SZENZOR

Gazdaságmérnöki Kft.

Információ- és adatvédelmi vezető képzés

Egy cég adat- és információvédelmének kialakításának első lépései

Készítette:

Enyedi Tamás Károly

Témavezető:

Móricz Pál

Budapest, 2005. február

SZENZOR

Gazdaságmérnöki Kft.

Információ- és adatvédelmi vezető képzés

Enyedi Tamás

Szakdolgozati feladatkiírása

2005. február

EGY CÉG ADAT- ÉS INFORMÁCIÓVÉDELMI RENDSZERÉNEK ALAPVETŐ KÉRDÉSEI

Budapest, 2005 március 3.

Dr. Ködmön István
Oktatási igazgató

Témavezetői vélemény:

- A szakdolgozat a képzés követelményeinek megfelel. Beadható.
- A szakdolgozat nem adható be, mert

  ……
  ……
  …..……

Budapest, 2005 március. 3.

Móricz Pál
témavezető

KIVONAT

A dolgozat egyik multinacionális vállalat egy magyarországi telephelyének személy és adatbiztonságát mutatja be. Elemzéseiben kitér a három legfontosabb védelmi metódusra és összehasonlítja azokat, fontosságukat tekintve. A személyvédelmet (humán), az informatikai biztonságot és a vagyontárgyak biztonságát összehasonlítva a humán védelmet kell kiemelten kezelni –mint valamennyi kockázati tényező alapját. A megfelelő munkaerő kiválasztás és a kiválasztás utáni betanítás, munkavégzés az adott HR osztály, illetve az alkalmazott munkahelyi vezetőjének közvetlen feladata.

Nem lehet egy dolgozatban részletes elemzést készíteni az összes adatvédelmi kockázati tényezőről, ám a megfelelő vezetőkkel megosztva a tapasztalatokat –leszűrve a konzekvenciákat, az adott területek védelme érdekében meg lehet hozni a szükséges intézkedéseket.

Kulcsszavak:

- személyvédelem
- HR
- kockázat
- informatikai biztonság
- vagyonvédelem

TARTALOMJEGYZÉK

BEVEZETÉS

Az adat és az információ a közhasználatban többféle jelentéssel bír. A magyar értelmező kéziszótár szerint: Az adat "valakinek vagy valaminek a megismeréséhez, jellemzéséhez hozzásegítő tény, részlet." Az adat önmagában nem hordoz semmilyen jelentést, nincs szövegösszefüggése. Az információ értelmezett adat, mely bizonytalanságot oszlat el, jelentéssel bír, aminek alapján valamiféle ítélet alkotható, ez pedig adott célú cselekvést indíthat el. Más források szerint, az adat: „a hír vagy információ értelmezhető, lejegyezhető formája. Valakinek vagy valaminek a megismeréséhez hozzásegítő tény, részlet”.

Adatokkal, információkkal mindennap találkozunk. Amikor felkelünk, megnézzük a hőmérőt, eldöntjük, hogy milyen melegen öltözzünk. Bekapcsoljuk a rádiót, meghallgatjuk a híreket, a reggeli műsorokat; bevásárolunk a reggelihez... és még sorolhatnám a sokféle tevékenységet, melyet nap-mint nap végzünk és információval találkozunk. Bár lehet, hogy személy szerint számunkra nem tartalmaznak fontos, -sőt: létérdekű- adatot az előbb felsorolt tevékenységek, ám biztosak lehetünk benne, hogy vannak olyanok, akik számára ezek elemi fontossággal bírnak. A ruhakereskedő például nem teszi ki a kellő profit reményében a nyári kollekciót a kirakatába –télen. a rádió bemondója, hírszerkesztője a fontosabb blokkok előtt helyezi el a hirdetéseket, míg az élelmiszerbolt eladója pontos árakat ír a termékeken lévő árcédulára. Hogy miért? –hogy a számára keletkezzen haszon, ne pedig a versenytársainál.

A konkurenciaharc nem ujkeletű. Amióta megszületett az első emberpár kíváncsi volt, hogy milye van a másiknak, mit szerezhet meg magának. Már időszámításunk előtt is öldöklő háborúk folytak egy-egy kereskedelmi területért, termékért. A háborúkban többnyire az erősebb győzött –vagy az, akinek több, pontosabb információja volt az ellenfeléről. Ez manapság is így van, az maradhat meg a piacon, aki valamiben több, jobb a másiknál –de ezt hogyan lehet eldönteni? –mindenekelőtt ismerni kell az ellenfelet, minél több információt beszerezni róla, ezzel egyidőben meggátolni Őt abban, hogy megszerezze a rólunk szóló adatokat, melyeket, mint információ felhasználhat.

Rohanó társadalmunkban csak az számíthat sikerre, aki a saját magáról szóló információt meg tudja tartani/védeni; míg a másikról be tudja szerezni. Mindkettő módszerre külön specialisták szakosodtak. Az adatok megtartása, védelme mindig legális keretek között kell, hogy maradjon, míg sokszor előfordul, hogy illegális módszerekkel jutnak mások a mi adatainkhoz.

Dolgozatom arra próbál rámutatni, –példákkal alátámasztva-, hogy melyek azok a területek egy gyorsan fejlődő vállalatnál, ahol adatbiztonsági réseket látva egy esetleges második fél kihasználhat akár információszerzésre vagy akár szándékos károkozásra is.

Munkahelyem egy ujonan alakult cég –nemzetközi háttérrel, ahol ezt a dolgozatot szeretném felhasználni/felhasználtatni az adat és információvédelem elsők közti szabályzási lépéseire. A folyamatokhoz, üzemeltetéshez csatolt biztonsági intézkedések többsége már kialakításra került –ám célszerű azokat bizonyos időközönként újra és újra elővenni, megvizsgálni több szempontból, javaslatokat tenni a biztonsági intézkedéseknek ésszerű és gazdaságos fejlesztésére.

A dolgozatban bemutatott példák általánosak, több szakirodalom, illetve munkahelyi tapasztalataim alapján írtam le őket, ezek nem tartalmaznak olyan konkrét adatokat, melyek felhasználásával esetleges belső szabályokat, nyilatkozatokat sértenék.

2. CÉGISMERTETÉS

A cég pár éve alakult, egy multinacionális vállalat egyik divíziójaként –abból történő kiválással. A világ számos országában helyezkednek el telephelyei, melyek egymástól független vezetéssel –de mégis bizonyos folyamatokat centralizálva működik. A cég tevékenységét tekintve „backoffice" tevékenységet folytat más vállalatoknak. Jelenleg közel 800 munkavállaló dolgozik a vizsgált telephelyen, ez egy forgalmas, könnyen megközelíthető helyen helyezkedik el, ám mégis szeparáltan a külső behatásoktól.

