ELŐADÁSOK NYOMDAKÉSZ ANYAGA

A MAGYAR ELEKTRONIKUS KÖZIGAZGATÁSI RENDSZER BIZTONSÁGI ANALÍZISE

Krasznay Csaba, krasznay@ik.bme.hu
Szigeti Szabolcs, szigi@ik.bme.hu
Budapesti Műszaki és Gazdaságtudományi Egyetem Informatikai Központ

A Ket. végrehajtási rendeletei

Az elektronikus közigazgatás Magyarországon nagy lökést kapott az új Közigazgatási Eljárási Törvény (Ket.) 2005. novemberi életbe lépésével. Elindult az Ügyfélkapu, valamint az azon keresztül elérhető elektronikus közigazgatási szolgáltatások egyre bővülő halmaza. Ezek az interneten elérhető szolgáltatások azonban új biztonsági kihívásokat is jelentenek az üzemeltetőknek.

Az általános biztonsági alapelvek használatának szükségességét a Ket. 195/2005 (IX. 22.) számú kormányrendelet írja elő, mely az informatikai rendszerek biztonsága mellett ezek együttműködő-képességéről is rendelkezik. A jogszabály kimondottan az elektronikus ügyintézés eszközeit szabályozza, melyek felügyelete a Miniszterelnöki Hivatalt vezető miniszter illetve az informatikai és hírközlési miniszter hatáskörébe tartozik.

A rendelet IV. fejezete foglalkozik a minőségirányítási követelményekkel. Követelményként jelenik meg az informatikai rendszerek átgondolt tervezése és tervszerű üzemeltetése. Bár csak utalás található rá, a jogalkotó feltehetőleg az ISO 9001 és az ISO 17799-es szabványokat vette alapul a követelmények megalkotásánál, azonban ezen szabványok szerinti minősítések megszerzése nem kötelessége, csak lehetősége a hivataloknak, és valószínű, hogy ezek a szabványok nem is alkalmazhatóak egy az egyben erre a környezetre. Általános gond egy nagy szervezetnél, hogy a folyamatok jelentős része nem dokumentált. A rendeletben ezeknek a dokumentációknak a fontossága hangsúlyosan szerepel. Előírják a kockázatelemzést is, melyet kétévente kell elvégeznie a hatóságoknak. Ezek alapján biztonsági osztályokba kell sorolni a különböző tevékenységeket. Mivel várhatóan a hatóságoknál nem lesz meg a humán erőforrás ezeknek az előírásoknak a betartására, a jogszabály előrelátóan szabályozza ezen tevékenységek kiszervezésének feltételeit is.

A biztonsági követelményekkel foglalkozó V. fejezet az ügyfél azonosításának kérdésével kezdődik. Ez gyakorlatilag az SSL kapcsolatok és az egyedi azonosítók, időbélyegzők használatát írja elő. A további bekezdésekben a rendelet foglalkozik a naplózás, az üzletmenet-folytonosság, a mentés és az archiválás kérdéseivel. Külön kiemeli az elektronikusan aláírt dokumentumok archiválásának fontosságát is. Előírja a vírusvédelem használatát is. A szabályok lehetőséget nyújtanak a titkosított adattovábbításra. A hozzáférési és fizikai biztonság megfelelő kialakítása is része a követelményeknek.

A VI. fejezetben jelennek meg az interoperabilitás kérdései. A jogalkotó felismerte annak a helyzetnek a tarthatatlanságát, hogy egy országon belül az egymással összefüggő folyamatok különböző formátumokat használnak, így gyakorlatilag ellehetetlenítsék a hatékony elektronikus közigazgatás kialakulását. A jogszabály nem írja elő kötelezően az együttműködést, de ajánlja azt, lehetőleg a nemzetközi nyílt szabványok alapján.

Összességében ez a rendelet nagyon fontos területet próbál meg szabályozni, melyre régóta szükség volt. Előnye, hogy az informatikai biztonságot egységesen kezeli, nem ragad ki egyes részeket belőle. Folyamatosan készülnek el a műszaki specifikációk is, melyekből az elektronikus közigazgatási rendszerek fejlesztői építkezni tudnak. A rendelet betartását a folyamatban levő rendszerfejlesztéseknél 2007. novemberéig kell megoldani, új rendszereknél viszont már maradéktalanul figyelembe kell venni. Érdekes lehet áttekinteni azonban, hogy néhány, már működő rendszernél mennyire vették figyelembe a biztonságot. Mivel külső szemlélőként csak az állampolgár és a hivatal közötti interfészt lehet megvizsgálni, a továbbiakban ezek analízisét folytatjuk le.

