periodikus kockázatelemzés
- Újratanúsítás
- A környezetet érintő változások hatásainak elemzése

- SLA megállapodások ellenőrzése

Átvizsgálás és kivonás

- A változások hatásait folyamatosan monitorozni kell
- Ha a változások olyan hatásokat váltanak ki a rendszerből, hogy azt már nem lehet gazdaságosan/biztonságosan üzemeltetni, akkor ki kell vonni a működésből
- A kivonásra megfelelő stratégiát kell kidolgozni.

A fentiek szerint a biztonsági tesztelési követelményeket már a funkcionális követelmények meghatározásánál figyelembe kell venni, majd háromféle részletességgel kell végrehajtani: kód (azaz részegység és modul teszt), rendszer/alrendszer és integrált környezet (más néven elfogadási teszt) szinten. Ez a három megközelítés egymástól lényegesen eltérő módszertan használatát kívánja meg, amit az értekezés 3. fejezete mutat be.

A telepítés fázisáig az elsődleges felelősség a fejlesztőé, utána már az üzemeltetést végző közigazgatási szervé. Látni kell azonban azt, hogy gyakorlatilag az egész életciklusban közösen kell dolgozniuk, hiszen például a megfelelő specifikációt a későbbi felhasználó nélkül nem lehet megírni, míg az üzemeltetési fázis során felderített sebezhetőségeket sem lehet befoltozni a fejlesztő részvétele nélkül. A Common Criteria jól szabályozza a felelősségeket az átadásig, utána azonban már nem feltétlenül ilyen világosak az elvárások. Kiindulópont lehet az Information Technology Infrastructure Library (ITIL) vagy más néven ISO 20000 szabvány, mely az üzemeltetés folyamatát, és az abban résztvevő entitások működésére ad útmutatást, de a gyakorlatban nagyon ritka ennek közigazgatáson belüli alkalmazása. [32] Az értekezésben kizárólag a fejlesztés folyamatával foglalkozom.

A fejlesztési folyamatra azonban teljes, jól szabályozott rendszer található a KIB 25. ajánlásban. A korábban meghatározott hármas tagolás itt két szintre redukálódik, ugyanis a fejlesztőkkel szembeni elvárásoknál nem lehetnek túl nagy eltérések. Alap és fokozott szinten a Common Criteria szerinti EAL3, kiemelt szinten EAL4 az elvárás. A jelenlegi központi közigazgatási rendszerek fejlesztések egy részénél az értekezés szerinti fokozott szinten is EAL4 az elvárás, **ez azonban véleményem szerint túlzott követelmény**, mert nincs akkora hozzáadott értéke a biztonság növeléséhez, ami indokolná az ezzel járó kiemelt dokumentálási kényszert.

Az EAL3 és EAL4 értelmezése gyakran problémát okoz a fejlesztőknek. Ez tulajdonképpen nem más, mint az ún. Értékelési Garanciaszint (Evaluation Assurance Level), mely azt írja

elő, hogy a fejlesztés folyamatát milyen szinten kell dokumentálni, illetve milyen részletes vizsgálatot kell lefolytatni. Az EAL3 és EAL4 szint között jelentős eltérés a gyakorlatban nincs. A fő problémát két dolog jelenti, egy módszertani és egy szoftverfejlesztőkre jellemző. A módszertani probléma az, hogy a Common Criteria a vízesés-modellre alkalmazható a legjobban, a napjainkban divatos módszertanokra, pl. az agilis eljárásra nehézkesen húzható rá. A szoftverfejlesztők esetén pedig **tapasztalatom szerint** az a probléma, hogy jellemzően projektről projektre más eljárásokkal dolgoznak, amelyek többnyire nincsenek megfelelően dokumentálva, így a Common Criteria szerinti fejlesztéshez nincsenek meg a szükséges alapok. A következő ábra mutatja be az egyes Értékelési Garanciaszintek elvárásait.

Garanciaosztály	Garanciacsalád	Garanciakomponensek Értékelési Garancia Szintek szerint						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Fejlesztés	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Útmutató dokumentumok	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Életciklus támogatása	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Biztonsági Előirányzat	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1

értékelése	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tesztek	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Sebezhetőség-vizsgálat	AVA_VAN	1	2	2	3	4	5	5

2. táblázat: Common Criteria Értékelési Garanciaszintek, forrás: CC 2. kötet

Ahogy látszik az EAL3 és az EAL4 szint között minimális különbség van, a tervezési és a sebezhetőség-vizsgálati fázisban vannak eltérések. Tervezési fázisban a legjelentősebb eltérés az, hogy az értékelőnek a forráskódot is elemeznie kell a szabványban meghatározott szempontok alapján. A közös pontok az alábbiak:

- Tervezés:
  - architektúra leírás;
  - funkcionális specifikáció;
  - logikai terv.
- Dokumentáció:
  - telepítési dokumentáció;
  - üzemeltetési dokumentáció.
- Életciklus támogatás:
  - konfigurációmenedzsment rendszer és eljárásai;
  - fejlesztési eszközök;
  - fejlesztői környezet biztonsági intézkedései;
  - fejlesztési folyamat leírása.

- Tesztelés:
    - funkcionális tesztelés;
    - tesztlefedettség és tesztmélység elemzés;
    - független tesztelés.
- Sebezhetőség-vizsgálat

Ezen lépések mindegyike szerepel a szoftver életciklusában, így azon szervezeteknek, melyek a gyakorlatban is használják az életciklus-modellt, a Common Criteria alkalmazása nem jelenthet problémát. Akik nem használnak ilyen modellt, azoknak sem okozhat túlságosan komoly munkát az eszerinti fejlesztés, hiszen a Common Criteria kizárólag a fejlesztett rendszer biztonsági funkciói esetén várja el ezt a dokumentációs szintet. Az előző fejezetben pedig bemutattam, hogy a fejlesztett biztonsági funkciók köre erősen limitált. Két olyan terület van a követelmények között, aminek **tapasztalatom szerint** nincs hagyománya, kultúrája hazánkban, ez pedig a fejlesztői környezet biztonsága és a sebezhetőség-vizsgálat. Jelen fejezet a fejlesztőre vonatkozó elvárásokkal foglalkozik, a következő pedig a sebezhetőség-vizsgálat módszertanait járja körül.

2.2 Az IT biztonság szervezeti és belső szabályozási követelményei a kritikus alkalmazások fejlesztőinél

A közigazgatási rendszerek fejlesztőinél többnyire nem jellemző az információbiztonság széleskörű megléte, hiszen ezt nagyon ritkán várják el tőlük. Szerencsés esetben, jellemzően akkor, ha a cég a fejlesztésen kívül más tevékenységgel is foglalkozik, van valamilyen belső biztonsági szabályozás. Nemzetvédelmi szempontból azonban kiemelten fontos, hogy a fejlesztőkkel szemben egységes elvárások jelenjenek meg, hiszen egy kód kiszivárgása, vagy hátsó kapu elrejtése komoly problémákat jelenthet.

Mindhárom biztonsági szinten elvárható tehát a rendszer fejlesztőjétől, hogy biztonsági tevékenységeit megfelelően dokumentálja. A legkézenfekvőbb megoldás erre egy olyan szabályzati rendszer létrehozása, mely kielégíti mind a szabványok, mind a jogszabályok jelentette követelményeket. A KIB 25. ajánlás Informatikai Biztonsági Irányítási Rendszerrel foglalkozó része pontosan megnevezi, hogy milyen elemekből kell állnia egy szabályzati rendszernek, melyet három szintre lehet osztani. [33]

- **Informatikai Biztonsági Politika (IBP)**: „Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során."
- **Informatikai Stratégia**: „Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú)."
- **Informatikai Biztonsági Szabályzat (IBSZ)**: „Az Informatikai Biztonsági Szabályzat rögzíti az Informatikai Biztonsági Irányítási Rendszer (IBIR) működéséhez, működtetéséhez szükséges folyamatokat, megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információfeldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológiafüggetlen tudjon maradni."
- **Informatikai Felhasználói Szabályzat (IFSZ)**: „A dokumentum részletesen szabályozza a felhasználók kötelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket."
- **Eljárásrend gyűjtemény**: „Az eljárásrend gyűjteménybe tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszerfüggetlenül megkövetel."

Az IBP és a Stratégia alkotja a szabályzati rendszer első szintjét, az IBSZ és az IFSZ a másodikat, az eljárásrend pedig a harmadikat. Ezeknek koherens egészet kell alkotniuk, nem szabad ellentmondásokat létrehozni, amiről az értékelő szervezetnek is meg kell győződnie.

A gyakorlatban a fejlesztési és üzemeltetési folyamatot nem kizárólag egy szervezet fedi le, hanem egy fővállalkozó és több alvállalkozó együttesen. Ilyenkor különösen nehéz megállapítani, hogy ki, mennyire tudja betartani az elvárt biztonsági szintet. **Alapelvként azt javaslom**, hogy a közigazgatási szervnek arról kell meggyőződnie, hogy a fővállalkozó, aki elsődlegesen felelős a fejlesztés és üzemeltetés sikeres végrehajtásáért, megfelelő szabályzati rendszerrel dolgozik. Az alvállalkozóknak minden esetben minimálisan a fővállalkozó szabályzataiban foglalt elveket kell teljesíteniük, ezeknél alacsonyabb biztonsági szint nem megengedett. Ez a megoldás kellően rugalmas, mégis biztonságos lehet.

Javaslatom szerint az alvállalkozók ellenőrzése minden esetben a Fővállalkozó Biztonsági Vezetőjének a feladata, aki ezt belső auditok során teszi meg. A belső auditokról készített feljegyzések, valamint a szúrópróbaszerű ellenőrzés adnak garanciát arra a szervezet által megbízott külső auditornak, hogy a fejlesztésben részt vevő minden szervezet megfelelő biztonsági szinten dolgozik.

Mivel a megrendelőnek érdemi beleszólása nincsen a fejlesztés folyamatába, így szerződéses feltételként kell megfogalmaznia azt az igényét, hogy a fejlesztés biztonságát, így a szabályzati rendszert ellenőrizhesse. **Erre három lehetséges megoldást mutatok be**.

- Előírhatja a Common Criteria vagy KIB 25. szerinti fejlesztést, melynek részeként a megrendelő által megbízott auditor ellenőrizheti a fejlesztés biztonsági környezetét. Hátránya, hogy a Common Criteria módszertan nem szab konkrét követelményeket, deklaráltan az auditorra van bízva annak eldöntése, hogy a környezet megfelelően biztonságos vagy nem az, de azért a szabályozandó területeket meghatározza. Alap, fokozott és kiemelt szinten is kötelező lehet.

- Elrendelheti a fejlesztés nemzetbiztonsági ellenőrzését. Ilyenkor a teljes fejlesztési folyamat kontrollálható, a fő elveket a 92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól határozza meg. Fokozott szinten opcionális, kiemelt szinten kötelező lehet. [34]

- Elvárhatja az ISO 27001-es tanúsítvány meglétét a fejlesztési folyamatra. Ekkor a megrendelő megbízik egy általa nem felkért harmadik személyben, és elfogadja, hogy a fejlesztő által benyújtott fejlesztés-biztonsági dokumentumok helytállóak. Ez a megoldás objektív, hiszen a szabvány konkrét védelmi intézkedéseket tartalmaz, melyek működésének ellenőrzése is szabvány szerint történik, hátránya viszont, hogy

az értékelést végzővel semmilyen közvetlen kapcsolata nincs a megbízónak. Alap biztonsági szinten opcionális, fokozott és kiemelt szinten kötelező lehet.

Az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. kormányrendelet (a továbbiakban: Rendelet) hatálya azokra a Közbeszerzési törvény (2003. évi CXXIX. törvény a közbeszerzésekről, a továbbiakban: Kbt.) szerinti egyszerű közbeszerzési eljárás mindenkori értékhatárait elérő vagy azt meghaladó értékű beszerzésekre terjed ki, melyek – a Rendelet címének megfelelően – államtitkot, szolgálati titkot (újabban minősített adatot), illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintenek, illetve különleges biztonsági intézkedést igényelnek. [35][36]

A Rendelet értelmező részében kerül meghatározásra két, máshol nem definiált fogalom, az alapvető biztonsági érdeket érintő és a különleges biztonsági intézkedést igénylő beszerzés fogalma. Az ország alapvető biztonsági érdekével kapcsolatos a beszerzés, ha a beszerzés tárgya közvetlenül kapcsolódik az ország lakosságának fizikai, környezeti, egészségügyi, gazdasági, honvédelmi biztonságát befolyásolni képes építési beruházáshoz, árubeszerzéshez, illetőleg szolgáltatás megrendeléséhez. Különleges biztonsági intézkedést igényel a beszerzés, ha a beszerzés tárgyának előállításánál, az előállításhoz szükséges alapanyagok és termékek szállításánál, illetőleg a felhasználásnál, a beszerzés tárgyának szállításánál hatóság vagy jogszabály különleges követelményt ír elő, illetve az általánostól eltérő élőerős vagy technikai ellenőrzés szükséges. Azért is fontos ez a két fogalom, mert akkor is lehetővé teszi a Rendelet alkalmazását, ha a beszerzés tárgya minősített adatot, illetőleg nemzetbiztonsági érdeket nem érint.

A Rendelet nagyon részletesen szabályozza az ajánlattevők ellenőrzését, magát a beszerzési eljárást, de a beszerzési eljárás utáni, a teljesítés biztonsági követelményeire vonatkozó előírást, vagy elvárást nem ad. Persze erre nem is lenne szükség, ha ezek a követelmények máshol megjelennek. Nézzük részletesen a követelményekre vonatkozó előírásokat informatikai fejlesztések esetén.

Ha a beszerzés minősített adatot érint, akkor a 2009. évi CLV. törvény a minősített adat védelméről (a továbbiakban: titoktörvény), továbbá a 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól lenne a mérvadó. [37] Itt néhány olyan szabály megjelenik, amit a fejlesztőnek a fejlesztői környezetben be kell tartania:

24. § (2) A rejtjeltevékenységet folytató szerv a rejtjelző eszközök, módszerek üzemeltetésével, tárolásával, valamint fejlesztésével, gyártásával kapcsolatos helyiségek fizikai biztonságának kialakításakor biztosítja, hogy a rendszer rejtjelzéssel kapcsolatos elemeihez felügyelet nélkül kizárólag olyan személy férhessen hozzá, akinek a munkaköre ellátásához az feltétlenül szükséges, más személy hozzáférését korlátozza, még akkor is, ha rendelkezik a megfelelő szintű személy biztonsági tanúsítvánnyal.

41. § (4) Nemzeti minősített adat rejtjelzésére csak olyan rejtjelző eszköz alkalmazható, amelynek fejlesztője, illetve gyártója rendelkezik a minősített adat kezeléséhez szükséges, jogszabályban meghatározott személyi és tárgyi feltételekkel, és amely szerv esetében az NBF a rejtjelző eszközre vonatkozóan – a létrehozására vonatkozó döntéstől a tervezést, a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást is érintően, a rendszer egyes elemeinek vagy egészének a kivonásáig és megsemmisítéséig – megbízhatóan meggyőződött arról, hogy nem áll fenn a bizalmasság elve sérülésének veszélye.

48. § (1) Az NBF engedélye szükséges továbbá: *b)* a rejtjelző eszközzel kapcsolatos fejlesztési, gyártási tevékenységhez,

Mindez arra utal, hogy minősített adatot kezelő rendszer fejlesztése esetén vannak olyan előírások, amelyek a fejlesztő biztonsági környezetét ellenőrizhetővé teszik. A 92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól további támpontot ad ehhez.

11. § (1) Bizalmas vagy magasabb minősítési szintű minősített szerződés végrehajtásában kizárólag érvényes és megfelelő szintű telephely biztonsági tanúsítvánnyal rendelkező gazdálkodó szervezet vehet részt.

A megbízó és a fejlesztő közötti kapcsolatot az alábbiak szerint rendezi a jogszabály:

13. § (1) A minősített szerződések részletes biztonsági előírásait a szerződés részét képező külön dokumentum, a projekt biztonsági utasítás tartalmazza. A projekt biztonsági utasításnak függeléke a projekt minősítési jegyzék.

(2) A projekt biztonsági utasítás az alábbiakról rendelkezik:

a) a minősített szerződés végrehajtásában részt vevő szervek feladat- és hatásköréről, a biztonsági szervek és személyek, így a biztonsági vezetők pontos feladat- és hatásköréről,

b) a minősített adatok helyszíni tárolásának speciális szabályairól,

c) a minősített adatok belföldi és külföldi továbbításának szabályairól, a megbeszéléseken, előadásokon történő felhasználás egyedi rendelkezéseiről, továbbá a minősített adatok alvállalkozónak történő átadásának feltételeiről,

d) a minősített szerződés teljesítését követő eljárásrendről, így a minősített adatok átadónak történő visszaszolgáltatásáról.

Ez a felsorolás pontosan illeszkedik a 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló jogszabály elvéhez. [38] Ebből kiderül, hogy milyen biztonsági szerepkörök szükségesek az együttműködésben, illetve milyen fizikai biztonsági intézkedéseket kell a fejlesztőnek megtennie. A logikai, azaz informatikai biztonsági intézkedésekről azonban egyik jogszabály sem szól.

Ha a beszerzés alapvető biztonsági, nemzetbiztonsági érdeket érint, illetve különleges biztonsági intézkedést igényel, de minősített adat kezelése nem történik, akkor erre vonatkozóan nem találunk útmutatást a magyar jogszabályi rendszerben. Ugyanis az alapvető biztonsági, nemzetbiztonsági érdeket érintő beszerzések megvalósítása során követendő biztonsági elvárásokra nincs előírás. Tulajdonképpen a Rendelet szerinti valamennyi eljárásban a beszerzés tárgyának előállításánál, az előállításhoz szükséges alapanyagok és termékek szállításánál, illetőleg a felhasználásnál, a beszerzés tárgyának szállításánál az ajánlatkérőnek – esetleg az illetékes nemzetbiztonsági szolgálatnak – kellene különleges követelményt előírni. Ilyen követelményrendszernek azonban semmilyen nyilvános említése nem ismert.

A KIB 28. ajánlás „Közigazgatási Operatív Programok IT biztonsági környezete, követelményrendszere” című dokumentuma az általam vázolt gondolatmenethez hasonló, de részletesen nem kifejtett módon közelíti meg az e-közigazgatási informatikai rendszerek fejlesztésének kérdését. [39] Ez tehát magas szintű elvárásokat fogalmaz meg, **amivel véleményem szerint jelen értekezés összhangban van,** és bár a biztonsági szintek megfogalmazásában vannak eltérések**, dolgozatom felhasználható az ajánlás gyakorlati megvalósításában.**

Megállapítom tehát, hogy a magyar jogszabályok még a minősített adatokkal foglalkozó rendszerek tekintetében sem írnak elő a fejlesztői környezetre informatikai biztonsági követelményeket (legalábbis nyilvános utalás nincs erre), de legalább kiindulópontot jelentenek a személyi és fizikai biztonsági intézkedésekre. Ennek mentén a kiemelt biztonsági

szint jól meghatározható, de az alap és fokozott biztonsági szinten orvosolni kell ezt a hiányosságot.

2.3 Az elektronikus közigazgatási alkalmazások fejlesztőire vonatkozó személyi követelmények

Mindhárom biztonsági szintben közös, hogy nem szabad a fejlesztőknek előzetes kontroll nélkül hozzáférést adni a fejlesztői környezethez, nem megengedhető, hogy felügyelet nélkül dolgozzanak, és ki kell találni, hogy milyen módon lehet hozzáférésüket megszüntetni. Ehhez fel kell állítani egy olyan belső biztonsági irányítási és ellenőrzési szervezetet, mely a fejlesztőket munkájuk során kontrollálni tudja. Erre a KIB 25. számú ajánlásának 1-2., már idézett kötete ad ajánlást, mely szerint ki kell jelölni a Biztonsági Vezetőt, az Informatikai Biztonsági Vezetőt, az Informatikai Biztonsági Fórumot, valamint a szakterületi (fejlesztési és üzemeltetési) vezetőt. Ezt a biztonsággal kapcsolatos szervezeti felépítést mindhárom területen érdemes betartani. A kiemelt biztonsági szinten a személyi követelményeket a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelettel kell összhangba hozni. **A következőkben ajánlást teszek a közigazgatási alkalmazások fejlesztését végző szervezetek biztonsággal kapcsolatos szerepköreire és ezek felelősségi területeire.**

A **fejlesztéssel megbízott szervezet vezetője**, vagy kiemelt projekteknél a fejlesztés projektvezetője az Informatikai Biztonsági Fórum vezetője, azaz a biztonsági terület elsődlegesen neki tartozik beszámolóval.

Feladata:

- hatályba lépteti az Információbiztonsági Szabályzatot,
- értékeli a kockázatelemzést,
- felülvizsgálja az információk osztályozását,
- meghatározza a munkavégzés helyszíneit,
- utasítja a vállalkozókat információbiztonsági kérdésekben,
- kezdeményezi a felhasználói jogosultságok visszavonását, elrendeli az azonnali visszavonást,
- engedélyezi új eszközök beszerzését,

- értékeli az incidenseket.

Felelős:

- az adatvagyonleltár naprakészen tartásáért,
- az információbiztonsági tudatosság építéséért,
- a speciális információbiztonsági tudás megszerzésének biztosításáért,
- a képzések értékeléséért,
- a szankcionálásért,
- a belső auditok elrendeléséért és értékeléséért.

Az Informatikai Biztonsági Fórumot, és általában a fejlesztési projektet egy adminisztratív szervezet, a **projektiroda** támogatja, amelynek szerepet lehet adni a biztonsági keretrendszerben is. Ebben az adminisztratív szervezetben kell elhelyezkednie kiemelt szinten a jogszabályban megfogalmazott titkos ügykezelő szerepkörnek is.

Feladata:

- hardver- és szoftvereszközök nyilvántartása,
- a belépési naplók archiválása,
- a jogosultságok nyilvántartása,
- a forráskódok őrzése,
- az üzemeltetési feljegyzések őrzése,
- kiemelt szinten a 90/2010. (III. 26.) Korm. rendelet 8. §-ban megfogalmazott feladatok ellátása.

Felelős:

- a jogosultságok kiadásáért és visszavonásáért,
- kiemelt szinten a minősített adatok kezeléséért.

A **Biztonsági Vezető** és az **Informatikai Biztonsági Vezető** szerepkört ugyanaz a személy is betöltheti az ajánlás szerint. A fejlesztési környezet biztonsági aspektusaiért elsősorban ő a felelős. A kormányrendeletben meghatározott biztonsági vezető szerepkört is ez a személy tölti be kiemelt biztonsági szinten.

Feladata:

- az adatvagyonleltár elkészítésének támogatása,
- védelmi intézkedések megfogalmazása,
- az Informatikai Biztonsági Fórum és a fejlesztési/üzemeltetési vezető támogatása információbiztonsági kérdésekben,
- a vagyontárgyak kiadásának és visszavételének felügyelete,
- a kiemelt jogosultságok ellenőrzése,
- a karbantartási terv jóváhagyása,
- kiemelt szinten a 90/2010. (III. 26.) Korm. rendelet 6. §-ban megfogalmazott feladatok ellátása.

Felelős

- az adatvagyonleltár rendszeres felülvizsgálatáért,
- a kockázatelemzés elkészítéséért,
- a sebezhetőség-vizsgálat elkészítéséért,
- a védelmi intézkedések bevezetéséért,
- a vállalkozók információbiztonsági szabályzatainak felülvizsgálatáért,
- az Informatikai Felhasználói Szabályzat kidolgozásáért és karbantartásáért,
- az információbiztonsági oktatásokért,
- a belső auditok végrehajtásáért,
- a szabálysértések kivizsgálásáért,
- vállalkozók telephelyeinek ellenőrzéséért,
- az információbiztonsági eszközök karbantartásáért,
- a jogosultságok ellenőrzéséért,
- az üzemeltetés és a fejlesztés biztonsági ellenőrzéséért,
- az új rendszerek biztonságos üzembe állításáért,
- a megfelelő visszaállításért,

- az információbiztonsági incidensek kezeléséért,
- az üzletmenet-folytonossági intézkedések kialakításáért,
- kiemelt szinten a minősített adatok védelméért.

A **fejlesztési vezető** elsősorban az alkalmazás biztonságáért felelős, a fejlesztői környezet biztonságával kapcsolatban viszonylag kevés feladata van.

Feladata:

- A fejlesztés során keletkezett információk Információbiztonsági Szabályzat szerinti kezelése
- A Biztonsági Vezető és az Üzemeltetési Vezető támogatása az Információbiztonsági Szabályzatban leírtak teljesítésében

Felelős:

- A fejlesztés során keletkezett információk minősítéséért,
- A fejlesztői jogosultságok kiosztásáért

Az **Üzemeltetési Vezető** az a személy, aki a fejlesztéshez használt eszközök üzemeltetéséért felelős. A Biztonsági Vezetővel közösen felel a biztonságos fejlesztői környezet kialakításáért.

