HADMÉRNÖK

IV. Évfolyam 1. szám - 2009. március

Krasznay Csaba
Zrínyi Miklós Nemzetvédelmi Egyetem
csaba@krasznay.hu

A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁS BIZTONSÁGÁNAK ELEMZÉSE ÉS TOVÁBBLÉPÉSI LEHETŐSÉGEI

Absztrakt

A 2009-2010-es évek jelentős fejlődést hozhatnak a magyar e-közigazgatásban. Bár az informatikai biztonsági szempontok kiemelt szerepet képviselnek, jelenleg nincsenek egységes elvek és gyakorlatok ebben a körben a megfelelően biztonságos rendszerek fejlesztéséhez. A tanulmány áttekinti a magyar elektronikus közigazgatás fejlesztési irányait, majd bemutatja az ebből adódó várható műszaki kockázatokat. Mindezt a Common Criteria szabvány formalizmusával teszi, tekintettel a kormányzati elvárásokra. Ezután bemutatja azt az ajánlásrendszert, mely a tervezés és kivitelezés során felhasználható, és a japán példa elemzésével az ideális fejlődési irányt is felvázolja. Végül egy biztonsági teszt segítségével bemutatja a közigazgatási rendszerek általános biztonsági állapotát, és javaslatot tesz a tudományos alapokon nyugvó előrelépésre.

In 2009 and 2010 a huge development is expected in the Hungarian e-government system. Although information security aspects have an emphasized role solid principals and practices hasn't been identified for the developments. This study reviews the design directions of the Hungarian e-government and presents some predictable IT security risks. This is done by the formalism of Common Criteria standard considering the governmental expectations. In the following chapter the author studies the current recommendations which are useable during the design and implementation and then outlines the ideal direction with the analysis of the Japanese example. Last it represents the overall security situation of the Hungarian e-government system and proposes some scientific topics for the improvement.

Kulcsszavak: *elektronikus közigazgatás, Common Criteria, biztonság, fenyegetések ~ e-government, Common Criteria, security, threats*

Bevezetés

A magyar közigazgatásban az informatika évtizedek óta jelen van, és néhány központi intézménynél található eszközparkot számos hazánkban működő multinacionális cég is megirigyelhetné. Ez a több évtizedes fejlődés azonban csak az elmúlt években jutott el arra a szintre, hogy ezeket a rendszereket a lehető legjobban összehangolják annak érdekében, hogy létrejöhessen a valódi szolgáltató állam, a Magyar Köztársaság állampolgárainak és üzleti szereplőinek lehető legjobb kiszolgálására. A korábbi szigetszerű alkalmazásoktól való elszakadás első jelentős lépése a kormányzati portálon 2005. április 1-én indult Ügyfélkapu volt, mely az okmányirodai szolgáltatások bizonyos fokú elektronizálásával először tette lehetővé, hogy az állampolgárok interneten keresztül intézzék hivatalos ügyeiket. Az Ügyfélkapu indulása eltelt közel négy évben az Ügyfélkapu és más e-közigazgatási szolgáltatások felhasználói tábora több százezresre duzzadt, mely Magyarország lakosságához képest még nem nagy szám, de mindenképpen biztató.

Ezen a területen az igazán jelentős fejlődés azonban a 2009-2010-es években várható, ugyanis az Európai Unió több tízmilliárd forintnyi fejlesztési keretet ad az államigazgatás elektronizálására az Elektronikus Közigazgatás Operatív Program (EKOP) keretein belül. Tekintettel arra, hogy ezek a fejlesztések minimum egy évtizeden keresztül meghatározzák a Magyar Köztársaság központi és önkormányzati informatikai rendszereit és fejlesztési irányait, elengedhetetlenül fontos, hogy ezeknek az alkalmazásoknak szerves része legyen az információbiztonság is. Ennek egyrészt anyagi okai vannak, hiszen a biztonságot jelentő sértetlenség, bizalmasság és rendelkezésre állás megvalósítása akkor a legolcsóbb és leghatékonyabb, ha azt már a tervezési fázisban is figyelembe veszik, másrészt nagyon fontos nemzetbiztonsági érdekek is fűződnek ehhez. Az új generációs hadviselés, melynek eklatáns példáját láthattuk akár az orosz-észt, orosz-grúz vagy éppen az izraeli-palesztin vitáknál-háborúknál, az első lépések egyikeként az érintett országok kormányzati információs rendszereinek kiiktatását tartalmazza. A tervezett fejlesztések eredményeképp Magyarország közigazgatási infrastruktúrája átléphet a XXI. századba, de ezáltal sokkal inkább ki lesz téve a XXI. század kihívásainak is.