A multinacionális háttér a cégcsoport több telephelyét jelenti, amely számos kontinensen helyezkedik el. A hazánkban lévő telephely ezek közül a legkisebb. A szervezeti felépítés egyvonalas jellegű. A szervezeti hierarchia tetején a vezető alatt az adott munkafolyamatokból alkotott szervezeti egységek vezetői helyezkednek el, ezek alatt a kisebb csoportok vezetői, majd pedig a képzeletbeli piramis alján a munkavállalók. Ezek a szervezeti egységek kisebb egységekből állnak, annak függvényében, hogy melyik cégnek milyen jellegű tevékenységet szolgáltatnak. Az alábbi nagy csoportokat különbözetjük meg működésük szerint: a „voice" folyamatokat, amikor a megrendelő számára telefonos szolgáltatást végeznek; a „finance" folyamatokat, amelyben pénzügyi tevékenységekkel foglalkoznak a megrendelők számára, illetve az ezeket kiszolgáló helyi „support" folyamatokkal foglalkozó kisebb szervezeti egységek alkotnak egy-egy nagyobb csoportot.

A cég tevékenysége során hozzáférést kell, hogy kapjon a megbízók informatikai hálózatához, illetve meghatározott adataihoz. Ezek a tevékenységek, munkák sok esetben egyszerű adatbázisból való lekérdezések minimális rendszerhozzáférési jogokkal, ám némely esetben, ahol az ügyfélnek nyújtott alap és felsőszintű számítástechnikai támogatásra épülő szolgáltatási folyamatokat végeznek ott bővített informatikai jogokkal kell rendelkezniük. A pénzügyi folyamatokat tekintve a megbízók számos adatfeldolgozási, könyvelési feladatot bíznak a cégre.

A backoffice tevékenységgel foglalkozó cégek szerepe és száma az eltelt pár évben megsokszorozódott, a telephelyeket egyre inkább a keleti régiók országaiba való áthelyezésekkel. Az áthelyezések annak köszönhetők, hogy egy-egy adott multinacionális cég bizonyos folyamatait nem szükséges külön-külön országokban végezni, hanem célszerű centralizálni. Azon a területen, ahol ezeket a folyamatokat végzik következőkről kell gondoskodni: a megfelelő nyelvismeret, a megfelelő munkakörnyezet, illetve az infrastrukturális kialakítás. Mindezen tényezők a gazdaságpolitikai környezetet is figyelembe véve azt eredményeik, hogy a fejlődő keleti /esetleg távolkeleti –ázsiai/ országokba tevődnek át ezek a folyamatok, hiszen a felsorolt opciók közül a legmagasabb költséggel a humán erőforrás havi munkabére jár –és ahogy a földgolyón egyre keletebbre haladunk ez az összeg –viszonyítva az amerikai/európai uniós átlagkeresetekhez – egyre csökken. Ezt felismerve, hogy egy ilyen tevékenységgel foglalkozó cég kialakítása a megtérülési rátához hasonlítva viszonylag kis befektetéssel jár, egyre több ilyen cég jelent meg a szolgáltató piacon, melyek a piaci telítődéssel egyre inkább konkurenciává válnak egymásnak.

3. MIT IS KELL VÉDENI?

A különböző adatvédelmi szabványok ajánlásai alapján célszerű elsődlegesen meghatározni, melyek azok a kockázati tényezők, amelyek befolyásolhatják a cég adatainak védelmét, külső fél számára megnehezíteni/lehetlenné tenni a hozzáféréseket, illetve azokat olyan szinten elemezni, hogy megérik-e a ráfordítást a megtett intézkedések, melyek megakadályozzák az adatok elvesztését. Ezeknek mindig meg kell felelni a hatályos törvényeknek, rendeleteknek; ezért azokat minden esetben jogi tanácsadóval jóvá kell hagyatni.

Egy külső fél számára felhasználható információk az alábbi főbb csoportokba sorolhatók be megszerzési kockázatuk szerint, illetve az ellenük hozandó intézkedési területek szerint:

- Fizikai
- Logikai
- Adminisztratív
- Humán

A fizikai védelem:

Az adatok fizikai védelmén mindazon intézkedéseket értjük, amely meggátolják azok a külső behatásokra való sérülését, esetleges megsemmisülését vagy egy külső fél számára való megszerezhetőségét.

Elsődlegesen gondoskodni kell magának a munkaterületnek a fizikai védelméről. A fizikai védelemnek ki kell terjednie az esetleges rongálódásra, illetve a teljes megsemmisülésre. Ebben az esetben célszerű egy mindentől független csoportot erre a célra kialakítani, felkérni a működtetésre, amely önállóan tevékenykedik –figyelembe veszi az adott területen dolgozók igényeit és azokat a lehető legjobban próbálja szinkronizálni a védelmi szintekkel. A fizikai védelembe beletartozik a tűzvédelem, illetve a vagyontárgyak, illetve maguk az adathordozók védelme is. Az „adathordozók" között kiemelten kell kezelni a humán tényezőt –hiszen az emberi agyban tárolt információ reprodukálhatatlan és nem készíthető minden egyes eltárolt információról dokumentáció.

A fizikai védelmet egy külsős biztonsági szolgálat kiválóan el tudja látni, hiszen erre képzett szakemberekből áll –belső vezetéssel és belső szabályozással. Működésüket kellő módon segíthetik a telephelyen és a közvetlen vonzáskörzetében elhelyezett térfigyelő eszközök. A főbb dolgok, melyeknek mindenképp szerepelni kell a szerződésben –mint védendő objektumok, értékek: személyi vagyontárgyak, cég tulajdonát képező vagyontárgyak. Az eszközök védelménél gondolni kell külső behatásra történő káreseményekre, illetve a személyek által okozott szándékos vagy véletlenszerű káreseményekre.