Feladata:

- a projektiroda támogatása,
- új eszközök specifikálása,
- az erőforrás-kihasználás ellenőrzése,
- az incidensek értékelése

Felelős:

- a kiemelt jogosultságokért,
- az üzemeltetési folyamatokért,
- a rendszerfejlesztés koordinálásáért,
- az üzemeltetési rend kialakításáért,
- a vírusvédelemért,

- a mentésekért,
- a visszaállításért,
- a határvédelmi eszközök üzemeltetéséért,
- a karbantartásért,
- a hibabejelentések kezeléséért

Fontos, hogy ezek a szerepkörök megfelelően megbízhatók legyenek, ezért a szerződéskötés során nevesíteni és ellenőrizni kell őket. **Ehhez javaslatom szerint az egyes szerepköröket a következő bekezdés szerint kell átvizsgálni.**

A **projektvezető** a közigazgatási fejlesztések esetén mindenkor a kormányrendeletben leírt személyi biztonsági tanúsítvánnyal kell, hogy rendelkezzen, hiszen nagy a valószínűsége annak, hogy a fejlesztés során olyan összefüggéseket, információkat kap meg a közigazgatási informatika belső működéséről, amelyekhez egyfajta bizalom kell az állam részéről. A **projektiroda** munkatársai, a **Biztonsági, Fejlesztési és Üzemeltetési vezető** alap és fokozott biztonsági szintek esetében erkölcsi bizonyítvány benyújtására kötelezettek, kiemelt esetben a Biztonsági vezetőnek és a projektiroda titkos ügykezelőjének személyi biztonsági tanúsítványra, a többi szerepkörnek felhasználói engedélyre és titoktartási nyilatkozatra van szüksége. A **Biztonsági Vezetőnek** emellett rendelkeznie kell az ISACA Certified Information System Manager (CISM) vizsgájával, mely nemzetközileg elfogadott biztosítékot ad arról, hogy képes a feladatát teljesíteni. Az államigazgatásban ez utóbbi követelmény túlzottnak tűnhet, de piaci fejlesztő esetében elvárható. Mindhárom biztonsági szinten a megrendelő államigazgatási szerv elvárhatja azt, hogy a fejlesztő az erkölcsi bizonyítványon kívül bemutassa az alkalmazottak biztonsági háttérellenőrzésének folyamatát és eredményét.

A **fejlesztésben résztvevő**, valamint a **fejlesztői környezetet üzemeltető** személyek ellenőrzése is kritikus. Alap és fokozott szintű esetben minden érintettnek erkölcsi bizonyítvánnyal kell rendelkeznie, be kell nyújtania önéletrajzát és iskolai bizonyítványait. Fokozott esetben a vállalkozó háttérellenőrzéssel egészíti ki ezt, mely során meggyőződik a benyújtott iratok és információk hitelességéről, valamint nyílt források felhasználásával győződik meg az érintett megbízhatóságáról. Kiemelt esetben mind a fejlesztőknek, mind az üzemeltetőknek felhasználói engedéllyel és titoktartási nyilatkozattal kell rendelkezniük.

2.4 Logikai védelmi intézkedések a fejlesztői környezetben

A közigazgatási rendszerek információbiztonsággal kapcsolatos műszaki követelményeit a KIB 28. ajánlás „IT biztonsági követelményrendszer - biztonsági szintek követelményei" című dokumentuma határozza meg 3 szinten a már korábban ismertetett módon. A fejezetben ezek a követelmények jelennek meg, **melyeket átfordítok a fejlesztési környezet követelményeire**. Az eredeti követelmények leírása a forrásban elolvasható, azokat **a fejlesztéssel kapcsolatosan értelmezem a jelen fejezetben**.

Az általános fejlesztői környezetet három jól elhatárolható részre bontjuk. Az első a fejlesztői munkaállomás, mely alap esetben a fejlesztő saját tulajdonában is lehet, és mely bizonyos feltételekkel az interneten keresztül is elérheti a központi rendszereket, fokozott esetben a vállalkozó telephelyén és üzemeltetésében, kiemelt esetben pedig a megrendelő telephelyén, a megrendelő üzemeltetésében van. A második a központi fejlesztői architektúra, mely a szerverek hardvereit, operációs rendszereit, és a fejlesztéshez közvetlenül nem kötődő alkalmazásokat jelenti. A harmadik részt azok az alkalmazások jelentik, melyek közvetlenül a fejlesztési folyamathoz kapcsolódnak, pl. verziókezelők, keretrendszerek, fejlesztői wiki. A három részre egységes követelmények vonatkoznak, kivéve ott, ahol ez külön jelzésre kerül. Amennyiben az adott területre a vállalkozónak vagy a megrendelőnek van már szabályzata, alapértelmezésben ahhoz kell igazodni, kivéve, ha jelen követelmények erősebb feltételeket támasztanak, mert ilyenkor a belső szabályokat ezekhez a követelményekhez kell igazítani.

Konfiguráció kezelés

KK-1 Konfiguráció kezelési szabályzat és eljárásrend: A konfigurációkezelési szabályzatot a fejlesztői környezet vállalkozó vagy megrendelő által üzemeltetett informatikai rendszereire kell kidolgozni.

KK-2 Alapkonfiguráció: A fejlesztői környezet tervezésénél olyan egységes rendszerek tervezésére kell törekedni, melyek üzemeltetése könnyen megoldható. Ez elsősorban az operációs rendszerek, az irodai alkalmazások és a böngészők egységes beállítására vonatkozik.

KK-3 Konfigurációváltozások: A beállított konfigurációk módosításáról minden esetben feljegyzést kell készíteni, melyet a Biztonsági Vezető és az üzemeltetési vezető együttes jóváhagyásával lehet végrehajtani. A feljegyzés akár egy e-mail is lehet.

KK-4 A konfigurációváltozások felügyelete: A jóváhagyott változások hatásait a rendszeres felülvizsgálatok során kell ellenőrizni, illetve ha érezhető negatív hatásuk van, azonnal be kell avatkozni.

KK-5 A változtatásokra vonatkozó hozzáférés-korlátozások: Konfigurációváltozást csak kiemelt jogosultsággal rendelkező felhasználó hajthat végre.

KK-6 Konfigurációs beállítások: A fejlesztői rendszerek konfigurációjának megállapításakor törekedni kell az ajánlásokban javasoltak betartására. Amennyiben ez működésképtelenné teszi a fejlesztői rendszert, a Biztonsági Vezető felelőssége a kockázatok értékelése után a beállítások enyhítésének engedélyezése.

KK-7 Legszűkebb funkcionalitás: Minden vállalkozó vagy megrendelő által felügyelt rendszeren csak azokat a hálózati és helyi szolgáltatásokat szabad engedélyezni, melyek feltétlenül szükségesek a rendszer működéséhez.

KK-8 Informatikai rendszer komponenseinek leltára: A projektirodának és az üzemeltetési vezetőnek közösen kell gondoskodnia a fejlesztési projekt eszközeinek leltározásáról.

Rendszer és információ sértetlenség

RS-1 Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend: A szabályzatnak elsősorban a vírusvédelem szabályait kell tartalmaznia, ezen kívül jelen pontok közül azokat, melyeket a különböző biztonsági szinteken meg kell valósítani.

RS-2 Hibajavítás: Ahol lehet, automatikus hibajavítást kell alkalmazni. A rendszeres felülvizsgálatok során meg kell vizsgálni, hogy milyen egyéb hibajavításokat szükséges telepíteni.

RS-3 Rosszindulatú kódok elleni védelem: Minden olyan rendszerre víruskeresőt kell telepíteni, melyre ez lehetséges. Lehetőség szerint olyan víruskeresőt kell telepíteni, mely központilag menedzselhető és más védelmi termékekkel csoportosan kezelhető.

RS-4 Behatolás-észlelési eszközök és technikák: Minden olyan rendszerre host alapú behatolás detektáló (Intrusion Detection System – IDS) kell telepíteni, melyre ez lehetséges. Ezeknek lehetőleg központilag menedzselhetőnek és más védelmi termékekkel együttműködőnek kell lennie.

RS-5 Biztonsági riasztások és tájékoztatások: A biztonsági riasztásokat e-mailen kell továbbítani az üzemeltetésért felelős személyeknek és az üzemeltetési vezetőnek. A

rendszeres felülvizsgálatok során szúrópróbaszerűen kell ellenőrizni, hogy ezeket megfelelően kezelték.

RS-6 A biztonsági funkcionalitás ellenőrzése: A rendszeres felülvizsgálat során ki kell térni a biztonsági funkcionalitás tesztelésére is, melynek során a Biztonsági Vezető dönt a tesztelendő funkciók köréről.

RS-7 Szoftver és információ-sértetlenség: Ha a víruskereső rendszer vagy az IDS részeként beállítható a fájlrendszer sértetlenségének védelme is, akkor törekedni kell ennek használatára.

RS-8 Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem: A kéretlen levelek szűrésére elégséges a munkaállomásokra telepített levelezőrendszerek adta lehetőségek használata.

RS-9 A bemeneti információra vonatkozó korlátozások: A rendszerbe csak hitelesítés után, megfelelő jogosultsággal lehet információt bejuttatni.

RS-10 A bemeneti információ pontossága, teljessége és érvényessége: A bemeneti információk szűrésénél a rendszerek adta lehetőségekre kell támaszkodni, külön input validációs védelmi intézkedések bevezetése nem szükséges.

RS-11 Hibakezelés: A fejlesztői rendszerek jellegükből adódóan számtalan debug információt szolgáltatnak, így nem szükséges a hibaüzeneteket elrejteni.

RS-12 A kimeneti információ kezelése és megőrzése: A kimeneti információk kezelését nem szükséges külön szabályozni.

Azonosítás és hitelesítés

AH-1 Azonosítási és hitelesítési szabályzat és eljárásrend: Azonosítási és hitelesítési szabályzatot kell kialakítani, mely érvényes a fejlesztéshez használt munkaállomásokra, szerverekre és központi szolgáltatásokra (pl. verziókezelő, szerveren futó alkalmazásfejlesztői eszköz, dokumentációs rendszer stb.).

AH-2 Felhasználó azonosítása és hitelesítése: Minden fejlesztő egyedi azonosítóval (pl. felhasználónév, e-mail cím) rendelkezik. Ezt az egyedi azonosítót köteles használni a munkaállomásához, a szerverekhez és a központi szolgáltatásokhoz való hozzáférésre. Alap esetben az interneten keresztüli hozzáférés erős hitelesítést igényel (pl. VPN), a helyi hozzáférés nem. Fokozott szinten csak helyi hozzáférés megengedett, ilyenkor nem szükséges

erős authentikáció. Kiemelt szinten még a helyi hozzáféréshez is hardver alapú erős authentikáció szükséges.

AH-3 Eszközök azonosítása és hitelesítése: Fokozott és kiemelt biztonsági szinteken minden fejlesztői munkaállomást azonosítani és hitelesíteni kell. A munkaállomások azonosítása a 802.1x protokollon alapul.

AH-4 Azonosító kezelés: Külön kell kezelni a fejlesztői és a környezet adminisztrátori azonosítókat. Anonim hozzáférést nem lehet engedélyezni. Az azonosítók nyilvántartása és kezelése a projektiroda feladata. Amikor egy felhasználó elhagyja a projektet, azonosítóját vissza kell vonni, és archiválni kell.

AH-5 A hitelesítésre szolgáló eszközök kezelése: A jelszavak, illetve az erős hitelesítés eszközeinek kiadását a fejlesztő vagy a megrendelő szabályaihoz kell igazítani. Ezek hiányában a projektiroda gondoskodik a jelszavak és az erős hitelesítés eszközeinek kibocsátásról. A kezelési folyamatokat ilyenkor a legegyszerűbb módon kell kialakítani.

AH-6 A hitelesítésre szolgáló eszköz visszacsatolása: A jelszavak beírása, illetve az erős authentikáció olyan formában történjen meg, hogy a felhasználó lássa a hitelesítés folyamatát és eredményét. Egyetlen rendszeren sem engedhető meg, hogy a jelszavak leolvashatók legyenek a képernyőről, vagy azokat titkosítatlanul tárolják. Ez elsősorban a fejlesztői eszközöknél lehet körülményesen teljesíthető feltétel. Az eszközök kiválasztásánál ezért ezt a szempontot is figyelembe kell venni.

AH-7 Hitelesítés kriptográfiai modul esetén: A fejlesztési folyamatban kicsi a valószínűsége kriptográfiai modul használatának. Ha mégis igény van ilyenre, akkor az ajánlás szerint kell eljárni.

Hozzáférés ellenőrzése

HE-1 Hozzáférés ellenőrzési szabályzat és eljárásrend: Létre kell hozni egy olyan jogosultsági szabályzatot, mely egyértelműen meghatározza, hogy a fejlesztői rendszerekben mely személyek vagy szerepkörök (pl. alkalmazásfejlesztők, adatbázis-fejlesztők, fejlesztési vezetők, tesztelők, stb.) milyen jogosultságokkal rendelkeznek.

HE-2 Felhasználói fiókok kezelése: A felhasználói fiókok kezelése mindig a környezet üzemeltetőinek a feladata, akik a jogosultságokat akkor adhatják ki, ha a fejlesztési vezető ezt engedélyezte. A jogosultságok visszavonása a fejlesztő projektből való kilépése esetén automatikusan megtörténik, de az Informatikai Biztonsági Fórum vezetőjének joga van a

hozzáférést azonnali hatállyal megszűntetni. Fokozott és kiemelt esetben elvárt egy jogosultságkezelő rendszer használata.

HE-3 Hozzáférés ellenőrzésének érvényre juttatása: A fejlesztői környezetben csak olyan rendszereket szabad használni, melyek lehetővé teszik az egyéni vagy szerepkör alapú csoportos jogosultságok beállítását. Különösen igaz ez a verziókezelő rendszerre, ahol a különböző verziók ellenőrzésének és kiadásának joga különböző személyeknél van.

HE-4 Információ áramlás ellenőrzés érvényre juttatása: Az egyes eszközök között megengedett az összeköttetések kialakítása, azaz az információ továbbítása abban az esetben, ha a két rendszer azonos biztonsági szinten van, vagy a célrendszer biztonsági szintje magasabb, mint a forrásrendszeré. Az információ átadása alacsonyabb biztonsági szintre nem megengedett. A gyakorlatban ez azt jelenti, hogy pl. fokozott szinten a központi rendszerben létrejött kódot nem lehet alap szintű biztonsági követelményeknek megfelelő laptopra másolni.

HE-5 A felelősségek szétválasztása: A fejlesztői, minőségbiztosítói/tesztelői, üzemeltetői és biztonsági auditori szerepköröket mindenképpen külön személyeknek kell ellátniuk, ezek között személyi átfedés nem lehet.

HE-6 Legkisebb jogosultság: A fejlesztési vezetőnek pontosan meg kell határoznia a fejlesztésben résztvevők feladatait, és ezeknek megfelelően kell hozzáférést biztosítani a rendszerekhez. Nem megengedett az a fejlesztői gyakorlat, hogy a programozók teljes hozzáféréssel rendelkeznek a központi rendszerekhez. Saját munkaállomásukon megengedett a kiemelt jogosultságok használata. A fejlesztői, tesztelői és éles környezeteket el kell választani, a fejlesztők hozzáférése és adminisztratív ellenőrzése szintről szintre változik.

HE-7 Sikertelen bejelentkezési kísérletek: A sikertelen belépési kísérleteket naplózni kell, azokra nem szükséges automatikus válaszlépéseket adni, elégséges a rendszeres felülvizsgálat során kitérni rájuk. Amennyiben a fejlesztői rendszer engedi, a fiókok automatikus felfüggesztését engedélyezni kell.

HE-8 A rendszerhasználat jelzése: Amennyiben a fejlesztői rendszer engedélyezi, a bejelentkezés előtt tájékoztatást vagy hivatkozást kell adni a rendszer használatának szabályairól a bejelentkezési képernyőn. Amennyiben erre nincsen lehetőség, úgy elfogadható a felhasználói azonosító létrehozása előtt megismertetni a felhasználókat ezekkel a szabályokkal, amit ők aláírásukkal nyugtáznak.

HE-9 Értesítés előző bejelentkezésről: Amennyiben erre lehetőség van, a bejelentkezés után a képernyőn fel kell tűntetni az előző bejelentkezés időpontját és a sikertelen belépési kísérletek számát. Ha a rendszer ezt nem engedi, akkor nem szükséges a követelményt teljesíteni.

HE-10 Egyidejű munkaszakaszok kezelése: A párhuzamos bejelentkezések számát nem szükséges limitálni, egy fejlesztő többször is bejelentkezhet a rendszerekbe, akár különböző gépekről is.

HE-11 A munkaszakasz zárolása: Minden hozzáférést, legyen az munkaállomás, szerver vagy fejlesztői eszköz, zárolni kell 1 óra inaktivitás után. A fejlesztői rendszereknél ez csak akkor követelmény, ha az eszköz képes erre.

HE-12 A munkaszakasz lezárása: A szerverekhez való távoli hozzáférést 1 nap inaktivitás után le kell zárni, azaz ki kell léptetni a felhasználót. Ez alól indokolt esetben kivételt lehet tenni.

HE-13 Felügyelet és felülvizsgálat — hozzáférés ellenőrzése: Minden rendszernek naplóznia kell a belépési kísérleteket, akár sikeresek, akár nem. A Biztonsági Vezetőnek havonta meg kell vizsgálnia a belépési statisztikákat, és amennyiben gyanús tevékenységet észlel, azt ki kell vizsgálnia. A rendszeres felülvizsgálatok során a belépési információk valódiságát szúrópróbaszerűen, a belépő személy megkérdezésével kell ellenőrizni.

HE-14 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek: A fejlesztők saját munkaállomásukon a munkaállomásra való belépés után külön azonosítás és hitelesítés nélkül használhatják a saját rendszerükre telepített eszközöket. Nem szükséges külön hitelesítés azokhoz a fejlesztői rendszerekhez (pl. wiki), melyek eléréséhez korábban már egyébként is hitelesíteniük kellett magukat (pl. VPN csatlakozás), és csak olvasási műveleteket hajtanak végre. Minden más esetben el kell végezni az azonosítási és hitelesítési műveleteket.

HE-15 Automatikus jelölés: A kimenő információk jelölése megegyezik a projekt minősítésével (pl. bizalmas, titkos stb.). Automatikus jelölés használata nem szükséges.

HE-16 Automatikus címkézés: A címkézések a szoftverfejlesztési módszertan alapján történnek, ezen kívül automatikus címkézés használatára nincs szükség.

HE-17 Távoli hozzáférés ellenőrzése: Alap szinten a fejlesztők interneten keresztül távolról hozzáférhetnek a rendszerekhez, fokozott szinten a vállalkozó telephelyén történik a fejlesztés, kiemelt esetben pedig a megbízó biztosít munkaterületet. Távoli hozzáférés tehát

csak alap esetben megengedett, de ilyenkor is gondoskodni kell ennek ellenőrzéséről és erős authentikációt felhasználó hozzáférésről (SSL, VPN). Kiemelt jogosultságú hozzáférés interneten keresztül nem megengedett.

HE-18 A vezeték nélküli hozzáférésre vonatkozó korlátozások: Alap és fokozott esetben megengedett a telephelyen vezeték nélküli hálózat használata a megfelelő biztonsági szint kiépítésével.

HE-19 A hordozható és mobil eszközök hozzáférés-ellenőrzése: Hordozható és mobil eszközöket csak alap biztonsági szintű fejlesztéseknél szabad használni. Ezek akár a fejlesztők saját tulajdonában is állhatnak. A mobil eszközökön azonban minden esetben meg kell valósítani az egyedi azonosítást és hitelesítést, a vírusvédelmet, a kritikus szoftverek automatikus frissítését, valamint a fejlesztéssel kapcsolatos információkat titkosítani kell. A mobil eszközökről kiemelt jogosultságot igénylő központi műveletek nem megengedettek.

HE-20 Külső informatikai rendszerek használata: A fejlesztéssel kapcsolatos információk csak a vállalkozó és a megrendelő rendszerein tárolhatók. Alap esetben a fejlesztők saját tulajdonú számítógépein is lehetnek ilyen információk, de csak olyan részletezettséggel, mely a teljes rendszer biztonságos működését nem befolyásolja (pl. részkódok, felhasználói dokumentumok fejezetei stb.)

Naplózás és elszámoltathatóság

NA-1 Naplózási és elszámoltathatósági szabályzat és eljárásrend: A munkaállomásokon, szervereken és fejlesztői rendszerekben az adott termék biztonsági ajánlásaiban szereplő részletezettséggel kell lokális naplózást folytatni. A naplóállományok hozzáférésekkel kapcsolatos bejegyzéseit havi szinten kell ellenőrizni, más bejegyzéseket a rendszeres felülvizsgálat illetve rendkívüli események kivizsgálása során kell áttekinteni.

NA-2 Naplózandó események: A naplózandó események körét a fejlesztői rendszer biztonsági ajánlásai és lehetőségei alapján kell meghatározni a fejlesztői rendszer tervezése során.

NA-3 A naplóbejegyzések tartalma: A naplóbejegyzéseket a biztonsági ajánlások és a rendszer adta tartalommal kell létrehozni. A részletezettségnek olyannak kell lennie, hogy abból az esemény visszakövethető legyen.

NA-4 Napló tárkapacitása: A naplózás tervezésénél becsléseket kell készíteni a várható logmennyiségre vonatkozóan, és ezek alapján kell az élesben tartott naplóállományoknak

tárhelyet biztosítani. A gyakorlatban elégséges az adott fejlesztői szerver háttértára, mely a megfelelő archiválás mellett nem jelent szűk keresztmetszetet.

NA-5 Naplózási hiba kezelése: A naplózási hibákról a rendszerek automatikus e-mailben riasztják az üzemeltetőket, akik a lehető leghamarabb beavatkoznak a hiba elhárítása érdekében.

NA-6 Napló figyelése, vizsgálata és jelentések készítése: A naplóállományok átvizsgálásához elégséges az adott rendszer adta lehetőségeket használni (pl. grep, Windows Event Manager).

NA-7 Naplócsökkentés, naplóriport készítése: A hozzáférésekről havi szinten riportot kell előállítani, amit az adott rendszer adta lehetőségekkel lehet generálni (pl. reguláris kifejezésekkel).

NA-8 Időbélyegek: A fejlesztői szervereket és a vállalkozó tulajdonában álló munkaállomásokat egy központi órához kell szinkronizálni.

NA-9 A napló-információk védelme: A naplóbejegyzésekhez csak kiemelt jogosultsággal lehet hozzáférni, törlésük csak az archiválás után megengedett. A törlést az üzemeltetési vezető a Biztonsági Vezető jelenlétében hajthatja végre.

NA-10 Letagadhatatlanság: A letagadhatatlanságot a naplóállományokban tárolt felhasználói azonosítók biztosítják. Amennyiben visszaélést követnek el, az adott felhasználó projektben való részvétele a kivizsgálás végéig felfüggeszthető. Amennyiben a kivizsgálás során nem tisztázódik a felhasználó felelőssége, és a visszaélés szintje ezt megköveteli, a kivizsgálásba külső felek is bevonhatók. Mivel a naplóállomány sértetlensége nem teljeskörűen biztosított, azt kizárólagos bizonyítékként felhasználni nem lehet.

NA-11 A naplóbejegyzések megőrzése: A naplóállományokat rendszeres időközönként archiválni kell, és azt a projekt végéig meg kell őrizni.

Rendszer- és kommunikációvédelem

RV-1 Rendszer- és kommunikációvédelmi szabályzat és eljárásrend: Létre kell hozni egy olyan szabályzatot, mely egyértelműen meghatározza a rendszerekre és a kommunikációra vonatkozó szabályokat. A szabályok alapvetően a bevett gyakorlatra kell, hogy épüljenek.

RV-2 Alkalmazások szétválasztása: A központi fejlesztői eszközök esetén a felhasználói és üzemeltetői felületeknek el kell különülniük.

RV-3 Biztonsági funkciók elkülönítése: Amennyiben a fejlesztés logikailag vagy biztonságilag megkívánja, a fejlesztői rendszereket el kell választani egymástól, például ha egyes modulok biztonsági szintje kiemelt, másoké csak fokozott.

RV-4 Információmaradványok: Az információmaradványok kérdésével a fejlesztői környezetben nem szükséges foglalkozni.

RV-5 Szolgáltatásmegtagadás elleni védelem: A fejlesztői rendszer rendelkezésre állása nem kritikus, így szolgáltatás megtagadásos támadás ellen preventív védelem beépítése nem szükséges. Amennyiben ilyen támadás bekövetkezik a Biztonsági Vezetőnek meg kell vizsgálnia az esetleges javító intézkedések bevezetésének lehetőségeit.

RV-6 Erőforrás-prioritás: Az előző ponthoz hasonlóan kell az erőforrások prioritását kezelni.

RV-7 A határok védelme: A fejlesztői rendszernek nem lehet olyan eleme, mely az internetről direkt módon elérhető. Ezért olyan határvédelmi rendszert kell kialakítani, mely alap biztonsági esetben lehetővé teszi az internetről érkező erős authentikációs megoldások használatát (SSL, VPN, stb.), más esetben azonban teljesen elszigeteli a fejlesztői rendszereket az internet felől. A belső hálózatot úgy kell kialakítani, hogy a fejlesztői szerverek és a fejlesztői munkaállomások külön hálózati szegmensben helyezkedjenek el, és csak a feltétlenül szükséges kapcsolatok legyenek engedélyezve. A fejlesztői szervereket esetlegesen külön-külön alhálózatokba lehet szervezni szeparációs célból.

RV-8 Az adatátvitel sértetlensége: Interneten keresztüli munkavégzés során minden fejlesztéssel kapcsolatos információ sértetlenségét garantálni kell. Ez azt jelenti, hogy vagy sértetlenséget garantáló hálózati kapcsolatot kell felépíteni (SSL, VPN) vagy digitálisan aláírt üzeneteket kell küldeni (e-mail).

RV-9 Az adatátvitel bizalmassága: Az előző ponthoz hasonlóan titkosított módon kell az adatátvitelt folytatni mind online (SSL, VPN), mind aszinkron esetben (e-mail).

RV-10 A hálózati kapcsolat megszakítása: A hálózati kapcsolatot nem szükséges automatikusan megszakítani a fejlesztői rendszerben.

RV-11 Megbízható útvonal: A korábban ismertetett eseteken kívül nem szükséges megbízható útvonal felépítése.