Az e-közigazgatás kerete

A magyar elektronikus közigazgatás előtt álló feladatokat az E-közigazgatás Program 2008-2010 című tanulmány részletezi (Miniszterelnöki Hivatal, 2008). Ez hét átfogó programot azonosít, melyek együttesen alkotják az e-közigazgatás keretét. A hét program a következő:

- Interoperabilitási Átfogó Program
- Ügyfélközpontú szolgáltatások átfogó program
- Online infrastruktúra átfogó program
- Integrált ügyfélszolgálat átfogó program
- Integrált kormányzati funkciók átfogó program
- Megosztott e-közigazgatási szolgáltatások átfogó program
- Tudásmenedzsment átfogó program.

Az információbiztonságot alapjaiban érintő, ezért talán a legfontosabb program az Interoperabilitási **Átfogó Program**, melyre összesen 3397 millió forint áll rendelkezésre. A program keretében először ki kell dolgozni az E-közigazgatási Keretrendszert, mely az oly fontos elveket rögzíti, mint az alkalmazásfüggő IT-biztonsági követelmények, szabványok, vagy éppen az alkalmazásfejlesztési keretrendszerek. A Keretrendszer kialakítására 2004 óta vannak törekvések, számos szabvány, ajánlás készült el az elmúlt években, ám ezek bevezetése, és különösen felhasználása nem az elvárható mértékben történt meg. Figyelemre méltó, hogy az EKOP keretében a további alpontokban részletezett fejlesztések egy része úgy

indult meg, hogy a Keretrendszer elemei nem ismertek, így továbbra is komoly kockázata van a szigetrendszerek kialakulásának.

A program második eleme a Nyilvántartások interoperabilitásának előmozdítása, mely leszögezi, hogy a cél biztonságos web-szolgáltatás alapú működés, azaz egy technológiai irányvonalat is felvázol (web service alapú működés). A nyilvántartások együttműködése egyben abba az irányba mutat, hogy központi adattárházak jönnek létre, melyek nyitottabbá válnak a mostani szigetalkalmazásoknál. Ennek pozitív hozadéka a hatékony működés, de az adattárházakban, bizonyos keretek között hozzáférhetővé váló tárolt adatok komoly nemzetbiztonsági kockázatot jelentenek, emellett figyelemmel kell lenni a személyes adatok védelmére is, hiszen ez a megoldás olyan központosításra ad lehetőséget, mely veszélyezteti a személyes adatok védelméről szóló alapvető alkotmányos jogot. A tervezés során komolyan mérlegelni kell tehát a hatékonyság-biztonság arányát.

Az **Ügyfélközpontú szolgáltatások átfogó program** az EU által megjelölt 20 szolgáltatás elektronizálásának előremozdítását tűzi ki célul 9540,7 millió forint forrásból. Az Egyablakos vámügyintézés megvalósítása, A cégbírósági rendszerek korszerűsítése, Civil szervezetek nyilvántartásának, valamint a csőd és felszámolási eljárások modernizációja, A családtámogatási ellátások folyósításának korszerűsítése, Földhivatali adatok elektronikus non-stop szolgáltató rendszere, valamint az Anyakönyvi nyilvántartás reformja projektből álló program konkrét szolgáltatásokat nevez meg. Ezek közül 2008-ban a cégbírósági rendszerek korszerűsítése történt meg, az új rendszer azonban komoly vitákat váltott ki az érintettek között. Fél év után elmondható, hogy a rendszer jól működik, de a tervezésnél, fejlesztésnél és bevezetésnél érezni lehetett a központi stratégia hiányát. Az egységes elvek hiányában nem garantálható, hogy a rendszer jelentős átalakítás nélkül képes lesz együttműködni más, később kialakításra kerülő rendszerekkel. A további fejlesztéseknél ezért szem előtt kell tartani a későbbiekben publikálásra kerülő E-közigazgatási keretrendszert, mert enélkül nem érhető el a kívánt hatékonyság. Ennek és más projekteknek a további tanulsága, hogy a műszaki megvalósításnál szinte minden esetben valamilyen egyedi, speciális magyar megoldás jön létre, sem a műszakilag legegyszerűbb, sem a Nyugat-Európában már bevált alkalmazások nem felelnek meg a projektgazdáknak.