Az Ügyfélkapu analízise

A magyar elektronikus közigazgatás zászlóshajója a kormányzati portálon elérhető Ügyfélkapu, mely arra hivatott, hogy ezen keresztül legyenek elérhetők a független hivatalok szolgáltatásai. Jelenleg az APEH, a Belügyminisztérium okmányirodai rendszerét és a felsőoktatási felvételi rendszert lehet közvetlenül igénybe venni az Ügyfélkapun keresztül.

De mi is az Ügyfélkapu? Több értelmezés látott már napvilágot a szakmai körökben. Egyesek egy olyan portálnak tekintik, mely az országban található, egymástól függetlenül fejlődő e-közigazgatási rendszerek elérhetőségeit tárolja. Ennek a funkciónak azonban nem tesz eleget, hiszen pl. több önkormányzati rendszer nem érhető el róla. Mások egy single sign-on (SSO) beléptető rendszernek gondolják, azonban műszakilag ennek a kritériumait sem teljesíti, hiszen pl. az APEH rendszerénél az Ügyfélkapus belépés után további hitelesítésre van szükség. Valójában az Ügyfélkapu a felsorolt két funkciónak az ötvözete, melyek közül technikailag egyiket sem oldja meg tökéletesen.

Az SSO funkcióra érdemes inkább koncentrálni, hiszen a jogszabályok alakulása szerint inkább ebbe az irányba mozdul majd el a rendszer. Definíció szerint a single sign-on a szoftveres autentikációnak egy olyan speciális formája, mely a felhasználókat egyszer hitelesítve több szoftveres rendszer szolgáltatásaihoz engedi hozzáférni. A hitelesítés (authentication) az a folyamat, melynek során egy számítógép, számítógépes program vagy egy másik felhasználó megpróbál meggyőződni arról, hogy az a számítógép, számítógépes program vagy felhasználó, aki kapcsolatba akar lépni vele, az-e, akinek állítja magát. Ezt előzi meg az azonosítás (identification), melynek során az ügyfél személyazonosságát oly módon kell alátámasztani, hogy az elektronikus azonosítás egy korábban, hitelesítés-szolgáltató vagy a regisztrációs szerv által végzett, az ügyfél személyes megjelenését igénylő személyazonosításhoz legyen köthető, azaz ez vagy elektronikus aláírással, vagy okmányirodai megjelenéssel teljesíthető.

Az azonosítás jogszabályilag alaposan körbe van járva, ezért nem érdemes különösen kielemezni. Az igazi szakmai problémák a hitelesítésnél kezdődnek. Az informatikai biztonság egyik alaptétele a kétlépcsős hitelesítés. Ez olyan protokollt jelent, mely két egymástól független módon állapítja meg a személyazonosságot és a jogosultságokat. Alapvetően három tényezővel hitelesíthető valaki: tudás alapján (pl. jelszó), birtok alapján (pl. egy intelligens kártya, amit birtokol) vagy biometrikus jellemzők alapján (pl. ujjlenyomat).

Ebből kell legalább két, egymástól független módszert alkalmazni a biztonságos hitelesítéshez.

Természetesen kockázatelemzéssel kell eldönteni, hogy milyen megoldást kell használni. A jól működő elektronikus közigazgatásban nincs szükség az állampolgár jelenlétére az ügyintézéshez, a folyamatokat azonban nagyon át kell gondolni biztonsági szempontból. Ez azt jelenti, hogy pl. egy születési anyakönyvi kivonatot interneten lehet igényelni, amit a hivatal postán küld ki az állampolgárnak. Mivel a születési anyakönyvi kivonat nem tartalmaz fényképet, ha illetéktelen kezekbe kerül, akár visszaélések is elkövethetők vele, pl. új személyi igazolványt lehet vele igényelni. Egy hiteles személyi igazolvány pedig nagy érték a bűnözőknek. Ebből a példából is látszik, hogy a jól működő e-közigazgatási rendszereknél igenis a lehető legkomolyabb hitelesítési eljárásokat kell alkalmazni. Az Ügyfélkapun kétféle megoldást láthatunk. Egyik az egylépcsős jelszó, azaz tudásalapú megoldás, melyet okmányirodai azonosítás után lehet megkapni, a másik egy kétlépcsős, jelszó és elektronikus aláírással kombinált, azaz tudás és birtok alapú hitelesítés, melyhez nem szükséges személyes megjelenés az okmányirodában. Látszik, hogy a második megoldás képviseli elvileg a biztonságosabb megoldást. A gyakorlat azonban az, hogy az Ügyfélkapu üzemeltetői nem hangsúlyozzák a második megoldás biztonságosabb voltát, sőt az ügyfeleknek sokszor úgy tűnhet, hogy az elektronikus aláírás csak megkeseríti az életüket, hiszen a szerzők tapasztalatai szerint az Ügyfélkapu elektronikus aláíró szoftverének rendelkezésre állása minősíthetetlenül alacsony, ráadásul adminisztratív eszközökkel még nehezítik is a felhasználását.