RV-12 Kriptográfiai kulcs előállítása és kezelése: A kriptográfiai kulcsokat, melyeket pl. digitális aláírásra vagy SSL hozzáféréshez generálnak, úgy kell előállítani, hogy ez a

legkisebb adminisztratív terhet jelentse a fejlesztők számára. Lehetséges piaci tanúsítványok használata, de akár OpenSSL alapú PKI megoldások használata is.

RV-13 Jóváhagyott kriptográfia alkalmazása: A kriptográfiai kulcsokat a bevált algoritmusokkal kell generálni. Így többek között elfogadott az RSA, AES, SHA-1 vagy SHA-256 algoritmusok használata.

RV-14 Sértetlenség-védelem nyilvános hozzáférés esetén: A fejlesztői rendszerben nem lehetnek nyilvános hozzáférésű szerverek.

RV-15 Telekommunikációs szolgáltatások korlátozása: A fejlesztés során csak olyan IP alapú telekommunikációs megoldásokat lehet használni, melyek adatútvonala befolyásolható, azaz a kapcsolat létrehozásához nem lép fel idegen szerverre. Így megengedett belső csevegő rendszer és belső kiépítésű VoIP használata, de nem megengedett a széles körben elterjedt Skype, MSN Messenger és hasonlók felhasználása annak ellenére, hogy ezek elméletileg megfelelő titkosítást használnak.

RV-16 Biztonsági paraméterek továbbítása: A fejlesztői rendszerek közötti adatátvitel során különleges biztonsági paraméterek hozzárendelése nem szükséges.

RV-17 Nyilvános kulcsú infrastruktúra-tanúsítványok: A nyílt kulcsú kriptográfia kulcsaihoz tartozó tanúsítványok sajátak vagy hitelesítés-szolgáltató által kibocsátottak is lehetnek.

RV-18 Mobil kód korlátozása: A vállalkozó által üzemeltetett munkaállomásokon a böngészőket a biztonsági ajánlásaik szerint kell beállítani. Ezen belül a mobil kódok korlátozását is az ajánlások szerint kell beállítani.

RV-19 Interneten Keresztüli Hangátvitel (VoIP): A VoIP alapú hangátvitel használata megbízható szolgáltató közbeiktatásával megengedett.

RV-20 Biztonságos név-/címfeloldó szolgáltatások (Hiteles forrás): A belső használatú DNS szerverre nincsenek különleges biztonsági előírások.

RV-21 Biztonságos név-/címfeloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás): A belső használatú DNS szerverre nincsenek különleges biztonsági előírások.

RV-22 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén: A belső használatú DNS szerverre nincsenek különleges biztonsági előírások.

RV-23 Munkaszakasz hitelessége: A munkaszakaszok hitelességével kapcsolatban nincsenek különleges biztonsági előírások.

Az egyes biztonsági szintek részletes követelményeit a 3. mellékletben található táblázatban foglalom össze.

2.5 Fizikai biztonsági követelmények a fejlesztés helyszínén

Az informatikai rendszerek fizikai biztonsági követelményeit hagyományosan jól szabályozza a magyar jogszabályi környezet, sőt sokszor csak ezt a területet szabályozza. A fejlesztői környezetre vonatkozóan azonban ezen a területen sem találhatunk előírásokat. Az e-közigazgatási környezetben két olyan mérvadó forrást találhatunk, melyből az elvárások levezethetők. Egyrészt a KIB 25. számú ajánlásának Információbiztonsági Irányítási Követelményei alap és fokozott esetben, másrészt a 90/2010. (III. 26.) Korm. rendelet 9. fejezete kiemelt szinten ad támpontot. Ezekben különböző biztonsági szintek és biztonsági zónák vannak meghatározva, melyeket egységes rendszerbe foglalva levezethetők a fejlesztői környezet fizikai biztonsági intézkedései. [40]

A fizikai biztonság tehát a biztonsági zónákra, létesítményekre és műszaki berendezések biztonságára fókuszál. Az ISO 27002 szabvány alapján a KIB 25. ajánlás az alábbi felosztást használja:

- Biztonsági szegmensek
    - Biztonsági határok
    - Beléptetési intézkedések
    - Létesítmények és helyiségek biztonsága
    - Védelem a külső és környezeti fenyegetettségek ellen
    - Munkavégzés a biztonsági szegmensekben
    - A kiszolgáló területek és raktárak biztonsági elkülönítése
- A berendezések fizikai védelme
    - A műszaki berendezések elhelyezése és védelme
    - Energiaellátás
    - A kábelezés biztonsága
    - A berendezések karbantartása

- A telephelyen kívüli berendezések védelme
- A berendezések biztonságos tárolása és újrafelhasználása
- Az eszközök selejtezése, elvitele

A KIB 25. ajánlás 5 szintű skálát használ, melyet a kárérték várható szintje alapján sorol be. Mivel a műszaki előírásokat ehhez a skálához igazítja, valamilyen módon **meg kell ezt feleltetnem** az értekezésben használt három biztonsági szintnek. Ehhez a kárértékeknél definiált adatminősítések szolgáltatnak információt. Ha társítjuk még a kormányrendelet 17. §-nak meghatározásait, akkor egyértelműen kialakul az összerendelés

- 0. szint: „nem védett adat (nem minősített) bizalmassága, sértetlensége, vagy rendelkezésre állása sérül.” = alap biztonsági szint.
- 1. szint: "Korlátozott terjesztésű!" minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, személyes adatok bizalmassága vagy hitelessége sérül, csekély értékű üzleti titok, vagy belső (intézményi) szabályzóval védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = fokozott biztonsági szint.
- 2. szint: „Bizalmas!” minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, személyes adatok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, közepes értékű üzleti titok vagy egyéb jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = Korm. rendelet szerinti II. osztályú biztonsági terület = kiemelt biztonsági szint.
- 3. szint: „Titkos!” minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül. = Korm. rendelet szerinti I. vagy II. osztályú biztonsági terület = kiemelt biztonsági szint.
- 4. szint: „Szigorúan titkos!” minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, nagy tömegű szenzitív személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, nagy értékű üzleti titok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = Korm. rendelet szerinti I. osztályú biztonsági terület = kiemelt biztonsági szint.

Alaposabban szemrevételezve a követelményeket, levonható az a következtetés, hogy a KIB 25. ajánlás lefedi mindhárom biztonsági szintet, de a követelmények nem arányosan változnak, ezért szükség van az ajánlás szintjeinek újradefiniálására. Ezt támasztja alá az is, hogy a fizikai biztonsági követelményeket taglaló fejezet is három csoportba osztja az öt szintet. Emellett a kormányrendelet sem a minősítési szintek szerint tesz különbséget a biztonsági területek között, bizalmas minősítés felett a hozzáférés mértéke különbözteti meg a két követelményrendszert. **Az értekezésben ezért a következő, az alkalmazás céljainak jobban megfelelő minősítési rendszert javasolom használni.**

- 0. szint: nem védett adat (nem minősített) bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = alap biztonsági szint.
- 1. szint: személyes adatok bizalmassága, hitelessége vagy rendelkezésre állása sérül, csekély értékű üzleti titok, vagy belső (intézményi) szabályzóval védett adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = alap biztonsági szint.
- 2. szint: szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága, hitelessége vagy rendelkezésre állása sérül, közepes értékű üzleti titok vagy egyéb jogszabállyal (orvosi, ügyvédi, biztosítási, banktitok stb.) védett bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = fokozott biztonsági szint.
- 3. szint: "Korlátozott terjesztésű!" minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, nagy tömegű szenzitív személyes adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, nagy értékű üzleti titok bizalmassága, sértetlensége, vagy rendelkezésre állása sérül. = fokozott biztonsági szint.
- 4. szint: „Bizalmas!” minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, „Titkos!” minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, „Szigorúan titkos!” minősített adat bizalmassága, sértetlensége, vagy rendelkezésre állása sérül, = Korm. rendelet szerinti I. vagy II. osztályú biztonsági terület = kiemelt biztonsági szint.

Mivel a fejlesztői környezetnek egyenszilárdságú védelmet kell nyújtania a későbbi üzemeltetési környezettel, egyértelműen adódnak a fizikai biztonsági elvárások. Fontos leszögezni, hogy az elvárások azért ilyen szigorúak, mert bár lehet, hogy minősített adatokat kezelő rendszer fejlesztője nem találkozik minősített adattal, de a megrendelő közigazgatási szerv részére ezzel lehet azt a garanciát biztosítani, hogy az alkalmazás az első kódsortól

kezdve megbízható, nem szivárog ki olyan dokumentáció vagy forráskód-részlet, ami a későbbiekben aláásná a rendszer biztonságát.

Az előző fejezetben a munkavégzés három területét különböztettem meg: az első a fejlesztői munkaállomás, a második a központi fejlesztői architektúra, a harmadik részt pedig azok az alkalmazások jelentik, melyek közvetlenül a fejlesztési folyamathoz kapcsolódnak. Ez praktikusan két biztonsági zónát jelent. A fejlesztői munkaállomások általában az adminisztratív zónában helyezkednek el, a fejlesztői architektúra és alkalmazások pedig a biztonsági szegmensben helyezkednek el. Kivétel ez alól az alap biztonsági szinten meghatározott fejlesztői munkaállomások köre, melyre a KIB 25. ajánlás telephelyen kívüli berendezések védelméről szóló előírásokat kell alkalmazni.

2.6 Következtetések

A jelenlegi központi közigazgatási rendszerek fejlesztésének egy részénél túlzott biztonsági követelményeket fogalmaznak meg. Ráadásul a szoftverfejlesztők tapasztalatom szerint projektről projektre más eljárásokkal dolgoznak, amik többnyire nincsenek megfelelően dokumentálva, így a Common Criteria szerinti fejlesztéshez nincsenek meg a szükséges alapok. Kiemelten két olyan terület van, aminek tapasztalatom szerint nincs hagyománya, kultúrája hazánkban, ez pedig a fejlesztői környezet biztonsága és a sebezhetőség-vizsgálat, így ezeket vettem alaposabb vizsgálat alá.

A második fejezetben **a fejlesztőkkel szembeni fizikai, adminisztratív és logikai követelményeket határoztam meg**. Alapelvként azt javasoltam, hogy a közigazgatási szervnek arról kell meggyőződnie, hogy a fővállalkozó, aki elsődlegesen felelős a fejlesztés és üzemeltetés sikeres végrehajtásáért, megfelelő szabályzati rendszerrel dolgozik. Az alvállalkozók ellenőrzése minden esetben a Fővállalkozó Biztonsági Vezetőjének a feladata, aki ezt belső auditok során teszi meg. Mivel a megrendelőnek érdemi beleszólása nincsen a fejlesztés folyamatába, így szerződéses feltételként kell megfogalmaznia azt az igényét, hogy a fejlesztés biztonságát, így a szabályzati rendszert ellenőrizhesse. Erre három lehetséges megoldást mutattam be.

Áttekintettem a KIB 28. ajánlás releváns részeit, és megállapítottam, hogy az magas szintű elvárásokat fogalmaz meg, amivel véleményem szerint jelen értekezés összhangban van, és bár a biztonsági szintek megfogalmazásában vannak eltérések, **dolgozatom felhasználható az ajánlás gyakorlati megvalósításában**. Emellett megállapítottam, hogy a magyar jogszabályok még a minősített adatokkal foglalkozó rendszerek tekintetében sem írnak elő a

fejlesztői környezetre informatikai biztonsági követelményeket, de legalább kiindulópontot jelentenek a személyi és fizikai biztonsági intézkedésekre.

A fejezetben **ajánlást tettem a közigazgatási alkalmazások fejlesztését végző szervezetek biztonsággal kapcsolatos szerepköreire és ezek felelősségi területeire**, **valamint ezek átvilágítási követelményeire**. Emellett a KIB 25. és 28. ajánlás logikai és fizikai követelményeit **átfordítottam a fejlesztési környezet követelményeire**, az értekezésben használt besorolást követve.

3. FEJEZET

AZ ELEKTRONIKUS KÖZIGAZGATÁSI ALKALMAZÁSOK SEBEZHETŐSÉGI TESZTELÉSE ÉS ENNEK SZERVEZETI HÁTTERE

Az elmúlt években folyamatosan kapunk híreket arról, hogy egy-egy informatikai rendszer kiesése milyen károkat okozott egy adott ország normális működésében. A komoly hadi- és informatikai kultúrával rendelkező országok éppen ezért a XXI. század elejének egyik legkomolyabb kihívásaként kezelik a kritikus információs infrastruktúrák védelmének, vagy éppen támadásának kérdését. Tanulmányok sora, például Clay Wilson kongresszusi beszámolója elemzi, hogy milyen láncreakciót válthat ki egy kritikus információs rendszereket érintő átfogó – informatikai, elektromágneses és fizikai támadásokat is magába foglaló – cselekménysorozat. [41] Magyarországon is egyre többet foglalkoznak ezzel a közkeletű néven kiberhadviselésnek nevezett területtel, hiszen a kockázatok hasonlóak, mint minden fejlett, vagy akár fejlődő ország esetén. [42]

Jelen fejezetben megkísérlem felvázolni egy olyan, kritikus információs infrastruktúrákat érintő támadás forgatókönyvét, mellyel akár napokig tartó működési zavarok érhetők el hazánkban.[3] Természetesen ez csak egy lehetséges támadási forgatókönyv, mely az utóbbi években végrehajtott valós támadások elemzésével alakul ki. A végrehajtáshoz szükséges információk mindegyike nyílt forrásból származik, amely mindenki számára rendelkezésre állhat. A támadások mindegyike aránylag kis költséggel, kevés ember bevonásával végrehajtható. Ugyanakkor ezen akciók legnagyobb kockázata pontosan ebben áll. A szcenárió túlmutat az elektronikus közigazgatáson, célom ezzel bemutatni, hogy a sebezhetőség-vizsgálati módszerek során milyen összetett támadási eszköztárra kell számítani.

A fenyegetések ismertetése után ismertetésre kerül egy olyan szervezet felállításának lehetősége, mely katonai, kormányzati és civil szakemberek bevonásával hatékonyan tudja kivédeni az informatikai támadásokat, illetve fel tudja készíteni a kritikus információs infrastruktúrákat az ilyen kihívásokra. Kutatásomnak nem célja, hogy meghatározza a kibervédelem szervezetét, de olyan részeredményeket, meglátásokat ismertetek, melyek

[3] A kritikus információs infrastruktúrákkal behatóbban nem foglalkozom, erről ld. Kovács László „Kritikus információs infrastruktúrák Magyarországon” c. tanulmányát, mely elhangzott a Robothadviselés 7. Tudományos Szakmai Konferencián.

további kutatások alapja lehet, emellett bemutatja, hogy a sebezhetőség-vizsgálatok során milyen humán erőforrásra lehet támaszkodni. Ezt támasztja alá az a kérdőíves kutatás is, mely a magyar hacker közösség kibervédelemhez való viszonyát mutatja be.

A fejezet második részében bemutatom, hogy milyen szakmailag elfogadott módszerek állnak rendelkezésre a közigazgatási alkalmazások biztonsági tesztelésére. A jógyakorlatokból kiindulva olyan behatolás-tesztelési eljárás kerül kidolgozásra, melynek alapján az érintett szervezetek egységes, ellenőrizhető teszteket hajthatnak végre saját kritikus alkalmazásaikon.

3.1 Kibertámadási forgatókönyv a magyar kritikus információs infrastruktúrák ellen

Az események láncolatának bemutatása előtt hangsúlyozni kell, hogy 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 jelentenek csak. Akkor azonban, ha az informatikai támadásokat kiegészítik az információs rendszerek egyes – jól megválasztott – elemei ellen végrehajtott fizikai támadások, akkor a kár óriási lesz. Az informatikai támadás és a kibertámadás közötti különbséget pontosan ez adja: kibertámadás esetén fizikai támadás is indul az információs rendszerek ellen. Ebben az esetben a megtámadott rendszerek, és közvetett módon, azok egymástól való kölcsönös függősége miatt, számos más rendszer működésképtelenné válik néhány óráig, vagy akár több napig, több hétig is. Ebben az esetben a probléma már nemcsak hazai vonatkozású lesz, hanem nemzetközivé is válik, hiszen nagyon kevés rendszertől eltekintve ezek a rendszerek országhatárokon átnyúló felépítésűek, amelyek ráadásul nemcsak egymás fizikai működésétől függenek, hanem szolgáltatásaikban is nagyban egymásra vannak utalva.

Számos bekövetkezett támadás elemzésével és értékelésével, valamint a Digital Pearl Harbor elnevezésű amerikai szcenárió tapasztalatainak felhasználásával a Digitális Mohácsnak elnevezett támadás lehetséges forgatókönyvét három egymást követő részre lehet osztani.[4] [43][44]

Az első rész a felderítés és az információszerzés. A támadásokat megelőzően a majdani támadóknak szükséges a sebezhető és sérülékeny pontok behatárolása. A tapasztalatok szerint ez az információgyűjtés elvégezhető kizárólag nyílt források felhasználására támaszkodva is, bár a gyanú szerint sokszor titkosszolgálati adatgyűjtés is támogatja ezt. A forgatókönyv

[4] A Digitális Mohács forgatókönyv Dr. Kovács Lászlóval közös publikációként jelent meg a hivatkozott helyen.

összeállításakor a nyílt források közül is csak az internet, illetve annak e célra történő felhasználhatósága került vizsgálat alá. A tapasztalatok szerint egy – az információs rendszerek elleni – támadáshoz, illetve támadássorozathoz megfelelő mennyiségű és minőségű adat szerezhető az internet segítségével, anélkül, hogy bármilyen titkos vagy védett rendszerbe informatikai betörést kellene végrehajtani. Természetesen titkosszolgálati módszerekkel vagy aktív informatikai eljárásokkal lényegesen pontosabb információk állhatnak a támadók rendelkezésére.

A második részben – a felderítést követően – pszichológiai műveletek végrehajtása jelenhet meg, amelyek jól tetten érhetőek a legtöbb terrorista jellegű támadás elsődleges céljai között. Bár jelen forgatókönyv nem definiál konkrét elkövetőket, vagy elkövetői csoportokat, mégis a potenciális támadók számára a támadások pszichológiai hatása figyelemre méltó lehet. Már ekkor is jelen lehetnek informatikai támadások – pl. hamis hírek elhelyezés online hírportálokon –, amelyek felhívják a figyelmet a közelgő támadásokra. Ennek komoly jelentősége van, hiszen naponta tapasztaljuk, hogy a médiában bemutatni egy-egy informatikai támadást igen nehéz feladat, ennek következtében számos alkalommal még a sikeres támadásokat és azok következményeit is elhallgatják a megtámadott rendszerek üzemeltetői. Ebben élen járnak a bankok, bár az ő esetükben (is) komoly anyagi veszteséget okozhat – akár közvetett módon, pl. bizalomvesztés miatt – egy-egy ilyen támadás. Így többé-kevésbé érthető, ha nem, vagy nem szívesen ismertetik az ilyen eseteiket. Ugyanakkor azt is el kell mondani, hogy a kritikus ágazatok közül pont a pénzügyi szektor, ezen belül is a bankok azok, amelyek a lehető legtöbb figyelmet fordítják a fizikai védelem mellett az információs rendszereik védelmére.

A harmadik, egyben a legfontosabb fázis a kritikus információs infrastruktúrák komplex támadásának megtervezése és végrehajtása a megszerzett adatok és információk alapján. Mindezeknek megfelelően a Digitális Mohács forgatókönyv a következő sorrendben határozza meg a megtámadni kívánt célokat:

- elektronikus média;
- műsorszórás;
- internetes média;
- pénzügy;
- közlekedés;
- telekommunikáció;
- internet;

- villamosenergia-szolgáltatás.

Elektronikus média

Az első támadási célpont tehát az elektronikus média. A különböző kereskedelmi és közszolgálati médiumok természetesen ma már számítógépeket alkalmaznak a műsorok szerkesztésére és műsormenet biztosítására. Ezek támadhatóak informatikai eszközökkel, ráadásul ezen médiumok internetes oldalai is komoly látogatottsággal bírnak. Az adásmenetbe való beavatkozás jelentheti az adás teljes leállítását is, de például a képernyőkön lévő információcsíkok hamis hírekkel történő megjelenítése sem elképzelhetetlen. Ugyanebben az időben az adott médium weboldalán elhelyezett – szintén hamis – hírek már komoly hatást gyakorolhatnak a nézőkre, hiszen máris két –, bár ebben az esetben egymástól egyáltalán nem független – hírforrás mondja ugyanazt. A pszichológiai hadviselés tehát elkezdődik, amely tovább fokozható, amennyiben elérjük, hogy ne legyen földfelszíni műsorsugárzás. A hazai földfelszíni műsorsugárzás nagyban függ a budapesti Széchenyi-hegyen található adótól. A bárki által elérhető Google Earth szolgáltatás segítségével nagyon világosan látszik, hogy ez az adó és átjátszó komplexum a környező utakon szabadon – néhány tízméteres – távolságra megközelíthető. Ez a távolság már bőven elegendő, hogy a támadó a közelben egy elektromágneses impulzus bombát elhelyezzen. Ennek receptje az interneten nem túl hosszas kutakodás után szintén elérhető. Ez a bomba nem a hagyományos kinetikus energiával, hanem egy óriási, nagyon rövid ideig tartó elektromágneses energia-impulzussal pusztít. Amennyiben ez az akár több gigawattnyi energia félvezetőket, elektronikus áramköröket tartalmazó berendezésekre jut, akkor azok ideiglenesen, vagy véglegesen használhatatlanná válnak. Esetünkben ez azt jelenti, hogy ha a Széchenyi-hegyi adótorony közvetlen közelében egy jól irányított ilyen elektromágneses impulzus bomba működésbe lép, akkor hazánk jelentős területén megszűnik a földfelszíni műsorsugárzás.

A U.S. Army War College által 2009-ben tartott „New Media and the Warfighter” workshop keretében elemzésre került a 2006-os Izrael és a Hezbollah közötti konfliktus új médiákat érintő vetülete. [45] A workshop összefoglalója kiválóan bemutatja, hogy mindkét fél élt a kibertér adta lehetőségekkel. Az elektronikus média megzavarására, és a sugárzott tartalom módosítására példa az Izraeli Védelmi Erők (IDF) 2006 júliusában végrehajtott akciója, melynek során a Hezbollah al-Manar nevű televíziójának adásába avatkoztak be, gúnyos és fenyegető üzeneteket küldve a nézőknek. Ugyanebben a konfliktusban került sor a Google Maps használatára is, melyet állítólagosan mindkét fél felhasznált a célpontok kijelöléséhez.

Tapasztalataink szerint, amennyiben nincs tévé, illetve rádióműsor, akkor az emberek jelentős része az internetes médiumok felé fordul hírekért.

Internetes hírportálok

Hazánkban megközelítőleg 1,5 millió ember látogat meg legalább egy internetes hírportált naponta. Ez a szám már önmagában is jelentős, de abban az esetben, ha nincs elérhető TV és rádió, akkor nagy valószínűséggel ez a szám eléri, vagy akár meg is haladja a 2,5-3 milliót. Ekkor már komoly befolyásoló tényezőként lehet számolni ezekkel a hírportálokkal a lakosság egészét tekintve. Itt következik a pszichológiai hadviselés következő fázisa. Hamis híreket elhelyezni a különböző hírportálokon, lévén azok meglévő, és többször bizonyított sebezhetősége és sérülékenysége, ha nem is könnyű feladat, mégis lehetséges. [46] Amennyiben ezek a hamis hírek egymással összefüggenek, illetve a különböző blogokon is megjelennek, már komoly mértékű pánikot is okozhatnak. Ilyen hamis hír lehet többek között egy pénzügyi válságra utaló figyelmeztetés. Az események ezután már igen gyorsan – látszólag egymással összefüggésben – követik egymást.

Szintén a már említett libanoni háborúban lehetett megfigyelni azt, hogy az izraeli médiumok beszámolóikban elsősorban a Hezbollah által az internetre feltöltött, szinte valós idejű hírekre támaszkodtak, mert a hivatalos tájékoztatások sokszor órákat késtek. Ezzel jelentősen tudták befolyásolni az izraeli közvéleményt. A hírek terjesztéséhez más országok feltört internetes hálózatait használták.

Pénzügy – banki rendszer

A hamis hírekkel párhuzamosan a pénzügyi rendszer informatikai hálózatait is támadások érik. Természetszerűleg hazánkban a közigazgatás pénzügyi működését tekintve a Magyar Államkincstár elleni támadással lenne elérhető a legnagyobb kár. Közvetett információk alapján azonban ez mind fizikailag, mind informatikailag megfelelően védve van. Ugyanakkor, a social engineering, azaz az emberi hiszékenységet kihasználó támadások itt sem zárhatók ki teljes mértékben. További támadási felület lehet az önkormányzatok informatikai kapcsolata a Kincstárral. Itt külön meg kell említeni újra azt a tényt, hogy egy-egy önkormányzat különösen sebezhető a nem egységesen, és számos helyen nem megfelelő szinten védett saját informatikai hálózata révén. Az ezek sebezhetőségére vonatkozó tanulmányok – a hálózatok támadható pontjainak meglehetős részletességgel történő bemutatásával – szintén elérhetőek az interneten. [47]

Ugyanakkor, a pénzügyi szektor további szereplői természetesen a különböző bankok. E bankok, illetve ezek központjai két-három nagyobb centrumban helyezkednek el Budapest belvárosában. Korábban már történt utalás rá, hogy informatikai támadást intézni közvetlenül a bankok ellen nagyon nehéz, hiszen kimagaslóan jó védelemmel rendelkeznek ezen a téren. Ennek ellenére, pont a centralizált fizikai elhelyezkedésük miatt a kommunikációs rendszereik – telefon-, fax-, internet-kapcsolat – fizikai elérése, majd azok működésképtelenné tétele egyszerre több bankot is megfoszthat a létfontosságú infrastruktúrától. Itt nem kell hatalmas dolgokra gondolni: néhány utcai kábelalagút szerelőnyílásának leemelése után hozzáférhetővé válnak azok a hagyományos és optikai kábelek, amelyek a gerincét jelentik az említett infrastruktúráknak. Bár a legtöbb pénzintézet rendelkezik tartalék telephellyel és vészforgatókönyvekkel erre az esetre, egyidőben történő kiesésük óriási problémákat okozna.

