XXVI. Országos Könyvvizsgálói konferencia – 2018

Adatvédelem, információ-biztonság a könyvvizsgálatban

Tusnádiné Ágoston Márta

Amikor felmerül az adatvédelem illetve az információ-biztonság témaköre, mindig elgondolkozom azon, hogy milyen értelemben közelítjük meg a kérdést. Rendkívül fontos az **adatvesztés elleni intézkedések** meghozatala – és általában erre már fel vagyunk készülve –, beleértve a mentések ellenőrzését is. De ugyanígy kiemelt feladatunk **megvédeni az általunk kezelt adatokat** (saját és ügyfeleink információit) annak érdekében, hogy azok ne kerüljenek illetéktelen kézre.

Nem jelent újdonságot, hogy a könyvvizsgálat során üzleti titkokat kezelünk, ezek védelmére jogszabály is kötelez bennünket. Mit minősítünk üzleti titoknak és mi az, ami elvárható egy könyvvizsgálótól az ügyfelei üzleti titkainak, adatainak védelme érdekében?

Egyrészt a szerződésben titoktartási kötelezettséget vállalunk. Ez kiterjed a szóbeli kommunikációra valamint a papír alapú és elektronikus adatok, információk védelmére is. Én most csak ez utóbbi témakörrel szeretnék foglalkozni.

Másrészt a digitalizáció hatására a papír alapú dokumentumokat felváltja az elektronikus adat és információ. Az elektronikus adatok védelme pedig sokrétű feladatot ró ránk. Ezekből szeretnék néhányat példa jelleggel bemutatni.

Az adatok átvétele az ügyféltől (IMPORT adatok):

Milyen formában adja át ügyfelünk elektronikus adatait? Egyre gyakoribb kérésünk az ügyfél felé, hogy egy-egy papír alapú dokumentumot szkennelt formában juttasson el nekünk. Emellett ügyfeleink is egyre több elektronikus adatot használnak, tárolnak. Nem utolsó sorban nekünk is sokkal hatékonyabb az elektronikus adatokkal dolgozni.

A könyvvizsgálat során az import adatok leggyakoribb formája:

- e-mail (technológiailag nem támogatja a GDPR elveit)
- pen drive (ügyfelenként szeparáltan, titkosítási lehetőség!)
- a könyvvizsgáló webes/felhő alapú tárhelye (ennek biztonsága a könyvvizsgáló hatáskörébe tartozik)
- az ügyfél webes/felhő alapú tárhelye (a biztonságot az ügyfél nyújtja)
- független ingyenes felhő alapú tárhely (az adatbiztonság erősen kérdéses)

Az adatok kezelése a könyvvizsgálati munka során:

A könyvvizsgálók nagy része szoftverrel végzi a könyvvizsgálatot. Felmerül a kérdés, hogy honnan férünk hozzá az alkalmazott szoftverhez illetve az adatbázishoz?

- az irodai gépen/szerveren fut a program és csak irodai környezetben használjuk
- a laptopon fut a program és itt vannak az adatok is (legnagyobb fokú kitettség az adatvesztésre)
- laptopon fut a program de az adatok egy távoli gépen (irodában, saját szerveren) vannak
- távoli szerveren vagy felhőben vannak az adatok (a program saját gépről, laptopról fut)
- távoli szerveren vagy felhőben fut a program is és az adatok is ott vannak.

Hasonlóan több megoldás létezik pl. egy excel tábla használatára is. Ez is lehet bármely helyi számítógépen/laptopon vagy szerveren/webes tárhelyen/felhőben is.

A fenti lehetőségek közül szeretném kiemelni a laptopról történő használatot és az adatok tárolásának helyét.