Az adatok tárolása napjainkban többnyire digitalizáltan, vagy papírra nyomtatottan történik –ez utóbbi a hatályos törvények alapján a különböző hitelesítések miatt szükséges. Sajnos a mindennapi munka mellett nagy tömegben keletkeznek papír alapú dokumentumok, nyomtatványok. Ezeknek a kezelése egy több száz főt foglalkoztató vállalatnál nehezen megoldható. A legegyszerűbb megoldás az lenne, ha minden számítógép mellé rendelni lehetne egy-egy nyomtatót és faxot –ez kivitelezhető egy pár főt

alkalmazó kis cégnél, ám egy ekkora méretű vállalatnál nem. Mindenképpen szükség van arra, hogy közösen használt hálózati nyomtatók, faxok üzemeljenek, melyeknek mindenki számára elérhetőnek kell lenniük. Felvetődik a kérdés, hogy ha mindenki használja őket, akkor hogyan lesznek az egyes dokumentumok megkülönböztetve, hogy az adott felhasználók lehetőleg ne lássák a másik által kinyomtatott adatokat. Erre különböző módszerek vannak, legelterjedtebb egy mágneses chipkártya használata –mely korlátozza a kinyomtatni szánt dokumentumok hozzáférhetőségét. Bár így le lehet szűkíteni a kinyomtatott és „gazdátlan" dokumentumok számát, ám mindig keletkeznek selejt darabok. A fel nem használt nyomatok számára egy iratmegsemmisítőt célszerű üzemeltetni minden nyomtató mellett, illetve gondoskodni kell arról, hogy a telephelyet kinyomatott dokumentum ne hagyhassa el, akár irodai szemétként sem. A biztonsági szolgálatnak egyik feladat kell, hogy legyen ezek ellenőrzése, illetve a kinyomtatott és a későbbiekben fel nem használt dokumentumok megsemmisítése/megsemmisíttetése.

A digitalizált adatok tárolása, a későbbi felhasználásuk miatt vagy egy egyszerű adathordozón történik vagy pedig egy fixen szerelt adattároló egységen. Az egyszerű adathordozót (CD, mobil HDD, stb.), melyen a mentett állományok találhatók célszerű a mobilitásuk miatt biztos helyen elzárva tartani –erre kiválóan alkalmas egy páncélszekrény, amely a biztonsági szolgálat közvetlen felügyelete alatti területén található és szigorúan szabályozva van mindazok száma és személye, aki ezekhez az adatokhoz hozzáférhetnek.

A Biztonsági szolgálatok működése szempontjából a legcélszerűbb az adott telephelyen csak egy olyan közlekedési útvonalat üzemeltetni, melyen a dolgozók ki és beléphetnek a cég területére. Ebben az esetben a mozgások alkalmával ellenőrizni lehet a személyek által szállított eszközöket, értékeket –ám egy ilyen szintű ellenőrzés csak az eszközök fizikai eltulajdonítása ellen véd –magukat az információhordozókét nem lehet ilyen szinten felügyelni. Gondoljunk arra, hogy az eltelt pár évben mennyit fejlődött az informatika. Ezelőtt pár évvel egy adathordozó akár egy fél táska méretet is elérhette, míg manapság az akkorinak akár a több tízszeresét is, meghaladó adattartalom is elférhet egy, pl. USB meghajtón, amely akár egy pénzérme nagyságú is lehet.

Az adatvédelemnek ennél a részénél nő meg az informatika, illetve az informatikai szervezet szerepe, felelőssége. Az adott részlegnek gondoskodia kell arról, hogy a tárolt adatokról megfelelő mentés készüljön. A mentési eljárásokat az adott szervezeti egységgel egyeztetni kell előtte, hiszen az adott szervezet tudja megmondani milyen gyakorisággal dolgoznak egy adott adatbázisban vagy éppen mekkora esetleges adatveszteséget tudnak elviselni az általuk nyújtott szolgáltatásban. Az adott adatokról készített mentéseket biztonságos helyen kell tárolni, célszerű azokat egy másik helyszínen, a készítési helyüktől akár több kilométerre tárolni –egy esetleges katasztrófahelyzetre is gondolva. A mentésekkel kapcsolatban azt is írásban kell rögzíteni, hogy az adott szervezetnek mennyi időre visszamenőleg kellenek/kellhetnek azok az adatok, melyek archiválásra kerültek. Célszerű már az infrastruktúra kialakításánál az archiválási rendszereket, szabályzásokat figyelembe venni. Az adatok mentése legegyszerűbb metódus alapján egy előre beállított parancsfájl alapján kell, hogy működjön.

Az adatok védelmi szabályzásánál az egyik legszigorúbban kell, hogy kezelésre kerüljön, hogy fizikai kontaktusba ki és mikor, esetleg milyen körülmények között juthat. Célszerű már s szervezeti egységek kialakításánál kellően elhatárolni azokat a folyamatokat, területeket melyek semmi körülmény között nem lehetnek olyanok, hogy bárki hozzáférhet. Egy ilyen területre tipikus példa a szerverszoba. Itt maguk a szerverek és a legfontosabb informatikai eszközök találhatók –ezért az egyik legkiemeltebben őrzött

területnek kell lennie. Az őrzési mechanizmus sok területet ölelhet fel –egészen a legegyszerűbbektől –a bejárati ajtó elé telepített őrszolgálattól a kamerák rendszeréig, illetve az esetleges belső károk kiküszöbölésére különféle szenzorok beépítéséig. Ha már az őrzési mechanizmus kielégítő –megfelel a védendő érték/anyagi ráfordítási arányoknak, akkor meg kell határozni mindazoknak a személyek listáját, akik a szerverszobában elhelyezett adatokhoz, információhordozókhoz hozzáférhetnek. Ez a hozzáférés lehet többféle: fizikai bejutás magába az objektumba, vagy a rendszergazdák álma: távoli elérése a bent elhelyezett eszközöknek és azok távmenedzselése. Mindkét lehetőség bizami, hiszen az adott munkahelynek –köszönhetően a digitalizáció gyors fejlődésének- szinte az összes fontos adatai itt vannak tárolva, melyekhez a hozzáférést csak kevés személynek lehet - illetve az adatok biztonságát tekintve- szabad biztosítani.

Minden esetben a fizikai védelemnél gondoskodni kell a hatályos jogszabályoknak a személyiségre vonatkozó részeinek betartásáról. Könnyű belátni, hogy kialakíthatunk egy közel tökéletes rendszert, amely minden külső és esetleges belső behatástól megvédi az adatainkat, nyomon követi az esetleges behatolásokat –ám ha az intézkedéseinkkel, szabályzásainkkal vétünk a mindenkori hatályos jogszabályok ellen, akkor az abból származó utólagos károk –amelyek az adott intézkedések folyományai lehetnek, akár a védelemre költött anyagi ráfordítások akár többszörösét is elérhetik. Az egyik legegyszerűbb példa erre a biztonsági kamerák használata. Ez a módszer az egyik legelterjedtebb a fizikai adatvédelem megvalósítói között, hiszen magát a megfigyelő rendszert elég csak egy-egyszeri beruházással kialakítani –azt lehet akár több éven keresztül is minimális ráfordítással üzemeltetni. Ám a hatályos jogszabályok elég szigorúan rendelkeznek az ilyen megfigyelésekről. Az adott helyszíneken, ahol az említett térfigyelő eszközök működnek –minden esetben fel kell rá hívni a figyelmét, a helyiséget használóknak, illetve a közvetlen munkahelyeket nem lehet figyelni ezekkel a kamerákkal –azok felvételei akár személyiségi jogokat is sérthetnek.