2011 elején Egyiptom vezetése 5 napra lekapcsolta az ország internet-elérését, így próbálva megállítani a tiltakozási hullámot. Az OECD 2011. február 4-én kelt rövid elemzésében rámutat arra, hogy ennek közvetlen költsége legalább 90 millió USD-ra tehető, de közvetett hatása ennél jóval magasabb, hiszen több hálózatfüggő iparág, így a pénzintézetek sem tudtak működni. [48] A fenti példa azt mutatja, hogy egy összehangolt, gondosan megtervezett támadás során a pénzintézeti szektor Magyarországon is valószínűleg milliárdos károkat szenvedne.

Közlekedés

A pénzügyi terület támadása után következhet a közlekedés támadása. A forgatókönyvben csak a budapesti metró és a BKV forgalomirányításának zavarása, illetve Budapest 3-4 frekventált helyén lévő közlekedési jelzőlámpa működésébe történő beavatkozás kerül felvillantásra.

A budapesti 3-as metróvonal csúcsidőben 26-27 ezer utast szállít irányonként minden órában. A metró biztonsági, valamint forgalomirányítási megoldásai nagyon részletes technikai leírásokkal, képekkel és ábrákkal nyíltan hozzáférhetőek az interneten. [49] Alapszintű elektronikai és informatikai ismeretekkel, valamint némi helyismeret birtokában, a metró alagútjaiban ezek megtalálhatóak és manipulálhatóak. Az alagútba való bejutás sem megoldhatatlan feladat, hiszen a budapesti metró esetében még a közelmúltban is láthattunk különböző videómegosztó portálokon olyan amatőr videókat, amelyeket fiatalok készítettek – az egyébként közel sem veszélytelen – metrókocsik ütközőin történő „utazásaikról”.

Ha egy szerelvény leállása megtörténik a metróalagútban két állomás között, akkor több száz ember rekedhet ott. Amennyiben a biztosító berendezések meghibásodása miatt nem csak egy szerelvényt kell leállítani, akkor akár több ezer ember is az alagutakban reked hosszabb-rövidebb ideig. A pszichológiai hatás itt is komoly mértékű lesz, főleg akkor, ha ezeket a metróleállásokat előre – akár néhány perccel azok bekövetkezése előtt – az online médiumokon bejelentik a támadók.

A másik „találomra" kiválasztott cél a BKV forgalomirányítása, illetve ezen belül is az elektronikus járműkövető rendszer. Ez a rendszer az interneten nyilvánosan elérhető információk szerint egy olyan elektronikus és informatikai megoldásokat közösen tartalmazó rendszer, amely néhány helyen vezetéknélküli internet technológiát (WLAN) is használ. [50] Abban az esetben, ha ezen a WLAN-on keresztül a támadók be tudnak hatolni a vállalat rendszerébe, akkor annak működése befolyásolható vagy akár le is állítható. Ha a budapesti tömegközlekedési járművek közül csak a belvárosban közlekedők, illetve a főbb közlekedési csomópontok – pl. autópályák bevezető szakaszai, hidak – környékén lévő járatok járművei esetében sikerül azt elérni, hogy a diszpécserek nem, vagy csak késve kapjanak információt a járművek pillanatnyi helyzetéről, akkor az nagy valószínűséggel rövid időn belül komoly torlódásokhoz vezet. Jól megválasztva az egyébként is csúcsforgalmat jelentő napszakot, valamint a közlekedés szempontjából a hétköznapokon is neuralgikus pontokat, olyan mértékű torlódás okozható, amely már Budapest határain is túl fog nyúlni. Számos – az autópályák bevezető szakaszai mellett található – logisztikai központ csak nehezen, vagy egyáltalán nem lesz megközelíthető, a mentők és tűzoltók közlekedése szintén nehézkessé válik, és alapvető ellátási problémák is felléphetnek nagyon rövid időn belül. A közlekedési nehézségeket tovább fokozva egyszerű fizikai rombolással – néhány kulcsfontosságú helyen lévő – forgalomirányító jelzőlámpa működésének megakadályozása következik. Ez összességében csak a megfelelő helyek előzetes kiválasztásában jelenthet némi nehézséget, mivel fizikailag – és tegyük hozzá informatikailag – ezek az eszközök csak minimális mértékben vannak védve. Ráadásul nyitott szemmel járva a városban a „forgalomirányítás" felirat messziről szembeszökik azokon a kapcsolószekrényeken, amelyek gyakorlatilag minden forgalomirányító jelzőlámpával ellátott kereszteződés közelében megtalálhatóak.

2006. augusztus 21-én a Los Angelesben működő forgalomirányítási rendszert törte fel két dolgozó. [51] Ezen a rendszeren keresztül több forgalomirányító lámpa működését befolyásolták. Szerencsére nem történt ebből tragédia, de rámutat arra, hogy a rendszerek alapos ismeretével nem elképzelhetetlen egy ilyen támadás.

Kommunikáció és internet-szolgáltatás

A következő célpont a telekommunikáció valamint az internet-szolgáltatás.

Közigazgatásunk és gazdaságunk is jelentős mértékben függ a különböző telekommunikációs szolgáltatásoktól és az internet alapú megoldásoktól. A tőzsdétől kezdve a már említett bankokon keresztül számos gazdasági társaság és vállalat, illetve maga a közigazgatás is csak nehezen vagy egyáltalán nem működik ezen szolgáltatások nélkül. Az informatikai támadások ezeken a területeken csak részleges károkat okozhatnak, mivel a védelem itt a legfelkészültebb. Ugyanakkor e rendszerek fizikai infrastruktúrái közel sem ilyen jól védettek. A közelmúltból is emlékezetesek lehetnek azok a példák, amikor véletlenül – pl. talajmunkák végzése során –, vagy szándékos módon – pl. kábellopások miatt –, kommunikációs gerincvezetékeket vágtak el. Egy-egy ilyen esetben több ezer ügyfél nem jutott napokig telefon- és internet-szolgáltatáshoz. [52] Az egyik nagy telekommunikációs cégünk gerincvezetékének véletlen elvágása pedig, más – ezzel egy időben, de e kábelvágás közvetett hatására bekövetkezett – műszaki hiba miatt azt okozta, hogy Magyarország internetes adatforgalma közel a tizedére esett vissza több órán keresztül.

Az egyik legnagyobb hazai mobiltelefon-szolgáltató rendszerében bekövetkezett rendszerhiba miatt több millió ügyfél közel fél napig csak akadozva tudta használni a GSM hálózatot. [53]

Ezek persze jelentős részben műszaki meghibásodások, de ott a figyelmeztető jel, amely nagyon komolyan felhívja figyelmünket e rendszerek sérülékenységére.

Az Oroszország és Grúzia közötti 2008-as konfliktus egyik kiegészítő tevékenysége volt Grúzia internetes forgalmának elvágása a külvilágtól. Ahogy a NATO kibervédelemmel foglalkozó Cooperative Cyber Defence Centre of Exellence központjának elemzéséből kiderül, a fegyveres beavatkozás mellett mindkét fél informatikai műveleteket is végrehajtott. [54] Ezek közül az egyik – nem megerősített – tevékenység volt Grúzia internetes blokád alá helyezése. Ennek módja az volt, hogy az ország felé irányuló lekérdezéseket Oroszország felé irányították, majd ezeket elkezdték szűrni. A technológia hatékonyságát mutatja Pakisztán esete, ahol a Youtube-szolgáltatást próbálták letiltani az országban, de egy rossz konfiguráció miatt az oldal teljesen elérhetetlenné vált az egész világon. [55]

Villamosenergia-szolgáltatás

A teljes káosz a villamosenergia-szolgáltatás bénításával érhető el. Ma már közhely, hogy áram nélkül nincs semmi. Az eddig felsorolt rendszerek mindegyike csakúgy, mint az összes infrastruktúraelem, függ a villamos-energiától. Ennek megfelelően az egész országra kiterjedő

igazi és nagymértékű kár a villamosenergia-rendszer bénításával, esetleges pusztításával érhető el.

Gyakran felteszik a kérdést: a villamosenergia-rendszer működésképtelenné tételéhez az erőműveket, ezen belül is az atomerőművet kell-e támadni? A válasz egyértelmű: nem. A villamosenergia-szolgáltatás biztosításában és koordinációjában a rendszerirányító a központi elem. Ezért nem az erőművek, hanem a rendszerirányító lesz a célpont, kiegészítve néhány kulcsfontosságú helyen lévő távvezetékkel. Az informatikai támadás ebben az esetben kevés szerepet kap, hiszen a rendszerirányító többszörösen védett, fizikailag is leválasztott informatikai hálózatokat használ. Ugyanakkor többek között a SCADA felügyeleti és adatgyűjtő rendszer alkalmazása magában rejti a támadhatóság veszélyét.

A támadást megelőzően az információszerzésben itt is szerepet kap az információtechnológia, hiszen az interneten csak néhány kattintás és elénk tárul a rendszerirányító pontos címe, és térképen még az épület pontos elhelyezkedését is láthatjuk. Hasonlóan a földfelszíni műsorszórás hazai központi adótornyának épületéhez, a villamosenergia rendszerirányítójának budapesti épülete is nagyon közelről megközelíthető. Ez egy elektromágnes impulzus bomba alkalmazása esetén azt eredményezheti, hogy az épületben használt számítógépek és elektromos berendezések üzemképtelenné válnak. A támadó eszköz egy – az épület közvetlen közelében – parkoló autóban, akár távirányítással is működésbe hozható, amely a későbbi felderítést majdhogynem lehetetlenné teszi, hiszen a jármű később egyszerűen el fog hajtani, hiszen fizikai (de még elektromos) kár nem keletkezett benne.

Nem úgy a rendszerirányító számítógépekre alapozott információs rendszereiben. Még abban az esetben is komoly fennakadás feltételezhető a villamosenergia-ellátás koordinációjában, és ezáltal az ország villamosenergia-ellátásában, ha bizonyos rendszerek az elektromágneses impulzusok ellen megfelelő szintű védelemmel rendelkeznek.

A támadás következő fázisa néhány kulcsfontosságú nagyfeszültségű távvezeték fizikai rombolása. Ezek a már említett Google Earth segítségével nagyon pontosan meghatározhatóak, hiszen a műholdas fényképeken kitűnően látszanak. Maga a rombolás pedig ezen információk birtokában már sokkal könnyebben végrehajtható.

A Stuxnet kártékony kód megjelenése óta tudni lehet, hogy a SCADA rendszerek bizonyíthatóan sérülékenyek a klasszikus informatikai támadásokkal szemben, ami jelentősen befolyásolhatja egy tetszőleges ipari létesítmény, így a villamosenergia-termelő intézmények működését. A Stuxnet iráni atomlétesítmények berendezései ellen irányult, hatására komoly

zavarok keletkeztek. [56] Bár a kód igen kifinomult volt, és számos nem nyilvános információval kellett rendelkezni a megírásához, tapasztalatként leszűrhető, hogy nem lehetetlen egy ilyen támadás kivitelezése.

3.2 Kibervédelem az önkéntes tartalékos haderő keretei között

A Digitális Mohács forgatókönyv nem foglalkozik az elkövetők személyével. Ugyanakkor a támadások mind a terrorista jellegű, mind az országok közötti konfliktusok esetén bekövetkezhetnek. Ezek valószínűsége azonban eltérő. A tapasztalatok szerint a független csoportok, hacktivisták által elkövetett incidensek előfordulási lehetősége a legnagyobb, hiszen ezek a társulások nem kontrollálhatók, vagy kontrolljuk nem bizonyítható. Magyarország esetében is az ilyen támadásnak van a legnagyobb valószínűsége, hiszen a konfliktusokkal teli szomszédságpolitika bármikor elérheti azt a hatást, hogy a kormányoktól független szélsőséges csoportosulások néhány tízezer dollárnyi befektetéssel, mely akár nacionalista vállalkozói rétegtől vagy az alvilágtól is származhat, sikeresen zavarják meg hazánk mindennapos működését. [57] Többek között erre példa a Dél-Koreát ért kibertámadás 2009-ben és azóta többször is. [58] Az országok közötti hasonló konfliktusok bekövetkezési valószínűsége kicsi, ám az informatikai kémkedés valószínűleg mindennapos, így a kritikus információs infrastruktúrák védelme mindenképpen kiemelt fontosságú.

Míg a komoly hadi költségvetéssel rendelkező országoknak lehetősége van olyan hivatásos állomány létrehozására, amelynek elsődleges feladata a kibervédelem, a Magyarországhoz hasonló, szerény anyagi és humán lehetőségekkel rendelkező országoknak támaszkodnia kell a civil szférára is a védelem kialakításában. Észtország, mely elsőként szenvedett el összehangolt informatikai támadást, éppen ezért úgy döntött, hogy önkéntesekből álló kibervédelmi egységet hoz létre. [59] Az észt védelmi miniszter kezdeményezésére a kormány olyan döntést hozott, melynek keretében az ország IT biztonsággal foglalkozó szakembereiből egy speciális egységet állítanak fel az ország Védelmi Ligáján belül. A cél az, hogy 10 éven belül teljes értékű egységként működjön ez az egyébként civilekből álló csoport. A kiképzés célja elsősorban az, hogy a jelentkezők megismerjék a hadsereg működését, a hadviselés szabályait. Hasonló együttműködést javasol a Tartalékos Tisztek Nemzetközi Szövetsége (Inter allied Confederation of Reserve Officers – CIOR) is, mely 2011-ben rendezett varsói konferenciáján nyilatkozott a tartalékosok és hivatásosok közötti szoros kapcsolat kiépítéséről a kibervédelem területén. [60]

Magyarországon a 2001. évi XCV. törvény a Magyar Honvédség hivatásos és szerződéses állományú katonáinak jogállásáról teremt jogi alapot arra, hogy az észt kezdeményezéshez hasonló megoldás hazánkban is működhessen**.** [61] **Az önkéntes tartalékos kibervédelmi egység létrehozásának indokait az alábbiakban foglalom össze**:

- Anyagi indokok: az informatika és azon belül az informatikai biztonság átlagon felüli bérezést jelent az ezen a területen dolgozó szakembereknek. Ezzel a hivatásos szolgálat nem lehet versenyképes. Az önkéntes tartalékos rendszerben azonban lehetőség adódik arra, hogy az arra nyitott állampolgárok és az őket foglalkoztató cégek különösebb anyagi áldozatvállalás nélkül közreműködhessenek a nemzetvédelemben.
- Humán indokok: az informatikai védelemmel foglalkozó hivatalos szervek állományát tekintve számosságában csak annyi ember alkalmazása szükséges, ahány a békeidejű védelmet operatív módon ellátja, illetve stratégiai szinten képes irányítani az ország informatikai védelmét. Amennyiben az országot informatikai támadás éri, hirtelen van szükség nagyobb létszámú szakértőre.
- Tulajdonjogokkal kapcsolatos indokok: jelenleg nincsenek meghatározva a nemzeti kritikus információs infrastruktúrák, és a jogszabályok sem adnak lehetőséget arra, hogy komoly állami kontroll legyen ezeken a legtöbbször piaci fenntartású intézményeken. Amennyiben a vonatkozó intézmények biztonsági üzemeltetésért felelős szakemberei is részt vesznek a szervezett védelemben, ez az akadály kiküszöbölhetővé válik.
- Hatásköri indokok: jelenleg több szervezet felelős az ország informatikai védelméért, kiemelten a Nemzeti Hálózatbiztonsági Központ. Ezek a szervezetek azonban korlátozott lehetőségekkel és állománnyal rendelkeznek. Egyedül az önkéntes tartalékos állomány kihasználása teremti meg a jogi lehetőséget arra, hogy krízis esetén nagy számban, rendkívüli védelmi felhatalmazással rendelkező szakembereket lehessen bevonni a védekezésbe.
- Tudástranszferrel kapcsolatos indokok: elismerve a hivatásos állományban szolgálók tudását, tapasztalatát és képességeit, meg kell állapítani korlátaikat is, melyek egy rendkívüli szituációban hátrányt jelentenek. Ezek a szakértők jellemzően nem rendelkeznek azzal a speciális tudással illetve gondolkodásmóddal, mely egy-egy részterület, pl. a SCADA biztonság, hacktivista támadás esetén szükséges lehet. A

civil területen dolgozó, speciális szakismeretekkel rendelkező emberek bevonásával a hivatásos állomány átfogóbb képet kaphat, stratégiai szinten jobban meg tudja tervezni az ország védelmét.

Az önkéntes tartalékos állomány integrálásának lehetősége tehát adott, azonban annak részletei kidolgozásra várnak, nem csak Magyarországon, de a világ más részein is. Jelen dolgozatban **nem célom** azzal, foglalkozni, hogy a Magyar Honvédség milyen módon tudja megoldani a civil szféra bevonását a kibervédelembe, de **a tervezés alapjául néhány szempontot ajánlok, amelyeket a következőkben ismertetek.**

3.2.1 Az önkéntes tartalékos kibervédelmi haderő tagjai

A bevonandó civil szakembereket négy területről érdemes bevonni: kritikus információs infrastruktúrák IT biztonsági szakemberei, IT biztonsági tanácsadó cégek dolgozói, felsőoktatási hallgatók, a magyar hackerközösség tagjai. Ezek a csoportok többször közös halmazt alkotnak, de tudásukban, gondolkodásmódjukban jól kiegészítik egymást.

A kritikus információs infrastruktúrák üzemeltetőinek bevonása triviálisan adódik. Ez a csoport az első, amely érzékeli a saját rendszere ellen indult támadást. A Digitális Mohács forgatókönyv szerinti összehangolt támadásban az első figyelemfelkeltő jelek innen érkezhetnek. Ezeknek a személyeknek jogában és lehetőségében áll megtenni a szükséges első védelmi lépéseket, az ország ellen szervezett támadás esetén pedig végrehajtani azokat a stratégiai védekezési mechanizmusokat, melyet az operatív törzs meghatároz. Ez a csoport rendelkezik azzal a szaktudással, rendszer- és helyismerettel, mely az adott kritikus információs infrastruktúra működéséhez szükséges alkalmazásokkal kapcsolatos.

Az IT biztonsági tanácsadó céges szerepe speciális. Sokszor kiterjedt formális és informális kapcsolatban állnak a kritikus információs infrastruktúrák tulajdonosaival, nemegyszer a biztonsági eszközök tervezése és üzemeltetése is az ő kezükben van. Ez a csoport rendelkezik a legösszetettebb információvédelmi tudással, mely hatékony segítség lehet a stratégiai védelem megszervezésénél.

A felsőoktatási hallgatók megcélzása kettős. Számos helyen oktatnak információbiztonsággal kapcsolatos tárgyakat, ezért számos hallgató a későbbiekben az előző csoportok valamelyikébe fog tartozni. Egyrészt korai megkeresésük nyitottabbá teheti őket a honvédelem ügye iránt, mint azokat az idősebb szakmabelieket, akiknek a katonai szolgálathoz negatív kép csatlakozik. Másrészt körükből könnyebben fel lehet tölteni a hivatásos állományt, mint a piacról elcsábítani másokat.

Végül a hackerközösség tagjainak bevonását az indokolja, hogy egy feltételezett támadás elsősorban ilyen látásmóddal és technikával kerülne végrehajtásra. A védekezésre a legjobb felkészülés olyan szimulált támadás, amit magasan kvalifikált, gyakorlott hackerek hajtanak végre. Ennek a megközelítésnek a létjogosultságát mi sem jelzi jobban annál, mint hogy az USA Védelmi Minisztériumának Defense Advanced Research Projects Agency (DARPA) szervezete hivatalosan is programot hirdetett a hackerközösségek számára a nemzetvédelemmel kapcsolatos együttműködésre. [62]

3.2.2 Információvédelmi stratégia kialakítása

A Magyar Köztársaság Kormánya által kidolgozott Digitális Megújulás Cselekvési Terv a következő feladatokat tűzi ki a kritikus információs infrastruktúrák védelmének területén:

- A kritikus információs infrastruktúra-védelem vezetésének és a védelmi stratégia kidolgozásának kormányzati kézbe vétele, a vonatkozó EU irányelvnek megfelelően.
- Az állam vezetésével, kidolgozott módszertan alapján a nemzeti kritikus infrastruktúra, valamint az európai kritikus infrastruktúra elemek kijelölése, illetve a kijelölések folyamatos felülvizsgálata.
- A kritikus információs infrastruktúravédelmi szabályok és feladatok állami kijelölése.
- Összkormányzati szinten a kritikus információs infrastruktúrák védelme területén a tudatosság növelés és az oktatás, továbbképzés. [63]

Ezen lépések végrehajtása nélkül nincs értelme az önkéntes tartalékos megoldás bevezetésének, hiszen nem egyértelmű, mik is a védendő infrastruktúrák. Amennyiben azonban a fenti lépések sikerrel végrehajtódnak, a kibervédelmi egység bevonásával éves szinten gyakorlatokat lehet végezni, melyek megtervezéséhez az EU, a NATO, valamint az USA hasonló gyakorlatai szolgálhatnak példaként. Ezeken az eseményeken a Nemzeti Hálózatbiztonsági Központ munkatársai aktívan részt vesznek, és Magyarországon működő szervezetek részvételével hazai viszonyokra ültetve is tartanak gyakorlatokat. Ezek azonban korlátozott terjedelműek, mind szervezetileg, mind technikailag. [64]

Fel kell hívni a figyelmet arra, hogy a kiberhadviselés hadászati és harcászati szintű alkalmazása még kidolgozás alatt álló terület, így kevés nemzetközi minta áll rendelkezésre, és ezek sem a Magyarországhoz hasonló adottságú országokban. Éppen ezért jelentős politikai és kutatási erőfeszítéseket kell tenni annak érdekében, hogy a kiberhadviselés elfogadottá és hatékonnyá váljon a Magyar Honvédségen belül is. Talán elősegítheti ezt az a

tény, hogy a világ vezető hatalmai kivétel nélkül hangsúlyozzák a kibervédelem fontosságát. Hillary Clinton amerikai külügyminiszter szavaival „a kibertámadások jelentik az egyik új biztonsági fenyegetést”. [65]

3.2.3 A célcsoportok együttműködési hajlandósága

A nemzeti kibervédelemben más országokhoz hasonlóan tehát be lehet vonni a helyi hackerközösséget is. Ehhez viszont valamilyen párbeszédet kell kialakítani a védelmi szervek és a közösség tagjai között. Több országban ez informális szinten, az USA-ban formálisan is megtörtént. Magyarországon azonban ez nem jellemző, pedig ez a közösség a legfőbb forrása az informatikai védelemért felelős személyeknek, akár állami, akár magánszervezet esetén. Valamilyen módon ezért érdemes megtudni, hogy mit gondolnak ezek a szakemberek a nemzetvédelemről. Reprezentatív felmérés a közösség rejtőzködő volta miatt nem lehetséges, ám az 1-2000 főre tehető csoport bizonyos csatornákon elérhető. **2009-ben a Hacktivity hackerkonferencia levelezőlistáját választottam egy célzott kérdőív kiküldéséhez, mely 600 címet tartalmazott**. A címzettek majdnem 20%-a, 187-en válaszoltak a kérdésekre. Ez az önkéntes tartalékos csoport célszemélyeinek kb. 10%-át fedi le. [66]

A kérdőív összesen négy kérdésre keresett választ, hangvételében alkalmazkodva a célcsoport kommunikációs szokásaihoz:

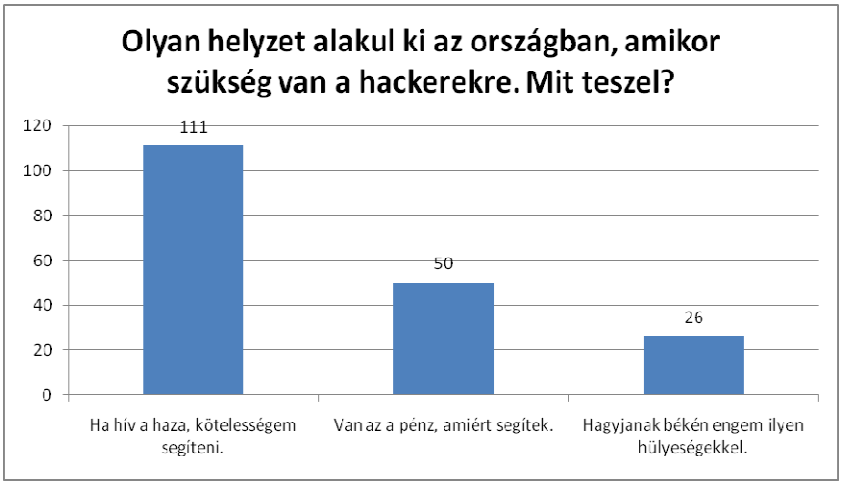
- Olyan helyzet alakul ki az országban, amikor szükség van a hackerekre. Mit teszel?
- Az IT biztonság melyik motivációját érzed leginkább magadénak?
- Hova sorolnád be magadat?
- Mi a véleményed a Magyar Honvédségről?

Ezekkel a kérdésekkel a válaszadók hazafiságának mértékét kívánta felmérni, valamint a hackerek lehetséges szerepét a nemzetvédelemben, helyüket a munkaerőpiacon és a védelmi szervekről alkotott véleményüket.

