HADMÉRNÖK

IV. Évfolyam 4. szám - 2009. december

Krasznay Csaba
csaba@krasznay.hu

SZOFTVERFEJLESZTŐI KÖVETELMÉNYEK MINŐSÍTETT KÖRNYEZETBEN: ADMINISZTRATÍV KÖVETELMÉNYEK

Absztrakt

A közigazgatás elektronizálása korábban nem látott ütemű és kiterjedtségű szoftverfejlesztéseket tett szükségessé olyan környezetekben is, melyek a Magyar Köztársaság működése szempontjából közvetve vagy közvetlenül kritikusak. A kifejlesztésre kerülő rendszerek azonban a legtöbbször nem szigetszerűen működnek, közvetlenül nem kezelnek állam- és szolgálati titkokat, így nem érvényesek rá a Titokvédelmi Törvény elvárásai. Jelen tanulmány bemutatja, hogy milyen személyi, szervezeti és szabályzati követelményeket kell szabni azon fejlesztőkkel és a fejlesztői környezettel szemben, akik ilyen, többnyire a 143/2004-es kormányrendelet keretében dolgoznak.

Electronization of public administration needs such enormous software developments as never before in high level security environments which are directly or indirectly critical for the normal operation of the Hungarian Republic. Most newly developed system doesn't operate alone, doesn't handle state secrets directly so the requirements of the State Secrets Protection Act are not valid for this area. The study, which is the first part of a two-part series, presents personnel, organizational and policy requirements for those developers and environments who work in the context of Edict 143/2004 about public procurement related to state secrets.

Kulcsszavak: *közigazgatás, szoftver fejlesztés ~ public administration, software development*

Bevezetés

Napjaink általános szoftverfejlesztéseiről – melyek közé a legtöbb e-közigazgatási projekt is tartozik – elmondható, hogy bár a biztonság erős kritériumként jelenik meg, ez elsősorban a fejlesztett funkciókra és nem a fejlesztői környezetre vonatkozik. Pedig gyakori, hogy a fejlesztők nem egy adott telephelyen dolgoznak, hanem otthonról, internetes kapcsolaton keresztül, nem kontrollált munkaállomásokon, hanem saját számítógépen, és olyan fejlesztést segítő eszközök felhasználásával, melyek a projekt általános biztonsági szintjének az elvárásit nem teljesítik. Ennek eredménye, hogy a kódok nem megfelelően kontrollált környezetben keletkeznek, továbbítódnak és tárolódnak, így komoly, akár egy-egy kritikus államigazgatási folyamatot is érintő bizalmassági és sértetlenségi kockázatok jelentkeznek.

A szoftverfejlesztési életciklus biztonsági vonatkozású része minden esetben egy kockázatelemzéssel kezdődik, melynek során fel kell mérni, hogy a kifejlesztésre kerülő termék pontosan milyen információs vagyont fog kezelni. Az életciklus során végig figyelembe kell venni az információs vagyon besorolását, tehát nem elégséges, hogy csak az élesüzemű működés során gondoskodunk a megfelelő védelemről. Már a tervezéstől kezdve folyamatosan biztosítani kell, hogy bármilyen, a rendszerrel kapcsolatos információ olyan védelmi szintű biztosítást kapjon, amilyet majd a végleges rendszer kap. A fejlesztői környezet kialakításánál tehát fő elvként az éles rendszerrel kell párhuzamot vonni. Azok az alkalmazások, melyeket köztisztviselők tízezrei használnak majd az interneten keresztül, egészen más fejlesztői környezetben alakulhatnak ki, mint azok, melyeket csak néhány száz felhasználó láthat szeparált, lokális hálózatról. A tanulmányban éppen ezért három védelmi szintet lehet meghatározni, mely megfelel a Közigazgatási Informatikai Bizottság (továbbiakban KIB) 25. [1] és 28. számú ajánlásában [2] leírt három szintnek: az államtitkot feldolgozó rendszerek (kiemelt), a belső használatú, bizalmas információkat kezelő rendszerek (fokozott), valamint a széles körben, interneten keresztüli hozzáférést biztosító rendszerek (alap) fejlesztőire határozunk meg követelményeket.