Mielőtt a kétlépcsős megoldást elemeznénk, tekintsük át, milyen veszélyeket rejt magában az egylépcsős hitelesítés. Az Ügyfélkapu felhasználóinak 99%-a jelenleg ezt a megoldást használja. Az APEH 2005/4-es tájékoztatója, mely „Veszélyes lehet a túlzott bizalom” címmel jelent meg, időben figyelmeztet arra a veszélyre, hogy ha egy állampolgár Ügyfélkapus azonosítója kikerül idegen személyhez, azaz pl. megadja a jelszavát a könyvelőjének, az nemcsak az adóbevallását nyújthatja be, hanem az ő nevében más államigazgatási eljárásokat is kezdeményezhet. Az Ügyfélkapu felhasználóinak a nevében tehát – a szolgáltatások adta lehetőségeken belül – bármit meg lehet tenni a jelszó ismeretében. Szakmai körökben pedig igen jól ismerik azokat az ún. social engineering (az emberi tényezőt, hiszékenységet kihasználó) támadásokat, amikkel a felhasználóktól meg lehet szerezni ezeket a jelszavakat.

A legdivatosabb social engineer támadás az ún. phising, azaz adathalász támadás. A phising célja olyan érzékeny adatok megszerzése, mint a jelszavak vagy bankkártya számok oly módon, hogy ezeket az adatokat hivatalos elektronikus kommunikációnak álcázva kérik a felhasználóktól, akik önként adják azt át. Ha az Ügyfélkapu felhasználóinak száma elér egy kritikus pontot, nagy valószínűséggel megjósolható egy olyan támadás bekövetkezése, amikor a magyar felhasználók tömegével kapnak olyan e-maileket, melyek Ügyfélkapus fejléccel közlik a címzettekkel, hogy egy rendszerhiba miatt eltűntek a jelszavak az adatbázisból, ezért legyenek szívesek az e-mailben található linkre kattintatni, és az ott található űrlapon beírni a felhasználónevüket és jelszavukat. A link mutathat pl. a www.magyarorszag.hn hondurasi domain névre, esetleg egy Verisigntól szerzett SSL kulccsal hitelesítve, így az átlagos felhasználó észre sem fogja venni, hogy nem a hivatalos oldalt nézi. Az ilyen csalások már több milliárd dollárnyi kárt okoztak, a leghatékonyabban internetes banki rendszerek, illetve ún. identity theft (identitáslopás) támadásoknál használhatók fel.

Itt pedig vissza is értünk az APEH közleményének érdemi részéhez. Az identitáslopás ugyanis az áldozat személyi adataival való visszaélés, melynek kivédésére egész Európában a személyi igazolványok szolgálnak. A nem megfelelő hitelesítéssel ezt a biztonságot veszítjük el, hiszen a rendszer a megfelelő jelszó birtokában korábban azonosítottnak tart bennünket, így hozzáférést enged az elektronikus közigazgatási rendszerhez.

Minden támadásba maximum annyi pénzt érdemes fektetni, amennyi hasznot az a támadás hozhat. A fenti social engineer támadás kis befektetés mellett nagy haszonnal kecsegtet. Emellett számos „hagyományos" informatikai támadásnak van még kitéve az egylépcsős azonosítás. A teljesség igénye nélkül említsük meg a célzott trójai programokat, amiket egy Zafi.A-hoz hasonló lokális, csak magyar féreg terjeszthet. A trójain keresztül működő jelszólopó alkalmazás megírása nem nagy feladat egy hozzáértőnek. Belső hálózaton, ahol sokan használják az Ügyfélkaput, a Man-in-the-middle (beékelődéses) támadással még a titkosított adatcsatornán keresztül is megszerezhetők a jelszavak. Nehezebben kivitelezhető támadás, és napjainkban kevésbé hatékony, de elvileg lehetőség van a phising támadáshoz hasonló eredményt elérni a DNS cache poisoning támadással is. Ekkor egy módosított DNS válasszal a felhasználó akkor is a hamisított weboldalra lesz irányítva, ha a jó címet írja be a böngészőjébe. A támadás kivitelezésére számtalan műszaki megoldás létezik, ezért rendkívül fontos, hogy ne egy-egy partikuláris megoldás ellen védekezzünk, hanem a rendszer biztonsági szintje legyen olyan, amely általában megakadályozza a sikeres támadást.

