WEB SERVICE FENYEGETÉSEK E-KÖZIGAZGATÁSI KÖRNYEZETBEN

Krasznay Csaba, csaba.krasznay@hp.com
HP Magyarország Kft.

Bevezetés

A 2009-2010-es években számos olyan szoftver- és rendszerfejlesztés valósul meg Magyarországon hazai és Európai Uniós forrásból, melyek segítik az e-közigazgatás fejlődését. Ezek technológiai iránya a szolgáltatás-orientált architektúra (SOA) felé mutat. Ez a megoldás új, eddig még kevéssé vizsgált informatikai biztonsági fenyegetéseket rejt magában, melyekkel a közigazgatási ajánlások kevéssé foglalkoznak, a biztonságos alkalmazásfejlesztés érdekében azonban szükséges a terület részletes elemzése.

A tanulmány bemutatja a magyar központi közigazgatási rendszerek jelenlegi és tervezett, nyilvánosan megismerhető architektúráját, fejlesztési irányait, valamint a web service helyét ebben a környezetben. Ismerteti továbbá azokat a szabványokat, ajánlásokat, melyek az ilyen típusú megoldásokra vonatkoznak, és behatárolják a fejlesztők lehetőségeit. Kiemelten foglalkozik a magyar elektronikus közigazgatási keretrendszerrel.

Bemutatja továbbá azokat az ismert, tipikus támadási módokat, melyek speciálisan a szolgáltatás-orientált architektúrákra vonatkoznak, valamint azokat az általános védelmi intézkedéseket, melyek segítségével a támadások kivédhetők. Az aktuális trendek alapján megállapítható, hogy a kifinomult informatikai támadások már nem hálózat és operációs rendszer szintjén történnek, hanem alkalmazási szinten, kiemelten a webes alkalmazások területén. Mivel a szolgáltatás-orientált architektúra igen komplex megoldásokra ad lehetőséget, a képzett támadónak jó esélyei vannak észrevétlenül jogosulatlan hozzáférést szerezni a rendszerhez. A szoftvertervezőknek, fejlesztőknek pedig – tekintettel arra, hogy a komplex rendszert sokan kivitelezik – nagy az esélyük arra, hogy olyan hibát vétenek, mely megkönnyíti a támadók dolgát. Ahány rendszer, annyiféle védelmi intézkedés képzelhető el, de meghatározhatók olyan megoldások, melyek általános alkalmazásával ezek a hibák minimalizálhatók.

A magyar e-közigazgatási SOA környezet

A Magyar Köztársaság kormánya, alkalmazkodva az ipari trendekhez és az EU e-közigazgatási ajánlásaihoz, a szolgáltatás orientált architektúrát (SOA) választotta fejlesztési iránynak. Ez a törekvés mind az írott stratégiákban, mind az eddigi központi fejlesztéseknél tetten érhető. A Közigazgatási Informatikai Bizottság (KIB) 28. számú ajánlásából [1] azonban részletesen megismerhetjük azt a fejlesztési elképzelést, melyet a következő évek kiemelt közigazgatási informatikai rendszereinél meg kell valósítani.

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.

A követelménytár e-közigazgatási architektúrájáról szóló részében leírt modell szerint [2] a magyar e-közigazgatás központi eleme az ún. e-közigazgatási sín lesz, mely szolgáltatási szinten köti össze a különböző szakrendszereket. Ennek előfeltétel az, hogy a szakrendszerek képesek legyen csatlakozni ehhez a sínhez, azaz olyan szolgáltatásokat, 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, hogy kommunikáljanak annak érdekében, hogy a kért szolgáltatás végrehajtódjon.

A sín a szakrendszer-specifikus szolgáltatások mellett alapszolgáltatásokat is nyújt. A tervek szerint hat olyan alapszolgáltatás lesz, 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;
- Hitelesítésszolgáltató, mely nem részletezett módon OCSP 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 a jól ismert szolgáltatásokat nyújtja az állampolgár és a közigazgatás között (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 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.