Jogszabályi követelmények

Az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. kormányrendelet [143/2004. (IV. 29.) Korm. rendelet az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól] (a továbbiakban: Rendelet) hatálya azokra a Közbeszerzési törvény [2003. évi CXXIX. törvény a közbeszerzésekről] (a továbbiakban: Kbt.) szerinti egyszerű közbeszerzési eljárás mindenkori értékhatárait elérő vagy azt meghaladó értékű beszerzésekre terjed ki, melyek – a Rendelet címének megfelelően – államtitkot, szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintenek, illetve különleges biztonsági intézkedést igényelnek.

A Rendelet értelmező részében kerül meghatározásra két, máshol nem definiált fogalom, az alapvető biztonsági érdeket érintő és a különleges biztonsági intézkedést igénylő beszerzés fogalma. Az ország alapvető biztonsági érdekével kapcsolatos a beszerzés, ha a beszerzés tárgya közvetlenül kapcsolódik az ország lakosságának fizikai, környezeti, egészségügyi, gazdasági, honvédelmi biztonságát befolyásolni képes építési beruházáshoz, árubeszerzéshez, illetőleg szolgáltatás megrendeléséhez. Különleges biztonsági intézkedést igényel a beszerzés, ha a beszerzés tárgyának előállításánál, az előállításhoz szükséges alapanyagok és termékek szállításánál, illetőleg a felhasználásnál, a beszerzés tárgyának szállításánál hatóság vagy

jogszabály különleges követelményt ír elő, illetve az általánostól eltérő élőerős vagy technikai ellenőrzés szükséges. Azért is fontos ez a két fogalom, mert akkor is lehetővé teszi a Rendelet alkalmazását, ha a beszerzés tárgya államtitkot, szolgálati titkot, illetőleg nemzetbiztonsági érdeket nem érint.

A Rendelet nagyon részletesen szabályozza az ajánlattevők ellenőrzését, magát a beszerzési eljárást, de a beszerzési eljárás utáni, a teljesítés biztonsági követelményeire vonatkozó előírást, vagy elvárást nem ad. Persze erre nem is lenne szükség, ha ezek a követelmények máshol megjelennének. Nézzük részletesen a követelményekre vonatkozó előírásokat informatikai fejlesztések esetén.

Ha a beszerzés államtitkot, szolgálati titkot érint, akkor az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény (a továbbiakban: titoktörvény), továbbá a minősített adat kezelésének rendjéről szóló 79/1995. (VI. 30.) Korm. rendelet lenne a mérvadó. Jelenleg azonban ezek a jogszabályok nem jutnak érvényre, tudniillik a titoktörvény 30. §-ának (2) bekezdése előírja, hogy a "Kormány - az érintett állami szervek vezetőivel egyetértésben - a minősített adatot kezelő információs rendszerek létesítésének és működésének rendjét 1995. december 31-ig határozza meg". Ez a nemzeti titkaink vonatkozásában a mai napig nem történt meg. A titoktörvény új változata 2002 óta parlament általi elfogadásra vár. Emiatt a kormány már nem kíván a régi titoktörvény szerinti szabályozással foglalkozni.

Ez viszont azt jelenti, hogy a nemzeti titkaink vonatkozásában nincs érvényes jogi előírás erre a területre vonatkozóan. Persze van azért ebben a témakörben – nem jogi, hanem logikai alapon –felhasználható előírás. A rejtjeltevékenységről szóló 43/1994. (III. 29.) Korm. rendelet 16. § (1) bekezdése például a rejtjelzőeszközök vonatkozásában előírja, hogy "fejlesztő, gyártó, javító munkahelyet … megfelelően őrzött, illetve megfelelő biztonsági felszerelésekkel ellátott, elkülönített helyiségben kell elhelyezni, ahová az oda beosztottakon kívül csak az irányítási és ellenőrzési joggal rendelkezők léphetnek be". A jelenleg hatályos magyar jogszabályokban a minősített adatot kezelő információs rendszerekre vonatkozóan más előírás nem található.