Az Ügyfélkapu tehát magában hordozza mindezeket a veszélyeztetettségeket. Állíthatjuk, hogy az első támadás bekövetkezésének ideje csak attól függ, hogy mikor lehet nagy haszonnal végrehajtani az információszerzést. Ráadásul mindegyik megoldás az állampolgárokra fókuszál, melyet nem lehet az Ügyfélkapu biztonsági elemeinek fejlesztésével kiküszöbölni. El kell kezdeni tudatosan áttérni a kétlépcsős azonosításra.

A kétlépcsős azonosítás jelenleg az Ügyfélkapun az elektronikus aláíráson alapul. A felhasználó beírja a jelszavát, majd egy felugró ablakban elektronikusan aláír egy űrlapot, mellyel elismeri, hogy belépett a rendszerbe. Ez elméletileg jó megoldás, hiszen tudás és birtok alapú a hitelesítés. Két gond van azonban: az egyik, hogy a digitális aláírást ilyen esetben nem így szokták használni, a másik, hogy a saját, majdnem egy éves tapasztalataink alapján a lehető legritkábban működik az elektronikus aláíró szoftver.

A nyílt kulcsú infrastruktúra három alapvető dolgot teljesít: a bizalmasságot (azaz lehet vele titkosítani), a sértetlenséget (azaz lehet vele digitálisan aláírni) és a hitelességet. A hitelességet műszakilag az ún. challenge-response (kérdés-válasz) megoldással oldják meg. Ekkor a szerver küld egy kérdést (bitsorozatot), melyet a felhasználó a titkos kulcsával titkosít, és visszaküldi a szervernek. A szerver a nyilvános kulccsal visszafejti a bitsorozatot, és ha az az, amit elküldött, engedi hozzáférni a felhasználót a rendszerhez. Az Ügyfélkapu mostani megoldása fából vaskarika. Mivel az Elektronikus aláírás törvény szerint az elektronikus aláírásra szolgáló titkos kulcsot ilyen megoldásra nem lehet használni, a hagyományos challenge-response helyett egy űrlap aláírása lett az autentikáció alapja. Ehhez természetesen külön szoftverre volt szükségük a rendszerfejlesztőknek, ahelyett, hogy bármelyik operációs rendszerből, mindegyik böngészőbe beépített szolgáltatást használtak volna fel. A jelenleg alkalmazott elektronikus aláíró szoftver így csak Windows/Internet Explorer alól érhető el, meglehetősen sztochasztikusan, ami feltehetőleg a rendszer üzemeltetőinek a felelőssége.

Az Ügyfélkapu tehát egy nem biztonságos és egy biztonságos, de technikailag, szakmailag nehezen kezelhető hitelesítési megoldást tartalmaz. A rendszer tervezőinek, üzemeltetőinek ezért komoly a felelőssége abban, hogy az esetleges támadásokat kivédjék. Az, hogy jelenleg ilyen a rendszer, nem elsősorban a műszaki tervezőknek köszönhető, hanem a magyar adatvédelmi szabályoknak valamint a közigazgatáson belüli szétoszló hatásköröknek és felelősségeknek. Ahelyett, hogy a jó műszaki gyakorlatokhoz igazították volna a jogszabályokat, a jogszabályokhoz kellett kitalálni egy informatikai „Frankensteint". A javítás lehetősége azonban adott, bízzunk benne, hogy a megfelelő átalakítások tervei már a felelősök asztalán vannak.

Egyéb megoldások

Sajnos azonban el lehet mondani, hogy létezik ennél rosszabb megoldás is hazánkban. Az Egységes Magyar Munkaügyi Adatbázis, melyben elvileg a magyar munkavállalók jelentős részének személyes adatai szerepelnek, az Ügyfélkapunál lényegesen gyengébb hitelesítési technikát használ. A felhasználónév a cég adóazonosítója, mely nyilvános adat. A jelszó egy 5 számjegyből álló PIN kód. Ez összesen 100000 lehetséges kódot jelent, melyet célzott támadással néhány perc alatt brute force (nyers erő) módszerrel fel lehet törni. Mivel a rendszer látszólag semmi védelmet nem nyújt ez ellen, azaz nem tilt le három próbálkozás után, nem növeli a próbálkozások közötti időt, ideális terep egy kezdő hackernek. Hozzá kell tenni, hogy ebben az esetben a védelem a szolgáltató oldaláról növelhető, azonban a nyilvános információk alapján ilyen támadás kivédésére nem készültek fel.