Az első kérdésre adott három lehetséges válasz a következő volt:

- Ha hív a haza, kötelességem segíteni.
- Van az a pénz, amiért segítek.
- Hagyjanak békén engem ilyen hülyeségekkel!

Előzetes feltételezésként megfogalmazódott, hogy a válaszadók szeretik hazájukat, és készen állnak egy krízishelyzetben ingyen segíteni. Ezt a válaszok megerősítették.

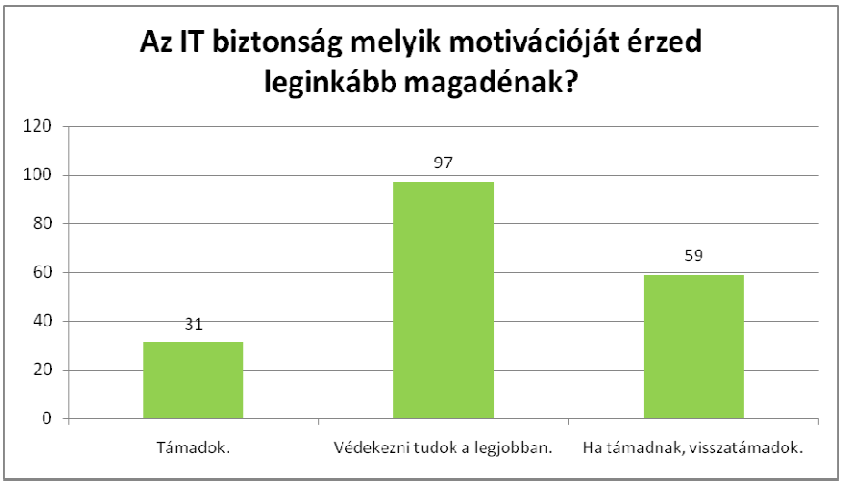


2. ábra: Hacktivity kérdőív, 1. kérdésre adott válaszok

A kibervédelem elsősorban az infrastruktúrákat üzemeltetők és a megfelelő állami szervek feladata, nem a hackereké. Ők viszont birtokában vannak annak a tudásnak, amellyel tudnak támadni, vagy támadást szimulálni, esetleg külső támadás után visszavágni. A második kérdésre - *Az IT biztonság melyik motivációját érzed leginkább magadénak?* - adott lehetséges válaszok a következők voltak:

- Támadok.
- Védekezni tudok a legjobban.
- Ha támadnak, visszatámadok

Az előzetes várakozások azt mutatták, hogy a válaszolók többsége a támadást fogja fő motivációnak megnevezni. Ez azonban nem igazolódott.

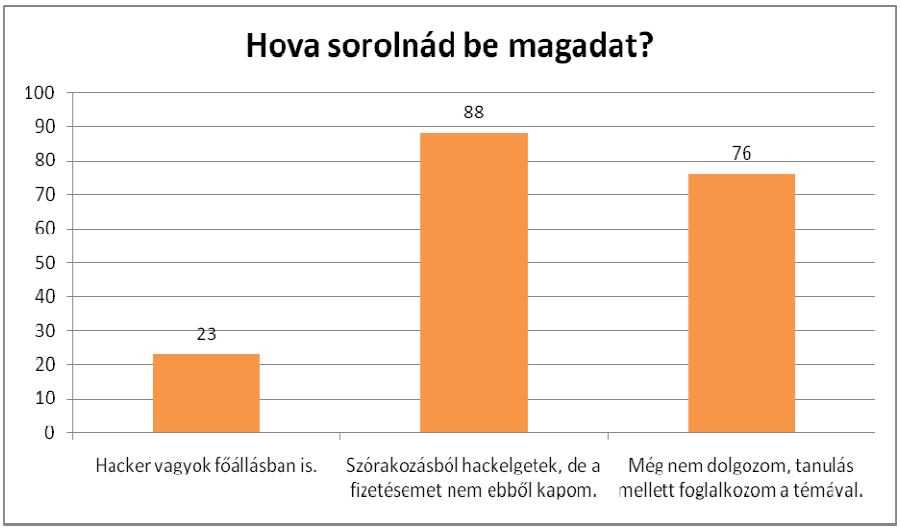


3. ábra: Hacktivity kérdőív, 2. kérdésre adott válaszok

A harmadik kérdés - *Hova sorolnád be magadat?* - a cél annak mérése volt, lehetnek-e a hackerek egy esetleges kibervédelmi csoport alkotói. Az országban ugyanis van néhány hivatásos etikus hacker, és van sok olyan egyetemista, aki azzá válhat. Mellettük pedig van sok olyan szakemberünk, akik számára a hackelés hobbi, más jelenti nekik a megélhetést. A lehetséges válaszok erre a kérdésre a következők voltak.

- Hacker vagyok főállásban is.
- Szórakozásból hackelgetek, de a fizetésemet nem ebből kapom.
- Még nem dolgozom, tanulás mellett foglalkozom a témával.

Előzetesen arra számítottunk, hogy néhány hivatásos hacker mellett erős felsőoktatási háttérrel rendelkezik az ország. Ez beigazolódott.

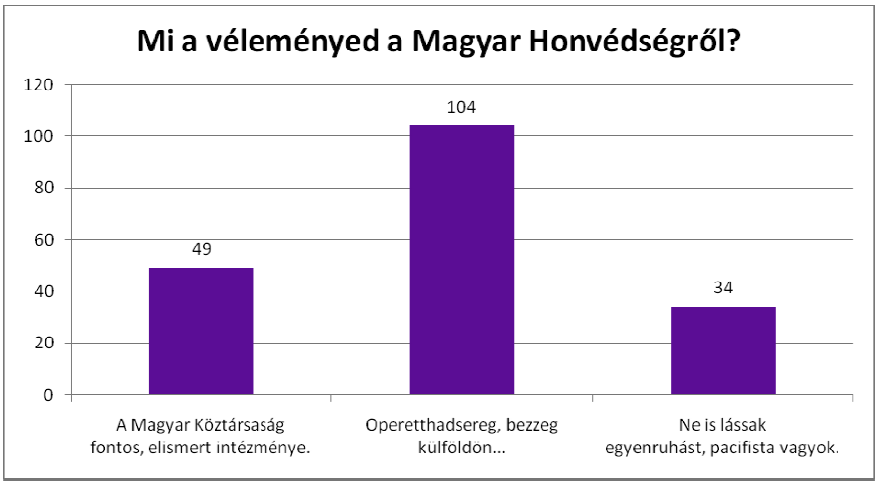


4. ábra: Hacktivity kérdőív, 3. kérdésre adott válaszok

A közösség és a hivatalos szervek közötti együttműködés elengedhetetlen feltétele, hogy mindkét fél megbízzon valamennyire a másikban. Ehhez viszont egy pozitív képet kell kialakítani magáról annak a szervnek, amely az együttműködést kezdeményezi. A kérdés a Magyar Honvédségre vonatkozott - *Mi a véleményed a Magyar Honvédségről?* -, de tetszőlegesen helyettesíthető más védelmi szervezettel is. A kérdés mérte továbbá azt is, hogy a válaszadók hogyan viszonyulnak a hadviseléshez. A három válasz:

- A Magyar Köztársaság fontos, elismert intézménye.
- Operetthadsereg, bezzeg külföldön...
- Ne is lássak egyenruhást, pacifista vagyok.

Előzetesen azt vártuk, hogy a válaszadók többsége nem pacifista, de meglehetősen negatív képe van a Magyar Honvédségről. Ez is beigazolódott.



5. ábra: Hacktivity kérdőív, 4. kérdésre adott válaszok

A válaszok alapján tehát a hacker-közösség szereti az országot és kész megvédeni a maga eszközeivel. A válaszadók fele kész támadni vagy visszatámadni egy esetleges konfliktus során. Magyarországon van néhány hivatásos hacker, és hatalmas utánpótlás az egyetemeken, mellyel érdemes számolni, illetve valamilyen módon támogatni az ilyen képzéseket. A Magyar Honvédségnek viszont sokkal pozitívabb képet kell kialakítania, ha ezen a területen elfogadják a javaslatainkat.

Néhány érdekes összefüggésre is fény derült. A hivatásos hackerek fele pénzért, másik felük ingyen segítene. Az etikus hackereknek nincs jó véleményük a Magyar Honvédségről, ugyanakkor a hobbihackereknek van a legjobb benyomásuk a testületről. A hazafiak nem pacifisták. A hobbihackerek készen állnak támadni és visszatámadni. Ami pedig talán a legjobb hír a tanulmány szempontjából, hogy a diákok hazafiak és nem pacifisták.

Ezt a közösséget tehát érdemes figyelembe venni a kibervédelem tervezésénél. Ehhez aktívan részt kell venni a hacker-konferenciákon, pozitív képet kell építeni a Honvédségről, esetleg támogatást kell szerezni egy kiber-gyakorlathoz, melybe be lehetne vonni a hazafias hackereket is. De mindenekelőtt el kell kezdeni a stratégiai gondolkodást ezen a téren is.

3.3 Biztonságtesztelési módszertanok

Az előző alfejezetek bemutatták, milyen összetett támadások fenyegethetik Magyarország kibervédelmét. Az értekezés szempontjából a legfontosabb kérdés azonban az, hogyan lehet megfelelő alkalmazásfejlesztési eljárásokkal kiküszöbölni a magyar elektronikus közigazgatási rendszerek ellen irányuló összetett informatikai támadásokat. Az előző fejezetek részletesen foglalkoztak azzal, hogy az alkalmazásfejlesztőknek milyen

erőfeszítéseket kell megtenniük annak érdekében, hogy a közigazgatás alkalmazásai megfelelően biztonságosak legyenek. **A következő alfejezetek arra koncentrálnak, hogy az előzőekben javasolt kritikus információs infrastruktúrák védelméért felelős szervezet, akár az önkéntes tartalékos kibervédelmi egység milyen eljárásokkal tudja tesztelni az alkalmazások biztonsági kontrolljainak hatékonyságát.**

A biztonsági tesztelések módszertanával több, mérvadó ajánlás is foglalkozik. Ezek közül a legjelentősebbek az Open Source Security Testing Methodology Manual, mely az Institute for Security and Open Methodologies kiadványa, a NIST SP 800-115 Technical Guide to Information Security Testing and Assessment ajánlás, mely az amerikai kormányzat szabványa és az OWASP Testing Guide, amit az Open Web Application Security Project keretében fejlesztenek.[67] [68] [69] Az alkalmazások tesztelésének módszertanát ezek együttes használatával érdemes összeállítani.

A biztonsági tesztelési módszertanok csoportosítására jelenleg nincs egyezményes megállapodás, a tesztelt rendszerek ismeretétől kezdve, a hozzáférés mértékén át, a bevetett tesztelési eszközökig számos taxonómia létezik. Néhány fogalom azonban gyakran előfordul a szakirodalomban, **ezeket rendszerezem az alábbiakban, és alakítom ki az értekezésben használt terminológiát**.

- *Biztonsági funkcionális tesztelés*: az újonnan fejlesztett rendszer (alkalmazás) beépített védelmi kontrolljainak megfelelőségi ellenőrzése. Más néven white-box tesztelésnek is hívják, kódközeli megközelítésnek minősül. Pl. nézzük meg, hogy tényleg legalább 8 karaktert kell-e megadni jelszónak. Összefoglalva **forráskód szintű ellenőrzésnek** tekintjük.

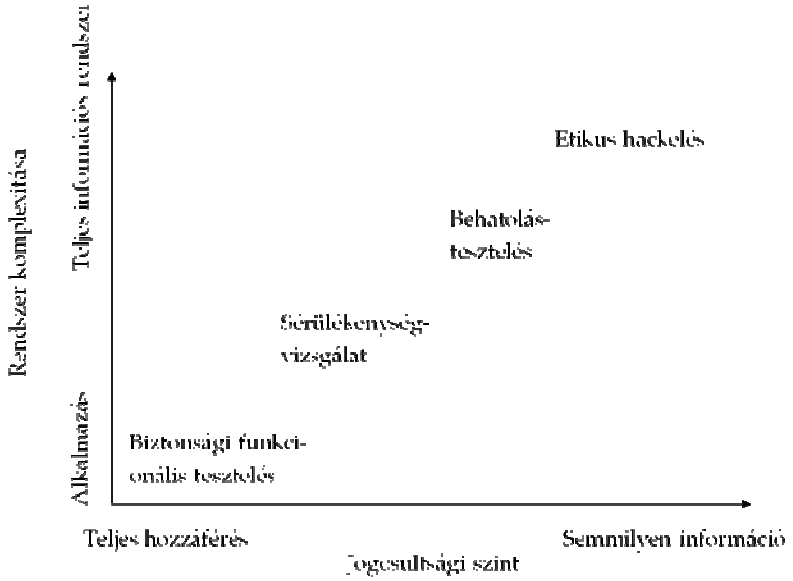
- *Sérülékenység-vizsgálat*: a rendszer (alkalmazás) védelmi kontrolljainál előforduló sebezhetőségek felderítése, tipikusan automatikus eszközökkel. Más néven black-box tesztelésként ismert, modulszintű vizsgálatnak tekinthető. Pl. egyes bemeneteken olyan adatok megadása, melyekre a rendszer egyébként védett információkat ad át. Összefoglalva **alkalmazásszintű ellenőrzésnek** nevezhetjük ezt az eljárást.

- *Behatolás-tesztelés:* az újonnan fejlesztett vagy már működő rendszer védelmi kontrolljainak kijátszása műszaki megoldásokkal, bármilyen kapcsolódó környezeti infrastruktúra felhasználásával. Két alfaja létezik, a Blue teaming, melynek során a tesztelő pontosan ismeri a tesztelt infrastruktúrát, és a Red teaming, melynél

semmilyen ismerettel nem rendelkezik. Ezt a fajta tesztelést **rendszerszintű ellenőrzésnek** kell felfogni.

- *Etikus hackelés*: a működő rendszer védelmi kontrolljainak kijátszása bármilyen technikával, a rendszer előzetes ismerete nélkül. Ebbe beletartozik az emberi ráhatással (social engineering) történő támadás is. Ez a **szervezet szintű ellenőrzés** definícója.

A fenti technikákat a jogosultsági szint és a rendszer komplexitása szerint a következő ábra mutatja be.



6. ábra Biztonságtesztelési eljárások

A fenti módszerek közül a sérülékenység-vizsgálat és a behatolás-tesztelés a legelterjedtebb, használatát több forrásban is kötelező előírásként találhatjuk meg. A tipikusan amerikai szabványok, jogszabályok az informatikai biztonság egyik alapkövének tekintik az ilyen típusú teszteléseket. Az alábbi felsorolás összefoglalja a legelterjedtebb követelményeket.

- Payment Card Industry Data Security Standard (PCI DSS): a nagy bankkártya-cégek kártyaadatok biztonságos elektronikus kezelésére vonatkozó előírása az ellenőrzés egyik legfontosabb alapkövének tekinti a sérülékenység-vizsgálatokat. A tanúsításhoz szükséges kétszintű vizsgálat mellett már az érintett rendszerek fejlesztését követően, a megrendelő számára is előírt a biztonsági tesztelés elvégzése. Az előírás 6.5 követelménye szerint a webes alkalmazásokat az OWASP útmutatói alapján kell fejleszteni és ezeket mintavételes módszerrel kell ellenőrizni (biztonsági funkcionális

tesztelés), majd a 6.6 követelmény szerint manuális vagy automatikus módszerrel (sérülékenység-vizsgálat) legalább évente vagy minden változás után, egy erre specializálódott szervezettel (belső vagy külső) teszteltetni kell, és az esetleges hibák kijavítása után ezt a tesztet meg kell ismételni. [70]

- Federal Information Security Management Act (FISMA): Az USA 2002-ben elfogadott e-kormányzati törvénye alapján a központi ügynökségek valamennyi informatikai rendszerét biztonságos körülmények között kell üzemeltetni.[71] Az alapvető követelményeket a NIST SP 800-53 szabvány tartalmazza, mely a magyar Közigazgatás Informatikai Bizottság 28. ajánláshoz hasonlóan három besorolási szintet határoz meg a rendszerekre.[72] Az előírások között RA-5 jelzéssel szerepel a sérülékenység-vizsgálat. Ez az automatikus eszközökkel végrehajtott tesztelést preferálja, melynek eredményeit egységes formájú jelentésben kell bemutatni. A vizsgálatot a szervezet által meghatározott időközönként vagy a rendszert érintő új sebezhetőség megjelenésekor kell végrehajtani. Közepes biztonsági szinten az automatikus eszköz használatát integrálni kell a változáskezelési eljárások közé, kiemelt szinten pedig a sebezhetőség-vizsgálati folyamatot kell továbbfejleszteni. A külső értékelő által végzett, akár komplex vizsgálat (behatolás-tesztelés) nem kötelező elem, de ajánlott teszteljárásként fel van tűntetve.
- Control Objectives for Information and related Technology (CObIT): Az elsősorban pénzintézeti szektorban használt IT irányítási ajánlás a DS5.5 Security Testing, Surveillance and Monitoring részben javasolja az informatikai rendszerek rendszeres biztonsági tesztelését, ám ennek módját nem jelzi. Az erre vonatkozó RACI táblázat viszont már nevén nevezi a sérülékenység-vizsgálatot, melynek végrehajtása a Megfelelőség, Audit, Kockázat és Biztonság szerepkör feladata. A biztonsággal kapcsolatos folyamat érettsége akkor tekinthető meghatározottnak, 3-as szintűnek, ha legalább ad hoc módon történnek ilyen vizsgálatok. [73]
- ISO/IEC 27002: A legismertebb információbiztonsági szabvány a 12.6. fejezetben foglalkozik a sérülékenység-vizsgálattal. Eszerint a szervezetnek bizonyos időközönként fel kell mérnie rendszerének technikai sebezhetőségeit, és megfelelő védelmi intézkedésekkel csökkenteni kell az ezekből eredő kockázatokat. A szabvány nem ad útmutatást a vizsgálat pontos végrehajtására, akár a gyártóktól érkező vagy hiteles forrásokban megjelent információk rendszeres olvasása is kielégíti a követelményeket. A lényeg, hogy a szervezet rendelkezzen ilyen típusú folyamattal. A

KIB 28. ajánlás ezt a szellemiséget követi az RS-2 Hibajavítás követelményben, de a folyamat szerepét meglehetősen eljelentéktelenítve.

- Common Criteria: Az értekezésben már többször megemlített szabvány az alkalmazásfejlesztés biztonsági követelményei között kiemelten tartja nyilván a biztonsági tesztelést. A biztonsági funkcionális teszteléssel és a sebezhetőségek felmérésével két külön osztály foglalkozik (ATE és AVA osztályok). Ezek ismertetésére az értekezés a későbbiekben részletesen kitér.

A biztonsággal foglalkozó szabványok és ajánlások túlnyomó többsége tehát foglalkozik a biztonsági tesztelésekkel, de ezt eltérő szigorúsággal teszi. Elemezve a különböző követelményeket, meg lehet állapítani, hogy elsősorban az automatikus eszközökkel végzett sérülékenység-vizsgálat elvárt. Ez azonban nem mindig elég. Jelen értekezésben a korábbi fejezetekben bevezetett módon három biztonsági szintet állapítottam meg az e-közigazgatási alkalmazások védelmére. **A biztonsági teszteléseket is ehhez igazítom az alábbiak szerint**.

- Alap biztonsági szint: interneten keresztül elérhető, állampolgárokat kiszolgáló rendszerek (C2G és G2C rendszerek). A fő kockázat ebben az esetben abban rejlik, hogy az alkalmazás felülete elérhető a hozzáférési jogosultsággal nem rendelkező internet-felhasználók milliárdjai számára, de a jogosultsággal rendelkező felhasználók száma is rendkívül magas. A kibertámadások elsődleges célpontjai az ilyen, jellemzően kormányzati portálok. Nemzetbiztonsági szempontból ezen rendszerek kiesése kisebb kockázatot rejt, de állampolgárok tömegeit érintheti negatívan, ráadásul jelentős imázsvesztést tud elszenvedni a kormányzat egy ilyen portál sikeres támadása esetén. Működésük hasonlatos a bankkártya-adatokat kezelő kereskedelmi portálokhoz, ezért a biztonsági tesztelést a PCI DSS szabványban előírtak szerint kell végrehajtani, ami biztonsági funkcionális tesztelést és a nyílt internet felé irányuló oldalakat érintő automatikus sérülékenység-vizsgálatot jelent. Kiemelt jelentőségű szolgáltatások esetén a behatolás-tesztelés is indokolt lehet, azaz az alkalmazás mellett az azt futtató, internet felől elérhető infrastruktúrát is meg kell vizsgálni.
- Fokozott biztonsági szint: belső, egymással adatcserét folytató közigazgatási rendszerek (G2G rendszerek). Elsődleges kockázat a tömeges adatszivárgás, illetve sikeres támadás esetén a közigazgatás működésének ellehetetlenítése. A fő veszélyt elsősorban a jogosultsággal rendelkező belső felhasználók jelentik. Külső támadások sikeres véghezviteléhez komoly, nem csak informatikai eszközöket igénybe vevő

felderítés szükséges. Ezeknél a rendszereknél nem elsősorban az alkalmazáshibákat használják ki a támadók, hanem az emberi hibákra építenek. Éppen ezért a gyakorlati tapasztalat alapján a fejlesztők nem is fordítanak kellő figyelmet a biztonságos programozásra, tehát ha egy külső támadó hozzáférne a rendszer felületéhez, számos hibát találna, amivel kompromittálhatná a rendszert. A biztonsági tesztelés során ezért a biztonsági funkcionális tesztelésre és az etikus hackelésre kell a hangsúlyt fektetni, különös tekintettel a social engineering jellegű tesztesetekre.

- Kiemelt biztonsági szint: minősített adatokat kezelő rendszerek: a 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól meghatározza, hogy milyen személyi, adminisztratív és fizikai biztonsági intézkedéseket kell megtenni az elektronikusan kezelt minősített adatok védelme érdekében. A felsorolt intézkedések alapján igen kicsi a valószínűsége annak, hogy jogosulatlan külső támadó hozzáférne ezekhez az adatokhoz. A Stuxnet vizsgálata során is kiderült, hogy a belső, jogosult felhasználók hibája illetve közreműködése nélkül nem lett volna sikeres a kártékony kód bejuttatása. Ebből okulva a biztonsági tesztelést a biztonsági funkcionális tesztelésre kell kihegyezni, illetve a blue-teaming módszert használó behatolás-tesztelést kell felhasználni.

A követelmények jól mutatják, hogy a vizsgálat típusai elsősorban a felhasználók támadási képességeiből, és rendszerismeretük szintjéből indul ki, nem lineárisan erősödik a bevetett támadási potenciál. Éppen ezért szükségessé válik a tipikus támadói profil bevezetése mindhárom szintre, mely az előző fejezetekben már ismertetett Common Criteria szabvány alapján lehetséges. Szintén szükséges a különböző műszaki tesztelési eljárások ismertetése, mely segít a tesztelőnek eldönteni, hogy pontosan milyen eszközhöz nyúljon a teszt kivitelezésénél. A következő alfejezetek erre a két területre koncentrálnak.

3.4 Támadói profilok a Common Criteria alapján

Egy alkalmazás biztonsági teszteléséhez a legjobb kiindulópontot a Common Criteria (CC) szabvány adja, melynek Common Evaluation Methodology (CEM) című kiadványának B melléklete részletesen leírja egy értékelő feladatait. [74] A CC terminológiájában a sebezhetőségi felmérés az a folyamat, melynek során a termék hibáinak vagy gyengeségeinek a létét és kihasználhatóságát elemzik. A tesztelést az értékelő végzi értékelői tesztelés módszerével. Alapszinten csak a nyilvános forrásból hozzáférhető sebezhetőségeket kell

felderíteni (az ISO 27002 és a KIB 28. ajánlásoknak megfelelően), ám a rendszer biztonsági besorolása szerint ennél sokkal részletesebb vizsgálatokra is sor kerülhet. A sérülékenység-vizsgálat három lépésből áll: a lehetséges sebezhetőségek felderítése, a sebezhetőség kockázati besorolása és a sebezhetőség kihasználása annak megerősítésére, hogy a hiba az adott környezetben valóban kihasználható.

A CC öt típusba sorolja a sebezhetőségeket:

- Megkerülés (bypassing): Ebbe a kategóriába tartozik minden olyan hiba, melynek során a rendszer beépített biztonsági eljárásait megkerülik, pl. jogosulatlan hozzáférés, kriptográfiai védelem megkerülése.
- Meghamisítás (tampering): Olyan sebezhetőségek, melynek kihasználásával a termék működése módosítható, pl. a biztonsági funkciók leállítása vagy a fizikai módosítás.
- Direkt támadások (direct attacks): A permutációt vagy véletlenszerűséget felhasználó védelmi eljárások tesztelése tartozik ebbe a körbe, pl. jelszóhosszúságokon alapuló támadások.
- Megfigyelés (monitoring): Az információk átvitelének vagy kiszivárgásának figyelése és felhasználása, pl. információs csatornák lehallgatása, rejtett csatornák alkalmazása, elektromágneses sugárzás figyelése.
- Nem megfelelő használat (Misuse): Ez alatt a termék nem megfelelő dokumentációját, helytelen konfigurációját és szokásostól eltérő használatát értjük.

