ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
HADTUDOMÁNYI KAR
KATONAI MŰSZAKI DOKTORI ISKOLA

KRASZNAY CSABA

A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSI ALKALMAZÁSOK INFORMÁCIÓBIZTONSÁGI MEGOLDÁSAI

CÍMŰ DOKTORI (PHD) ÉRTEKEZÉSÉNEK
SZERZŐI ISMERTETÉSE

TUDOMÁNYOS TÉMAVEZETŐ:
PROF. DR. KOVÁCS LÁSZLÓ MK. ALEZREDES

BUDAPEST, 2011.

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 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[1]) ajánlás alapján olyan **Védelmi Profil eszköztár kidolgozása**, mely a Magyar Köztársaság elektronikus közigazgatási szolgáltatásaiban 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-

[1] 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.

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.

AZ ELVÉGZETT VIZSGÁLAT TÖMÖR LEÍRÁSA FEJEZETENKÉNT

Az **első 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**.

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.

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.

A **harmadik 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.

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

SZAKMAI ÖNÉLETRAJZ

Név: **Krasznay Csaba**
Születési év: **1979. október 11.**
Születési hely: **Budapest**
Telefon: **+36-30-2020290**
E-mail cím: **csaba@krasznay.hu**

Iskolai végzettség

2008-2011: Zrínyi Miklós Nemzetvédelmi Egyetem, PhD tanulmányok a Katonai Műszaki Doktori Iskola Védelmi Elektronika tudományszakán. Kutatási téma: Az elektronikus közigazgatási rendszerek biztonsága

1998-2003: Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar villamosmérnöki szak, Számítógépek rendszer és alkalmazástechnikája főszakirány, Távközlésmenedzsment mellékszakirány. Diplomamunka témája: biztonságos elektronikus kereskedelmi rendszer PKI alapon.

1994-1998: Táncsics Mihály Gimnázium

Szaktanfolyamok / szakvizsgák

2011: BCS
ITIL Version 3 Intermediate Certificate Service Offerings & Agreements minősítés

2010: Examination Institute for Information Science
ITIL V3 Foundation Certificate in IT Service Management minősítés

2010: PCI Security Standards Council
PCI DSS Awarness Training

2008: Kormányzati Személyügyi Szolgáltató és Közigazgatási Képzési Központ
Közigazgatási oktató

2008: Nemzeti Hírközlési Hatóság
Elektronikus aláírással kapcsolatos szolgáltatási szakértő minősítés

2008: EC-Council
Certified Ethical Hacker minősítés

2007: Hunguard Kft.
Common Criteria szakértő minősítés

2006: International Information Systems Security Certification Consortium $(ISC)^2$
Certified Information Systems Security Professional (CISSP) minősítés

2006: Information Systems Audit and Control Association
Certified Information Security Manager (CISM) minősítés

2005: Information Systems Audit and Control Association
Certified Information Systems Auditor (CISA) minősítés

2005: Informin Kft. ISO 9001 és BS 7799 belső auditor

2001: BME Informatikai Központ
E-business megoldástervező: a tanfolyam az IBM e-business keretrendszere által felölelt technológiák és eszközök gyakorlati alkalmazására koncentrál. Megismerteti az Internetes alaptechnológiákat és hozzájuk kapcsolódó IBM-es eszközöket, ezek együttes alkalmazását komplex e-business feladatok megoldására.

2001: BME Informatikai Központ
E-business alapok: bevezető tanfolyam, amely röviden tárgyalja az Internet felépítését és jelentőségét az üzleti világ szempontjából, valamint egyszerűsített formában megismertet az Internet és az e-business működésével.

Egyéb ösztöndíjak / díjak / tagságok

2011: Informatikai Biztonság Napja: Az év útmutató biztonsági szakembere díj

2010: Magyary Zoltán E-közigazgatástudományi Egyesület: elnökségi tag

2006: Information Systems Audit and Control Association (ISACA): az Etikai Bizottság tagja

2004: Magyar Elektronikus Aláírás Szövetség (MELASZ): tag (korábban elnökségi tag)

2001: Tudományos Diákköri Konferencia I. helyezés a Szociológia és kommunikáció szekcióban a Digitális aláírás elterjedésének lehetőségei és korlátai című dolgozattal

Gyakorlati tapasztalatok

2009-: HP Magyarország
informatikai biztonsági tanácsadó
informatikai biztonsággal kapcsolatos projektekben való részvétel

2007-2009: Kancellár.hu Zrt.
informatikai biztonsági tanácsadó
informatikai biztonsággal kapcsolatos projektekben való részvétel (tanácsadás, oktatás, sérülékenységelemzés)

2003-2006: BME Informatikai Központ
tudományos munkatárs
informatikai biztonsággal kapcsolatos projektekben való részvétel (elektronikus aláírás, vírusok, Common Criteria, CERT, PKI, e-kormányzat, informatikai biztonság)

2003: E-group Hungary Rt.
informatikai biztonsági szaktanácsadó
a Signed Document eXpert elektronikus aláíró és hitelesítő szoftver felkészítése Common Criteria EAL 3 szintű minősítésére

2002-2003: Prohardver Kft.
informatikai szakértő
a cég hálózati és biztonsági infrastruktúrájának kialakítása és felügyelete

2002: BME Informatikai Központ
szakértő
az elektronikus aláírással kapcsolatos kutatásokban való részvétel

2001: Miniszterelnöki Hivatal Informatikai Kormánybiztosság

megfigyelő
részvétel a Kormányzati Hitelesítő Központ koncepcióját kidolgozó szakbizottságban

2001: BME Informatikai Központ - Hírközlési Felügyelet
tesztelő
részvétel a Minősített hitelesítés-szolgáltatók minősítési eljárási módszertanának kidolgozásában

2001: BME Híradástechnikai Tanszék Elektronikus Adatbiztonság Labor
hallgató
részvétel az E-group Hungary Rt. által támogatott BME E-biz Labjának munkájában

1998-2001: Medincorp Kft.
web fejlesztő
a www.informed.hu, Magyarország legnagyobb orvosi szakportáljának fejlesztésében való részvétel

1997-2000: Carnett Bt.
kereskedő
új számítógépek összeszerelése és értékesítése, hibás gépek eseti szervízelése

Nyelvtudás

felsőfokú szakmai angol nyelvismeret (középfokú C nyelvvizsga)
középfokú spanyol nyelvismeret (középfokú B nyelvvizsga, alapfokú C nyelvvizsga)

2011. november 14., Budapest

Krasznay Csaba