Két jelentős negatív példa után lássuk, hogyan lehetne védekezni! Az ideális megoldás egy kétlépcsős hitelesítés megvalósítása lenne. Erre Magyarországon számos példát láthatunk. Elég bármelyik magyar bank internetes rendszerét megnézni. Van, ahol már a beléptetésnél, de legkésőbb a tranzakció elkezdésénél felhasználják a mobiltelefont. A Nemzeti Hírközlési Hatóság adatai alapján 2005 decemberében 9.320.169 aktív SIM kártya volt az országban. Azaz gyakorlatilag minden magyar állampolgár rendelkezik egy olyan eszközzel, mely a birtok alapú azonosításhoz felhasználható. A banki rendszerekben működő megoldással minden fenti támadási lehetőség kivédhető, hiszen az ügyintézéshez egy SMS-ben kapott, internetes csatornától független információ szükséges. Ilyen megoldásra egyetlen jogszabályban vagy ajánlásban még csak utalás sincs, szemben például az elektronikus aláírás túlzott szabályozásával, amely téma az öt informatikai tárgyú végrehajtási rendelet mindegyikében megjelenik, holott csak néhány százan, nagy jóindulattal néhány ezren használják azt.

A másik ideális megoldás, melyet pl. a szlovén kormányzati portálon használnak, a tanúsítvány alapú challenge-response hitelesítés, amit a fentiekben vázoltunk. Ekkor az intelligens kártyán (pl. személyi igazolvány) található egy elektronikus aláíráshoz és egy hitelesítéshez használható titkos kulcs. A hitelesítési kulcsot beléptetéshez, a másikat az elektronikus ügyiratok aláírásához használják. Erre vonatkozó kezdeményezés már volt Magyarországon is, a tanulmányként elérhető „IAS - Egységes specifikációk az eKözigazgatás kommunikációjának hitelességére" dokumentumban, azonban ezt nem vezették be.

Pozitív magyar példa Angyalföld és Ferencváros önkormányzata, ahol az elektronikus aláírást úgy használják, ahogy rendeltetésszerűen kell. Kitöltött elektronikus űrlapokat lehet elektronikusan aláírni, így azok hitelesek lesznek. Ezzel a papíralapú kommunikáció megszűnhet állampolgár és hivatal között. A végcél ez lenne, ehhez azonban alapos

szemléletváltás szükséges a jogalkotóknál. Amíg ez nem történik meg, a súlyos lemaradásunk a többi Európai Uniós országhoz megmarad, sőt folyamatosan növekedni fog.

Köszönetnyilvánítás

A mű a Nemzeti Kutatási és Technológiai Hivatal Támogatásával valósult meg. Külön köszönet illeti Sikolya Zsolt urat, az Informatikai és Hírközlési Minisztérium munkatársát, aki a jogi háttér feltárásánál segítette munkánkat.

Irodalomjegyzék

[1] 195/2005 (IX. 22.) Korm. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról

[2] „Veszélyes lehet a túlzott bizalom”, Tájékoztató 2005/4, Adó- és Pénzügyi Ellenőrzési Hivatal, http://www.apeh.hu/megyek/veszprem/hirlevel/dec_15_veszelyeslehetatulzott.pdf

[3] Single sign-on definition, Wikipedia, http://en.wikipedia.org/wiki/Single_sign_on

[4] Authentication definition, Wikipedia, http://en.wikipedia.org/wiki/Authentication

[5] 193/2005 (IX. 22.) Korm. rendelet az elektronikus ügyintézés részletes szabályairól

[6] Two-factor authentication, Wikipedia, http://en.wikipedia.org/wiki/Two-factor_authentication

[7] Phising definition, Wikipedia, http://en.wikipedia.org/wiki/Phising

[8] Identity theft definition, Wikipedia, http://en.wikipedia.org/wiki/Identity_theft

[9] Challenge-response authentication definition, Wikipedia, http://en.wikipedia.org/wiki/Challenge_response

[10] Državni portal e-uprava, http://e-uprava.gov.si/e-uprava/

[11] Ferencváros e-önkormányzat, http://www.ferencvaros.hu/eonko/

[12] Angyalföld e-önkormányzat http://www.bp13.hu/wps/portal/e-onkormanyzat