A logikai védelem:

Az adatok biztonsága érdekében különböző fizikai védelmet alakíthatunk ki, ám ezek nem minden esetben kielégítők. Bizonyos esetekben, magában a használt alkalmazásokban szoftvereken belül kell definiálni a megfelelő hozzáférési jogokat.

Elsődlegesen azt kell szem előtt tartani, hogy ki, milyen módon lehet része annak az informatikai hálózatnak, amely az adatokat tartalmazza (lehet a cég infrastruktúrájának az eleme, pl. egy olyan számítógép, amely nincs rákapcsolva a belső hálózatra csak direkt az internetre, itt a dolgozók mindenféle szűrés nélkül megnézhetnek tetszőleges honlapokat, illetve gyakorolhatják a számítógéphasználatot, anélkül, hogy veszélyeztetnék a mindennap használt a cég működtetésében létfontosságú rendszereket. Minden egyes felhasználót, aki a fenti paraméterekkel rendelkező gép elé ül, tájékoztatni kell arról, hogy mindazon adatok, amelyet erre a gépre ment, vagy letölt nem archiválódnak, és bármikor megsemmisítésre kerülhetnek. Ezzel egyidőben le kell tiltani mindazon perifériákat, melyek alkalmasak egy külső adattároló csatlakoztatására, és azon keresztül a lementett adatok kimásolására). Amennyiben ez a jogosultsági jogkör létrejön –az adott személy munkahelyi vezetőjének kell kijelölnie, hogy a szervereken tárolt adatok közül melyekhez férhessen hozzá a felhasználó. Amikor belép a céghez egy új ember, minden esetben ezeket a jogokat, jogköröket tisztázni kell, és azt írásban dokumentálva a megfelelő biztonsági szolgálat, HR, illetve az informatika részére el kell juttatni. Célszerű az új belépők számára egy folyamatot felállítani, mely végeztével az összes rendszerhozzáférés,

belépési jogosultság elkészül a megfelelő osztályokon, így azzal külön-külön nem kell törődni.

A fent leírtak alapján a belső jogosultságokat a rendszerekhez megkaphatják a felhasználók és azon belül a jogosultságokat, jogköröket könnyen lehet szabályozni, ám sokszor igény van arra, hogy az adott rendszert vagy rendszereket akár a kialakított hálózaton kívülről –akár egy szállodai szobából is elérjék. Magát a hálózat védelmét a különféle informatikai eszközök és szoftverek hivatottak biztosítani; ezek, mint például a tűzfalak könnyen konfigurálhatók és csak minimális azoknak a köre, akik ezt megtehetik. Ezen eszközök karbantartóinak rendszeresen frissíteniük kell a tudásukat, illetve ellenőrizniük kell a védelmi eszközök nalófájljait esetleges betöréseket keresve, valamint megtenni ellenük a szükséges megfelelő lépéseket.

Sajnos az adatok/adatbázisok így is könnyen kerülhetnek illetéktelen kezekbe. (Gondoljunk csak arra, hogy az informatikai levelezőrendszerek használatával az egész világon már szinte nincs is szükség fizikai adathordozókra két számítógép között) Ebben az esetben a megfelelő biztonsági intézkedésekkel azt lehet elérni, hogy a megszerzett adat nem lesz felhasználható csak hosszadalmas dekódolások után. (egyik korábban népszerű filmsorozatban azután hogy a titkos ügynök megkapta a feladatot, automatikusan megsemmisítette magát a háttértár, amelyen az üzenet volt tárolva –természetesen az üzenet lejátszásáéhoz is szigorú hitelesítéseken kellett keresztülmenni. –Ebben az esetben felvetődik az a kérdés, hogy megéri -e az ilyen komoly és szigorú adatvédelem, hiszen az üzenet nem volt többször lejátszható és az ügynöknek nagyon oda kellett figyelnie, hogy véletlenül se tévessze el a célszemélyt, akit meg kellett védenie vagy éppen az ellenkezője...)

Szintén emberi mulasztási kérdéseket felvető probléma az, hogy ha napközben megszakítják a dolgozók a munkájukat, akár egy rövid pihenőre, vagy akár étkezési szünetekre, az éppen aktuális dokumentumokat, adathordozókat az asztalukon hagyják, azzal a szándékkal, hogy így könnyebb lesz folytatni a megkezdett munkát. Sajnos a papíralapú dokumentációkezelésnél ez ellen nem tehetünk semmit –csak a felhasználók figyelmét tudjuk rá felhívni, hogy tárolják az éppen nem használatban lévő dokumentumaikat zárt helyen. A számítógépeken tárolt digitalizált adatok védelmét lehetővé teszik a napjainkban elterjedt operációs rendszerek védelmi mechanizmusai, amelyek –beállításuktól függően- bizonyos idő elteltével, ha nem történik a számítógéppel olyan jellegű munkavégzés, amely feltételezi, hogy a gép használója az eszköz előtt van, úgy lezárja a betekintést a számítógép monitorára, melyet csak maga a felhasználó –vagy amennyiben adminisztratív okokból szükséges egy rendszeradminisztrátor oldhat fel.

Szervezés, adminisztratív védelem:

Az adatok védelmének a megszervezése az egyik legfontosabb kulcspont az adatbiztonságban. Az adott védelmi mechanizmusokat egymáshoz kell igazítani, szinkronizálni. Külön-külön is hatásosak a meghozott intézkedések, beállítások -ám mindazokat úgy kell használni, hogy semmiképpen se gátolják egymást, illetve egymást kiegészítve érhetjük el az adataink lehető legmagasabb fokú védelmét.

Egyik legegyszerűbb példa erre a munkaidő megszervezése. Az általános munkaidőhöz igazítva van szükség a különféle védelmi folyamatok elvégzésére. Az eszközök és a telephely fizikai védelmét ekkor lehet elvégezni, tökéletesíteni. A biztonsági szolgálat ekkor tudja a cég tulajdonát képező eszközök fizikai meglétét ellenőrizni, az adott zárral felszerelt helyiségek behatolás elleni védelmét ellenőrizni. Az informatikának

háttértárolókon elhelyezett adatok mentését semmiképp sem szabad munkaidőbe szervezni, hiszen akkor az adatbázis nem lesz használható a felhasználók számára. Bár ezzel a saját munkaidejüket kell, hogy meghosszabbítsák, ám ebben az esetben ez a szervezeti egység a kiszolgáló –és neki kell alkalmazkodnia a felhasználók által kért üzemidőhöz. A biztonságos rendszer az emberi tényező kiiktatásával –automata metódust követve- készíti el az adott mentéseket, replikákat. Minden egyes esetben a rendszer teljes biztonságossá tételének érdekében a mentés befejeztével –akár a másnapi tényleges munkaidő tartama alatt- ellenőrizni kell az archiválásra került adatokat.