A biztonsági kérdéseket az ajánlás három részbe sorolja.

- Foglalkozni kell az állampolgárok személyiségi és adatvédelmi jogaival, melynek 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 PKI alapú működésre (elsősorban az SSL/TLS felhasználására), 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. Ezek a következők: Microsoft .NET 3.0, Sun OpenESB, Oracle SOA Suite, IBM Websphere. Természetesen más keretrendszerek is számításba jöhetnek, ám reálisan a felsorolt négy termék használata valószínű azok piaci pozíciója miatt. 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 sebezhetőség. A megfelelő biztonsági szint eléréséhez azonban szükséges lefektetni, hogy milyen biztonsági környezet és beállítás mellett tekinthetők ezek a keretrendszerek elfogadhatónak.

Fejlesztési ajánlások

Az ajánlás fejlesztési útmutatója [3] reálisan értékeli a sikeres fejlesztéshez szükséges kritériumokat. Több olyan pontot ír le, melyek összessége szükséges ahhoz, hogy egy közigazgatási fejlesztés sikeres lehessen. Ezek leírása az ajánlásban található meg, az alábbi pontokban a felvetések információbiztonsági vonatkozásait tárgyaljuk.

- Szervezeti felépítés: a siker elengedhetetlen feltétele, hogy a szervezet olyan eszközként lássa az informatikai fejlesztést, mely segíti a munkáját. Az informatika minden esetben szolgálja a szervezetet, és nem fordítva. Ehhez azonban jelentős szemléletváltás szükséges, mely nem csak a közigazgatásra, hanem sokszor az üzleti szférára is érvényes. Vonatkozik ez a szemléletmód a szervezet részéről a projektbe delegált biztonsági felelősre is, akinek kulcsszerepe van a biztonságos rendszer kialakításában.
- Az intézmény érettsége a technológia befogadására: a köztisztviselők körében sokszor jelentős ellenállást lehet tapasztalni az informatikával szemben. Fontos az ő meggyőzésük is arról, hogy a technika, és ezen belül a biztonsági megoldások nem ellenségük, hanem az ő érdekükben kerülnek bevezetésre.
- Iteratív megközelítés: kibővítve az ajánlás értelmezését, a szoftverfejlesztés módszertanának is iteratív megközelítésűnek kell lennie, hiszen a közigazgatási szerv nem szoftverfejlesztő, így sokszor kell visszacsatolást kapnia a fejlesztőtől arra vonatkozóan, hogy merre halad a projekt. Ezt időben és pénzben is bele kell kalkulálni a projektbe. A védelmi intézkedések tervezését is ebből a nézőpontból kell megközelíteni.
- A közigazgatás és az informatika közötti elkötelezettség: komplex, több résztvevős projekteknél óhatatlanul előkerülnek azok a konfliktusok a közigazgatási szervek között, melyek a fejlesztő munkáját megnehezítik, sokszor ellehetetlenítik. Ezek kezelésére fel kell készülni. El kell például dönteni, hogy melyik résztvevő biztonsági igényeit kell kielégíteni.
- Irányítási keretrendszer: a fejlesztési projekt olyan irányítást igényel, mellyel a projekt mindkét fél részéről kézben tartható. Ezért fontos valamilyen projektvezetési

módszertan felhasználása, mely tudás kisebb szervezeteknél nem feltétlenül van meg. Ez komoly kockázat lehet egy fejlesztési projektben.