Az **Online infrastruktúra átfogó program** 18044,6 millió forintból a központi alapinfrastruktúra fejlesztését tűzi ki célul. Része az elektronikus fizetés és az elektronikus azonosítás megvalósítása, a Központi Elektronikus Szolgáltató Rendszer bővítése, valamint az Informatikai Biztonsági Központ (IBK) továbbfejlesztése. Ezek informatikai biztonsági szempontból is alapvető figyelmet érdemelnek.

Az elektronikus fizetési rendszerben az állampolgárok elektronikusan (POS, VPOS terminálokon) tehetnek eleget a közigazgatás által kirótt fizetési kötelezettségeiknek, így előreláthatólag komoly összegeket fog továbbítani, ezért kiemelt támadási cél lehet. Az elektronikus azonosítás jelentős előrelépést jelenthet az Ügyfélkapu és a hasonló rendszerek hitelesítési megoldásaiban, hiszen jelenleg ezek nem teljesítik a kor követelményeit az egyszerű, jelszavas beléptetési eljárásukkal. Hosszú évek óta nyitott kérdés az erős autentikáció megvalósítása, melyre jó esély kínálkozik ezzel a projekttel. Biztosítható lehetne továbbá a sértetlenség és a letagadhatatlanság is, mely jelenleg csak jogi szinten biztosított, műszakilag nem.

A Központi Rendszer kialakítása az első lépés volt a szolgáltató állam létrehozásában. Több éves működése során folyamatosan fejlesztik, egyre több hivatal kapcsolódik rá, használja a szolgáltatásait. Az igazán nagy kockázata azonban éppen ebben rejlik. Bár a csatlakozáshoz bizonyos alapvető információbiztonsági követelményeknek eleget kell tenni, ezek folyamatos fenntartása kétséges, és sok csatlakozó esetén külön ellenőrző célszervezet nélkül lehetetlen is. Mivel a Központi Rendszer felépítése és működése államtitok, nem lehet felmérni, mekkora a kockázata annak, hogy egy, a KR-re csatlakozó számítógépről indulva

sikeres támadást lehessen a teljes közigazgatási rendszer ellen indítani. A nyugati tapasztalatokból kiindulva azonban biztosan állítható, hogy a lehető legszigorúbb ellenőrzés nélkül akár ellenérdekelt országok, akár terrorista szervezetek vagy magányos elkövetők komoly károkat tudnak okozni az ilyen szinten integrált rendszerekben.

Az elhárítás fontos szereplője az Informatikai Biztonsági Központ, azaz a Cert-Hungary Központ, melynek működéséről, hatékonyságáról, eszközeiről nem áll rendelkezésre információ. A Központ folyamatos fejlesztése látatlanul is kiemelt fontosságú. Működéséről azonban fontos tudnia a szűk szakmai közvéleményen kívül a széles társadalomnak is, hiszen funkciója alapján akár rendvédelmi szervnek is tekinthető lenne, így az állampolgárok biztonságérzetének növelésében fontos szerepe lehetne.

Az **Integrált ügyfélszolgálat átfogó program** biztonsági szempontból közvetlenül nem releváns, így a jelen írás nem vizsgálja. Az **Integrált kormányzati funkciók átfogó program** elemei azonban olyan fontos, nemzetgazdaságilag és nemzetbiztonságilag fontos fejlesztéseket tartalmaznak, hogy nem lehet szó nélkül elmenni mellettük. A Központi Gazdálkodási Rendszer segítségével a Magyar Köztársaság teljes költségvetési rendszere átláthatóvá válik, így a belőle származó információk rossz szándékú felhasználásával akár a teljes nemzetgazdaságot befolyásolni lehet. Védelme ezért kiemelten fontos. Az Adóalany-centrikus adatszolgáltatási modell szintén adattárházat hoz létre, itt az adótitkok megőrzése válik elsődleges kérdéssé. A Biztonságos elektronikus összeköttetés a Nemzetbiztonsági Szakszolgálat folyamatait érinti, így a technológiája, bár szakmailag az egyik legérdekesebb feladat, számomra nem ismert. A programra 13881 millió forint áll rendelkezésre.

