ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM
Doktori Tanácsa

PÓSERNÉ OLÁH VALÉRIA

Közigazgatási informatikai rendszerek informatikai biztonsági kérdései

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Budapest
2011.

ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

PÓSERNÉ OLÁH VALÉRIA

Közigazgatási informatikai rendszerek informatikai biztonsági kérdései

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Témavezető:

Prof. dr. Haig Zsolt, mérnök ezredes, PhD

Budapest
2011.

A tudományos probléma megfogalmazása

Mivel az informatikai rendszerek az élet minden területén jelen vannak, így a közigazgatás feladatköreiben, szolgáltatásaiban is nagyobb teret hódítanak maguknak. A személyi számítógépek és a belőlük alkotott kisebb-nagyobb hálózatok elterjedésének, az első vírusok megjelenésének, a számítástechnika felgyorsult fejlődésének köszönhetően az informatikai biztonság kérdése is egyre bonyolultabb lett. NATO és EU tagságunk is újabb információbiztonsági követelményeket támaszt hazánk informatikai rendszerei, köztük a közigazgatás rendszereivel szemben.

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

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

A közigazgatási informatikai rendszereket fenyegető veszélyek feltárása, elemzése, valamint a korszerű védelmi módszerek alkalmazhatóságának vizsgálata tudományos kutatást igényel.

Kutatási célok

Munkám során az alábbi kutatási célokat tűztem ki:

1. Megvizsgálni a közigazgatási szervek informatikai rendszereit, a rendszer modellezése alapján bemutatni és elemezni azok működési folyamatait, az alkalmazott informatikai

biztonsági szabályzókat és a működtető személyzet szemléletmódját; feltárni azok hiányosságait és meghatározni fejlesztésük lehetséges irányait, követelményeit.

2. Elemezni a közigazgatási informatikai rendszerek elleni lehetséges támadókat, a támadások fajtáit és ez alapján rendszerezni és csoportosítani a veszélyforrásokat.
3. Az informatikai biztonság szempontjából elemezni, értékelni és összehasonlítani a közigazgatási informatikai rendszerekben leggyakrabban alkalmazott nyílt- és zárt forráskódú operációs rendszereket és javaslatokat tenni további alkalmazhatóságukra vonatkozóan.
4. Kockázatelemzési modellre alapozva megvizsgálni a közigazgatási informatikai rendszerekben alkalmazható korszerű védelmi megoldásokat, azok működési elveit és javaslatokat tenni alkalmazhatóságukra a közigazgatási informatikai rendszerek informatikai biztonságának növelése érdekében.

Az alkalmazott kutatási módszerek

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

Az értekezés felépítése

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

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

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

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

Az értekezés végén összegeztem következtetéseimet, főbb megállapításaimat, megfogalmaztam az általam elért új tudományos eredményeket és ajánlásokat fogalmaztam meg a további felhasználásra vonatkozóan.

Összegzett következtetések

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

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

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

Az e-közigazgatási keretrendszer informatikai biztonsági követelményrendszerét tanulmányozva **elemeztem** a szervezeti informatikai biztonság megteremtésének, fenntartásának alapvető feltételeit és **megfogalmaztam az informatikai biztonsági stratégia célkitűzéseit, követelményeit,** bemutattam egy **lehetséges felépítését**, a célkitűzések alapján végrehajtandó legfontosabb **feladatokat,** azok rendszeres felülvizsgálatának kérdéseit.

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

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

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

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

Ezt követően egy aktuális kérdésre kívántam választ adni, hogy nyílt vagy zárt forráskódú operációs rendszerek használata a célszerűbb a közigazgatási informatikai rendszerek számítógépein. Ezért **teszteltem, megvizsgáltam és összehasonlítottam** a közigazgatási informatikai rendszerekben **leggyakrabban alkalmazott szerver operációs rendszerek több**

szolgáltatását a biztonságos alkalmazás szempontjából, és **megállapítottam**, hogy **a nyílt forráskódú operációs rendszerek alkalmazása** a szoftverek beszerzésének költségei terén ugyan **költségcsökkentő tényezőként szolgálhatna**, képességeit tekintve nem rosszabb, mint a zárt forráskódú operációs rendszerek biztonsági szolgáltatásai. Azonban a biztonságos működtetéshez szükséges **szaktudás hiányzik**, problémát jelentene a közigazgatás **saját fejlesztésű**, tipikusan Microsoft alapú alkalmazásainak átállítása és ezzel **jelentős sérülékenység kerülne a rendszerbe**, azért is, mert **sokkal kedveltebb célpontjai a támadásoknak**.