Ha a beszerzés alapvető biztonsági, nemzetbiztonsági érdeket érint, illetve különleges biztonsági intézkedést igényel, akkor sem találunk útmutatást a magyar jogszabályi rendszerben. Ugyanis az alapvető biztonsági, nemzetbiztonsági érdeket érintő beszerzések megvalósítása során követendő biztonsági elvárásokra nincs előírás. Tulajdonképpen a Rendelet szerinti valamennyi eljárásban a beszerzés tárgyának előállításánál, az előállításhoz szükséges alapanyagok és termékek szállításánál, illetőleg a felhasználásnál, a beszerzés tárgyának szállításánál az ajánlatkérőnek – esetleg az illetékes nemzetbiztonsági szolgálatnak – kellene különleges követelményt előírni. Ilyen követelményrendszernek azonban semmilyen nyilvános említése nem ismert.

Személyi és szervezeti követelmények

Mindhárom környezetben közös, hogy nem szabad a fejlesztőknek előzetes kontroll nélkül hozzáférést adni a fejlesztői környezethez, nem lehet őket felügyelet nélkül dolgozni hagyni, és ki kell találni, hogy milyen módon lehet hozzáférésüket megszüntetni. Ehhez fel kell állítani egy olyan belső biztonsági irányítási és ellenőrzési szervezetet, mely a fejlesztőket munkájuk során kontrollálni tudja. Erre a KIB 25. számú ajánlásának 1-2. kötete [1] ad ajánlást, mely szerint ki kell jelölni a Biztonsági Vezetőt, az Informatikai Biztonsági Vezetőt, az Informatikai Biztonsági Fórumot, valamint a szakterületi (fejlesztési és üzemeltetési)

vezetőt. Ezt a biztonsággal kapcsolatos szervezeti felépítést mindhárom területen érdemes betartani.

A fejlesztéssel megbízott szervezet vezetője, vagy kiemelt projekteknél a fejlesztés projektvezetője az Informatikai Biztonsági Fórum vezetője, azaz a biztonsági terület elsődlegesen neki tartozik beszámolóval.

Feladata:

- hatályba lépteti az Információbiztonsági Szabályzatot,
- értékeli a kockázatelemzést,
- felülvizsgálja az információk osztályozását,
- meghatározza a munkavégzés helyszíneit,
- utasítja a vállalkozókat információbiztonsági kérdésekben,
- kezdeményezi a felhasználói jogosultságok visszavonását, elrendeli az azonnali visszavonást,
- engedélyezi új eszközök beszerzését,
- értékeli az incidenseket.

Felelős:

- az adatvagyonleltár naprakészen tartásáért,
- az információbiztonsági tudatosság építéséért,
- a speciális információbiztonsági tudás megszerzésének biztosításáért,
- a képzések értékeléséért,
- a szankcionálásért,
- a belső auditok elrendeléséért és értékeléséért.

Az Informatikai Biztonsági Fórumot, és általában a fejlesztési projektet egy adminisztratív szervezet, a projektiroda támogatja, akiknek szerepet lehet adni a biztonsági keretrendszerben is.

Feladata:

- hardver- és szoftvereszközök nyilvántartása,
- a belépési naplók archiválása,
- a jogosultságok nyilvántartása,
- a forráskódok őrzése,
- az üzemeltetési feljegyzések őrzése.

Felelős:

- a jogosultságok kiadásáért és visszavonásáért.

A Biztonsági Vezető és az Informatikai Biztonsági Vezető szerepkört ugyanaz a személy is betöltheti az ajánlás szerint. A fejlesztési környezet biztonsági aspektusaiért elsősorban ő a felelős.