A **Megosztott e-közigazgatási szolgáltatások átfogó program** 600 millió forintos kerete az elektronikus levéltár és a területi alkalmazás-szolgáltató központok (ASP-k) létrehozására került elkülönítésre. A levéltár projekt a dokumentumok hosszútávú hitelességének biztosítása miatt érdekes információbiztonsági feladat, ám sokkal több figyelmet érdemelnek az ASP központok. Ezek ugyanis tipikus példái a hatékonyságnövelés-biztonságromlás formulának – legalábbis a magyar tapasztalatok alapján. Az önkormányzati informatikát központosítani szándékozó ASP-k lényegesen hatékonyabb működést jósolnak, mint ahogy az jelenleg történik. A legtöbb önkormányzat esetében az informatikai üzemeltetési szint csak jobb lehet a jelenleginél. Az önkormányzati adatvagyon néhány helyre koncentrálása azonban felveti azt a kockázatot, hogy a támadónak nem 3200, csak néhány központot kell hatalmába kerítenie a területi közigazgatás megbénításához. Ezért a kiemelt biztonsági ellenőrzés ezeknél a szervezeteknél alapvető fontosságú.

A **Tudásmenedzsment átfogó programra** tervezett 739,5 millió forint egy része közvetve hasznosul az információbiztonság területén. Mind a Tudásportálnak, mind a közigazgatási képzéseknek tartalmazniuk kell az információbiztonsági ismereteket három szinten (felhasználó, menedzser, informatikus). Az alapos és megfelelő oktatás nélkül, a szemlélet kialakulása nélkül ugyanis elképzelhetetlen a biztonságos magyar e-közigazgatás.

A magyar e-kormányzati informatikát érintő fenyegetések

Az e-közigazgatási stratégia alapján megállapítható a tervezett komplex magyar e-kormányzati infrastruktúra néhány jellegzetessége. A létrejövő megoldások centralizáltak lesznek, interneten vagy az Elektronikus Kormányzati Gerinchálózaton (EKG) keresztül elérhetővé válnak, alapvetően szolgáltatás orientált architektúra (SOA) alapon fogják tervezni, valamint webes technológiákra fog 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 cikk, mely az Ügyfélkapu néhány sebezhetőségére hívta fel a figyelmet (Szigeti et al., 2006). 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 adnak opcionális választ, ám a második fenyegetés továbbra is érvényes marad.

A tervezett technológia ismeretében azonban további, releváns fenyegetéseket lehet megállapítani. 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.

A **centralizálásból** eredő elsődleges fenyegetés az, hogy a korábban szétosztott információk egy földrajzi helyen, akár egy belső hálózaton sőt, a virtualizációt figyelembe véve akár egy számítógépen is találhatók. Védelmi intézkedéseket 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 ez a következőképp van megfogalmazva.

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 és operációs rendszerek használatát, valamint azt, hogy az alkalmazás olyan környezetben fut, mely megfelel az EKG csatlakozási követelményeinek (84/2007. (IV. 25.) Korm. rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről).

A.CERTIFIED: Az Értékelés Tárgyát futtató operációs rendszer, valamint a vele közvetlen kapcsolatban levő hálózati elemek rendelkeznek Common Criteria vagy azzal egyenértékű tanúsítással.

P.EKG: Az Értékelés Tárgyát futtató infrastruktúra eleget tesz a 84/2007. (IV. 25.) Korm. rendeletnek.

A szolgáltatás orientált 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 (Shah, 2008). A szerző négy speciális támadási pontot, és ezen belül számos fenyegetést azonosít. Mivel ezek részletes ismertetése meghaladja jelen cikk kereteit, a fenyegetéseket a támadási pontok, vektorok alapján lehet csoportosítani.

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. A második támadási pontot a **struktúra szintű támadások** jelentik, hiszen a korábbi, kizárólag HTML alapú struktúrák kétirányú, pl. XML formátumban leírt struktúrákra változtak. Ennél 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 tudjuk meghatározni.