Az automatizmussal sok emberi tényezőt, rizikófaktort ki lehet iktatni, ám a beüzemelt automata rendszerek is elromolhatnak, hibásan működhetnek. Mindezen hibás működést megelőzni nem lehet –hiszen automata rendszerekről van szó és azoknak a kialakításánál el, kell érni a lehető legjobb, legbiztosabb teljesítményi faktort- ám gondoskodni kell esetleges ilyen esetek bekövetkezésekor a rendszer által küldött riasztásokról. Amennyiben ez nem történik meg, úgy abban az esetben a következő hibákkal kell számolni: az archiválásra kijelölt adatok nem mindegyike kerül a mentési eszközre –ebben az esetben akár több órás fáradtságos munkával lehet kideríteni, hogy melyek voltak azok az adatok, amik nem kerültek lementésre. A másik verzió az, hogy a rendszer egy hiba folytán nem ellenőrzi vissza az adatokat –és pl. hibás adathordozóra történik a mentés, ahonnan nem lehet az adatokat visszaállítani. Ebben az esetben, ha nem vesszük észre ezt a hibát, akkor esetleg a korábbi mentést kell visszatölteni, ha az is hibás, akkor a korábbit .... Ekkor akár több hetes, hónapos munka veszhet kárba.

Nem elég a mentéseket elkészíteni, gondoskodni kell azoknak a megfelelő helyen történő tárolásáról, illetve amennyiben szükség van rá, akkor annak gyors hozzáférhetőségéről. Célszerű egy másik telephelyen –megfelelő biztonsági intézkedések mellett tárolni azokat, ahová csak a kijelölt személyek léphetnek be biztonsági kísérettel. Felvetődik az a kérdés, hogy hogyan kerülnek át a biztonságos helyiségbe a mentett dokumentumok. Lehetséges ez informatikai hálózaton keresztül, ha a két végpont elég távol van egymástól, ám amennyiben egy informatikai adattámadás (romboló vírusok) éri a céget, akkor azok az adatok teljesen kiszolgáltatottak lesznek –mindezek figyelembevételével célszerű ismét a humán erőforrásokat igénybevenni és azokat felhasználni a dokumentumok biztonságos helyre való szállításánál. Azok mozgatásáról, biztonságos elhelyezéséről mind az informatikának, mind pedig a biztonsági szolgálatnak kell gondoskodnia. Az informatika felelőssége maghatározni azt, hogy az adathordozók milyen körülmények között tartalmazzák biztonságosan az adatokat, melyek azok az intézkedések, amelyek magát az adathordozót védhetik meg a külső behatásoktól. A biztonsági szolgálat szerepe a mentések biztonságos szállítása és őrzése.

A riasztásokra és az automatizált rendszerekre egy példa:

Bizonyos rendszereknek állandóan üzemelniük kell, hiszen például az informatikai rendszerek sem „pihennek”, mindig elérhetőnek kell lenniük ezért a rendszerek üzemeltetésében kiemelt figyelemmel kell kezelni őket. Napközben a felhasználók használják, míg este, éjszaka az automatizált mentési rendszerek. A rendszer biztonságát és az üzemeltetését figyelem előtt tartva az informatikai részleg egyik legnagyobb felelőssége, hogy az adott hibákról első kézből kapja meg a riasztásokat, hibajelzéseket. A hibajelzések közül a legelterjedtebb egy rövid szöveges üzenet küldése egy az adott célszemélynél állandóan üzemelő mobiltelefonra –így amennyiben az automata rendszer hibát észlel, akár másodperceken belül értesíteni tudja a kívánt személyt, aki megkezdheti a kialakult hiba elhárítását. Ezzel az intézkedéssel kiküszöbölhetjük, illetve a reagálási időt

minimalizálhatjuk az esetleges olyan hibák kialakulásakor, amelyek a felhasználók számára meggátolják a mindennapi munkavégzést. Ennek a rendszernek a biztonságosabbá tételéhez egy rendszeres üzenet küldése célszerű, amely minden nap, minden órájában megérkezik a célszemélyekhez, akiknek annak az elmaradása esetén is ellenőrizniük kell a rendszert –hiszen előfordulhat, hogy maga az üzenetküldő rendszer hibásodik meg.

Humán védelem:

Ebben a fejezetben magának a személyek által okozható esetleges károk, problémák megelőzésével foglalkozok. Itt a védelmi intézkedéseket több kategóriába lehet besorolni – ám ezeket célszerű a munkavállalónak a munkahelyén töltött időszakai szerint besorolni, osztályozni. Ennek a védelemnek a kialakításnál a HR-mint a jelölt kiválasztása, a csapat – mint közösségalkotás, munkahelyi vezető –mint az alkalmazott közvetlen felügyelete, illetve a korábban már említett IT és biztonsági szolgálatoknak van nagy szerepe.

A dolgozók első kapcsolata a leendő munkahelyükkel a megpályázni kívánt állásra történő jelentkezésükkel kezdődik. Ekkor közvetlen kapcsolatba a HR-rel kerülnek első lépésként. Már itt egy elsődleges ellenőrzésen kell a jelentkezőnek átesnie, melyek nagy vonalakban ki lehet szűrni az egyén megbízhatóságát –egy minden esetben mindenképpen kötelező háttérellenőrzést végezve. A felvételi elbeszélgetést mindenképpen úgy kell szervezni, hogy azon kiderüljön a jelölt megbízhatósága, adott szituációs gyakorlatokkal fel lehet mérni az egyén megbízhatóságát.

Amennyiben a személy megfelelt a munkaköri elvárásoknak, már attól a ponttól kezdve, mihelyst működési/működtetési adatokhoz juthat a munkaadó szervezetével, folymataival kapcsolatban a jogi osztály által már korábban elkészített adatvédelmi és egyéb nyilatkozatokat el kell fogadtatni vele. Ezek a nyilatkozatok nem gátolják meg az esetleges adatkiszivárgást –ám mind humán oldalról egy visszafogó tényező lehet, mind pedig egy esetleges bírósági ügyben ezen dokumentumok elfogadására és aláírására lehet hivatkozni. Amennyiben bármely bíróság előtt kell ezeket a dokumentumokat felhasználni –az adott védelmi rendszerek hibás működésére utalnak –ám ha ezek a nyilatkozatok kizárják az mindannak az esetleges lehetőségét, melyek kihasználásával egy külső fél információhoz juthat, vagy akár egy belső személy megsemmisítheti azokat- akkor ezeknek az aláírt dokumentumoknak komoly pszichés védelmi szerepük is, lehet. Nem elég viszont z adott dolgozóval egyszer aláíratni ezeket a dokumentumokat, hiszen a védelmi intézkedések is változnak/változhatnak, folyamatosan frissíteni kell az ott leírtakat, és azok elfogadtatását meg kell oldani az információk birtokosaival.