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

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

Elvégeztem egy, az értekezés korábbi részeiben feltárt fenyegetésekre és védelmi hiányosságokra koncentrálódó célzott, részleges **kockázatelemzést és hatáselemzést**, melynek **eredményei alapján javaslatot tettem a közigazgatás minden szervezetének** informatikai rendszereiben történő következő **védelmi megoldások bevezetésére, erősítésére:**

- **központilag vezérelt, integrált végpontvédelmi megoldások** bevezetése valamint központilag vezérelt **szoftver frissítési architektúra kialakítása** a hibás vagy manipulált alkalmazói, illetve rendszerprogramok, valamint a távoli munkavégzés során a távoli gépről rendszerbe kerülő sérülékenységek által okozott kockázatok elviselhető szintre redukálására;
- **Screened subnet tűzfal architektúra** kialakítása, **alkalmazás szintű tűzfallal történő üzemeltetése** a hálózatba való jogosulatlan bejutás kockázatának csökkente érdekében;
- **behatolás érzékelő, illetve -megelőző eszközök** alkalmazása a belső hálózaton történő támadások, illetve illetéktelen hozzáférési kísérletek érzékelésére és elhárítására;

- **integrált központi felhasználó- és hozzáférés-menedzsment rendszerek** bevezetése az illetéktelen adathozzáférés kockázatának csökkentése érdekében;
- **titkosítás** és **automatizált mentési rendszer** bevezetése a nyílt csatornákon történő kommunikáció, a levélforgalom, valamint az adathordozók elvesztése, sérülése, vagy eltulajdonítása kapcsán keletkező kockázatok elfogadható szintre történő csökkentésére;
- **napló- vagy esemény-feldolgozó rendszerek alkalmazása,** továbbá **a felügyelet ellátására külön munkakör létrehozása** a rendszer problémáinak, illetve az esetleges illetéktelen behatolás vagy kísérlet felderítésére.

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

Új tudományos eredmények

1. **Megalkotva** a közigazgatási informatikai rendszerek **funkcionális és strukturális modelljét**, és **elemezve** a működési folyamatait, biztonsági szabályzóit, **feltártam azok hiányosságait, felvázoltam a fejlesztés irányait, és meghatároztam** az e szervezetekben kialakítandó **informatikai biztonsági stratégiával szemben támasztott követelményeket, a stratégia lehetséges felépítését** és a hozzá kapcsolódó **informatikai biztonsági politikában foglalt feladatokat**.
2. A közigazgatási informatikai rendszerek **strukturális modelljére alapozva elemeztem** az azok elleni támadók körét és a támadások fajtáit, majd ennek eredményeként **megalkottam az e rendszerek elleni veszélyforrások (támadások) újszerű csoportosítását**.
3. A támadók körének és a támadási fajtáknak a **vizsgálata,** valamint a támadási célpontok arányának **statisztikai elemzése**, továbbá **saját tesztelési eredményeim alapján összehasonlítottam** a közigazgatási informatikai rendszerekben leggyakrabban alkalmazott operációs rendszereket a biztonságos alkalmazás szempontjából, és **igazoltam, hogy a zárt forráskódú operációs rendszerek további alkalmazása nem hátrányosabb, mint áttérni a** lényegesen nagyobb mértékben célpontnak számító **nyílt forráskódú operációs rendszerekre**.

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

Ajánlások

1. Javaslom a doktori (PhD) értekezésem közigazgatási szervezetek informatikai rendszerei biztonságának szabályozási kérdéseivel foglalkozó fejezetének felhasználását egy új, a közigazgatási informatikai rendszerek magasabb biztonsági szintre emelését megcélzó törvény megalkotásában, illetőleg a benne foglalt ajánlások figyelembevételét az egyes szervezetek informatikai biztonsági stratégiájának kialakítása során.
2. Javaslom az értekezésem felhasználását az államigazgatás informatikai irányultságú területére szakembereket képző felsőoktatási intézmények alap, mester és doktori képzésében tananyagként.
3. Javaslom továbbá az informatikai rendszerek elleni támadási formákról, valamint az alkalmazható védelmi megoldásokról szóló fejezeteit felhasználni az informatikai biztonság irányultságú alap, mester és doktori képzésben tananyagként.