T.CLIENT_SIDE: A támadó a kliens oldali alkalmazáson vagy böngészőn 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 webes technológiákra vonatkozó számtalan fenyegetés közül az OWASP Top 10 2007 (van der Stock et al., 2007) tartalmazza azokat, melyek ellen mindenképpen programozott védelmet kell nyújtani. Az itt felsorolt fenyegetések azonban nem csak webes, hanem más programozási környezetre is igazak. Ezek sorrendben: Cross Site Scripting (XSS), Injektálásos támadások, Kártékony fájlvégrehajtás, Nem biztonságos direkt objektumreferencia, Cross Site Request Forgery (CSRF), Információszivárgás és nem megfelelő hibakezelés, Feltört hitelesítés és sessionkezelés, Nem biztonságos kriptográfiai tárolás, nem biztonságos kommunikáció, Az URL szintű hozzáférés hibájának tiltása.

Ezen támadások elhárításának módjaira számtalan publikáció, ajánlás, műszaki megoldás van, melyek ismertetése nem célja a cikknek. Ki kell emelni Fleiner Rita írását (Fleiner, 2008), mely az injektálásos támadások módszereit és a védekezés módját ismerteti.

T.XSS: Egy támadó Cross Site Scripting támadást hajthat végre a nem megfelelő inputvalidálás miatt.

T.INJECTION: Egy támadó injektálásos támadást hajthat végre a nem megfelelő inputvalidálás miatt.

T.MALICIOUS_EXECUTE: Egy támadó kártékony kódvégrehajtást kezdeményezhet a nem megfelelő inputvalidálás miatt.

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.SESSION: A nem megfelelő sessionkezelés miatt a támadó hozzáférhet egy legális felhasználó jogosultságaihoz.

T.CRYPTO: A nem megfelelő kriptográfia használata miatt a felhasználói adatok dekódolhatóvá válnak.

T.INSECURE_COMMUNICATION: A nem titkosított adatátvitel miatt a hálózati forgalom lehallgathatóvá válik.

T.URL: Egy támadó olyan URL-hez férhet hozzá a nem megfelelő szerverbeállítás miatt, melyhez nincs jogosultsága.

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.

Biztonsági ajánlások az e-közigazgatás területén

Az alkalmazások, így az e-közigazgatási alkalmazások is akkor nevezhetők biztonságosnak, ha a futtatási környezetük biztonságos, a tervezésnél azonosított fenyegetésekre megfelelő védelmi intézkedéseket, más néven biztonsági funkciókat nyújtanak, valamint ha megvalósításuk is az elvárt biztonsági szinten történt. Az első feltételt a gyakorlatban az ISO 27000-es szabványcsalád implementálásával lehet elérni, a másik két feltételt pedig a Common Criteria (ISO 15408) szabvány felhasználása segíti elő.

A magyar közigazgatásban ennek a két szabványnak a használatára Dr. Muha Lajos doktori disszertációja tesz javaslatot (Muha, 2007). Ebben többek között javasolja a két szabvány közigazgatási meghonosítását is, Magyar Informatikai Biztonsági Irányítási Keretrendszer és Magyar Informatikai Biztonsági és Tanúsítási Séma elnevezésekkel. A disszertáció megjelenése óta ez a két rendszer hivatalosan, közigazgatási ajánlásként megjelent, teljes címe Magyar Informatikai Biztonsági Ajánlások. Tekintettel arra, hogy csak 2008. júniusában került kiadásra az ajánlás, felhasználásáról még nincsen tapasztalat. A cikk szempontjából fontos Common Criteria közigazgatási hasznosításáról azonban vannak külföldi beszámolók. A legjobban megismerhető bevezetést Japán tette meg, melynek folyamatáról rendszeresen beszámoltak az International Common Criteria Conference-en (ICCC).