Mivel a könyvvizsgálat számos esetben helyszíni munkát jelent, ezért fontos eszköz lett számunkra a notebook. Mondhatjuk, hogy anélkül nem megyünk sehova (beleértve a szabadságot is). A **laptop védelméről** azonban több szinten ajánlott gondoskodni:

1. védjük a saját adatainkat, készítsünk biztonsági mentést
2. védjük ügyfeleink üzleti titkait, korlátozzuk az adatokhoz való hozzáférést. Ezeket első lépésként egyszerűen meg tudjuk valósítani pl. az operációs rendszer (Windows) jelszavas védelmével és a könyvvizsgáló program indításakor a jelszó beállításával. A jelszó használat véleményem szerint a minimálisan elvárható adatvédelmi feladatok közé sorolható. A második lépés a laptopon tárolt file-ok titkosítása.
3. ne hagyjuk a laptopot őrizetlenül...

Az **adatok tárolására** több megoldás is jó lehet. A könyvvizsgálói munkához használt program, munkapapír file-ok, valamint az ügyféltől kapott file-ok tárolási helyének megválasztása szorosan összefügg a saját munkamódszerünkkel. Jó módszer lehet a saját gép (asztali/notebook) használata, vagy a távoli szerver használat is attól függően, hogy milyen internet elérési lehetőségünk van. Egy nagy teljesítményű mobil internet csomag esetén hasznunkra válhat a **távoli adatelérés**. Ahol pedig nincs megfelelő térerő, ott marad az **offline munkavégzés** és az utólagos mentés. Az adataink tárolásának (mentésének) helye legoptimálisabb esetben valamilyen **hibrid megoldást** jelent. Azaz laptop (titkosítva) / szerver / felhő... megoldások egyidejű alkalmazása. A szerver lehet a saját fenntartású irodai szerverünk, de lehet egy szerver-szolgáltatás keretében használt távoli szerver is. A felhő pedig egy olyan tárhely, melynek nem ismerjük a fizikai helyét, csak a fenntartóját. Előadásomban összevetem a "mammut cégek" által üzemeltetett felhőket a kisebb távoli szerver/tárhely használattal, mert az eltérő szempontok alapján bármelyik szimpatikus lehet egy adott funkcióra.

Csatlakozás az internetre:

Kiemelt üzleti titkokat tartalmazó notebook – mint például egy könyvvizsgáló számítógépe – esetében nem ajánlott az ügyfél wifi vagy kábeles hálózati kapcsolatának használata. A publikus "free wifi" pedig kifejezetten kerülendő. Ezek adatvédelmi beállítása és a szolgáltató által "elkapott" adatok sorsa nem ismert számunkra. A legbiztonságosabb internet elérést a saját pl. mobil internet előfizetésünk nyújtja.

Mindezekkel szorosan összefügg **mentések rendszere**:

Mivel a Számviteli törvény és a Standardok is megőrzési kötelezettséget írnak elő a könyvvizsgáló számára, ezért elengedhetetlen az adatok mentése. Erre különböző adatmentő szoftverek állnak rendelkezésre, amelyek e-mail-t is küldenek a mentés eredményéről. Az adatmentési szabályok kialakításánál érdemes figyelembe venni a gyakoriságot (napi, heti, havi mentések) és a földrajzi elhelyezkedést (a mentése decentralizált tárolása). Emellett fontos felállítani egy ún. **válság tervet** is például arra a nem várt eseményre, hogy mekkora az idő kiesésünk akkor, ha leáll a szerver a legnagyobb leterhelésünk időszakában?

Jól látszik, hogy a fenti rendszerek kialakítása nem könyvvizsgálói feladat. A legkorszerűbb és biztonságos technológiát érdemes alkalmazni, amihez szükség van rendszergazda bevonására, megbízására, aki garanciát vállal munkájáért.
A könnyvizsgálat során akkor tudjuk biztosítani ügyfeleink adatainak biztonságát, ha minden tőlünk telhetőt megteszünk ezek védelme érdekében.

Az információ biztonságának védelmére ajánlott **információ-biztonsági szabályzatot** készíteni és életbe léptetni. Ennek megfelelő alapja lehet az MSZ ISO/IEC 27001 szabvány (http://www.mszt.hu/web/guest/msz-iso-iec-27001).

Előadásomban a fentiek gyakorlati oldaláról fogok beszélni.

2018. szeptember