Feladata:

- az adatvagyonleltár elkészítésének támogatása,
- védelmi intézkedések megfogalmazása,
- az Informatikai Biztonsági Fórum és a fejlesztési/üzemeltetési vezető támogatása információbiztonsági kérdésekben,
- a vagyontárgyak kiadásának és visszavételének felügyelete,
- a kiemelt jogosultságok ellenőrzése,
- a karbantartási terv jóváhagyása.

Felelős

- az adatvagyonleltár rendszeres felülvizsgálatáért,
- a kockázatelemzés elkészítéséért,
- a sebezhetőségvizsgálat elkészítéséért,
- a védelmi intézkedések bevezetéséért,
- a vállalkozók információbiztonsági szabályzatainak felülvizsgálatáért,
- az Informatikai Felhasználói Szabályzat kidolgozásáért és karbantartásáért,
- az információbiztonsági oktatásokért,
- a belső auditok végrehajtásáért,
- a szabálysértések kivizsgálásáért,
- vállalkozók telephelyeinek ellenőrzéséért,
- az információbiztonsági eszközök karbantartásáért,
- a jogosultságok ellenőrzéséért,
- az üzemeltetés és a fejlesztés biztonsági ellenőrzéséért,
- az új rendszerek biztonságos üzembe állításáért,
- a megfelelő visszaállításért,
- az információbiztonsági incidensek kezeléséért,
- az üzletmenet-folytonossági intézkedések kialakításáért.

A fejlesztési vezető elsősorban az alkalmazás biztonságáért felelős, a fejlesztői környezet biztonságával kapcsolatban viszonylag kevés feladata van.

Feladata:

- A fejlesztés során keletkezett információk Információbiztonsági Szabályzat szerinti kezelése

- A Biztonsági Vezető és az Üzemeltetési Vezető támogatása az Információbiztonsági Szabályzatban leírtak teljesítésében.

Felelős:

- A fejlesztés során keletkezett információk minősítéséért,
- A fejlesztői jogosultságok kiosztásáért

Az Üzemeltetési Vezető az a személy, aki a fejlesztéshez használt eszközök üzemeltetéséért felelős. A Biztonsági Vezetővel közösen felel a biztonságos fejlesztői környezet kialakításáért.

Feladata:

- a projektiroda támogatása,
- új eszközök specifikálása,
- az erőforrás-kihasználás ellenőrzése,
- az incidensek értékelése.

Felelős:

- a kiemelt jogosultságokért,
- az üzemeltetési folyamatokért,
- a rendszerfejlesztés koordinálásáért,
- az üzemeltetési rend kialakításáért,
- a vírusvédelemért,
- a mentésekért,
- a visszaállításért,
- a határvédelmi eszközök üzemeltetéséért,
- a karbantartásért,
- a hibabejelentések kezeléséért.

Fontos, hogy ezek a szerepkörök megfelelően megbízhatók legyenek, ezért a szerződéskötés során nevesíteni és ellenőrizni kell őket. A projektvezető a közigazgatási fejlesztések esetén mindenkor nemzetbiztonsági ellenőrzésen esik át, alap esetben A típusú, fokozott esetben B típusú, kiemelt esetben C típusú átvilágítást kell igazolnia. A projektiroda munkatársai, a Biztonsági, Fejlesztési és Üzemeltetési vezető alap estben erkölcsi bizonyítvány benyújtására kötelezett, fokozott esetben A típusú, kiemelt esetben B típusú átvilágításon kell átesniük. A Biztonsági Vezetőnek emellett rendelkeznie kell az ISACA Certified Information System Manager (CISM) vizsgájával, mely nemzetközileg elfogadott biztosítékot ad arról, hogy képes feladatát teljesíteni. Kiemelt szinten a Biztonsági Vezető a felelős a titkos ügyiratkezelésért is, ezért Titkos ügykezelő bizonyítvánnyal kell rendelkeznie.