- Szolgáltatások granularitása: Az alkalmazás tervezésénél különös figyelemmel kell lenni arra, hogy az egyes szolgáltatások milyen komplexitású feladatokat végeznek el. Amennyiben a folyamatok elemzésénél kiderül, hogy bizonyos szolgáltatások több területen is előkerülnek, ezt a szolgáltatást érdemes csak egyszer megírni. Bizonyos védelmi szolgáltatásokat például érdemes egyszer megírni, és egységesen felhasználni, így biztosítva az egyenszilárdságú védelmet.
- Az újrahasznosítás jelentősége: Kibővítve az ajánlás értelmezését, kijelenthető, hogy jelentős fejlesztési költségeket lehet megtakarítani akkor, ha bizonyos szolgáltatásokat csak egyszer írnak meg, és azokat később más fejlesztésekben újrahasznosítják. Ehhez egyrészt a szolgáltatáskatalógus folyamatos karbantartása, másrészt még több alapvető központi, elsősorban biztonsági szolgáltatás fejlesztése szükséges.
- A szolgáltatás életciklusának tudatosítása: A szolgáltatás működése folyamatosan változhat, mielőtt leállítják. Például jogszabály módosítások, szabványváltozások miatt akár évente máshogy működhet. Ez a változás pedig érinti a szolgáltatást igénybe vevő más alkalmazásokat is, akiket erről értesíteni kell. Ennek a változáskezelésnek kulcsfontosságú szerepe van.
- A szolgáltatás minősége (QoS): Az ajánlás leírása mellett ebben a pontban meg kell emlékezni arról, hogy a különböző rendszerek különböző szolgáltatási szinteket írhatnak elő, amik függhetnek a szolgáltatást nyújtó rendszer QoS paramétereitől. Ebben a komplex környezetben nem szabad elhanyagolni ezt a szempontot a tervezésnél.
- Architektúra terv készítése: Ez a terv nem készíthető el a folyamatok pontos ismerete nélkül. Általános probléma, hogy a konkrét tervezési lépéseket már akkor meg kell tenni, amikor még nem készült el a folyamatok leírása.
- Informatikai biztonság: Az egyik legfontosabb kritérium a biztonságos rendszer elkészítése. A szükséges védelmi intézkedések meghozatala azonban kockázatarányosan és egyenszilárdságú módon kell, hogy történjen. Szükséges lenne ezért, hogy a szervezet minden fejlesztés előtt pontos vagyonleltárt és kockázatelemzést adjon át a fejlesztőnek, aki ennek hatására tudja a védelmi intézkedéseket megtervezni.
- Fejlesztői csapatok felállítása: A fejlesztők mellett mindig kell lennie egy információbiztonsági szakértőnek. A két szerepkör tökéletesen kiegészítheti egymást, ami biztonságos alkalmazások fejlesztéséhez vezet.
- Világos siker kritériumok: az információbiztonság területén ez egy komplikált kérdés, melyre külön tanulmányban lehet csak választ adni.

Az ajánlás részletesen leírja a fejlesztési életciklusban a biztonság helyét is [4]. Különösen érdekes az a megközelítés, hogy az életciklust a pályázat szemszögéből is meghatározzák. Eszerint a következő feladatokat kell teljesíteni.

1. Pályázati felhívás (projekt megfogalmazásakor) összeállításakor be kell építeni azokat a megvalósítandó feladatokat, amelyek garantálják a biztonsági követelmények kielégítését. Pályáztató feladata
2. A pályázat kötelező elemévé kell tenni a biztonság megvalósításához szükséges erőforrások tervezését a pénzügyi keret tervezésékor. Pályáztató feladata

3. A projekt monitoring követelményeiben szerepeltetni kell a biztonsági indikátorokat és azok rendszeres jelentését kötelezővé kell tenni. Pályáztató feladata
4. A pályázatok elbírálásakor az IT biztonsági követelményekre vonatkozó elvárásokat meg kell jelentetni és megfelelő súllyal kell az elbíráláskor, a támogatás odaítélésekor figyelembe venni. Elbíráló feladata
5. A finanszírozási, támogatási szerződésben meg kell jelentetni a biztonságra vonatkozó követelményeket és a be nem tartáskor alkalmazandó szankciókat. Támogató feladata
6. A pályázati anyag összeállításakor figyelembe kell venni a kiírásban megjelent követelményrendszert. Pályázó, projektgazda feladata
7. A megvalósítás tervezésekor be kell tervezni a biztonságra vonatkozó követelmények megvalósítását is. Pályázó, projektgazda feladata
8. Implementációs munkák során meg kell valósítani a biztonságra irányuló követelményeket, funkciókat. Pályázó, projektgazda, implementációt végző feladata
9. Az eredmények átvételekor, rendszer élesítéskor csak a biztonsági követelményeket igazoltan kielégítő rendszert szabad élesbe állítani. Pályázó, projektgazda, átvevő feladata
10. A támogatási összeg folyósítása előtt meg kell győződni a biztonságra vonatkozó követelmények érvényesüléséről. Felügyelő, támogató, projektgazda feladata
11. A megvalósított biztonsági szint fenntartása érdekében biztonsági rendszert kell üzemeltetni. Pályázó, projektgazda feladata

