Nálam nincs szükség adatvédelemre!

Gyakran hallani cégvezetőktől a címbeli kijelentést. Ez a cikk célul tűzte, hogy bebizonyítsa az állítás ellenkezőjét.

A MUNKAVÁLLALÓK ADATAIT KEZELNI KELL

Ha egy cég munkavállalókat foglalkoztat, a dolgozók személyes adatait kezeli. Kisebb méretű cégek esetén ez ritkán okoz problémát. A munkaviszony kapcsán rögzített adatkör, az adatkezelés célhoz kötöttsége, az adatkezelési műveletek többnyire azért nem okoznak vitát, mert a munkavállalók is belátják az adatkezelés szükségességét.

■ A problémák a határesetek tájékán szoktak kezdődni. Akár egy névkitűző is kivívhatja az adatvédelmi biztos rosszallását, ha a dolgozó munkáját nevének közzététele nélkül is el tudja végezni. Az alkalmassági tesztek, a pszichikai vagy hazugságvizsgálatok már csak akkor állják ki a jog próbáját, ha a munkáltató másként nem tudja biztosítani a szakszerű, biztonságos munkavégzést.

A CÉG ADATVAGYONA

A munkavállalói adatkezelés anomáliái tehát ritkán terelik a cégvezetés figyelmét az adatok megvédésének irányába. Sokkal forróbb kérdés lehet a cég, szervezet adatvagyonának védelme. A munkavállalók többsége úgy véli, ha távozik a cégtől, akkor ebből az adatvagyonból neki egy szelet kijár.

■ Reális veszélyt jelent az ilyen szemlélet egy vállalkozás számára? Feltétlenül. Sőt a veszély több rétege is azonosítható. Ezért a veszélyek felszámolásához is tudatosan kell hozzálátni.

■ „Nincsenek védendő adataink." Tipikus sztereotípia, amely a cégvezetés alacsony információbiztonsági tudatosságát mutatja. Az üzleti partnerek listája például akkor is érték, ha a referencialistából nagyrészt megismerhető. A munkatársak cégben megszerzett tapasztalataival, a kapcsolattartók listájával kiegészítve alkalmas arra, hogy a partnereket a konkurenciához csábítsák. Sőt, számos példa van arra is, hogy a távozó középvezető új céget alapít a magával vitt adatokra, ismeretekre alapozva. Nem egyszer korábbi munkatársait, beosztottjait is magával viszi a távozó kolléga.

A VÉDELEM RÉTEGEI

Ha az adatbiztonság iránti igény megjelent a cégvezetésben, egy igen jelentős akadály már elhárult. Természetesen nem dőlt le az összes fal. Kezdeti lépésként fel kell mérni a cég adatvagyonát. Nem csak azért, hogy tisztába legyünk azzal, milyen adatokat kezelünk, hanem azért is, hogy kiderüljön: mennyire értékesek, azaz milyen erős védelmet igényelnek.

■ A következő szint, hogy szabályozással tisztázzuk, a cég adatvagyonával a dolgozók nem rendelkezhetnek sajátjukként, még akkor sem, ha éppen távoznak, azaz a munkajogi kötelék is megszűnik közöttük, s a cég között. A cég tehát tudatosította a dolgozó (egyébként általános munkajogi kötelezettségként szabályozott) titoktartási kötelezettségét. Ezzel egy jogvitában a cég bizonyítási esélyei sokat javultak.

■ A belső szabályozás önmagában nem csodaszer. Arra is szükség van, hogy a munkatárs – sőt az is, akinek cégadatot szivárogtat ki – bizonyíthatóan felismerhesse, hogy titkot sért, bizalmas adatot tart magánál. A legegyszerűbb, ha a titok szintjét az adathordozón feltüntetjük. Ez különösen az elektronikus térben nehéz. Itt az értékes adattartalom kimásolásának veszélye fokozott. Azért fontos a titokminőség egyértelmű azonosítása, mert a „… elképzelhetetlen, hogy ne tudott volna róla…", vagy a „…megengedhetetlen…" típusú megfogalmazások érthetőek ugyan az adatszivárgás észlelése során kialakuló felháborodott légkörben, de vajmi keveset érnek egy jogvitában a bíróság előtt.

A VÉDEKEZÉSNÉL IS EREDMÉNYESEBB A MEGELŐZÉS

Ha valaki a fentieket következetesen végrehajtotta, és még mindig nem elégedett, akkor adatbiztonsági tudatossága már magas szintre hágott. Ami hiányzik az eddigiekből, az a prevenció. Bármilyen bravúrosan számoljuk is fel egy adatszivárgás következményeit, az nem lehet olyan sikeres, mint a megelőzés. A szabályozás, a folyamatszervezés, az információhoz való hozzáférés korlátozása (jogosultságmenedzsment) számos adatszivárgási lehetőséget előz meg. Akár úgy is, hogy a felderíthetőség révén elrettenti a könnyen megtévedő munkatársakat.

■ A legbiztosabb megelőzési eszköz, viszont az informatikai rendszer és a papiros alapú adatkezelés biztonsági felülvizsgálata, korszerűsítése. Ennek során beszerezhető olyan adatszivárgást megelőző célszoftver is, amely műszakilag is kikényszeríti a belső szabályozást.

Dr. Dósa Imre

adatvédelmi, biztonsági szakértő