A fejlesztésben résztvevő, valamint a fejlesztői környezetet üzemeltető személyek ellenőrzése is kritikus. Alap és fokozott esetben minden érintettnek erkölcsi bizonyítvánnyal kell rendelkeznie, be kell nyújtania önéletrajzát és iskolai bizonyítványait. Fokozott esetben a

vállalkozónak háttérellenőrzéssel kell ezeket kiegészíteni, mely során meggyőződik a benyújtott iratok és információk hitelességéről, valamint nyílt források felhasználásával győződik meg az érintett megbízhatóságáról. Kiemelt esetben mind a fejlesztőknek, mind az üzemeltetőknek B típusú nemzetbiztonsági ellenőrzést kell teljesíteniük.

Szabályzati követelmények

Mivel a megrendelőnek érdemi beleszólása nincsen a fejlesztés folyamatába, így szerződéses feltételként kell megfogalmaznia azt az igényét, hogy a fejlesztés biztonságát ellenőrizhesse. Erre három lehetséges megoldás van.

- Előírhatja a Common Criteria vagy KIB 25. szerinti fejlesztést, melynek részeként a megrendelő által megbízott auditor ellenőrizheti a fejlesztés biztonsági környezetét. Hátránya, hogy a Common Criteria módszertan nem szab konkrét követelményeket, deklaráltan az auditorra van bízva annak eldöntése, hogy a környezet megfelelően biztonságos vagy nem az, de azért a szabályozandó területeket meghatározza. Alap, közép és kiemelt szinten is kötelező lehet.

- Elrendelheti a fejlesztés nemzetbiztonsági ellenőrzését. Ilyenkor a teljes fejlesztési folyamat kontrollálható, hátránya viszont, hogy még annyi viszonyítási alapja sincs a fejlesztőnek a környezet kialakításához, mint a Common Criteria esetében. Fokozott szinten opcionális, kiemelt szinten kötelező lehet.

- Elvárhatja az ISO 27001-es tanúsítvány meglétét a fejlesztési folyamatra. Ekkor a megrendelő megbízik egy általa nem felkért harmadik személyben, és elfogadja, hogy a fejlesztő által benyújtott fejlesztés-biztonsági dokumentumok helytállóak. Ez a megoldás objektív, hiszen a szabvány konkrét védelmi intézkedéseket tartalmaz, melyek működésének ellenőrzése is szabvány szerint történik, hátránya viszont, hogy az értékelést végzővel semmilyen közvetlen kapcsolata nincs a megbízónak. Alap szinten opcionális, fokozott és kiemelt szinten kötelező lehet.

Mindhárom esetben elvárható az alkalmazás fejlesztőjétől, hogy biztonsági tevékenységeit megfelelően dokumentálja. A legkézenfekvőbb megoldás erre egy olyan szabályzati rendszer létrehozása, mely kielégíti mind a szabványok, mind a jogszabályok jelentette követelményeket. A KIB 25. ajánlás Informatikai Biztonsági Irányítási Rendszerrel foglalkozó része pontosan megnevezi, hogy milyen elemekből kell állnia egy szabályzati rendszernek, melyet három szintre lehet osztani.

- **Informatikai Biztonsági Politika (IBP)**: „Az Informatikai Biztonsági Politika kinyilvánítja a menedzsment biztonság iránti elkötelezettségét, a biztonsági célt, valamint magas szintű biztonsági elvárásokat fogalmaz meg, amelyek a biztonsági cél elérését szolgálják, és amelyeket érvényesíteni kell a védelmi intézkedések specifikálása során.”

- **Informatikai Stratégia**: „Az Informatikai Biztonsági Stratégia célja, hogy a szervezet üzleti igényeinek jövőbeni változásaival összhangban meghatározza az információbiztonság fejlesztésének tervét (középtávú, hosszú távú).”

