



## BIZTONSÁGOS? JÓL VÁLASSZA MEG HOL VÁSÁROL!

**A kancellár.hu szerint a magyarországi elektronikus kereskedelmi helyek biztonsága és a különböző törvényi szabályozóknak való megfelelésük erősen változó!**

- A vizsgált oldalak több mint 90%-a a felhasználó név, jelszó és egyéb érzékeny adatokat titkosítás nélkül fogadja. Kivételt csak a hitelkártyás tranzakció adatok képeznek, melyek közvetlenül a banki szerverekre jutnak el. A vásárlók munkamenetei több esetben is eltulajdoníthatónak bizonyultak, mely személyes adatok kiszivárgásához, a felhasználó identitásának ellopásához vezetnek.
- A legtöbb esetben teljes mértékben hiányzik vagy legalábbis részleges a fogyasztók érdekeinek érvényesítését segítő tájékoztatás. Az adatvédelmi szabályzatok hiányosak, a legtöbb adatkezelő elmulasztotta az adatvédelmi biztosnak - nyilvántartásba vétel végett - jelteni tevékenységét.
- Végső következtetésképp megállapíthatjuk, hogy a vásárlóknak a saját számítástechnikai környezetük frissen és biztonságosan tartásán túl (tűzfal, vírus és kémprogram védelem stb.), nagy figyelmet kell szentelniük megfelelő kereskedő kiválasztására. Nem megfelelő webshop választás miatt előfordulhat, hogy adataikat harmadik személy rendelkezésére bocsátják, vagy a titkosítatlan adatkapcsolat, gyenge jelszóválasztás miatt visszaélnek azonosítóikkal.

**Budapest, 2008. december 8.** - A karácsonyi vásárlási roham kezdete előtt a kancellár.hu Zrt. biztonsági szakértői egy tucat elektronikus kereskedelmi egységet (továbbiakban, webshop, webbolt, virtuális áruház stb.) informatikai biztonságát és adatvédelmi megfelelőségét vették górcső alá, meglepő eredménnyel.

A vizsgálatokra november második felében került sor, melynek keretében Magyarország 12 jelentős – független szervezet által kiválasztott - virtuális áruházát látogatták meg az információ és adatbiztonság szakértői. A vizsgált üzletek az alábbi területeken működnek:

- Könyvkereskedelem
- Szórakoztató elektronika, számítástechnika
- Vendéglátás
- Elektronikus fizetési megoldások
- Aukció
- Utazás
- Élelmiszer kereskedelem

A felmérések próbavásárlások segítségével történtek, melynek során a szakértők elemezték a vásárlás folyamatát és a rendszerek látható részeinek biztonságát.

„A kancellár.hu megalakulása óta küldetésének tekinti az információ biztonsági kultúra terjesztését, jelen kutatásunk is ezt a célt szolgálja. Ösztönözni kívánjuk a web áruházak üzemeltetőit olyan rendszerek építésére, melyekkel megvédhetik ügyfeleik és a saját





adataikat, valamint felhívjuk a vásárlók figyelmét a biztonságos kereskedő választás fontosságára.” - mondta Papp Péter a cég vezérigazgatója.

### Adatok titkosítás nélkül

A technológia elemzések célpontja a megvalósítási hiányosságok feltárása volt, melyek közül az egyik legkritikusabb a titkosítatlan adatkommunikáció. „A megvizsgált rendszerekből csak egy használ titkosított (SSL – Secure Socket Layer) adatkapcsolatot a vásárlói regisztráció és beléptetés során. Az összes többi áruház esetében az Interneten könnyedén lehallgatható formában utaznak a vásárlói adatok, úgy mint felhasználói azonosító, szállítási cím, email cím, jelszó stb.” – emelte ki Bártfai Attila a cég üzletfejlesztési igazgatója a felmérés vezetője. „Pozitívumként emelhető ki, hogy azon esetekben mikor a vásárló a kártyás fizetést választotta, a pénzügyi tranzakció a bank által üzemeltetett szerveren megy végbe, ahová az adatok titkosítottan jutnak el.” – tette hozzá. További feltárt jellemzők:

- A jelszavak komplexitására vonatkozó ajánlást a boltok mindössze 30%-a tesz. (Hány karakter legyen minimum a jelszó, milyen karaktereket tartalmazzon.)
- Láthatóan az aukciós web helyek a legszigorúbbak ebben a tekintetben, ők nem engednek túl rövid vagy egyszerűen kitalálható jelszót választani.
- A felhasználók jelszavainak szótár alapú próbálgatással történő kitalálása ellen nem védenek a boltok, nincs felhasználói azonosító kizárás pár percre vagy lassított válaszadás 3-4 sikertelen bejelentkezés után.
- A boltok egy része érzékeny a munkafolyamat lopásra, amelynek segítségével egy másik felhasználó jogosultságaihoz és adataihoz lehet jutni. A probléma kivédhető az üzemeltető által a felhasználók által bevitt fórum hozzászólások, termék értékelések megfelelő szűrésével.
- Több webbolt kockázatosan sok alkalmazást futtat az értékesítésre felállított szerveren. A sikeres külső támadások elkerülésére a Kancellár.hu javasolja, hogy az üzlet működtetéséhez nem feltétlen szükséges alkalmazásokat szüntessék meg, vagy telepítsék másik kiszolgálóra. A vizsgálatok során a bolti szervereken láthattunk postafiók, név szerver, fájl transzfer, VPN, távmenedzsment, időszerver és üresen hagyott web kiszolgálókat.

### Törvényi megfelelés – gyenge eredmények

A vizsgálatok második fő fókuszja a web áruházak törvényi megfelelése volt a következő szabályozók tükrében:

- Az **elektronikus kereskedelmi** szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről 2001. évi CVIII. **törvény** (továbbiakban: Eker törvény)
  - A vizsgált webáruházak **mindegyike eleget tesz** az Eker törvény által előírt közzétételi kötelezettségnek. A vizsgált honlapokon a törvény által előírt tartalmi elemek megtalálhatók.
- A **távollevők között kötött szerződésekről** szóló 17/1999. (II. 5.) Korm. **rendelet** (továbbiakban: rendelet)

- A távollevők között kötött szerződésekről szóló 17/1999. (II. 5.) Korm. rendelet szerint kötelező tájékoztatást a webáruházak nagy része megfelelően elérhetővé tette.
- Probléma azonban, hogy a fogyasztók/vásárlók érdekeinek érvényesítését célzó rendelkezések esetében - mint elállás joga és gyakorlásának feltételei, szavatossági és jótállási igények érvényesítése, kifogások érvényesítésének helye - előfordul, hogy a tájékoztatás hiányzik, erősen hiányos, vagy csak hosszás és célirányos kutatással lelhető fel.
- A **személyes adatok védelméről** és a közérdekű adatok nyilvánosságáról **szóló** 1992. évi LXIII. **törvény** (továbbiakban: Avtv.)
  - Az adatvédelmi törvény előírásainak követése mutatta a legnagyobb különbséget az egyes webáruházak között. Általánosságban megállapítható, hogy az adatvédelmi szabályok betartására a **szolgáltatók nem fektetnek nagy hangsúlyt** (megjegyzés: a kényszerítő intézkedések és szankciók használata az adatvédelem területén nem olyan erőteljes és nem általános).
  - A vizsgált webáruházak **egyharmada** egyáltalán **nem rendelkezik adatvédelmi tájékoztatóval**, egyharmada készített rövid („mutatóba készült”) adatvédelmi irányelveket (a jogszabály szövegét kiollózva, de semmit nem konkretizálva) és csupán egyharmada készített az Avtv. rendelkezéseit szem előtt tartva megfelelő, a jogszabály által előírt, minden tartalmi elemet szabályozó adatvédelmi szabályzatot.
  - Az adatvédelmi törvény szerint nem kell bejelenteni az adatvédelmi nyilvántartásba azt az adatkezelést, amely az adatkezelővel munkaviszonyban, tagsági, tanulói viszonyban, ügyfélkapcsolatban álló személyek adatait tartalmazza. Amennyiben azonban az adatkezelő például hírlevél kiküldéséhez vagy fórum működtetése során személyes adatokat kezel, köteles azt az adatvédelmi biztosnak nyilvántartásba vétel végett jelenteni. A vizsgált **webáruházak kétharmada nem tett ilyen bejelentést az adatvédelmi nyilvántartásba.**

### Kutatási feltételek és további tervek

kancellár.hu munkatársai előzetes jogi egyeztetés után a törvény által megszabott kereteken belül dolgoztak. A vizsgálatok nem lehettek egyenértékűek egy professzionálisan végrehajtott etikus betörési teszttel, mivel a szakértők nem léphették át a rendszer által biztosított jogosultsági határokat.

Az elektronikus kereskedelmi helyek vizsgálata egy sorozat első állomását alkotják, a kancellár.hu a következő évben rendszeresen publikálni fogja különböző területeken végzett felméréseit!