A fenti hibák felderítésére két útja lehet az értékelőnek. Egyrészt a vizsgálat során szembesülhet olyan sebezhetőségekkel, melyek kihasználása nem triviális, de minden valószínűség szerint lehetséges. Ezek többnyire olyan véletlen felfedezések, melyek a tesztelés „melléktermékei”, nem direkt ezekre volt kíváncsi a tesztelő. Példa lehet erre egy olyan teszteredmény, mely a termékben puffer túlcsordulást okoz, ami akár a védelmi funkciók megkerülését is lehetővé teheti alaposabb elemzés után. A másik lehetséges elemzési mód a valamilyen elvek alapján felépített analízis. Ez lehet nem strukturált, amelynek során az értékelő saját tapasztalata alapján általános sebezhetőségeket keres, fókuszált, ami egyes sebezhetőnek tűnő területek alapos elemzését jelenti, vagy módszertan alapján történő, a korábban felsorolt ajánlásokra épülő.

Az értékelési eljárás azonban elsősorban a támadási potenciál szintjétől függ. A tesztelés előtt el kell dönteni, hogy a termék milyen környezetben fog működni, és ennek alapján négy

kategóriába lehet sorolni a lehetséges támadói képességeket: alap, alap-erősített, mérsékelt, magas. A Közigazgatási Informatikai Bizottság 25. számú ajánlása szerinti besorolásban a magyar közigazgatási rendszereket alacsony és fokozott kihatású esetben alap-erősített, kiemelt kihatású esetben mérsékelt szintű sebezhetőség-vizsgálatnak kell alávetni. Ez azt jelenti, hogy az értékelő a tesztelést olyan támadási kapacitással végzi el, ami az előírt szinten meg van adva. **Jelen értekezésben illeszkedem ehhez a követelményrendszerhez**, az alap és a fokozott biztonsági szintet alap-erősített, a kiemelt biztonsági szintet mérsékelt részletezettséggel **dolgozom ki**. Természetesen az eljárás során felderíthetnek olyan sebezhetőségeket is, melyek az adott támadási szinten nem kihasználhatók, ilyenkor a fejlesztőnek/megrendelőnek kell meghoznia azt a döntést, hogy ezt a kockázatot elfogadja vagy nem.

A támadási potenciál kiszámolásához a CC kiváló segédletet nyújt. 5 paraméter segítségével meghatározható, hogy a tesztelő milyen körülmények között végezze el a vizsgálatát. Ezek a következők:

- a sebezhetőség sikeres kihasználáshoz szükséges idő (eltelt idő), lehetséges értékei: egy napnál kevesebb, egy nap és egy hét között, egy hét és két hét között, két hét és egy hónap között, egy hónap és hat hónap között, hat hónapnál több.
- a kihasználáshoz szükséges szakértelem (szakértelem szintje), lehetséges értékei: laikus (általános ismeretei vannak), profi (jól ismeri az adott terméktípust), szakértő (széleskörű ismeretei vannak a támadási technikákról), több szakértő (részterületek szakértői).
- a vizsgált termék felépítésének és működésének ismerete (termékismeret), lehetséges értékei: nyilvános információk (internetről elérhető), korlátozott információk (a fejlesztői közösségen belül ismert), érzékeny információk (csak egy speciális fejlesztői csapat által ismert), kritikus információk (csak néhány személy által ismert).
- a sikeres támadáshoz szükséges hozzáférés ideje és a próbálkozások száma (próbálkozási ablak), értékei: korlátlan (a támadás észrevétlen marad), egyszerű (egy napnál rövidebb ideig tartó hozzáférés, 10-nél kevesebb próbálkozás), mérsékelt (egy hónapnál rövidebb ideig tartó hozzáférés, 100-nál kevesebb próbálkozás), nehéz (legalább egy hónapig tartó hozzáférés vagy legalább 100 próbálkozás), nincs (a rendelkezésre álló idő vagy próbálkozásszám nem elégséges egy sikeres támadás véghezviteléhez).

- a támadás kivitelezéséhez szükséges hardverek és szoftverek (eszköztár), lehetséges értékei: szabványos eszközök (internetről szabadon letölthető), speciális eszközök (piacon beszerezhető), egyedi eszközök (adott célra fejlesztett), több egyedi eszköz (résztámadások egyedi eszközei).

A CC minden lehetséges értékhez egy számot rendel, melyek összege adja a támadási potenciált. A forgatókönyvek összeállításánál biztonsági szinttől függően külső vagy belső támadókkal számolok. Meg kell jegyezni, hogy az e-közigazgatási rendszerek üzemeltetői azzal számolnak, hogy legitim felhasználóik megbízhatóak, ezért a védelmet sokszor eszerint építik fel. Természetesen a gyakorlat azt mutatja, hogy az ilyen támadásokat is szimulálni kell. A támadói profilok felépítésénél ezt figyelembe vettem, ez azonban csak ajánlott, a cél az, hogy alapvető technikák felhasználásával jelentősen emeljük az ilyen rendszerek biztonsági szintjét. Hangsúlyozom, hogy a támadói profilok nem kockázatarányosan, hanem az értekezésben használt funkcionális megközelítés alapján lettek összeállítva. A kockázatarányos megközelítés más támadói profilokat eredményezhet, de eredményeim alapján ezek már analóg módon levezethetők.

Az alap biztonsági szint által megkövetelt alap-erősített támadási potenciál eléréshez a tesztelési forgatókönyv összeállításánál egy olyan támadóval számoltam, aki bár ismeri a támadási technikákat, azokat csak nyilvánosan elérhető eszközök felhasználásával tudja végrehajtani. Célja a könnyen azonosítható hibák felderítése, melyet segítenek a rendszerről kiszivárgó információk. A szakzsargonban script-kiddie névvel ellátott képességeket értem ide. Ehhez a paraméterek: eltelt idő két hét (nem ismeri a rendszert, idő kell az információgyűjtéshez), a szakértelem szintje profi (képes szakszerűen kezelni a támadási eszköztárat), a termékismeret korlátozott információ (nem ismeri belülről a rendszert, csak kiszivárgott információkra támaszkodhat), a próbálkozási ablak mérsékelt (a nagy informatikai zajban a támadási kísérletet lassan azonosítják), az eszköztár pedig szabványos (interneten elérhető eszközök). A sérülékenység-vizsgálatot tehát szabványos eszközökkel, automatikus módon lehet elvégezni.

A fokozott biztonsági szint szintén alap-erősített támadási potenciált feltételez, de a támadói profilt máshogy kell összeállítani. Itt elsősorban belső támadóra, vagy belső felhasználó által birtokolt tudásszinttel rendelkező külső támadóra kell felkészülni, akinek valamilyen szintű jogosultsága van a rendszerhez. A javasolt paraméterek a következők:

- az eltelt idő egy hét (a támadó hamar megtalálja a rést a védelmi rendszeren);

- a szakértelem szintje profi (a támadó felületesen ugyan, de ismeri a rendszer védelmi mechanizmusait, és azokat ki tudja kerülni);
- a termékismeret érzékeny szintű (pontosan ismeri a termék működését, de nem fejlesztői szinten);
- a próbálkozási ablak egyszerű (belső felhasználókat általában kevésbé figyelnek, mint külső támadásokat);
- a rendelkezésre álló eszköztár pedig szabványos (mivel jogosultsággal rendelkezik, nincs szükség speciális eszközökre).

Az etikus hackelés során tehát a szükséges rendszerinformációt és jogosultságot meg kell adni a tesztelőnek, aki a fenti paraméterek mellett próbálja kikerülni a biztonsági intézkedéseket.

A kiemelt biztonsági szinten a mérsékelt vizsgálat szimulált támadója olyan magas tudással rendelkező szakértő, aki képes hamar észrevenni az elemi hibákat, és ezekhez akár saját eszközöket is tud fejleszteni. A rendszer azonban megfelelően védett, arról semmilyen információ nem szivárgott ki. A Stuxnet féreg tanulságai alapján ezt a támadót jól képzett, rendszerismerettel rendelkező belső felhasználónak tekintjük, így a következők szerint lehet profilozni:

- az eltelt idő egy hét (még a minősített adatokat kezelő rendszerek is általában szabványos technológiákra épülnek, ahol egy képzett támadó ismer nem publikált hibákat);
- a szakértelem szintje szakértő (mély informatikai ismeretekkel rendelkezik a támadott technológiát illetően);
- termékismeret érzékeny (sok mindent tud a támadott rendszerről);
- a próbálkozási ablak egyszerű (hiszen a támadó pontosan ismeri a rendszert és annak hibáit);
- eszköztár speciális eszközök (feltételezve, hogy piaci technológiát használ a vizsgált rendszer).

A behatolás-tesztelést tehát olyan eszközökkel kell végrehajtani, melyek a piacon beszerezhetők, és ez akár jelentős anyagi befektetéssel is járhat.

3.5 Tesztelési módszerek

3.5.1 Forráskód- és alkalmazásszintű vizsgálatok

A Common Criteria a már említettek szerint két oldalról közelíti meg a biztonságtesztelés kérdését. Ezek mindig az alkalmazásra koncentrálnak, nem foglalkoznak az informatikai környezetet alkotó rendszerelemek biztonságával. A fejlesztőnek egyrészt bizonyítania kell az alkalmazásban implementált biztonsági funkcionalitás működőképességét, másrészt egy független értékelőnek körültekintő sebezhetőség-vizsgálatot kell végrehajtania.

A KIB 25. ajánlás besorolása szerint a Common Criteria értékelési garanciaszintjei közül az EAL2, EAL3 és az EAL4 jöhet számításba egy közigazgatási rendszer fejlesztésénél. Az értekezés besorolása szerint az alap és fokozott biztonsági szint EAL3, a kiemelt biztonsági szint EAL4 követelményű, így az ezekre vonatkozó tesztelési követelményeket érdemes megvizsgálni.

A biztonsági funkcionális tesztelésre az ATE osztály szab előírásokat. Mind EAL3, mind EAL4 szinten ugyanazok a követelmények jelennek meg melyek elsősorban a fejlesztőre vonatkoznak:

- ATE_COV.2: az implementált biztonsági funkciók tesztlefedettségének ellenőrzése. Eszerint minden biztonsági funkció interfészét le kell ellenőrizni, és ezt a tervezési dokumentációval összhangban kell megtenni.
- ATE_DPT.1: a tesztelési mélység elemzése. Ennek során azt kell bizonyítani, hogy minden egyes biztonsági funkció le lett tesztelve.
- ATE_FUN.1: a funkcionális tesztelés formai követelményeit határozza meg.
- ATE_IND.2: a független biztonsági funkcionális tesztelés módszerének meghatározása. Eszerint a független értékelőnek a fejlesztő által elvégzett biztonsági funkcionális tesztelés bizonyos részeit mintavételezett eljárással újra el kell végeznie.

A sebezhetőség-vizsgálatot független értékelőnek kell végrehajtania az AVA osztály útmutatása szerint (az értekezés ezzel a tesztelési típussal foglalkozik behatóan). EAL3 szinten az AVA_VAN.2, EAL4 szinten pedig az AVA_VAN.3 határozza meg a követelményeket.

- AVA_VAN.2: Az értékelőnek ebben az esetben először nyílt forrásokban kell ellenőriznie, hogy az alkalmazásban van-e bármilyen lehetséges sebezhetőség. Ezután

az útmutató dokumentumok, a funkcionális specifikáció, a tervezési dokumentumok és a biztonsági architektúra-leírás alapján kell sebezhetőségeket keresnie, ez azonban nem terjed ki a forráskód ellenőrzésére. Végül az azonosított sebezhetőségek mentén ki kell derítenie, hogy az adott hiba kihasználható-e. Tipikus alkalmazásszintű vizsgálatról van tehát szó.

- AVA_VAN.3: az AVA_VAN.2-höz képest annyi eltérést tartalmaz, hogy kódszintű ellenőrzést is végre kell hajtani.

Az OWASP Application Security Verification Standard Project (ASVS) a Common Criteriához hasonló elvek alapján különböző szintű ellenőrzésekre tesz javaslatot az elkészült alkalmazásban, így a hasznos kiegészítője lehet a szabványnak. [75] Az ASVS négy szinten határozza meg a webes alkalmazásokra vonatkozó biztonsági ellenőrzések körét, kimondottan a biztonsági funkcionális tesztelés megközelítéssel, azaz az infrastruktúra-elemek nincsenek a célkeresztben, csak az alkalmazás. Bár a dokumentum hivatalosan webes alkalmazásokra használható, kellően magas szintű ahhoz, hogy analóg módon más típusú alkalmazásokat is fel lehessen vele mérni. A Common Criteria-hoz képest jelentős előnye, hogy a biztonsági funkciókra konkrétabb tesztelési követelményeket határoz meg, mint a Common Evaluation Methodology.

A négy szint a következő: eszközökkel végrehajtott, manuális tesztelés és átvizsgálás, manuális átvizsgálás a tervek ismeretében, manuális átvizsgálás a tervek és a kód ismeretében. Az eszközökkel végrehajtott vizsgálat célja meggyőződni arról, hogy semmilyen kártékony kód nem került az alkalmazásba. Ez történhet a bináris kód dinamikus ellenőrzésével (Level 1A) vagy a forráskód statikus ellenőrzésével (Level 1B). Ideális esetben mindkét ellenőrzést le kell futtatni (Level 1). Ez a vizsgálat csak közvetlenül a fejlesztett kódot érinti.

A manuális tesztelés és átvizsgálás célja a fejlesztett kódok, illetve a biztonsági funkcionalitást biztosító, harmadik féltől származó komponensek vizsgálata. A vizsgálat során az eszközök használata támogatott, de a kívánt bizonyosságot nem kizárólag az eszköz által szolgáltatott eredmény adja, a tesztelőnek manuális módszerekkel is alá kell támasztania a megállapításokat. A Level 2 tesztelés szintén két altesztelési módszerből tevődik össze. Egyrészt manuális behatolási tesztelést kell végrehajtani (Level 2A), valamint manuális kódelemzés is elvárt (Level 2B).

A tervek átvizsgálása a harmadik vizsgálati szint (Level 3). A Level 2 szinthez képest eltérés az, hogy meg kell vizsgálni a harmadik féltől származó komponensek kódjait is. A negyedik szint (Level 4) tulajdonképpen teljes belső átvizsgálást jelent, melynek hatóköre kiterjed a fejlesztőeszközökre, a fordítókra, mindenre, aminek köze volt a kód létrehozásához.

Az ASVS az alábbi területeken javasol vizsgálatokat:

- Biztonsági architektúra
- Hitelesítés
- Session kezelés
- Hozzáférés-vezérlés
- Input validáció
- Kimenet kódolása, escape-elés
- Kriptográfia
- Hibakezelés és naplózás
- Adatvédelem
- Kommunikáció biztonsága
- HTTP biztonság
- Biztonsági konfiguráció
- Kártékony kód keresése
- Belső biztonság

Az ASVS erőforrásait elemezve, az e-közigazgatási rendszereket a különböző biztonsági szinteken az alábbi sebezhetőség-vizsgálatnak javaslom alávetni:

- Alap biztonsági szint: Level 1, hiszen a támadói profil szerint is elsősorban automatizált eszközöket használó külső felhasználókkal számolunk. Kisebb kockázatú online rendszereknél elég a Level 1A (automatikus vizsgálat a lefordított kódon) szint elérése.
- Fokozott biztonsági szint: Level 1B és Level 2A vizsgálat elvárt. A Level 1B vizsgálatot ad egyfajta bizonyosságot arról, hogy kódban nem követtek el hibát a fejlesztők, de az automatizált eszközök használatával ez nem jelent túlzott erőforrás-

igényt. A Level 2A vizsgálat a manuális behatolás-tesztelést jelenti, ami összhangban van az erre a szintre előírt etikus hackeléssel, azaz a kreatív hibakereséssel. Az értekezés fokozott szinten EAL3 értékelési szintet határozott meg, abban azonban nem található meg a forráskódelemzés követelménye. Mivel fontosnak és elvárhatónak tartom a kód legalább statikus elemzését ezen a szinten, az itt található ellentmondást úgy oldom fel, hogy kiterjesztem AVA_VAN.2-t a Level 1B követelményeivel.

- Kiemelt biztonsági szint: minimálisan a Level 2 szint teljesítése elvárt, de amennyiben erre lehetőség nyílik a Level 3 vagy a Level 4 vizsgálat sem elvetendő. A Level 2 szinttel megszerezhető az az alapvető bizonyosság, hogy a minősített adatokat kezelő rendszerben kicsi a kockázata valamilyen rejtett kártékony kód megjelenésének.

3.5.2 Rendszerszintű vizsgálatok

Az Open Web Applications Security Project (OWASP) keretében 2003 óta rendszeresen közzéteszik a webes alkalmazásokra vonatkozó nagy kockázatú sebezhetőségeket. Az OWASP Top 10 2010-es kiadása alapján a sérülékenység-vizsgálat olyan módszertana állítható össze, mely segít a legtipikusabb hibák felderítésében, így jelentősen növekedhet az alkalmazás biztonsági szintje. A rendszert érintő vizsgálatok során elsősorban ezekre kell koncentrálni, függetlenül attól, hogy épp az alkalmazást vagy valamelyik azt futtató infrastruktúra-elemet vizsgáljuk. A tesztesetek webes környezetre vannak kidolgozva, de analóg módon a legtöbb esetben más platformokon is használhatók.

A legnagyobb kockázatú hibák felsorolása az alábbiakban található.

A1 – Beszúrásos támadások (Injection): A beszúrásos hibák, melyek közé elsősorban az SQL, operációs rendszer és LDAP injection értendő, olyankor történnek, amikor a támadó nem megbízható adatokat küld a parancsfeldolgozó felé parancsként vagy lekérdezésként. A támadó kód eléri a parancsfeldolgozónál, hogy az nem kívánt parancsot hajtson végre, vagy érzékeny adatokat szivárogtasson ki.

A2 – Cross-Site Scripting (XSS): Az XSS hibák jellemzője, hogy egy alkalmazás nem megbízható adatokat vesz át és küld tovább a böngészőn keresztül megfelelő ellenőrzés és szűrés nélkül. Az XSS lehetővé teszi a támadónak, hogy szkripteket hajtson végre az áldozat böngészőjében, amivel el tudja téríteni a felhasználó session-jét, weboldalakat tud megváltoztatni, vagy át tudja irányítani a felhasználót egy kártékony oldalra.

A3 – Hibás hitelesítés és sessionkezelés (Broken Authentication and Session Management): Az alkalmazások hitelesítéshez és sessionkezeléshez kapcsolódó funkciói sok esetben nem megfelelően lettek implementálva, ezért lehetővé válik a jelszavak, kulcsok, session tokenek megszerzése, vagy más hibák előidézése, aminek segítségével a támadó más, jogosult felhasználó nevében tud eljárni.

A4 – Nem biztonságos direkt objektumhivatkozás (Insecure Direct Object References): Direkt objektumhivatkozásról akkor beszélünk, amikor a fejlesztő felfed egy hivatkozást valamilyen belső, implementációhoz szükséges objektum felé, mint pl. egy fájl, könyvtár vagy adatbázis tábla. Megfelelő hozzáférés-védelem vagy más biztonsági megoldás nélkül a támadó vissza tud élni ezekkel a hivatkozásokkal, és nem jogosult hozzáférést szerezhet az ezekben tárolt adatokhoz.

A5 – Cross-Site Request Forgery (CSRF): A CSRF támadás során a támadó kényszeríti az authentikált felhasználó böngészőjét arra, hogy egy hamisított HTTP kérést küldjön egy sebezhető webalkalmazás felé, mely tartalmazza az áldozat session cookie-ját és más hitelesítési információkat. Ez lehetővé teszi, hogy az áldozat böngészője olyan kéréseket küldjön a sebezhető alkalmazás felé a támadó nevében, melyről azt hiszi, hogy az legitim forrásból érkezik.

A6 – Helytelen biztonsági beállítások (Security Misconfiguration): A megfelelő biztonság eléréséhez meg kell határozni az alapvető beállításokat, és ezeket meg is kell valósítani az alkalmazásokban, keretrendszerekben, alkalmazásszervereken, webszervereken, adatbázis-szervereken és minden más érintett platformon. Mivel a legtöbb rendszer nem olyan alapbeállítással kerül telepítésre, mely az elvárható biztonsági szintet valósítja meg, ezeket a konfigurációkat meg kell határozni, implementálni kell, és folyamatosan fenn kell tartani. A folyamat során a szoftverek frissítéseire is figyelemmel kell lenni.

A7 – Nem megfelelő kriptográfiai tárolás (Insecure Cryptographic Storage): Számos webalkalmazás nem megfelelően kezeli az érzékeny adatokat, mint pl. a hitelesítési adatok, mert ezeket nem titkosított vagy lenyomatolt formában őrzi. A támadók ezért megszerezhetik vagy módosíthatják a gyengén őrzött adatokat, ami számos visszaéléshez vezethet.

A8 – URL hozzáférés korlátozásának hibája (Failure to Restrict URL Access): A webes alkalmazásokban fontos az URL-ek hozzáférési jogainak ellenőrzése, mielőtt a felhasználó elérne egy védett hivatkozást vagy akciógombot. A hozzáférési jognak ezt az ellenőrzését

viszont minden esetben meg kell tenni, amikor ezeket a védett oldalakat elérik, mert különben a támadó elérheti a rejtett oldalakat.

A9 – Nem megfelelő szállítási réteg védelem (Insufficient Transport Layer Protection): Az alkalmazások gyakran nem megfelelő hitelesítést, titkosítást és bizalmasság-sértetlenség védelmet használnak az érzékeny hálózati forgalomban. Amikor viszont használnak, akkor is gyenge algoritmusokkal, lejárt vagy érvénytelen tanúsítványokkal teszik ezt, vagy egyszerűen nem megfelelően használják a kriptográfia adta lehetőségeket.

A10 – Nem ellenőrzött átirányítások és továbbítások (Unvalidated Redirects and Forwards): A webes alkalmazások gyakran irányítják át vagy továbbítják a felhasználókat más oldalakra, és használnak nem hiteles adatokat a forrásoldal megállapítására. Megfelelő ellenőrzés nélkül a támadók átirányíthatják a felhasználókat adathalász vagy kártékony oldalakra, vagy a továbbításokkal nem jogosult hozzáférést szerezhetnek.

A Common Criteria szerint besorolás a következő:

- Megkerülés: A2, A4, A5, A8
- Meghamisítás: A1, A7, A10
- Direkt támadások: A3, A7
- Megfigyelés: A9
- Nem megfelelő használat: A6

Behatolás-tesztelés és etikus hackelés esetén szükséges az alkalmazáson kívül akár a teljes informatikai infrastruktúra automatizált vizsgálata is. Az értekezés nem foglalkozik ezzel a területtel, de a teljesség kedvéért meg kell említeni az infrastruktúra ellenőrzésére használt automatizált eszközök körét is. Ezek közé tartoznak azok a szoftverek, melyekkel az infrastruktúra felderítését lehet végrehajtani, melyekkel az operációs rendszerek válnak támadhatóvá, amik a hálózati elemekkel szemben hatékonyak, végül azok, melyek az alkalmazás közvetlen környezetét jelentő szoftvereket (adatbázisok, alkalmazás-szerverek) vizsgálják. Ezek együttes, célravezető használata támogatja a teljes körű vizsgálatot. [76]

3.5.3 Szervezet szintű vizsgálatok

A social engineering az emberi hiszékenységre, együttműködésre építő támadási forma, mely a szervezeti és humán sebezhetőségeket vizsgálja. Bár ezt az élet minden területén kihasználják, az SE kimondottan az információ megszerzésére irányul, ezen belül is

elsősorban az informatikai eszközökön tárolt adatokra fókuszálva. Az évtizedek során felhalmozott tapasztalat szerint az IT eszközök védelme egyre kifinomultabb, azonban az ezeket használó emberek biztonságtudatossága csak minimálisan növekedett. Így a legjárhatóbb támadási eljárás az emberi erőforrás kihasználása vagy, ahogy a közkeletű bölcsesség tartja, a legtöbb biztonsági probléma a billentyűzet és a szék között található.

A támadónak több olyan emberi tulajdonságot van lehetősége kihasználni, ami szinte kivétel nélkül minden potenciális áldozatban megtalálható. A legalapvetőbb ilyen tulajdonság a segítőkészség, de szóba kerülhet még a hiszékenység, a kíváncsiság és a naivság, amit a nagyon divatos adathalász-támadások során is előszeretettel használnak. A kihasználható tulajdonságok között beszélhetünk még a befolyásolhatóságról is, ami megvesztegetés, zsarolás, megfélemlítés útján érhető el. Emellett nem szabad elfeledkezni a dolgozók figyelmetlenségéről, hanyagságáról és alulképzettségéről sem.

De ki a támadó? Az emberi hiszékenységgel való visszaélést számos tényező motiválhatja, így a social engineer-ek is több csoportba oszthatók. [77]

- Hackerek
- Ipari kémek
- Külföldi államok által megbízott hivatásos hírszerzők
- Személyes adatokat ellopásával foglalkozó bűnözők
- Elégedetlen munkavállalók
- Konkurens vállalkozások megfigyelői
- Magánnyomozók
- Csalók
- Fejvadászok (akár bűnügyi, akár munkajogi értelemben)
- Terroristák

Az SE támadásokat két csoportba lehet sorolni. Egyrészt beszélhetünk humán alapú módszerekről, melyek közvetlen kontaktust feltételeznek a támadó és az áldozat között, másrészt azonosíthatunk számítógép alapú technikákat, melyeknél a kapcsolat közvetett, a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal.