- **Informatikai Biztonsági Szabályzat (IBSZ)**: „Az Informatikai Biztonsági Szabályzat rögzíti az IBIR működéséhez, működtetéséhez szükséges folyamatokat,

megadja az érintett szereplők (pl.: információbiztonsági vezető, üzemeltető, rendszergazda, fejlesztési vezető, adatgazda stb.) feladatait, felelősségeit, hatásköreit. Rögzíti az információfeldolgozó rendszer elemeivel (dolgozók, alkalmazások, technológiai elemek, helyiségek stb.) kapcsolatos biztonsági követelményeket. Az Informatikai Biztonsági Szabályzatot olyan mélységig kell elkészíteni, hogy technológiafüggetlen tudjon maradni."

- **Informatikai Felhasználói Szabályzat (IFSZ)**: „A dokumentum részletesen szabályozza a felhasználók kötelességeit az informatikai eszközök használata során, meghatározza azokat a peremfeltételeket, melyek között a felhasználó kapcsolatot létesít az informatikai osztállyal, vagy az adatgazdákkal. A szabályzat részletesen kifejti a felhasználó által elvégezhető és tiltott tevékenységeket, megadja a számonkérés formáját és módját, rögzíti a biztonsági események jelentésével kapcsolatos kötelezettségeket."

- **Eljárásrend gyűjtemény**: „Az eljárásrend gyűjteménybe tartozó végrehajtási utasítások olyan alacsony szintű szabályzatok, amelyek részletesen, rendszer specifikusan rögzítik azokat a tevékenységeket, melyeket az informatikai biztonsági szabályzat rendszerfüggetlenül megkövetel."

Az IBP és a Stratégia alkotja a szabályzati rendszer első szintjét, az IBSZ és az IFSZ a másodikat, az eljárásrend pedig a harmadikat. Ezeknek koherens egészet kell alkotniuk, nem szabad ellentmondásokat létrehozni, melyről a fejlesztőket értékelő szervezetnek is meg kell győződnie.

A gyakorlatban a fejlesztési folyamatot nem kizárólag egy szervezet fedi le, hanem egy fővállalkozó és több alvállalkozó együttesen. Ilyenkor különösen nehéz megállapítani, hogy ki, mennyire tudja betartani az elvárt biztonsági szintet. Alapelvként a megrendelőnek arról kell meggyőződnie, hogy a fővállalkozó, aki elsődlegesen felelős a projekt sikeres végrehajtásáért, megfelelő szabályzati rendszerrel dolgozik. Az alvállalkozóknak minden esetben minimálisan a fővállalkozó szabályzataiban foglalt elveket kell teljesíteniük, ezeknél alacsonyabb biztonsági szint nem megengedett. Ez a megoldás kellően rugalmas, mégis biztonságos lehet.

Az alvállalkozók ellenőrzése minden esetben a projekt Biztonsági Vezetőjének a feladata, aki ezt belső auditok során teszi meg. A belső auditokról készített feljegyzések, valamint a szúrópróbaszerű ellenőrzés ad garanciát arra a megrendelő által megbízott külső auditornak, hogy a fejlesztésben részt vevő minden szervezet megfelelő biztonsági szinten dolgozik.

ÖSSZEFOGLALÁS

A tanulmányban bemutatásra került, hogy egy, a közigazgatás működése szempontjából fontos alkalmazás létrehozása során milyen szervezeti, személyi és szabályzati követelményeket kell betartania a fejlesztőknek. A cikk következő, második részében bemutatásra kerülnek azok a műszaki szabályok, melyekhez ebben a környezetben alkalmazkodni kell. Ehhez a jelenleg hatályos ajánlások szellemében kell szabályokat alkotni, ugyanis közvetlen előírások nincsenek ezen a területen.

Irodalomjegyzék

[1] Berkes, Z., Déri, Z., Krasznay, Cs., Muha, L. (2008): Közigazgatási Informatikai Bizottság 25. számú ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR)

[2] e-Közigazgatási Keretrendszer Kialakítása projekt (2008): A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár, IT biztonsági műszaki követelmények