Egy szervezet működésében sokféle információval találkozunk, azokat megannyiképpen is csoportosíthatjuk. Az adott szervezeti egység vezetőjének, illetve a HR-nek a szerepe az információk hozzáférhetőségének kérdéseiben az, hogy mint a folyamatok legjobb ismerői –nekik kell meghatározni a feladatköröket, illetve tisztázni kell a személyek jogosultságait. A feladatkörök tisztázása akár egy jól megfogalmazott és könnyen érthető/értelmezhető és kellőképpen részletes munkaköri leírás is lehet, melyet az egyén a vállalatnál töltött ideje alapján a megfelelő mértékben mindig felül kell vizsgálni. A személyek jogosultságai szorosan kapcsolódik a munkaköri leíráshoz –ezek többnyire az IT és a biztonsági szolgálat számára elengedhetetlen fontosságúak. Tisztázni kell a jogosultságok kiosztásánál, hogy milyen jellegű adatokhoz férhet hozzá a felhasználó, illetve azt is, hogy adott esetben mely helyiségekbe szabad belépnie. Ezeknek a jogosultságok kiadásánál nagyon sokszor elkövetik azt a hibát a szervezeti kialakításokat alapul véve, hogy pl. az a vezető személy, aki a teljes szervezet legmagasabb fokán áll, bármelyik helyiségbe beléphet, rendelkezik mindazon azonosítókkal, amelyekkel minden adat számára

hozzáférhetővé válik. Ez egy téves döntés, hiszen a polihisztorok a társadalmunkban nem létezhetnek –oly nagy tudással kellene rendelkezniük, amely meghaladja egy humán kapacitását. A jogosultságok kiosztásánál neki is ebben az esetben egy egyszerű felhasználónak kell lennie –akinek pl. nincs belépési jogosultsága egyedül a szerverterembe.

A dolgozók számára ezeket az intézkedéseket világossá kell tenni, és többször el kell ismételni a számukra, hogy tudatosuljon –illetve a változásokról folyamatosan informálni kell őket. Nem elég csak bevezetni egy rendszert, azok használatát, esetleges felügyeletét meg kell ismertetni a vele kapcsolatban lévőkkel. Nem elég csak a használatára kioktatni a személyeket –hiszen ők nem gépek, hogy betanult műveletek alapján cselekedjenek, hanem magukat a folyamatokat és az esetleges kockázati tényezőket is el kell számukra magyarázni a könnyebb megérthetőség kedvéért. A legegyszerűbb példa egy ilyen oktatásra a tűzvédelmi oktatás, amely a Magyar törvények szerint kötelező minden munkavállaló számára. A munkavállalókat nem elég csak egyszer kiképezni az ilyen események bekövetkeztére –állandóan képezni kell, illetve a bevezetett folyamatokat ellenőrizni. A tűzriadó tervek megismerése és pontos végrehajtása/hajtatása kiválóan alkalmas erre a feladatra.

Az emberi tényezőket figyelembe véve nem szabad arra gondolni, hogy egy adott munkavállaló nagyon hosszú időt tölt le egy adott vállalatnál. Ennek komoly kockázati tényezőként kell szerepelni a rendszerek működésében, amely két fontos problémát vet fel: a helyettesítést, illetve az adott személy esetleges távozásakor megtenni szükséges intézkedéseket. A helyettesítés, helyettesítő folyamatok kialakulásánál a következő feltételeknek kell teljesülnie: szükség van egy olyan eszközre, személyre, aki el tudja látni a helyettesítő feladatait. Ez csak akkor teljesülhet, ha az adott munkáltató rendelkezik mind eszközparkban, mind pedig humán kapacitásban megfelelő tartalékokkal, amelyek képesek ellátni a kiesett folyamatok pótlását. Nem létezik az a rendszer, amelyet akár találomra is lehet helyettesíteni –mindenképpen szükség van egy pontos dokumentációra, amelyet a helyettesítettnek kell elkészítenie és minden esetben azt naprakészen vezetnie. Hiszen gondoljunk bele, hogy egy hirtelen súlyos egészségügyi változás, amely meggátolja a munkavállalót a mindennapi munkájának felvételében mekkora problémát, okozhat, ezért kell a pontos dokumentáció nyomon követése mellett szabályzatot kidolgozni az esetleges váratlanul bekövetkezendő helyettesítő cselekedetekre.

Szintén a helyettesítések témaköréhez tartozik –ám a legtöbb kárt a szolgáltatási folyamatban az okozhatja, ha egy munkavállaló véglegesen nem veszi fel a munkát, távozik a munkaadójától. Ebben az esetben az összes az adatvédelem kialakításában résztvevő szervezetnek/személynek ki kell dolgoznia egy folyamatot, amely a helyettesítést hivatott megoldani. A korábban említett kis időtartamra szóló helyettesítést alapul véve, mindenképp gondoskodni kell a munkafolyamatokhoz kapcsolódó pontos dokumentáció készítéséről, illetve azok átadásáról az arra kinevezett személynek, szervezetnek; így megvédve az üzleti folyamatokat és biztosítani a folytonosságukat. A távozóval kapcsolatban a legfontosabb intézkedéseket is egy szabályzatba kell rögzíteni, melyek elfogadtatása, aláírattatása a HR osztály feladata: jogi szempontból a kellő nyilatkozatok aláírása szükséges, melyben kötelezik a munkavállalót arra, hogy a munkavégzése során megszerzett információt nem osztja meg másokkal, a biztonsági szolgálatok –beleértve az IT-t is- feladatai közé tartozik az, hogy a kilépő dolgozó ne is tudjon a későbbiekben az általa korábban üzemeltetett rendszerekbe belépni, rendszereket használni –ezzel információhoz jutni, vagy éppen azokat megsemmisíteni.

A kockázati tényezőket további csoportokba lehet sorolni bekövetkezésük szerint: ezek közül megkülönböztetjük a véletlenszerű, illetve a szándékos károkozást. Míg az előbbi lehet gépek folyamatok hibája, egy előre nem látott esemény bekövetkeztével maga a folyamat, illetve a folyamat résztvevői megsérülnek, úgy a szándékos csak emberi beavatkozásra történhet. Ezt a szándékos beavatkozást a legnehezebb megelőzni és védekezni ellene. Az eszközök fejlődésével, a szabályzási folyamatok elavulásával, illetve az emberi elme egyre inkább találékonyságával szemben csak a jól bevezetett információvédelmi intézkedések összessége –azok szabályzata lehet az, melyek állandó ellenőrzésével, illetve folyamatos revíziójával, a védelmi mechanizmusok tesztelésével lehet biztonságos információvédelmi rendszert alkotni.