A humán módszerek a következők: [78]

- Segítség kérése
- Segítség nyújtása
- Kölcsönösség kihasználása
- Megszemélyesítés
- Shoulder surfing – képernyő lelesése
- Tailgating – bejutás a bejáraton más embert követve, annak tudtán kívül
- Piggybacking – bejutás a bejáraton más embert követve, annak tudtával
- Dumpster diving – információk felkutatása a hulladékban

A számítógép alapú támadások köre az alábbiak szerint alakul:

- Scam – hamisított weboldalak
- Adathalászat
    - Phishing – E-mail alapú
    - Vishing – VoIP alapú
    - Smishing – SMS alapú
    - Pharming – DNS eltérítésen alapuló
- Whailing – Vezetői IT eszközöket célzó támadás
- Baiting – Adathordozók szétszórása

A biztonsági tesztelést végző ezen technikák közül bármelyiket választhatja, ami a kívánt cél elérésében számára a legnagyobb segítséget nyújtja. A szervezeti biztonságot az összes adminisztratív, fizikai és logikai védelmi kontroll együttes használata jelenti, a social engineering ezek mindegyikét próbára teszi, ezért lehet ezt a módszert a szervezeti biztonság sebezhetőség-vizsgálatának felfogni. A tesztelés során minden esetben a megrendelővel egyeztetett technikát kell alkalmazni, ám jelen értekezés nem tűzte ki azt a célt, hogy a tesztelés garanciális feltételeit meghatározza. Javaslatom szerint a sebezhetőség-vizsgálatokat az adott szinten az általam meghatározott módon kell elvégezni, abból teszteseteket csak rendkívül indokolt esetben lehet elhagyni. Ez az egységesség biztosítja ugyanis az egyenszilárdságú védelmet.

Az alábbi táblázat foglalja össze a három biztonsági szint elvárásait.

	1. biztonsági szint (C2G, G2C)	2. biztonsági szint (G2G)	3. biztonsági szint (minősített adatokat kezelő rendszerek
Biztonsági tesztelés módja	Biztonsági funkcionális tesztelés, sérülékenység-vizsgálat	Biztonsági funkcionális tesztelés, etikus hackelés	Biztonsági funkcionális tesztelés, blue-teaming behatolás-tesztelés
Biztonsági tesztelés területei	Kód és alkalmazás	Kód és szervezet	Kód és rendszer
Támadói profil	Alap-erősített	Alap-erősített	Mérsékelt
Eltelt idő	2 hét	1 hét	1 hét
Szakértelem szintje	Profi	Profi	Szakértő
Termékismeret	Korlátozott információ	Érzékeny	Érzékeny
Próbálkozási ablak	Mérsékelt	Egyszerű	Egyszerű
Eszköztár	Szabványos	Szabványos	Speciális eszközök
Biztonsági funkcionális tesztelés szintje (ASVS)	Level 1A	Level 1B és Level 2A	Level 2
Automatizált eszközök használata	Alkalmazásra koncentrálva	Alkalmazás és infrastruktúra	Alkalmazás és infrastruktúra

3. táblázat: Tesztelési követelmények biztonsági szintenként

A tesztelési módszerek ilyen szintű csoportosítása lehetővé teszi a magyar elektronikus közigazgatási rendszerek biztonsági vizsgálatának összemérhető, megalapozott vizsgálatát.

3.6 Sebezhetőség-vizsgálati módszertan

A webes alkalmazások teszteléséhez az Open Web Application Security Project keretében megalkotott módszertanok tekinthetők a leghasznosabbaknak, legalábbis ezekre hivatkozik a legtöbbet a szakirodalom napjainkban. Mint az már többször leírásra került, ezek a módszerek nem csak webes környezetben használhatók. Az OWASP kétfelé bontotta az ellenőrzési folyamatokat. Az OWASP Code Review Guide (CRG) célja a létrehozott kódok manuális ellenőrzése, white-box módon. [79] Gyakorlatilag a manuális biztonsági funkcionális tesztelésnek felel meg, ami az OWASP Application Security Verification Standard Project

(ASVS) Level 2 B szinttől felfelé elvárt. Az értekezés besorolása alapján ez a kiemelt biztonsági szint követelménye. Mivel a kódok automatikus ellenőrzése alacsonyabb szinten is elvárt, így a CRG végrehajtása automatizált eszközökkel követelmény. Az OWASP Testing Guide (TG) a már elkészült alkalmazás black-box teszteléséhez, azaz sérülékenység-vizsgálatához ad segítséget. Ez viszont mindhárom biztonsági szinten elvárt.

A CRG tehát a kódok átvizsgálására készült, mely folyamat célja meggyőződni arról, hogy a forráskódban a megfelelő biztonsági kontrollok implementálásra kerültek és úgy működnek, ahogy a tervezés szerint működniük kell. Ellenőrzi továbbá azt is, hogy a biztonsági kódokért felelős fejlesztők követték a számukra megállapított eljárásrendeket. Mivel a behatolás-tesztelés, de még a sérülékenység-vizsgálat sem képes teljes körűen felderíteni az esetleges hibákat, egyedül a white-box tesztelésnél van lehetőség a rosszul megírt kódrészleteket átfogóan megtalálni. A biztonsági funkcionális tesztelés a humán erőforrás és a célszoftverek alkalmazását is szükségessé teszi. Az automatizált eszközök itt a leghatékonyabbak, de nem képesek teljes mértékben pótolni a tesztelési szakembert, hiszen az egyes kontextusok döntően befolyásolhatják a kódolás megfelelőségét vagy nem megfelelőségét.

A CRG a legfontosabb technikai kontrolloknak az authentikációt, az authorizációt, a sessionkezelést, az input validációt, a hibakezelést, az alkalmazás telepítését és a kriptográfiát tartja, többé-kevésbé összhangban a Common Criteria 2. kötetében leírt biztonsági funkcionális követelményekkel. A legkomolyabb programozáskor elkövetett hibaforrásoknak pedig a puffer túlcsordulást, az operációs rendszer és SQL injektálást, az adatvalidációt, a cross-site scriptinget, a cross-site request forgery-t, a naplózási hiányosságokat, a session sértetlenségét és a versenyhelyzeteket tartja, szinkronban az OWASP Top 10 megállapításaival. A CRG részletesen bemutatja azokat a tipikus hibákat, amiket a biztonsági funkciók implementálásánál el szoktak követni, illetve azt is, hogyan lehet a programozási hibákat felderíteni.

A biztonsági funkcionális tesztelés azonban idő- és erőforrás-igényes, tehát drága. Emellett a szükséges szakértői háttér is nehezen elérhető Magyarországon. Célravezetőbb a TG-ben leírt sérülékenység-vizsgálatokat végrehajtani, ami nem jelent ugyan akkora bizonyságot, mint a CRG folyamatai, de így is jelentősen tudja csökkenteni a támadási felületeket. A TG az OWASP Top 10 fenyegetéseit veszi sorra, és leírja, hogy milyen tesztelési eljárásokkal lehet meggyőződni arról, hogy a kész alkalmazás ellenáll ezeknek. Black-box tesztelés esetén az automatikus teszteszközök már körülményesebben használhatók, de még bevethetők. Ezért az

egyes tesztesetekhez konfigurálható céleszközöket szoktak használni, ami feltételezi, hogy a tesztelő jól ismeri ezt a területet.

A TG 10 kategóriában 66 tesztesetet határoz meg. Az alkalmazás típusától és megvalósításától függően kell ezeket végrehajtani.

Információszerzés:

- Webes keresők robotjai
- Felderítés webes keresők adatbázisában
- Alkalmazás belépési pontjainak azonosítása
- A webes alkalmazás ujjlenyomatának tesztelése
- Alkalmazás felderítése
- Hibaüzenetek elemzése

Konfigurációmenedzsment tesztelés

- SSL/TLS tesztelés
- DB Listener tesztelés
- Infrastruktúra konfigurációmenedzsmentjének tesztelése
- Alkalmazás konfigurációmenedzsmentjének tesztelése
- Fájlkiterjesztés kezelésének tesztelése
- Régi, mentett és nem hivatkozott fájlok
- Infrastruktúra és alkalmazás adminisztrátori interfészek
- HTTP metódusok és XST tesztelés

Authentikációs eljárások tesztelése

- Authentikációs adatok átvitele biztonságos csatornán keresztül
- Felhasználói adatbázis tesztelése
- Kitalálható (szótár alapú) felhasználói fiókok felderítése
- Nyers erejű tesztelés
- Az authentikációs séma kikerülésének tesztelése

- Sebezhető emléketető jelszó és jelszó visszaállítási lehetőségek
- Kilépés és böngésző cache menedzsment
- CAPTCHA kódok
- Többfaktorú authentikáció tesztelése
- Versenyhelyzetek kezelése

Sessionkezelés

- A sessionkezelési séma tesztelése
- Cookie attribútumok
- Session fixálás
- Kiterjesztett sessionváltozók tesztelése
- CSRF

Authorizáció tesztelése

- Elérési útvonalak tesztelése
- Az authorizációs séma kikerülése
- Jogosultság kiterjesztése

Üzleti logika

- Az üzleti logika tesztelése

Adatvalidáció:

- Nem perzisztens XSS
- Perzisztens XSS
- DOM alapú XSS
- Cross Site Flashing
- SQL Injection
- LDAP Injection
- ORM Injection

- XML Injection
- SSI Injection
- XPath Injection
- IMAP/SMTP Injection
- Kódbeszúrás
- Operációs rendszer parancsainak kiadása
- Puffer túlcsordulás
- Összetett adatvalidációs tesztelés
- HTTP splitting/smuggling tesztelés

Túlterheléses támadások (DoS) tesztelése

- SQL wildcard támadás
- Ügyfélfiókok zárolása
- DoS puffer túlcsordulások tesztelése
- Felhasználó által meghatározott objektumallokáció
- Felhasználói adatbevitel, mint körbeforgó számláló
- Felhasználó által bevitt adatok lemezre írása
- Erőforrás sikertelen elengedése
- Túl sok adat tárolása egy session-ben

Web service tesztelés

- Web service információszerzés
- WSDL tesztelés
- XML struktúra tesztelés
- XML tartalom szintű tesztelése
- HTTP GET paraméterek/REST tesztelés
- SOAP csatolások

- Visszajátszásos támadás

AJAX tesztelés

- AJAX sebezhetőségek
- AJAX tesztelés

3.7 Következtetések

Ebben a fejezetben bemutatásra került egy olyan kibertámadási forgatókönyv, mely nemzetközi példák elemzésével mutat rá, milyen reális, informatikai jellegű fenyegetésekkel kell számolni a kritikus információs infrastruktúrák területén. Ezen fenyegetések kivédése érdekében javaslatot tettem megfelelő humán állománnyal rendelkező szervezet létrehozására, melynek **alapjaira szintén javaslat született** az önkéntes tartalékos haderő jogszabályi kereteit kihasználva. Javaslatot tettem az önkéntes tartalékos kibervédelmi haderő tagjaira, az információvédelmi stratégia kialakítására, és **felmértem a célcsoportok együttműködési hajlandóságát** a 2009-es Hacktivity hackerkonferencia levelezőlistáján keresztül egy célzott kérdőív kiküldésével.

Ezután egészen magas szintről indulva áttekintetésre kerültek azokat a módszertanok, melyek segítenek meggyőződni az e-közigazgatási alkalmazás biztonsági szintjéről tesztelési módszerekkel. A szakirodalomban leggyakrabban előforduló fogalmakat rendszereztem, és **kialakítottam az értekezésben használt terminológiát a sebezhetőség-vizsgálatok területére**.

A korábbi fejezetekben bevezetett módon három biztonsági szintet állapítottam meg az e-közigazgatási alkalmazások védelmére. A biztonsági teszteléseket is ehhez igazítottam, **kidolgoztam az elvárható biztonsági tesztelések módszertanát a magyar közigazgatási rendszerekre**. Leírtam továbbá a számszerűsített támadási potenciálokat is, melyek szintén illeszkednek a szintekhez.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Értekezésem elején több hipotézist állítottam fel, melyek bizonyítását hosszasan vezettem le. Bebizonyítottam, hogy a magyar jogszabályi és műszaki szabályozási környezet nem elégséges ahhoz, hogy az alkalmazásfejlesztés biztonsági aspektusait pontosan meghatározza. Ezt a hiányosságot próbáltam kiküszöbölni. Bebizonyosodott továbbá az is, hogy bár a Common Criteria szerinti fejlesztések elvárásként megjelennek az e-közigazgatási fejlesztéseknél, nincs olyan egységes alap, amire támaszkodni lehetne. Bár az ajánlások ezt a megközelítést használják, de túl nagy szabadságot engednek a fejlesztőknek, ami véleményem szerint nem elfogadható. Szintén igaz ez a besorolási rendszerekre, ami az ajánlásokon belül is ellentmondásos, így ezek egységes, egyszerű megközelítése szükséges.

Az értekezésemben a hipotézisek vizsgálata során összességben számos olyan megállapítást, észrevételt tettem, melyek segítik a magyar elektronikus közigazgatási rendszerek, és közvetve hazánk biztonsági szintjének növelését, és alapul szolgálnak az általam elért új tudomány eredményekhez.

A dolgozat elején először több forrás elemzésével megjelöltem azokat az intézményeket, melyek a központi közigazgatáson belül informatikai szempontból kiemelt jelentőséggel bírnak, valamint javaslatot tettem a magyar jogszabályi rendszer kiterjesztésére információbiztonsági szempontból. Ezután elkészítettem egy Common Criteria szerinti Védelmi Profil eszköztárat, melynek alapján az e-közigazgatási rendszerek biztonsági funkcionalitása egységesen kialakítható.

Meghatároztam három olyan védelmi szintet, melyek a jelenlegi ajánlásokhoz képest könnyebb besorolást tesznek lehetővé. Ezekhez a védelmi szintekhez határoztam meg funkcionális és garanciális (ezen belül sebezhetőség-vizsgálati) követelményeket, így a gyakorlatban könnyen használható rendszert alkottam. Ehhez kapcsolódóan elemeztem a mértékadó ajánlások gyakorlati megvalósíthatóságát, és a jogszabályi háttér teljességét, és részletes adminisztratív, logikai és fizikai védelmi követelményeket határoztam meg a közigazgatási rendszerek fejlesztőivel szemben.

Témavezetőmmel felépítettem egy olyan kibertámadási forgatókönyvet, mely Magyarország ellen irányul, és ennek megvalósíthatóságát megtörtént esetekkel támasztottam alá. Javaslatot tettem a kibervédelem hazai alapjainak megvalósítására az önkéntes tartalékos haderőn belül, és kutatással bizonyítottam ennek megvalósíthatóságát a potenciális önkéntesek között.

Meghatároztam a közigazgatási rendszerek lehetséges támadóinak támadási potenciálját. Végül a biztonsági szintekhez kapcsolódóan biztonsági tesztelési módszertanokat írtam le.

Új tudományos eredmények

Összességében az alábbi új tudományos eredményeket értem el:

1. **Létrehoztam egy olyan Védelmi Profil eszköztárat**, melynek alapján lehetségessé válik a magyar közigazgatási rendszerek fejlesztése egységes biztonsági elvek alapján.
2. **Logikai, adminisztratív és fizikai kontrollokat határoztam meg**, melyek a magyar közigazgatási rendszerek fejlesztőire vonatkoznak.
3. **Javaslatot tettem a kibervédelem hazai alapjainak megvalósítására az önkéntes tartalékos haderőn belül**.
4. **Javaslatot tettem egy biztonsági tesztelési módszertanra**, mely a magyar közigazgatási rendszerek sebezhetőségeinek felderítését segíti.

Ajánlások és gyakorlati felhasználhatóság

Értekezésemet abból a célból írtam, hogy a közigazgatási rendszerek fejlesztésénél tapasztalt hiányosságok feloldásában segítsen. Mindhárom fejezetben olyan problémákra adtam megoldási javaslatot, melyek súlyos hiányosságként jelennek meg az alkalmazásfejlesztőknél és a megrendelőknél. Dolgozatomat ezért ajánlom:

- egyrészt azon szakemberek figyelmébe, akik a jogi és műszaki szabályalkotásért felelősek, másrészt azoknak, akik a közigazgatási rendszerek specifikálásáért és fejlesztéséért felelnek.
- Ajánlom a harmadik fejezetet azoknak, akik az ország és az egyes magánkézben levő kritikus információs infrastruktúrák kibervédelméért felelősek.
- Eredményeimet ajánlom széles körben felhasználni a közigazgatás egészében, akár műszaki ajánlás szintjén is.
- További kutatásra ajánlom a kibervédelem lehetséges megoldását az önkéntes tartalékos haderőn belül, hiszen számos izgalmas, megválaszolatlan kérdés található itt, a nemzetközi jogtól kezdődően a szervezési problémákon át a konkrét műszaki védelemig bezárólag.

TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓK JEGYZÉKE

Magyar nyelvű könyvfejezet

1. **Krasznay, Cs.**, *Az Informatikai Biztonsági Irányítási Rendszer bevezetése és működtetése*. In Muha, L. (szerk.), *A KIB 25. számú ajánlása: 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió*
2. **Krasznay, Cs.,** *Az elektronikus aláírás*. In Szigeti, Sz. (szerk.), *A KIB 25. számú ajánlása: 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX) 1.0 verzió*

Lektorált folyóiratcikkek

1. **Krasznay, Cs.**, *A magyar elektronikus közigazgatás biztonságának elemzése és továbblépési lehetőségei*, Hadmérnök, 2009. 1., http://hadmernok.hu/2009_1_krasznay.php, ISSN 1788-1919
2. **Krasznay, Cs.**, *Szoftverfejlesztői követelmények minősített környezetben: Adminisztratív követelmények*, Hadmérnök 2009. 4., http://hadmernok.hu/2009_4_krasznay.php, ISSN 1788-1919
3. **Kovács, L., Krasznay, Cs.**, *Digitális Mohács - Kibertámadási forgatókönyv Magyarország ellen*, Nemzet és Biztonság, 2010. február, http://neb.kezek.hu/letoltes.php?letolt=285, ISSN 1789-5286 (50%-os részvétel)
4. **Krasznay, Cs.**, *E-közigazgatási rendszerek és alkalmazások sebezhetőségi vizsgálata*, Hadmérnök 2010. 3., http://hadmernok.hu/2010_3_krasznay.php, ISSN 1788-1919

Idegen nyelvű kiadványban megjelent cikkek

1. **Krasznay, Cs., Szabó, Á.**, *Developing interoperable e-government solutions in Hungary*, eGOV INTEROP'06 Conference

Nemzetközi konferencia kiadványban megjelent lektorált idegen nyelvű előadások

1. **Krasznay, Cs.**, *Hackers in the national cyber security*, Cyter 2009 Conference Prague, 2009. június, ISBN 978-80-01-04372-1

2. **Krasznay, Cs.**, *Software Development Security in Complex IT Environments*, EuroCACS 2010 Conference, 2010. március

Hazai konferencia kiadványban megjelent magyar nyelvű előadás

1. **Krasznay, Cs.**, *Kéziszámítógépek biztonsága*, Hacktivity 2004 Konferencia
2. **Krasznay, Cs.**, *A Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma szerinti értékelőlaborok*, HiSec 2004 konferencia
3. **Krasznay, Cs.**, *Bluetooth biztonság*, Hacktivity 2005 konferencia
4. **Krasznay, Cs., Szigeti, Sz.**, *A magyar elektronikus közigazgatási rendszer biztonsági analízise*, Networkshop 2006 Konferencia
5. **Krasznay, Cs.**, *Common Criteria szerinti értékelések lehetőségei Magyarországon*, Informatikai Biztonság Napja 2006
6. **Krasznay, Cs.**, *Phishing és spam Magyarországon és a világban*, Hacktivity 2007 konferencia
7. **Krasznay, Cs.**, *A mobilkészülékek biztonsága*, Informatikai Biztonság Napja 2007
8. **Krasznay, Cs.**, *Információbiztonság a másik oldalról: hackerek Magyarországon*, Robothadviselés 7. Tudományos Konferencia
9. **Krasznay, Cs.**, *Web service fenyegetések e-közigazgatási környezetben*, Networkshop 2009 Konferencia
10. **Krasznay, Cs.,** *Naplózás e-kormányzati rendszerekben*, Networkshop 2010 Konferencia

IRODALOMJEGYZÉK

[1] **Haig, Zs., Várhegyi, I.** (2008.). *A cybertér és a cyberhadviselés értelmezése*, Hadtudomány folyóirat, 2008. elektronikus szám. (pp.: 16-28.). ISSN 1215-4121

[2] **HP DVLabs**. (2011. szeptember). *The 2011 Mid-year Top Cyber Security Risks Report*. (pp.: 14-20.). Letöltés dátuma: 2011. szeptember 15., forrás: HP DVLabs: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-7045ENW.pdf

[3] **Torma, A**. (1998.). A közigazgatási informatika jogi alapjai. In Ficzere, L., *Magyar közigazgatási jog. Általános rész.* (pp.: 488-506.). Budapest: Osiris Kiadó. ISBN: 9789633898772

[4] **Simon, P**. (2009. április 16.). *A gépiadatfeldolgozástól a kormányzati informatika előszobájáig*. Magyary Zoltán E-közigazgatástudományi Egyesület E-közigazgatás hazai története szimpózium, Budapest.

[5] **Varga, L**. (2010. április 13.). *A közigazgatási informatika kezdetei*. Jegyző és Közigazgatás. ISSN: 1589-3383.

[6] **Sikolya, Zs**. (2009. április 16.). *A közigazgatási informatikától az e-közigazgatásig.* Magyary Zoltán E-közigazgatástudományi Egyesület E-közigazgatás hazai története szimpózium, Budapest.

[7] **Nemzeti Fejlesztési Ügynökség**. (2011. szeptember 1.). *EKOP - Elektronikus közigazgatás Operatív Program eredmények.* Letöltés dátuma: 2011. szeptember 1., forrás: Nemzeti Fejlesztési Ügynökség honlapja: http://www.nfu.hu

[8] *38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról.*

[9] **Közigazgatási Informatikai Bizottság**. (2008.). *A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár*. Letöltés dátuma: 2011. szeptember 1., forrás: http://kovetelmenytar.complex.hu/

[10] **Közigazgatási Informatikai Bizottság**. (2008. december 3.). *A magyar e-közigazgatási architektúra*. (pp.: 14-53.). Letöltés dátuma: 2011. szeptember 1., forrás: E-közigazgatási Követelménytár: http://kovetelmenytar.complex.hu/document/koz/EKZ_EKK_EKOZIG_MAGYAR_KOZIG_RENDSZER_ARCHITEKTURA_081203_V3.DOC

[11] *223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról*.

[12] **Közigazgatási Informatikai Bizottság**. (2008. június). *A KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA) 1.0 verzió*. Budapest.

[13] **Szigeti, Sz., Krasznay, Cs**. (2006.). *A magyar elektronikus közigazgatási rendszer biztonsági analízise*. Networkshop 2006 Konferencia (old.: 65-69.). Miskolc: Nemzeti Információs Infrastrukúra Fejlesztési Program.

[14] **Shah, S**. (2008). *Web 2.0 Security: Defending Ajax, RIA, and SOA.*(pp.: 47-70.). Boston, Massachusetts: Charles River Media. ISBN: 1584505508

[15] **The Open Web Application Security Project**. (2010. október 16.). *OWASP Top 10 - 2010, The Ten Most Critical Web Application Security Risks*.

[16] **Közigazgatási Informatikai Bizottság**. (2008. augusztus 22.). *Útmutató az IT biztonsági szintek meghatározásához*. (pp.:18-26.). Letöltés dátuma: 2011. szeptember 1., forrás: E-közigazgatási Követelménytár: http://kovetelmenytar.complex.hu/doc.php?docid=EKZ_EKK_EKOZIG_ITBIZTONSAGISZINTEKMEGHATAROZASA_080822_V101.DOC

[17] *161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól*.

[18] **Wikipedia**. (2011. szeptember 3.). *Advanced persistent threat*. Letöltés dátuma: 2011. szeptember 15., forrás: Wikipedia - The Free Encyclopedia: http://en.wikipedia.org/wiki/Advanced_Persistent_Threat

[19] **Help Net Security**. (2011. szeptember 14.). *Cyber security leaders share their APT knowledge*. Letöltés dátuma: 2011. szeptember 15., forrás: Help Net Security: http://www.net-security.org/secworld.php?id=11621

[20] **Dajkó, P**. (2009. február 8.). *Súlyos üzemzavar az Ügyfélkapu rendszerében*. Letöltés dátuma: 2011. szeptember 15., forrás: IT Café: http://itcafe.hu/hir/ugyfelkapu_uzemzavar_meh.html

[21] **Miniszterelnöki Hivatal Informatikai Biztonsági Felügyelő**. (2009). *Részletes jelentés a Központi Elektronikus Szolgáltató Rendszer egyes szolgáltatásainak üzemzavarairól.* Budapest: Miniszterelnöki Hivatal.

[22] **Dajkó, P**. (2009. február 11.). *Fejek hullanak az Ügyfélkapu üzemzavara miatt*. Letöltés dátuma: 2011. szeptember 15., forrás: IT Café: http://itcafe.hu/cikk/ugyfelkapu_uzemzavar_baja_dedinszky_meh/hiba_hiba_hatan.html

[23] **Index**. (2009. május 29.). *Estére újraindult az Ügyfélkapu*. ISSN 1585-3241. Letöltés dátuma: 2011. szeptember 15., forrás: Index.hu: http://index.hu/tech/net/2009/05/29/lehalt_az_ugyfelkapu/

[24] **Dajkó, P**. (2009. január 23.). *Helyreállították az OEP informatikai rendszerét*. Letöltés dátuma: 2011. szeptember 15., forrás: IT Café: http://itcafe.hu/hir/oep_szoftverhiba.html

[25] **Közigazgatási Informatikai Bizottság**. (2008. augusztus 22.). *IT biztonsági követelményrendszer - biztonsági szintek követelményei*. (pp.: 26-101.). Letöltés dátuma: 2011. szeptember 15., forrás: E-közigazgatási Követelménytár: http://kovetelmenytar.complex.hu/doc.php?docid=EKZ_EKK_EKOZIG_ITBIZTONSAGIKOVETELMENYRENDSZER_080822_V101.DOC

[26] **International Organization for Standardization**. (2008. április 22.). *ISO/IEC 27002:2005 Code of practice for information security management*.