A 7. ICCC-n Kai Naruki előadásában (Kai, 2006) bemutatta a szabvány bevezetésének okait és eredményeit. A japán e-kormányzati rendszer, mely sok tekintetben a hasonló a magyarhoz, a 2004-es évben számos informatikai biztonsági incidenst élt át. Ezek többnyire a rossz rendszertervezés, a gyenge védelmi intézkedések, a konfigurációs hibák és a webalkalmazások hibái miatt következtek be. Ennek hatására a japán kormány 2005. decemberében kiadta a központi kormányzati rendszerekre vonatkozó biztonsági elvárásokat tartalmazó szabványát. Ez az érintett termékek Biztonsági Előirányzatának értékelését és elfogadását írta elő kötelező követelményként. A teljes kormányzati körben 2009-re tervezik bevezetni a kötelező értékelést és tanúsítást. 2006. májusától a Biztonsági Előirányzat mellett a funkcionális specifikációt (ADV_FSP.1) és az ábrázolások közti megfelelést (ADV_RCR.1) is ellenőrizték. Mindezt azért tették kötelezővé, mert a saját kimutatásuk szerint a vizsgált fejlesztések hibáinak 66%-a a követelménydefiníciónál és a specifikációnál jelent meg.

A CC értékelések bevezetését három lépcsőben képzelték el. Az első fázisban szemléletváltást vezettek be. Minden e-közigazgatási rendszert egy egységként kezeltek. Ezután elkezdték a CC ismereteket átadni a fejlesztőknek és kormányzati megrendelőknek. A második fázisban már építhettek a fejlesztők tapasztalatára, így ki tudták tágítani az értékelések hatókörét. A harmadik fázisban már a garanciális követelmények körét is bővíteni tudták, így a Biztonsági Előirányzat értékelésekről tovább tudtak lépni az EAL szerinti értékelések felé. Mindezek a tapasztalatok és lépések mintául kell, hogy szolgáljanak a magyar közigazgatásban is, ahol pontosan ugyanezek a problémák és feladatok állnak a megrendelők és fejlesztők előtt.

A 9. ICCC-n Yamada Yasuhide számolt be a japán séma kétéves előrehaladásáról (Yamada, 2008). 2003 és 2007 között 152 terméket tanúsítottak Japánban, mely jól mutatja a Common Criteria bevezetés sikerességét. Kialakult a tanúsítással foglalkozó szervezet is, melyben 10 tanúsító szakember dolgozik, akik évente 5-6 tanúsítást végeznek el, valamint oktatásokat tartanak és segédleteket írnak. 4 értékelő laboratórium működik, melyeknél egy termék értékelése 3 hónap – 1 év időtartamban történik. Az értékelések közel 70%-a EAL3 szinten történik. Összességében a Common Criteria bevezetése 3 év alatt sikeresnek tekinthető, mely példa lehet Magyarországnak is.

A jelenlegi helyzet

Az elmúlt években komoly erőfeszítéseket tett a magyar kormány annak érdekében, hogy a közigazgatás felkészüljön a digitális forradalom jelentette kihívásokra, elég csak arra gondolni, hogy a közigazgatási informatikai stratégiák alaposan tárgyalják a biztonsági kérdéseket, vagy arra, hogy a kiemelt fejlesztések tenderfelhívásaiban az informatikai biztonságnak jellemzően külön fejezetet szentelnek. A központi közigazgatási rendszerek tervezésénél és üzemeltetésénél ezért elmondható, hogy az informatikai biztonság alapvető szempont. Nem történt még meg azonban az a szemléletváltás, amit a japán példa mutat. A közigazgatási rendszereket nem tekintik még egy egységnek, így minél távolabb kerülünk a központi közigazgatástól, annál kevésbé találkozhatunk a megfelelő védelemmel. Az egységes szemlélet hiányát mutatja, hogy az egyes önkormányzati rendszerekben, ahol tárolhatnak szigorúan védendő adatokat, és ezek a rendszerek direkt vagy indirekt összeköttetésben állnak a központi közigazgatási rendszerekkel, jellemzően nem teljesítik az ajánlásokban megfogalmazott elvárásokat. A centralizáció irányába történő elmozdulás sokat lendíthet az egységes szemlélet kialakulásán, de addig hosszú út vezet.

Az önkormányzatok informatikai infrastruktúrája, mely az e-közigazgatási rendszer leggyengébb láncszemének tekinthető, fontos tárgya kell, hogy legyen a mindenkori vizsgálatoknak. A jelen tanulmánynak egyik fontos megállapítása volt, hogy a jövőben egyre inkább a webes technológiák kerülnek előtérbe. Emiatt érdemes volt elvégezni egy egyszerű biztonsági tesztet a magyar önkormányzatok honlapjaival.