Van egy olyan közös pont az előzőekben ismertetett védelmek között, amelynél mind a fizikai, mind pedig a logikai védelmet a lehető legteljeskörűbbé kell tenni. Ez a hordozható számítógépek használata. Ezeknek a használata közben minden korábban említett kockázati tényező szerepet kap. Ez az az eszköz, amely felett sem a biztonsági szolgálat sem pedig az informatikai szervezet nem diszponálhat, csak kis mértékben. Mindenekelőtt magának az eszköznek a használatát kell engedélyekhez kötni. Egy ilyen hordozható számítógép –amelyen a tárolt adatok tulajdonságai, mennyisége ellenőrizhetetlen, mindenképpen nagy fokú elkötelezettséget, megbízhatóságot tételez fel a laptop használójáról. Maga az eszköz, a hordozhatóságát kihasználva könnyű célpontja a fizikai eltulajdonításoknak, ezt különböző módszerekkel lehet megelőzni, melyekkel megszüntetjük ideiglenesen a hordozhatóságukat. (Kimondottan a laptopokhoz árulnak biztonsági zárakat) –Minden fizikai védelem feloldható, ezért a biztonsági szolgálat feladata a telephelyen lévő eszközök mozgásának, mozgathatóságának dokumentálása, illetve azok nyomonkövetése és esetleges számonkérése. Ám ha a notebook elhagyta azt a területet, ahol a biztonsági szolgálat felelősséggel tartozik érte, abban az esetben már a laptop használója tartozik felelősséggel. Sajnos hiába van a felhasználók figyelme fokozottan felhívva erre a problémára, nagyon sok hordozható számítógép esik áldozatul lopásoknak. Ezekben az esetekben nem maga az eszköz fizikai értéke a kár, hanem a rajta tárolt információ –hiszen az utazások alkalmával a felhasználó nem a szervereket használja adattárolásra, hanem a helyi meghajtókat –így az ott tárolt adatok is elvesznek. (munkahelyi tapasztalataim között találkoztam olyan vezetőségi taggal, akinek több éves adatállomány veszett el hasonló módon –mindenféle mentés nélkül!) Az informatikai szervezet szerepe ebben az esetben az, hogy egy esetleges hasonló helyzetben, ha illetéktelen kezekbe kerülnek az adatok, azt ne tudják felhasználni. Ez magának az eszköznek a teljes logikai védelmét feltételezi. Léteznek különböző módszerek, amelyek az eszköz illetéktelen használata esetén mind a notebook-ot, mind pedig a rajta tárolt adatokat hozzáférhetetlenné teszik, csak a megfelelő azonosítók felhasználása után. (hiába vannak az eszközön lévő adatok biztosítva –sajnos nagyon gyakran előfordulnak a következők: vagy elfelejtik a felhasználók a dekódoláshoz szükséges jelszavakat, vagy pedig a félregépelések miatt a rendszer letiltja őket és kénytelenek megfelelő informatikai segítségért folyamodni). A fent sorolt érvek miatt ezeket az eszközöket csak pontos és a felelősségi köröket részletező szabályzásokkal, és nyilatkozatokkal lehet védeni, mert a fent leírt esetleges adatkiszivárgás, amely laptopon keresztül történik, minden esetben visszavezethető a felhasználói felelőtlenségre –így azt szabályozni kell és a megfelelő szigorítási intézkedéseket meg kell hozni.

Mindezeket figyelembevéve és egy rizikó analízist készítve egy megalapozott és kellően áttekinthető adatvédelmi szabályzat kiadása a legcélszerűbb, melynek akár teljes áttekintése és elfogadása a munkavállaló első munkahelyi cselekedetei között kell, hogy szerepeljen –közvetlenül a munkaszerződésével egyidőben.

4. VÉDELMI INTÉZKEDÉSEK

Lehet készíteni mindent lefedő adatvédelmi szabályzatot, tökéletesen hermetikusan a világtól elzárt rendszert –ám mindezeket nem elég létrehozni - betartani és felügyelni is kell. Az intézkedéseket minden esetben ellenőrizni kell, hogy követhetőek-e, illetve a ráfordított erőforrások szinkronban vannak-e a védeni kívánt adatok fontosságával. Bizonyos szervezeteknél a személyi védelem akár azt is jelentheti, hogy a biztonsági szolgálat egy kijelölt tagja egy kis időre sem hagyja magára a munkahelyén dolgozó –vagy akár a munkahelyén kívül tartózkodó személyt. Ám lássuk be, hogy ilyen jellegű biztonsági intézkedések egy a miénkhez hasonló vállalatnál zavarná a munkavégzést (nem elősegítené) és fölösleges anyagi ráfordítással járna.

A fent leírtak egy általános, a miénkkel hasonló tevékenységi kört végző vállalatra vonatkoznak. Számunkra ezek közül a legnagyobb kockázati tényezők az alábbiak, melyek megelőzésére a legnagyobb gondot kell fordítani.

Mint a bevezetőben is megfogalmaztam, ez az az üzletág, amely még szinte kialakulóban van, illetve egyre inkább terjeszkedik lefedve minden olyan területet, ahol komoly versenyszituációba kerülne. Ezért a közeljövőben fokozottan figyelni kell mindazon adatokra, információkra, amelyek felhasználásával a konkurencia lépéselőnyhöz juthat velünk szemben. Ezek közül a korábban ismertetett általános kockázati tényezők közül az alábbiak, kialakítására kell a legnagyobb figyelmet fordítani:

Fizikai védelem: a szerződött biztonsági szolgálat működésének felügyelete, ellenőrzése bizonyos időszakonként. A szolgálat által nyújtott szolgáltatás/ok állandó tesztelése, esetleges hiba észlelése esetén, illetve azok elemzése során a megfelelő konzekvenciák levonása, javítása. A cég működtetésével kapcsolatos fontos adatok kezelőinek és az általuk erre a célra használt eszközök kiemelt védelme.

Logikai védelem: pontosítani és dokumentálni a jogosultságokat és ezeknek a kiadására egy általánosan elfogadott folyamatot kidolgozni. Gondoskodni az adatbázisok akár szervezeten belüli kódolásáról is, illetve bevezetni a munkaállomások elhagyása esetén az asztalokon lévő dokumentumok biztonságos tárolásának szükségességét. A vállalatcsoporton belüli telephelyek egymás közti kommunikációját biztonságossá tenni, a megfelelő hitelesítési kóddal érkező adatok feldolgozásának szabályozása.