[27] **International Organization for Standardization**. (2009. december 3.). *ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*.

[28] **Common Criteria Development Board**. (2009. július). *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1.*

[29] **Közigazgatási Informatikai Bizottság**. (2008. június). *A KIB 25. számú ajánlása: 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió*. Budapest.

[30] **Common Criteria Development Board**. (2009. július). *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1.*

[31] **National Institute of Standards and Technology**. (2008. október). *Security Considerations in the System Development Life Cycle, Special Publication 800-64 Revision 2*. (pp.: 11-40.). Gaithersburg, Maryland, USA.

[32] **International Organization for Standardization**. (2011. április 12.). *ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements*.

[33] **Muha, L. (szerk.)**. (2008. június). *A KIB 25. számú ajánlása: 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió*. (pp.: 28-57.). Budapest.

[34] *92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól*.

[35] *143/2004. (IV. 29.) Korm. rendelet az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól*.

[36] *2003. évi CXXIX. törvény a közbeszerzésekről*.

[37] *2009. évi CLV. törvény a minősített adat védelméről*.

[38] *90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről*.

[39] **Közigazgatási Informatikai Bizottság**. (2008. május 29.). *Közigazgatási Operatív Programok IT biztonsági környezete, követelményrendszere*. (pp.: 25-30.). Letöltés dátuma: 2011. október 4., forrás: Az E-közigazgatási Keretrendszer projekt eredményeként létrehozott követelménytár: http://kovetelmenytar.complex.hu/doc.php?docid=EKZ_EKZ_EKK_EKOZIG_KOP_ITBIZT_KORNYEZETE_080529_V1.DOC

[40] **Muha, L. (szerk.)**. (2008. június). *A KIB 25. számú ajánlása: 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió*. (pp.: 76-105.). Budapest.

[41] **Wilson, C**. (2005). *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.* Washington: Congressional Research Service, The Library of Congress.

[42] **Lynn, W. J.** (Sept/Oct. 2010). *Defending a New Domain: The Pentagon's Cyberstrategy*. Foreign Affairs. (pp.: 97-108.). ISSN: 0015-7120.

[43] **Caldwell, F., & Hunter, R**. (2002. október 4.). *'Digital Pearl Harbor': Defending Your Critical Infrastructure*. Letöltés dátuma: 2011. október 4., forrás: Gartner Research: http://www.gartner.com/pages/story.php.id.2727.s.8.jsp

[44] **Kovács, L., Krasznay, Cs.** (2010. február). *Digitális Mohács.: Egy kibertámadási forgatókönyv Magyarország ellen*. Nemzet és Biztonság. (pp.: 44-56.). ISSN 1789-5286.

[45] **Collings, D., Rohozinski, R.** (2009). *Bullets and Blogs: New media and the warfighter.* (pp.: 34-40.).Carlisle Barracks, Pennsylvania: U.S. Army War College.

[46] **IT Business Online**. (2009. május 19.). Feltörték az Indexet is. ISSN 1589-3464. Letöltés dátuma: 2011. október 4., forrás: IT Business: http://www.itbusiness.hu/print/hirek/ict/Feltortek.html.

[47] **Krasznay, Cs**. (2009. március). *A magyar elektronikus közigazgatás biztonságának elemzése és továbblépési lehetőségek*. Hadmérnök, (pp.: 197-207.). ISSN 1788-1919.

[48] **Organisation for Economic Co-operation and Development (OECD)**. (2011. február 4.). *The economic impact of shutting down Internet and mobile phone services in Egypt*. Letöltés dátuma: 2011. október 4., forrás: OECD: http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html

[49] **Bata, I.** (dátum nélk.). *Vasúti jelző- és biztosítóberendezések*. Letöltés dátuma: 2011. október 4., forrás: metros.hu: http://www.freeweb.hu/metros/mukod/bizber.html

[50] **Budapesti Közlekedési Vállalat**. (dátum nélk.). *Műholdas helyzet-meghatározásra (GPS) épülő intelligens forgalomirányító és utastájékoztató rendszer a városi közösségi közlekedésben*. Letöltés dátuma: 2011. október 4., forrás: http://www.bkvobuda.oasz.net/gps/index.htm

[51] **McMillan, R**. (2007. január 10.). *Two charged with hacking LA traffic lights.* ISSN: 0199-6649. Letöltés dátuma: 2011. október 4., forrás: InfoWorld: http://www.infoworld.com/d/security-central/two-charged-hacking-la-traffic-lights-827.

[52] **Index**. (2009. január 25.). *Meghalt a fél magyar internet*. ISSN 1585-3241. Letöltés dátuma: 2011. október 4., forrás: Index.hu: http://index.hu/tech/net/tcom090125/

[53] **Szalay, D**. (2009. december 4.). *A T-Mobile hálózati összeomlásának krónikája*. ISSN 0237-7837. Letöltés dátuma: 2011. október 4., forrás: Computerworld: http://computerworld.hu/leallt-a-t-mobile-orszagos-halozata.html.

[54] **Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., Vihul, L**. (2008). *Cyber Attacks Against Georgia: Legal Lessons Identified.* (pp.: 4-18.). Tallin: CCD COE Legal Task Team.

[55] **Brown, M., Zmijewski, E.** (2008). *Pakistan Telecom Hijacks YouTube*. Taipei.

[56] **Vámos, S**. (2011. február 24.). *A Stuxnet és hatásai*. Letöltés dátuma: 2011. október 4., forrás: OB121: http://ob121.com/publ_stuxnet.html

[57] **Index**. (2011. március 20.). *Meghekkelték a Magyar Hírlap honlapját*. ISSN 1585-3241. Letöltés dátuma: 2011. október 4., forrás: Index.hu: http://index.hu/kultur/media/2011/03/20/meghekkeltek_a_magyar_hirlap_honlapjat/

[58] **Raphael, J**. (2009. július 8.). *The U.S.-South Korea Cyberattack: How Did It Happen?* ISSN 0737-8939. Letöltés dátuma: 2011. október 4., forrás: PCWorld: http://www.pcworld.com/article/168084/the_ussouth_korea_cyberattack_how_did_it_happen.html

[59] **Estonian Ministry of Defence**. (2011. január 20.). *Government formed Cyber Defence Unit of the Defence League*. Letöltés dátuma: 2011. október 4., forrás: Estonian Ministry of Defence: http://www.mod.gov.ee/en/government-formed-cyber-defence-unit-of-the-defence-league

[60] **Inter allied Confederation of Reserve Officers.** (2011. június). *CIOR Congress highlights „Cyber Warfare”*. Letöltés dátuma: 2011. november 13., forrás: CIOR Newsletter: http://www.cior.net/getattachment/News/Newletter-archive/NEWSLETTER-CIOR-2-2011.pdf.aspx

[61] *2001. évi XCV. törvény a Magyar Honvédség hivatásos és szerződéses állományú katonáinak jogállásáról*.

[62] **Thomas, K**. (2011. február 16.). *Government Employs Hackers in Brave New Scheme*. ISSN 0737-8939. Letöltés dátuma: 2011. október 4., forrás: PCWorld:

http://www.pcworld.com/businesscenter/article/219725/government_employs_hackers_in_brave_new_scheme.html.

[63] **Nemzeti Fejlesztési Minisztérium**. (2010.). *Digitális Megújulás Cselekvési Terv 2010-2014*. Budapest.

[64] **Nemzeti Hálózatbiztonsági Központ**. (2011. március 17.). *COMEX-2010 gyakorlat - kommüniké*. Letöltés dátuma: 2011. október 4., forrás: CERT-Hungary: http://www.cert-hungary.hu/node/127

[65] **Habig, C**. (2011. február 5.). *Cyberspace Presents Complex Global Challenges*. Letöltés dátuma: 2011. október 4., forrás: Munich Security Conference: http://www.securityconference.de/Article-Details.57+M5c1e061d69d.0.html?&L=1

[66] **Krasznay, Cs**. (2009. június). *Hackers in the national cyber security*. Cyter 2009 Conference Prague. 2009. június. ISBN 978-80-01-04372-1

[67] **Herzog, P**. (2006.). *Open-Source Security Testing Methodology Manual 2.2.* Institute for Security and Open Methodologies.

[68] **Scarfone, K**. (2008.). *NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment.* Gaithersburg: National Institute of Standards and Technology.

[69] **Meucci, M**. *OWASP Testing Guide V3.0.* 2008.: Open Web Application Security Project.

[70] **PCI Security Standards Council LLC**. (2010. október). *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures Version 2.0.*

[71] **National Institute of Standards and Technology**. (2010. április 13.). *Federal Information Security Management Act (FISMA) Implementation Project*. Letöltés dátuma: 2011. október 4., forrás: NIST.gov - Computer Security Division - Computer Security Resource Center: http://csrc.nist.gov/groups/SMA/fisma/index.html

[72] **National Institute of Standards and Technology**. (2009.). *NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations.* Gaithersburg: National Institute of Standards and Technology.

[73] **IT Governance Institute**. (2007). *Control Objectives for Information and related Technology (COBIT®) v4.1.* Rolling Meadows: IT Governance Institute.

[74] **Common Criteria Development Board**. (2009. július). *Common Criteria for Information Technology Security Evaluation: Evaluation methodology, Version 3.1, revision 3.*

[75] **The Open Web Application Security Project**. (2009. június). *OWASP Application Security Verification Standard 2009*. (pp.: 4-16.).

[76] **McClure, S., Scambray, J., Kurtz, G.** (2009). *Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition.* McGraw-Hill Osborne Media. ISBN: 0071613749

[77] **Mitnick, K.** (2004.). *2-day Social Engineering Training Course Outline*. Letöltés dátuma: 2011. október 4., forrás: Mitnick Security Consulting, LLC: http://mitnicksecurity.com/media/msc_course_outline.pdf

[78] **Guenther, M**. (2001.). *Social Engineering Security Awareness Series*.

[79] **The Open Web Applications Security Project**. (2008). *OWASP Code Review Guide*.

ÁBRÁK JEGYZÉKE

TÁBLÁZATOK JEGYZÉKE

RÖVIDÍTÉSEK JEGYZÉKE

AES	Advanced Encryption Standard
APEH	Adó- és Pénzügyi Ellenőrzési Hivatal
APT	Advanced Persistent Threat
ASVS	Application Security Verification Standard Project
ÁSzSz	Államigazgatási Számítógépes Szolgálat
BCP	Business Continuity Plan
BKV	Budapesti Közlekedési Vállalat
BM	Belügyminisztérium

CAPTCHA	Completely Automatic Public Turing Test to Tell Computers and Humans Apart
CC	Common Criteria
CEM	Common Evaluation Methodology
CIOR	Inter allied Confederation of Reserve Officers
CISM	Certified Information System Manager
CObIT	Control Objectives for Information and related Technology
COTS	Commercial off-the-shelf
CRG	Code Review Guide
CSRF	Cross-Site Request Forgery
DARPA	Defense Advanced Research Projects Agency
DB	Database
DNS	Domain Name System
DOM	Document Object Model
DRP	Disaster Recovery Plan
EAL	Evaluation Assurance Level
EKG	Elektronikus Kormányzati Gerinchálózat
EKOP	Elektronikus Kormányzat Operatív Programján
EU	Európai Unió
FISMA	Federal Information Security Management Act
FÖMI	Földmérési és Távérzékelési Intézet
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GKM	Gazdasági és Közlekedési Minisztérium
GSM	Global System for Mobile Communications

HM	Honvédelmi Minisztérium
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IBIR	Informatikai Biztonsági Irányítási Rendszer
IBP	Informatikai Biztonsági Politika
IBSZ	Informatikai Biztonsági Szabályzat
IDF	Israel Defense Forces
IDS	Intrusion Detection System
IFSZ	Informatikai Felhasználói Szabályzat
IHM	Informatikai és Hírközlési Minisztérium
IM	Igazságügyi Minisztérium
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Információtechnológia
ITIL	Information Technology Infrastructure Library
KEKKH	Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala
KIB	Közigazgatási Informatikai Bizottság
KR	Központi Rendszer
KSH	Központi Statisztikai Hivatal
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MÁK	Magyar Államkincstár
MEH	Miniszterelnöki Hivatal

MIBÉTS	Magyar Informatikai Biztonsági Értékelés és Tanúsítási Séma
MSN	Microsoft Network
N.SIS	National Schengen Information System
NATO	North Atlantic Treaty Organization
NBF	Nemzeti Biztonsági Felügyelet
NIST	National Institute of Standards & Technology
NKÖM	Nemzeti Kulturális Örökség Minisztérium
OCSP	Online Certificate Status Protocol
OECD	Organisation for Economic Co-operation and Development
OEP	Országos Egészségpénztár
ORM	Object Relational Mapping
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
PM	Pénzügyminisztérium
RACI	Responsible, Accountable, Consulted, Informed
RIA	Rich Internet Application
RSA	Rivest, Shamir, & Adleman
RSS	Rich Site Summary
SCADA	Supervisory Control and Data Acquisition
SE	Social Engineering
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture

SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSI	Server-side Include
SSL	Secure Sockets Layer
SZÜV	Számítástechnikai és Ügyvitel-szervezési Vállalat
TCP/IP	Transmission Control Protocol/Internet Protocol
TG	Testing Guide
TLS	Transport Layer Security
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WSDL	Web Service Definition Language
XML	Extensible Markup Language
XML-RPC	eXtensible Markup Language - Remote Procedure Call protocol
XSS	Cross-Site Scripting
XST	XML streaming transformer

1. MELLÉKLET

	OE.FAILSAFE	OE.OPERATION	OE.MALWARE	OE.BOUNDARY_PROTECTION	OE.DLP	OE.SECURE_CONFIG	OE.SSL	OE.KEY	OE.PHYSICAL	OE.BACKUP	OE.SESSION	OE.LOG_MANAGEMENT
A.CERTIFIED						X						
A.FAILSAFE	X											
A.OPERATION		X										
A.PERSONNEL		X										
A.PHYSICAL									X			
A.SEGMENTATION				X								
P.EKG		X	X	X			X	X	X	X		X
T.AVAILABILITY	X											
T.CLIENT_SIDE			X	X								
T.CSRF				X								
T.DATA_LEAKAGE			X	X	X	X						
T.DIRECT_REFERENCE							X					
T.INFO_LEAKAGE						X						
T.INJECTION				X								
T.INSECURE_CLIENT			X	X								
T.INSECURE_COMMUNICATION							X					
T.PROTOCOL				X								
T.REDIRECT						X						
T.SERVER_S				X		X						

IDE										
T.SESSION				X				X		
T.STRUCTURE			X							
T.URL				X						
T.VIRTUALIZATION				X						
T.XSS			X							

4. táblázat: Fenyegetésekre, feltételezésekre és szabályzatokra vonatkozó környezeti biztonsági célok

	O.INPUT_VALIDATION	O.STRONG_AUTHENTICATION	O.LEAST_PRIVILAGE	O.IDENTITY	O.AUTHENTICATION	O.ROLE	O.FOUR_EYE	O.RBAC	O.LOG	O.ENCRYPT
P.EKG				X	X			X	X	X
T.CRYPTO										X
T.CSRF	X									
T.DATA_LEAKAGE			X		X			X		
T.INJECTION	X									
T.INSECURE_COMMUNICATION										X
T.SOCIAL_ENGINEERING		X								
T.STRUCTURE	X									
T.UNDETECTED_INCIDENT									X	
T.USER_ERROR			X	X	X	X	X			
T.XSS	X									

5. táblázat: Fenyegetésekre és szabályzatokra vonatkozó biztonsági célok

2. MELLÉKLET

	O.INPUT_VALIDATION	O.STRONG_AUTHENTICATION	O.LEAST_PRIVILAGE	O.IDENTITY	O.AUTHENTICATION	O.ROLE	O.FOUR_EYE	O.RBAC	O.LOG	O.ENCRYPT
FAU_GEN.1									X	
FCS_CKM.4										X
FCS_COP.1										X
FDP_ACC.1			X				X	X		
FDP_ACC.2			X				X	X		
FDP_ACF.1			X				X	X		
FDP_ETC.2			X					X		
FDP_ITC.1	X									
FIA_AFL.1					X					
FIA_ATD.1					X					
FIA_SOS.1					X					
FIA_SOS.2					X					
FIA_UAU.1					X					
FIA_UAU.5		X								
FIA_UAU.7			X							
FIA_UID.1				X						
FMT_MOF.1			X							
FMT_MSA.1			X							
FMT_MSA.2			X							
FMT_MSA.3			X							
FMT_MTD.1			X							
FMT_SMF.1			X							
FMT_SMR.1						X				
FMT_SMR.2						X				
FPT_STM.1									X	

6. táblázat: Biztonsági célokat megvalósító biztonsági célok

4. FEJEZET	Értekezés			KIB 28.		
	Alap	Fokozott	Kiemelt	Alacsony	Fokozott	Kiemelt
FAU_GEN.1	X	X	X	X	X	X
FCS_CKM.4	X	X	X		X	X
FCS_COP.1	X	X	X	X	X	X
FDP_ACC.1	X	X		X		
FDP_ACC.2			X		X	X
FDP_ACF.1	X	X	X	X	X	X
FDP_ETC.1	X	X			X	X
FDP_ETC.2			X			
FDP_ITC.1	X	X	X		X	X
FIA_AFL.1	X	X	X	X	X	X
FIA_ATD.1	X	X	X	X	X	X
FIA_SOS.1	X	X	X	X	X	X
FIA_SOS.2	X	X	X	X	X	X
FIA_UAU.1	X			X	X	X
FIA_UAU.2		X	X			
FIA_UAU.5	X	X	X		X	X
FIA_UAU.7	X	X	X	X	X	X
FIA_UID.1	X			X	X	X
FIA_UID.2		X	X			
FMT_MOF.1	X	X	X	X	X	X
FMT_MSA.1	X	X	X	X	X	X
FMT_MSA.2	X	X	X		X	X
FMT_MSA.3	X	X	X	X	X	X
FMT_MTD.1	X	X	X	X	X	X
FMT_SMF.1	X	X	X	X	X	X
FMT_SMR.2	X	X	X		X	X
FPT_STM.1	X	X	X	X	X	X

7. táblázat: Funkcionális követelmények az értekezésben és a KIB 28. ajánlásban

3. MELLÉKLET

	Biztonsági intézkedés neve	Alacsony	Fokozott	Kiemelt
		biztonsági osztály alapkonfigurációja		
Konfiguráció kezelés				
KK-1	Konfiguráció kezelési szabályzat és eljárásrend	KK-1	KK-1	KK-1
KK-2	Alap konfiguráció	KK-2	KK-2	KK-2
KK-3	Konfigurációváltozások	--	KK-3	KK-3
KK-4	A konfigurációváltozások felügyelete	--	KK-4	KK-4
KK-5	A változtatásokra vonatkozó hozzáférés korlátozások	--	KK-5	KK-5
KK-6	Konfigurációs beállítások	KK-6	KK-6	KK-6
KK-7	Legszűkebb funkcionalitás	--	KK-7	KK-7
KK-8	Informatikai rendszer komponens leltár	KK-8	KK-8	KK-8
Rendszer és információ sértetlenség				
RS-1	Rendszer és információ sértetlenségre vonatkozó szabályzat és eljárásrend	RS-1	RS-1	RS-1
RS-2	Hibajavítás	RS-2	RS-2	RS-2
RS-3	Rosszindulatú kódok elleni védelem	RS-3	RS-3	RS-3
RS-4	Behatolás észlelési eszközök és technikák	--	RS-4	RS-4
RS-5	Biztonsági riasztások és tájékoztatások	RS-5	RS-5	RS-5
RS-6	A biztonsági funkcionalitás ellenőrzése	--	--	RS-6
RS-7	Szoftver és információ sértetlenség	--	--	RS-7
RS-8	Kéretlen levélszemét (spam) és kémszoftverek (spyware) elleni védelem	--	RS-8	RS-8
RS-9	A bemeneti információra vonatkozó korlátozások	--	RS-9	RS-9
RS-10	A bemeneti információ pontossága, teljessége és érvényessége	--	--	--
RS-11	Hibakezelés	--	--	--
RS-12	A kimeneti információ kezelése és megőrzése	--	--	--
Azonosítás és hitelesítés				
AH-1	Azonosítási és hitelesítési szabályzat és eljárásrend	AH-1	AH-1	AH-1
AH-2	Felhasználó azonosítása és hitelesítése	AH-2	AH-2	AH-2
AH-3	Eszközök azonosítása és hitelesítése	--	AH-3	AH-3
AH-4	Azonosító kezelés	AH-4	AH-4	AH-4
AH-5	A hitelesítésre szolgáló eszközök kezelése	AH-5	AH-5	AH-5
AH-6	A hitelesítésre szolgáló eszköz visszacsatolása	AH-6	AH-6	AH-6
AH-7	Hitelesítés kriptográfiai modul esetén	AH-7	AH-7	AH-7

Hozzáférés ellenőrzése				
HE-1	Hozzáférés ellenőrzési szabályzat és eljárásrend	HE-1	HE-1	HE-1
HE-2	Felhasználói fiókok kezelése	HE-2	HE-2	HE-2
HE-3	Hozzáférés ellenőrzés érvényre juttatása	HE-3	HE-3	HE-3
HE-4	Információ áramlás ellenőrzés érvényre juttatása	--	HE-4	HE-4
HE-5	A felelősségek szétválasztása	HE-5	HE-5	HE-5
HE-6	Legkisebb jogosultság	--	HE-6	HE-6
HE-7	Sikertelen bejelentkezési kísérletek	HE-7	HE-7	HE-7
HE-8	A rendszerhasználat jelzése	HE-8	HE-8	HE-8
HE-9	Értesítés előző bejelentkezésről	--	--	--
HE-10	Egyidejű munkaszakasz kezelés	--	--	--
HE-11	A munkaszakasz zárolása	--	HE-11	HE-11
HE-12	A munkaszakasz lezárása	HE-12	--	--
HE-13	Felügyelet és felülvizsgálat — hozzáférés ellenőrzés	HE-13	HE-13	HE-13
HE-14	Azonosítás és hitelesítés nélkül engedélyezett tevékenységek	HE-14	HE-14	HE-14
HE-15	Automatikus jelölés	--	--	--
HE-16	Automatikus címkézés	--	--	--
HE-17	Távoli hozzáférés ellenőrzése	HE-17	--	--
HE-18	A vezeték nélküli hozzáférésre vonatkozó korlátozások	HE-18	HE-18	--
HE-19	A hordozható és mobil eszközök hozzáférés ellenőrzése	HE-19	--	--
HE-20	Külső informatikai rendszerek használata	HE-20	HE-20	HE-20
Naplózás és elszámoltathatóság				
NA-1	Naplózási és elszámoltathatósági szabályzat és eljárásrend	NA-1	NA-1	NA-1
NA-2	Naplózandó események	NA-2	NA-2	NA-2
NA-3	A naplóbejegyzések tartalma	NA-3	NA-3	NA-3
NA-4	Napló tárkapacitás	NA-4	NA-4	NA-4
NA-5	Naplózási hiba kezelése	NA-5	NA-5	NA-5
NA-6	Napló figyelése, vizsgálata és jelentések készítése	--	NA-6	NA-6
NA-7	Naplócsökkentés, naplóriport készítés	--	NA-7	NA-7

NA-8	Időbélyegek	NA-8	NA-8	NA-8
NA-9	A napló információk védelme	NA-9	NA-9	NA-9
NA-10	Letagadhatatlanság	--	--	--
NA-11	A naplóbejegyzések megőrzése	NA-11	NA-11	NA-11
Rendszer és kommunikáció védelem				
RV-1	Rendszer és kommunikáció védelmi szabályzat és eljárásrend	RV-1	RV-1	RV-1
RV-2	Alkalmazás szétválasztás	--	RV-2	RV-2
RV-3	Biztonsági funkciók elkülönítése	--	--	RV-3
RV-4	Információ maradványok	--	--	--
RV-5	Szolgáltatás megtagadás elleni védelem	--	--	--
RV-6	Erőforrás prioritás	--	--	--
RV-7	A határok védelme	RV-7	RV-7	RV-7
RV-8	Az adatátvitel sértetlensége	RV-8	--	--
RV-9	Az adatátvitel bizalmassága	RV-9	--	--
RV-10	A hálózati kapcsolat megszakítása	--	--	--
RV-11	Megbízható útvonal	--	--	--
RV-12	Kriptográfiai kulcs előállítása és kezelése	RV-12	RV-12	RV-12
RV-13	Jóváhagyott kriptográfia alkalmazása	RV-13	RV-13	RV-13
RV-14	Sértetlenség védelem nyilvános hozzáférés esetén	--	--	--
RV-15	Telekommunikációs szolgáltatások korlátozása	RV-15	RV-15	RV-15
RV-16	Biztonsági paraméterek továbbítása	--	--	--
RV-17	Nyilvános kulcsú infrastruktúra tanúsítványok	--	RV-17	RV-17
RV-18	Mobil kód korlátozása	--	RV-18	RV-18
RV-19	Interneten Keresztüli Hangátvitel (VoIP)	--	RV-19	RV-19
RV-20	Biztonságos név/cím feloldó szolgáltatások (Hiteles forrás)	--	--	--
RV-21	Biztonságos név/cím feloldó szolgáltatás (rekurzív vagy gyorsítótárat használó feloldás)	--	--	--
RV-22	Architektúra és tartalékok név/cím feloldási szolgáltatás esetén	--	--	--
RV-23	Munkaszakasz hitelessége	--	--	--

8. táblázat: Fejlesztői környezettel szembeni biztonsági követelmények különböző biztonsági szinteken