A webszerverek konfigurációja, a biztonságos honlapok kialakítása jól ismert és jól dokumentált feladat. Magyar közigazgatási ajánlás azonban nincs ebben a témában, pedig hasznos segédlet lenne az önkormányzati informatikusoknak. Néhány kiragadott követelmény:

- Webszervert saját DMZ-ben vagy webhosting szolgáltatónál kell tárolni!
- A webszerver dedikált host legyen, más szolgáltatás, virtuális szerver ne fusson rajta!
- Ki kell választani a megfelelő operációs rendszert, melynek biztonsági megerősítését el kell végezni!
- Rendszeresen frissíteni kell a szerveren található szoftvereket!
- Erős autentikációt kell használni ott, ahol csak lehet!
- Le kell tiltani minden felesleges írási, olvasási és végrehajtási jogot!
- Készítsünk külön partíciót a portál tartalmának!
- El kell távolítani minden olyan dokumentációt a szerverről, mely a portálmotor használatát mutatja be!
- Törölni kell minden alapértelmezett vagy teszt állományt!
- A szerver process limitált joggal fusson!
- Nem szabad fájlfeltöltést engedni a portálon keresztül!
- Vigyázni kell az ideiglenes fájlokkal, amik futás közben jönnek létre!
- Vigyázni kell a minősített iratokkal, hogy véletlenül elérhetővé váljanak a portálon!
- Folyamatosan naplózni kell!

Több önkormányzatnál végzett felmérés alapján kijelenthető, hogy ezeket a szabályokat kevéssé vagy egyáltalán nem tartják be, ami elsősorban az ismerethiánynak róható fel. A weboldalakon túl azonban sokkal fontosabb kockázat, hogy más rendszerek üzemeltetése sem az elvárt biztonsági szinten történik.

Jól jellemzi az önkormányzati weboldalak általános biztonságát az a teszt, aminek során olyan honlapokat kerestünk, melyek Joomla portálmotoron futottak. Egy 2008 közepén

megjelent hiba kihasználásával adminisztrátori jogosultságot lehetett ezeken a szervereken szerezni, amennyiben nem frissítették. A normál működés során, ha ideiglenes jelszót kérünk a portáltól, akkor az egy tokent ad válaszul. Ezt kell bemásolni a megfelelő mezőbe. Azonban egy ’ jel beírásával a "SELECT id FROM jos_users WHERE block = 0 AND activation = " " SQL parancs hajtódik végre, ami után szabadon átírhatjuk az adminisztrátor jelszavát. A támadás első lépéseként olyan portálokat kell keresni, melyeknél a célpont.com/index.php?option=com_user&view=reset&layout=confirm URL elérhető. A token mezőbe beírt ’ karakter után láthatóvá válik a jelszógenerálási mező. Az admin felhasználóval, és az itt beírt jelszóval a célpont.com/administrator oldalon ezután kiemelt jogosultsággal tudunk belépni. A Google-ba írt megfelelő keresőszó kombináció alapján megjelennek azok a portálok, melyek önkormányzatok kezelésében vannak, és feltehetőleg érzékenyek a fenti hibára. A 2008. októberi mérés alapján kb. 30 ilyen hibás honlap van, azaz az összes magyar önkormányzati honlap 1%-a egy egyszerű támadással kompromittálható.

További feladatok az e-közigazgatás biztonságáért

A magyar kormány jól láthatóan eltökélt az informatikai biztonság kultúrájának elterjesztésében. Az első fontos lépéseket megtette, vagy éppen megtenni készül. Ez a munka azonban lassan halad, a biztonsági fenyegetések egyre szaporodnak, így szükség van olyan tudományos munkára, mely segíti a lerakott alapokra történő építkezést. A cikk tapasztalatai alapján a következő fontos területek kutatása segítheti az általános biztonsági szint emelését.

Védelmi Profil meghatározása az elektronikus közigazgatási alkalmazásokhoz

Cél a Magyar Informatikai Értékelési és Tanúsítási Séma (ISO/IEC 15408, Common Criteria) ajánlás alapján olyan Védelmi Profil kidolgozása, mely a Magyar Köztársaság elektronikus közigazgatási szolgáltatásaiban használt alkalmazások funkcionális és garanciális követelményeit határozza meg, az elvárt működési környezet leírásával. 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.