Publikációs jegyzék

Lektorált folyóiratban megjelent cikkek

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

Konferencia kiadványban megjelent előadások

1. V. O. Póserné: *Comparing the webservers of the opensource and the closed source operation systems*, Proc of the 5th International Symposium on Applied Computational Intelligence and Informatics, Timisoara, Romania, IEEE Catalog Number CFP0945C-CDR, ISBN 978-1-4244-4478-6, Library of Congress 2009903350, 2009, pp. 169-172.
2. Póserné O. V.: *Az Internet adta hadászati lehetőségek és veszélyek*, Robothadviselés 4.

nemzetközi tudományos konferencia kiadványa, Budapest, 2005, pp. 136-148., ISBN 963 7060 08 1

3. Póserné O. V.: *Informatikai biztonság gyakorlatban*, Matematika-, fizika, számítástechnika főiskolai oktatók XXX. konferencia publikációs kiadvány-CD, Pécs, 2006, p. 5, ISBN-13: 978-963-7298-12-7
4. Póserné O. V. - Katona K. - Szénási S.: *A Delphi haladó eszközeinek alkalmazása*, Matematika-, fizika, számítástechnika főiskolai oktatók XXX. konferencia publikációs kiadvány-CD, Pécs, 2006, p. 6, ISBN-13: 978-963-7298-12-7
5. Póserné O. V.: *Számítógép-hálózati támadások*, Hadmérnök, Robothadviselés 6. tudományos szakmai konferencia Különszám, Budapest, 2006, p. 9, ISSN 1788-1919
6. Póserné O. V.: *A távoli munkavégzés biztonsági kérdései*, Hadmérnök, Robothadviselés 7. tudományos szakmai konferencia Különszám, Budapest, 2007, p. 9, ISSN 1788-1919
7. Póserné O. V.: *A kapcsolók hatása a hálózati biztonságra*, Informatika Korszerű Technikái Konferencia 2008, Dunaújváros, 2008, pp. 102-109., ISBN 978-963-87780-2-4
8. Póserné O. V. – Schubert T.: *Informatikai biztonság – szakirányú képzés a Budapesti Műszaki Főiskolán*, Informatika a felsőoktatásban 2008 konferencia publikációs kiadvány-CD, Debrecen, 2008, p. 8, ISBN 978-963-473-129-0
9. Póserné O. V.: *A magyar közigazgatás az informatikai biztonság szemszögéből*, Bolyai Szemle, 2008. XVII. évf. 4. sz., A Robothadviselés 8. Tudományos konferencia előadásainak szerkesztett változata, Budapest, 2008, pp. 157-166., ISSN 1416-1443

Szakmai-tudományos életrajz

Személyes adatok:

Név: Póserné Oláh Valéria
Szül. idő: 1962.03.20.
Lakcím: 2030 Érd, Takács u. 5.
Telefon: +36-70-604-3007
E-mail: poserne.valeria@nik.uni-obuda.hu

Végzettség:

Zrínyi Miklós Nemzetvédelmi Egyetem, Katonai Műszaki Doktori Iskola, levelező PhD hallgató
1991 - 1994: Kossuth Lajos Tudományegyetem TTK, Informatika tanár szak
1982 - 1985: Kossuth Lajos Tudományegyetem TTK, Programozó-matematikus szak

Nyelvismeret:

Angol: középfokú komplex szakmai nyelvvizsga
Orosz: általános C típusú alapfokkal egyenértékű

Informatikai ismeretek:

Programnyelvek: C#, Delphi, Pascal, HTML, Basic, PL1
Operációs rendszerek: Windows Server 2003/2008, Novell, Linux, Windows 9x/2000/XP/Vista/ Windows 7, Windows NT Workstation, MS DOS
Egyéb: IBM Tivoli Identity Manager, IBM Tivoli Directory Integrator, HP WebInspect, IBM Rational AppScan, PGP, OpenSSH, Access, Word, Excel, PowerPoint

Munkahelyek:

2004 - Óbudai Egyetem (2010-ig BMF), Budapest, adjunktus
2007 - 2010 Dunaújvárosi Főiskola, Dunaújváros, adjunktus
1995 - 2004 Szent István Egyetem VTI, Budapest, egyetemi tanársegéd, laboratórium vezető

1987 - 1995 Csiha Győző Szakközépiskola és Szakmunkásképző Intézet, Hajdúnánás, számítástechnika-matematika tanár

1985 - 1987 Üvegipari Művek, Orosháza, számítástechnikai programozó

Tudományos közéleti tevékenység

2008 - NJSZT tag

Budapest, 2011. június 22.

Póserné Oláh Valéria