Bár a folyamat helyes, az ajánlás nem ad támpontot arra vonatkozóan, hogyan történjen meg a biztonsági igények meghatározása. Az igények meghatározását jogszabályból, ajánlásból javasolja levezetni, azonban a helyes megközelítés szerint a tervezett rendszer által kezelt információvagyon felmérésével, az ezekre vonatkozó fenyegetések meghatározásával, majd a fenyegetések jelentette kockázatok priorizálásával kell kiválasztani a szükséges védelmi intézkedéseket. A kiírás során természetesen felhasználható az ajánlásban leírt védelmi intézkedések összessége axiómaként, ám ez a gyakorlatban túl sok, vagy éppen túl kevés is lehet. Amennyiben lehetséges, támaszkodni kell a Közigazgatási Informatikai Bizottság 25. ajánlása szerinti kockázatfelmérési módszertanra [5], és ez alapján kell meghatározni a védelmi igényeket. A következő fejezetben ezt a gondolatmenetet követjük.

Web service fenyegetések

Napjainkban az informatikai támadások jelentős része az alkalmazási szinten tapasztalható. Az alsóbb rétegeken olyan kifinomult védelmi megoldások érhetők el, melyek hatékonyan – de nem feltétlenül teljes körűen – védenek a támadások ellen. Az alkalmazások közül is előszeretettel a weben keresztül elérhető szolgáltatások állnak a célkeresztben. Ez még általában az egyes portálmotorokat érinti, de már rendelkezésre állnak olyan letölthető eszközök, melyek kimondottan a web service-ek sebezhetőségeinek felderítésére lettek kifejlesztve. A közigazgatási SOA architektúra, és a rajta elérhető web service-ek ezért olyan támadásoknak vannak kitéve, melyekre a KIB 28. ajánlás nem hívja fel külön a figyelmet.

A támadási vektorokat [6] szerint négy irányban lehet értelmezni. Származhatnak a kliens oldalról, a protokollokból, a struktúrából és a szerver oldalról. Ezek részletes ismertetése előtt elmondható, hogy a kliens oldali fenyegetésekre van a legkisebb hatása az e-közigazgatási rendszer fejlesztőjének, hiszen tipikusan tömeges, internetes hozzáféréseket kell kezelnie. Ennek megfelelően ezekre a fenyegetésekre minden esetben alaposan megtervezett védelmi

intézkedéseket kell implementálni. Az alábbi felsorolás a négy támadási pont e-közigazgatási rendszerek szempontjából legkritikusabb fenyegetéseit sorolja fel.

Kliens oldali fenyegetések:

- Ajax komponensek: a hibák főleg a JavaScript hibás használatából és a session-ök helytelen kezeléséből adódhatnak. A cross-site scripting (XSS) támadások elsődleges forrásai a rosszul megírt Ajax komponensek, de más „cross" támadások (cross-site Request Forgery, Cross-Domain támadások) is elsősorban innen erednek. Ezek többféle, elsősorban hitelesítést érintő támadásokat eredményezhetnek. Meg kell még említeni az üzleti logikák kiszivárgásának a veszélyét is, hiszen a fejlesztők sokszor a kliens oldalán, tiszta JavaScript megoldással hajtják végre a tevékenységet. Ez könnyen manipulálható, hiszen a programozott üzleti kontrollokat a kliens a saját gépén módosíthatja.
- Sérülékeny böngészők: a nem frissített böngészőkön keresztül olyan kémprogramok juthatnak be a klienshez, melyek a nem egyszer minősített információkat kiszivárogtatják. Talán ez a legveszélyesebb kliens oldali fenyegetés, hiszen az alkalmazás fejlesztőjének semmilyen hatása nincs a kliensek biztonsági szintjére.