Szervezés, adminisztratív védelem:

A védelmi intézkedéseket egymással összhangban, egy szabályzatban kell rögzíteni, melyet az alábbi szervezeti egységek vezetőinek ellenjegyeznie kell: HR, nagyobb szervezeti egységek vezetői, informatika, biztonsági szolgálat, jogi osztály és az adatvédelmi felelős személye.

Amennyiben ez a szervezet működésében egyik meghatározó dokumentum elkészült, azt minden munkavállalóval ismertetni kell, illetve azokkal is -kivonatolva, akik bármilyen kapcsolatba kerülnek az adott céggel.

A védelmi intézkedések ebben az osztályozásban többnyire a HR és a jogi osztály felelőssége, a dokumentációt elkészíteni –jogi formába önteni, majd megismertetni a munkavállalóval.

Laptop védelem:

Felhasználói szabályzat mielőbbi bevezetése, illetve elfogadtatása a már ilyen eszközöket használókkal. Meghatározni a felelősség kérdését, rögzíteni azt az egyén, illetve a kollektív szerződés megfelelő pontjai közt.

Humán védelem:

A rizikó analízisből is látszik, hogy a legjobban védendő ez a terület adatvédelmi szempontok alapján. A jelölt kiválasztásánál a lehető leghamarabb el kell dönteni, hogy az alkalmas-e a számára kiszemelt feladatra, még mielőtt mélyrehatóbb ismeretekre tesz szert az adott szervezeti egység működésében. Amennyiben megfelelőnek találták, úgy abban az esetben mindent el kell követni az adott munkáltatónak, hogy a munkavállalót megtartsák –magakadályozva az esetleges konkurenciához történő munkahelyváltását. A dolgozókat érdekeltté kell tenni abban, hogy a saját cégük fejlődését nyomonkövessék, illetve a megszerzett információt maradéktalanul dokumentálják, hiszen egy esetleges munkaidőből történő kiesés alkalmával a helyettesítő személynek, rendszernek mindenkor naprakész információval kell rendelkeznie az adott munkafolyamattal kapcsolatban. Lehetőség szerint meg kell előzni a dolgozók munkahelyükkel szemben érzett hangulatváltozásait; illetve azokat, amennyiben mégis bekövetkeznek a HR-nek, illetve az adott csoport vezetőjének kezelnie kell.

A kialakított szervezetet, rendszert állandóan ellenőrizni kell információ és adatvédelmi szempontokból. Az idő múlásával a vagyon megóvására tett intézkedések elavulhatnak, illetve hatályukat veszíthetik. Másik nagyon fontos tényező –és itt ismét a humán szerepéhez kell visszakanyarodni, hogy mindazon bevezetett intézkedések, de nincsenek állandó kontroll alatt tartva fokozatosan veszítenek a fontosságukból és egyre kevésbé tartják be őket. Ezen intézkedések ellenőrzése és betartása/betartatása az adott szervezeti egység biztonsági felelősének a feladata. Rendelkeznie kell mindazokkal a jogosultságokkal, hogy ellenőrizni tudja mind a biztonsági szolgálat, az informatika és a HR adatait, működését. Az ilyen jellegű ellenőrzések során lehet intézkedéseket hozni a korábban meghozott szabályzatok betartására, illetve az esetleges hiányosságokra való figyelemfelhívással. Amennyiben hiányosságra kerül sor a szervezet működésében, úgy azt javítani kell és meg kell találni az adott hiba kialakulásának körülményeit, kezdőpontját. A megtalált és pontosan beazonosított hibaforrást ki kell küszöbölni, majd meghozni a szükséges intézkedéseket, hogy lehetőség szerint ne ismétlődhessen meg ismét az említett hiba. Amennyiben ez sikeresen megtörténik úgy azzal módosítani kell az eredetileg kialakított biztonsági szabályzat ide vonatkozó pontjait, vagy akár magát a teljes szabályzatot.

ÖSSZEFOGLALÁS

Dolgozatom címe: „egy cég adat- és információvédelmének kialakításának első lépései” elég tág fogalomkört ölel fel. Nem volt célom –megfelelő engedélyek, szabályzások híján kidolgozni egy olyan rendszert, mely közel 100%-osan megvédi (esetleg) a cégem információt egy külső féltől –függetlenül attól, hogy azt csak kíváncsiságból teszi, vagy üzleti haszonszerzés céljából kívánja hasznosítani. Erre a célra nem egy „egyszerű” szakdolgozat alkalmas, hanem jól képzett szakemberek tanácsai, akik mint felkért tanácsadók segítenek kialakítani az adatvédelmi rendszert.

Mégis mire lesznek használhatók az itt leírtak? Elsődlegesen arra, hogy a cég vezetésének fel lehessen hívni a figyelmét arra, hogy manapság az információ a legnagyobb kincs –és akinek ez a kezében van, az uralja a piacot. Bízom benne, hogy az adott osztályok, csoportok vezetői a dolgozatban említett problémákat, megoldási javaslatokat megfogadják és hozzásegítik a vállalatot az adatvédelmének a lehető legjobbá való tételéhez; megvalósításukhoz.

A leírtak alapján –elemezve a korábban említetteket, a kockázati tényezőket; mindezekből a legtisztábban az a kép rajzolódik elő, hogy vannak olyan problémák –melyek ellen lehet védekezni, ám vannak olyanok, melyek elkerülhetetlenek –ám a valószínűségét a bekövetkezésüknek nagymértékben lehet csökkenteni. Míg az elsőre egy egyszerű mentési, archiválási szabályzat kidolgozása –és betartása! –megfelelő, addig a második szinte kivédhetetlen.

Az emberi tényező, mely számos esetben kiszámíthatatlan az, amit a legjobban figyelembe kell venni. Egy esetleges negatív inger (bérprobléma, munkaidőprobléma) hatására vagy akár véletlenül is kárt okozhat a munkavállaló, vagy pedig kiszolgáltathatja az általa birtokolt információt a konkurenciának –akár egy munkahelyváltással is, hiszen akkor a saját tudásával -mely nem osztható meg teljes mértékben senkivel- csökkenti az adott cég profitabilitását, vagy növeli a konkurenciáét. Ez ellen kell a legjobban védekezni, a lehetőség szerint a minimálisra csökkentve mindazon tényezők számát, amely egy esetleges humán cselekedetből származhatnak.

IRODALOMJEGYZÉK

Dolgozatom elkészítése során az alábbi szakirodalmakat, illetve a témaválasztásomhoz kapcsolódó cikkeket használtam fel:

1. www.bs7799.hu 2005. március 01.
2. KÜRT Computer Rendszerház Rt.: Informatikai tanúsítás és audit megvalósítása Magyarországon –2002
3. MH Online –adat és információvédelemmel foglalkozó cikksorozata

MELLÉKLETEK

1. Szervezeti ábra
2. Helyszín alaprajz
3. Rizikó analízis