Magyar Informatikai Értékelési és Tanúsítási Séma által megkövetelt garanciális követelmények alapdokumentumainak kidolgozása

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. A kutatási cél olyan alapdokumentumok elkészítése, mely az elektronikus közigazgatásban dolgozó fejlesztők számára egyértelművé teszi a tőlük elvárt, biztonsággal kapcsolatos tevékenységeket, és segítséget nyújt ezek elkészítésében. A feladat tudományos értékét az adja, hogy a szabvány csak magas szinten határozza meg a követelményeket, ennek értelmezése és gyakorlati használata kevéssé körüljárt terület.

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 a cél 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.

Minőségi mérőszámokat tartalmazó kritériumrendszer kidolgozása az e-közigazgatási alkalmazások biztonságára vonatkozóan

Az alkalmazások biztonságával szembeni leggyakoribb fenntartás az, hogy nem mérhető. Bár a szakirodalom számos, az informatika területén használatos mérőszámot ismer, az elektronikus közigazgatás biztonságához kapcsolódó mérési kritériumrendszer nem kidolgozott, pedig ez nagyban hozzájárulhat az ilyen alkalmazások elfogadásához és terjedéséhez. A cél ezért olyan biztonsági metrikák kidolgozása, melyek átfogó képet adnak az e-közigazgatási alkalmazásról.

Információbiztonsági oktatási tematika kidolgozása e-közigazgatási alkalmazásokat fejlesztőknek és megrendelőknek

Az alkalmazásokkal kapcsolatos biztonsági megfontolások mind a megrendelők, mind a fejlesztők számára kevéssé ismertek a gyakorlatban. Ennek eredménye, hogy sem az alkalmazások specifikálásában, sem a kifejlesztett alkalmazásokban nem, vagy nem helyesen jelennek meg a biztonsági igények, így a teljes rendszer biztonsági szintje kérdőjeleződik meg. Ennek kivédésére egy olyan oktatási rendszer kidolgozása a megoldás, mely mindkét fél számára érthetővé teszi a követelményeket. Ennek megfelelően a cél egy olyan tematika kidolgozása, mely jelentősen javít a terület megértésén és elfogadottságán.

Irodalomjegyzék

1. Fleiner, R. (2008, december). SQL injekcióra épülő támadások és védekezési lehetőségek. *Hadmérnök* , III. évf. 4. szám: 117-128. http://www.hadmernok.hu/2008_4_fleiner.pdf
2. Kai, N. (2006, szeptember 3). *Strategic ST Evaluation/Confirmation.* Common Criteria Portal: http://www.commoncriteriaportal.org/iccc/7iccc/t2/t2211000.pdf, Letöltve 2009. január 8.
3. Magyar Köztársaság Miniszterelnöki Hivatal Informatikai Államtitkárság. (2008, október 27.). *E-Közigazgatás Program 2008-2010.* Magyar Köztársaság Miniszterelnöki Hivatal Informatikai Államtitkárság: http://www.ekk.gov.hu/hu/ekk/letoltheto/e-kozig_program_2008-2010.pdf, Letöltve 2009. január 6.
4. Muha, L. (2007.). *A Magyar Köztársaság kritikus információs intrastruktúráinak védelme.* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem: http://phd.om.hu/disszertaciok/ertekezesek/2008/de_3938.pdf, Letöltve 2009. január 6.
5. Shah, S. (2008). *Web 2.0 Security: Defending Ajax, RIA, and SOA.* Boston, Massachusetts: Charles River Media.
6. Szigeti Szabolcs, Krasznay Csaba. (2006). A magyar elektronikus közigazgatási rendszer biztonsági analízise. *Networkshop 2006 Konferencia.* Miskolc: Nemzeti Információs Infrastrukúra Fejlesztési Program: 65-69.

7. van der Stock, A., Williams, J., & Wichers, D. (2008, szeptember 20.). *Open Web Application Security Project.* Top 10 2007 - OWASP: http://www.owasp.org/index.php/Top_10_2007 Letöltve 2009. január 7.
8. Yamada, Y. (2008, szeptember 23.). *Japanese CC Evaluation & Certification Activity Update*, Common Criteria Portal: http://www.commoncriteriaportal.org/iccc/9iccc/pdf/A2305.pdf Letöltve 2009. január 8.