Struktúra szintű fenyegetések:

- XML Node manipulálás: a web service környezetben a kliens és a szerver között XML formátumú üzenetek közlekednek, melyekbe a megfelelő védelem híján kártékony kódokat lehet beszúrni. A kártékony kód ebben az esetben a hagyományos, bináris kártevő mellett SQL injection, távoli kódvégrehajtás, vagy akár XSS is lehet. Szintén ebbe a körbe tartozik a parserek támadása, melyek során az XML üzenetbe olyan kódot injektálnak, mely a szerver oldali parsert támadja, ezzel többek között Denial-of-Service támadást előidézve.

Protokoll szintű fenyegetések:

- A protokoll fejlécének és tartalmának manipulálása: A KIB 21. és 28. ajánlások olyan üzenetformátumokat határoznak meg, melyek testre szabják a magyar közigazgatási igényeket. A saját megoldások miatt különösen oda kell figyelni ezeknek az üzeneteknek a tartalmára (pl. típusdefiníciókra), hiszen a legális üzenetben esetleg olyan kódokat, üzeneteket juttathat be egy támadó, mely az előző pontban részletezett támadásokhoz vezethet.

Szerver oldali fenyegetések

- Az alkalmazás szervert érintő támadások: A SOA környezetet olyan kereskedelmi megoldásokon futtatják, melyek ellen az internetről egyszerűen letölthető kódokkal lehet támadásokat indítani, ami az egész infrastruktúrát érintheti. Az applikációs szerver nem megfelelő telepítésével a futtató környezet, és azon keresztül az egész hálózat támadhatóvá válik.
- Alkalmazás hibák: A legsérülékenyebb a teljes SOA architektúrában maga az alkalmazás, amit tipikusan sok fejlesztő, több fejlesztési helyen, nem megfelelően kialakított fejlesztésbiztonsági kontrollok között hoz létre. A biztonsági funkciók nem megfelelő kialakítása hitelesítési (pl. jelszótörés), jogosultsági (pl. jogosultságemelés, nézetváltás), beszúrásos (pl. SQL injection) rendelkezésre állási (pl. Denial-of-Service), sessionkezelési (pl. megjósolható cookie) és adatszivárgási hibákhoz (pl. túl részletes hibaüzenetek) vezethetnek.

Védelmi intézkedések

A magyar (és más) elektronikus közigazgatási rendszerek kommunikációs irányai tipikusan az állampolgár-közigazgatás (C2G és G2C), a vállalkozások-közigazgatás (B2G és G2B), valamint a közigazgatás-közigazgatás (G2G). SOA szerinti adatátvitel minden irányban elképzelhető. Az első két esetben kiemelt szerepe van az Ügyfélkapunak, mely jelenleg is fogad XML formátumú dokumentumokat (pl. adóbevallások), és továbbítja azokat az érintett közigazgatási szerv felé. Ebben a környezetben a következő adatbeviteli pontokat kell kontrollálni:

- Humán ügyfél: egy nevesített személy küld e-mailben vagy weboldalon keresztül üzenetet, és ezeken a felületeken tud üzenetet is fogadni.
- Humán ügyintéző: olyan köztisztviselő, aki e-mailben vagy weboldalon keresztül tud üzenetet küldeni és fogadni.
- Ügyfélkapu: a Hivatali Kapun keresztül tud üzeneteket küldeni és fogadni.
- Kliens alkalmazás: olyan, közigazgatásilag nem kontrollált alkalmazás, mely humán szubjektumhoz nem feltétlenül köthető módon küld és fogad üzeneteket, pl. web service interfészen keresztül.
- Közigazgatási alkalmazás: olyan, közigazgatásilag kontrollált alkalmazás, mely humán szubjektumhoz nem feltétlenül köthető módon küld és fogad üzeneteket, pl. web service interfészen keresztül.

