Ügyszám: 2015/K/2007-3.

[…] részére

Tisztelt […]!

Konzultációs beadványában tanácsomat kéri a szakdolgozatával kapcsolatosan, melynek témája az intézményen belüli informatikai adatbiztonság. Szakdolgozatában felvázolt hipotézisek igazolására gyakorlatban is igazolni kívánja az informatikai rendszer sérülékenységét úgy, hogy az intézmény könyvtárának számítógépes rendszerét veszi célba, és a nyilvános terminálokra adatgyűjtő szoftvereket helyez el.

Az alábbi jogi háttérre kell tekintettel lennie:

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény rendelkezéseinek megfelelően kezelhet csak személyes adatokat. E törvény szerint személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete elrendeli.

Az adatgyűjtő szoftverek alkalmazásának célja, hogy a felhasználóra vonatkozóan személyes adatokat gyűjtsön. A törvény értelmében a szoftver telepítésével és használatával Ön adatkezelővé válik, és az Avtv. rendelkezései hatályosak lesznek az Ön tevékenységére. A kérdéses ügyben azonban nem értelmezhető sem a törvényi felhatalmazás, és az érintettek hozzájárulása is nehézkesen szerezhető be, hiszen a támadás feltételezi, hogy az érintettek tudta és beleegyezése nélkül történjék. Megfelelő jogalap nélkül azonban a tevékenység jogellenes lesz.

Továbbá az alábbi büntető törvényi tényállásokra is tekintettel kell lenni:

Visszaélés személyes adattal:

177/A. § (1) Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével

a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel,

b) az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget,

c) az adatok biztonságát szolgáló intézkedést elmulasztja,

és ezzel más vagy mások érdekeit jelentősen sérti, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(…)

(3) A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a személyes adattal visszaélést különleges személyes adatra követik el.

Számítástechnikai rendszer és adatok elleni bűncselekmény:

300/C. § (1) Aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(2) Aki

a) számítástechnikai rendszerben tárolt, feldolgozott, kezelt vagy továbbított adatot jogosulatlanul megváltoztat, töröl vagy hozzáférhetetlenné tesz,

b) adat bevitelével, továbbításával, megváltoztatásával, törlésével, illetőleg egyéb művelet végzésével a számítástechnikai rendszer működését jogosulatlanul akadályozza, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

(…)

Álláspontom szerint a számítástechnikai rendszer és adatok elleni bűncselekmény esetében a jogosulatlanul történő belépés illetve a jogosultság keretein való túllépés kiküszöbölhető, amennyiben az intézmény vezetésének felhatalmazásával teszteli a számítógépes rendszer biztonságát. Ezért az intézmény vezetésének engedélye elkerülhetetlen ahhoz, hogy megfelelő jogosultsággal bizonyítsa szakdolgozatában felvetett feltevései helyességét a gyakorlatban.

Azonban az intézmény részéről adott felhatalmazás sem elegendő azonban az adatgyűjtő szoftver esetére a felhasználók személyes adatai kezeléséhez. Az Avtv. értelmében a törvény célja annak biztosítása, hogy személyes adatával mindenki maga rendelkezzen. A személyes adatok védelméhez való jogot az Alkotmánybíróság információs önrendelkezési jogként értelmezte. Az érintettet megillető jog, hogy arról rendelkezzék, hogy személyes adatait kik, hol és milyen célra ismerhessék meg. A jog tehát kizárja annak lehetőségét, hogy az önrendelkezési jogot az érintett helyett más személy vagy szerv, vagy akár egy intézmény vezetősége gyakorolja. Az adatgyűjtő szoftver alkalmazásának lehetősége számos veszélyt hordoz magában, mert az intézmény tudomása ellenére is az érintettek beleegyezése nélkül jut személyes adatokhoz.

Megoldásként kínálkozik, ha az intézmény képviselőjének a jelenlétében (gyakorlati oktató) telepíti és teszteli az adatgyűjtő szoftvert néhány olyan érintett beleegyezésével, akik szoftver önkéntes „áldozataiként” adataik megadásával közreműködnek tesztelésben. A tesztelést követően azonban a szoftvert a visszaélések elkerülése érdekében szükséges eltávolítani. Ezzel az eljárással kivédhető, hogy a személyes adatokhoz jogellenesen jusson hozzá. Természetesen ez esetben az adatgyűjtő szoftver csak azoknak a személyeknek a személyes adatait szerezheti meg, akik a tesztelésben való részvételhez hozzájárultak. Álláspontom szerint egy ilyen rövid lefutású tesztelés is eredményesen igazolhatja egy informatikai rendszer sérülékenységét.

Egyebekben nyilvános terminálokra olyan szoftvert elhelyezni, amely személyes adatok gyűjtését végzi, sérti a felhasználók személyes adatok védelemhez fűződő jogát még akkor is, ha a gyűjtés nem hasztalan tevékenység, mert a felvetéseinek helyességét kívánja alátámasztani velük. Az adatvédelem oldaláról a törvényes határ ott húzódik, ahol Ön nem jut felhasználóra vonatkozó személyes adat birtokába vagy olyan felhasználók közreműködésével végzi, akik beleegyeztek adataik gyűjtésébe.

Remélem válaszaim hozzásegítették szakdolgozatának elkészítéshez. Adatvédelemmel kapcsolatos beadványával forduljon hozzám a jövőben is bizalommal.

Budapest, 2007. november 9.

Üdvözlettel:

Dr. Péterfalvi Attila