Küldő / Fogadó	Humán ügyfél	Humán ügyintéző	Ügyfélkapu	Kliens alkalmazás	Közigazgatási alkalmazás
Humán ügyfél		X	X		X
Humán ügyintéző	X	X	X	X	X
Ügyfélkapu	X	X		X	X
Kliens alkalmazás		X	X		X
Közigazgatási alkalmazás	X	X	X	X	X

A közigazgatási alkalmazás szempontjából nézve meg kell állapítani, hogy minden forrásból kaphat üzenetet, ráadásul különböző forrásokból különböző formátumú üzeneteket. A javasolt védelmi intézkedések mindegyikét egységesen kell használni, de hatékonyságuk különböző, hiszen más és más kockázatok jelentkeznek.

- Humán ügyféltől származó üzenet: ebben az esetben e-mailen vagy weboldalon keresztül történő közvetlen benyújtásról lehet beszélni, amikor a küldő által küldött SOAP üzenet tartalma nem kontrollálható. Ebben az esetben a legvalószínűbb az üzenet valamilyen manipulálása, tehát semmilyen ilyen jellegű üzenetben nem bízhatunk meg, még az sem biztos, hogy az a beküldő, akit a rendszer azonosított. Első védelmi vonalként az input validálást kell megvalósítani, mely történhet programozott módon (pontosan meghatározott inputformátumok kikényszerítése) és

eszköz felhasználásával (pl. XML tűzfal). Ezek együttes felhasználása már elég magas garanciát nyújt arra, hogy a web service-en keresztül a rendszer nem manipulálható. Emellett az erős authentikáció elvárt, de nem megkövetelt, hiszen az állampolgárnak ebben a környezetben nincs vagy nagyon alacsony jogosultsága van, ami már nehézzé teszi a külső támadó dolgát, valamint az ügyfelek nem megszabható infrastruktúrája miatt ez a megoldás reálisan nem elvárható az állampolgárok költségén.

- Humán ügyintézőtől származó üzenet: ebben az esetben a közigazgatási szervnél dolgozó személy kezdeményez valamilyen tevékenységet a rendszerben. Esetében az üzenet manipulálása nem komoly kockázat, azonban a jogosultságával könnyen visszaélhet. Ebben az esetben a visszakövethetőség a lényeges követelmény, így az erős authentikáció, a megfelelő jogosultság kialakítása, a felelősségek szétválasztása, valamint az alapos naplózás merül fel biztonsági funkcióként. Ezek mindegyike tipikusan infrastrukturális és adminisztratív védelmi intézkedésekkel valósulhat meg, melyek az alkalmazás biztonsági funkcióit egészítik ki.
- Ügyfélkaputól származó üzenet: az Ügyfélkapu Hivatali Kapu szolgáltatása üzeneteket továbbít a közigazgatási alkalmazás felé. A nyilvános, felsorolt funkcionalitása alapján elsősorban a küldő személyére, és a beérkeztetésre ad garanciát, formátumellenőrzésre vonatkozó működést nem publikáltak. Az Ügyfélkapunak, mint közvetítő rétegnek pedig nagy szerepe lehet abban, hogy a humán ügyféltől származó fenyegetések ellen első szintű védelmet nyújtson, így fokozva a közigazgatási alkalmazások biztonsági szintjét.
- Kliens alkalmazástól származó üzenet: ebben az esetben viszonylag egyszerű dolga lehet a fejlesztőnek, hiszen adminisztratív intézkedéseket hozhat a csatlakozó, közigazgatásilag nem kontrollált alkalmazásokra. Előírhatja, hogy a csatlakozó szerv milyen SOAP üzenetet küldhet, milyen járulékos biztonsági szolgáltatásokat kell használnia (pl. WS-Security), valamint akár KIB 25. ajánlás szerinti tanúsítást is elvárhat. A hangsúly ebben az esetben a WS-Security szolgáltatásainak használatán van.
- Közigazgatási alkalmazástól származó üzenet: a más közigazgatási rendszerekből származó üzenetek vagy illeszkednek a tervezett e-közigazgatási sínre, és ebben az esetben teljesítik a KIB 28. ajánlás biztonsági követelményeit, vagy olyan meglévő rendszerektől származnak, melyek működése nem vagy csak nagyon nehezen befolyásolható. Ez utóbbi esetben minden egyes rendszer minden adatcseréjét egyedileg kell kezelni, és garantálni a biztonságos adatbevitelt. Erre a célra egy olyan speciális web service használata javasolt, mely az adatkonverzió után képes a minimális biztonsági funkcionalitást biztosítani (pl. forrás hitelesítése, naplózás).

Összefoglalás

A jelenleginél sokkal centralizáltabbnak tervezett magyar e-közigazgatási rendszer lényegesen jobb lehetőségekkel kecsegtet az informatikai biztonság területén, és így közvetve hozzá tud járulni a hatékonyabb nemzetvédelemhez, ám addig még hosszú út vezet. A kiadott közigazgatási ajánlások megfelelő alapot jelentenek, de folyamatos fejlesztésük, és főleg kikényszerítésük nélkül ennek a hosszú útnak a Magyar Köztársaság nem fog a végére érni. A stratégiai irányok látszanak, a források rendelkezésre állnak, minden adott ahhoz, hogy a 2010-es években az e-közigazgatás biztonsági vonatkozásában az ország a világ élmezőnyébe tartozzon.

Irodalomjegyzék

[1] Közigazgatási Informatikai Bizottság (2009. március 24.), *A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár*, E-Közigazgatási Követelménytár: http://kovetelmenytar.complex.hu, Letöltve: 2009. március 25.

[2] e-Közigazgatási Keretrendszer Kialakítása projekt (2008. december 3.), *A magyar e-közigazgatási architektúra*, E-Közigazgatási Követelménytár: http://kovetelmenytar.complex.hu/document/koz/EKZ_EKK_EKOZIG_MAGYAR_KOZIG_RENDSZER_ARCHITEKTURA_081203_V3.DOC, Letöltve: 2009. március 25.

[3] e-Közigazgatási Keretrendszer Kialakítása projekt (2008. szeptember 19.), *Fejlesztési útmutató és menetrend (roadmap)*, E-Közigazgatási Követelménytár: http://kovetelmenytar.complex.hu/document/koz/EKZ_EKK_EKOZIG_FEJLESZTESI_UTMUTATO_%20080919_V2.DOC, Letöltve: 2009. március 25.

[4] e-Közigazgatási Keretrendszer Kialakítása projekt (2008. július 10.), *IT Biztonsági követelményrendszer érvényesítésének módja a közigazgatási informatikai rendszerek fejlesztések során*, E-Közigazgatási Követelménytár: http://kovetelmenytar.complex.hu/document/koz/EKZ_EKK_EKOZIG_IT_BIZT_KOV_RENDSZER_ERV_080710_V1.DOC, Letöltve: 2009. március 25.

[5] Közigazgatási Informatikai Bizottság (2008. június), *Magyar Informatikai Biztonság Irányítási Keretrendszer Informatikai Biztonsági Irányítási Rendszer*, Informatikai Államtitkárság: http://www.ekk.gov.hu/hu/kib/KIB-25-1-1_IBIR_V1_0_vegl.pdf, Letöltve: 2009. március 1.

[6] Shah, S. (2008). *Web 2.0 Security: Defending Ajax, RIA, and SOA*. Boston, Massachusetts: Charles River Media.