Ernst & Young Kft.
Ernst & Young Ltd.
H-1132 Budapest Váci út 20.
1399 Budapest 62. Pf.632, Hungary

Tel: +36 1 451 8100
Fax: +36 1 451 8199
www.ey.com/hu
Cg. 01-09-267553

Brázda Péter

Üzleti titkok és információk belső védelme

** Csak az a „Know-how" amit meg is tudunk védeni!**

I. Mit és kik ellen védjünk?

Minden cégben, vállalkozásban vannak értékek. Ezek lehetnek materiális, fizikai értékek, amiket fizikai eszközökkel, megfelelő módon „kulcsra zárva" relatív biztonságban tudhatunk.

Emellett viszont minden vállalatnál megvan az a tudásbázis, amitől a vállalkozásunk az, ami! Ami megkülönbözteti a konkurenciától.
Ez a tudás, „know-how" az, aminek értékéről és teljeskörű védelméről sokszor megfeledkeznek pedig ezek az értékek könnyen elérhetőek a munkavállalók, és megfelelő hozzáértéssel a kívülről érkező támadók, kíváncsiskodók részére is.

Az erősen digitalizálódó világban mindenki megtanulta, hogy az adatokat védeni szükséges.
A kívülről érkező támadások elleni védekezés, azok megakadályozása mára már jellemzően változó minőségben, de megoldott.
A külsős támadókkal szembeni védekezéssel ellentétben legtöbbször viszont nem is gondolunk arra, hogy saját munkavállalóink milyen könnyen válhatnak veszélyforrássá. Gondoljunk csak bele, hogy egy felmondási idejét töltő, konkurenciához, vagy csak hasonló munkakörbe átigazoló dolgozónk mennyi tudást vihet magával.
Ennek oka pedig nem is feltétlenül a szándékos károkozás vagy más előnybe juttatása, hanem csak az általa mindennap használt rutinok új helyre való átemelése.

Ezen rutinok átvitelével pedig könnyen kerülnek át a konkurenciához:

- szabályzatok, folyamatleírások
- kapcsolati listák
- kalkulátorok, módszertanok
- tervdokumentációk
- stb.

A fenti felsorolás jól példázza, hogy nem megfelelő védelem mellett tudásbázisunk, a cégünk jelentős értéke könnyen eltulajdonítható!

II. Hogyan védhetjük meg tudásbázisunkat a belső kockázatok ellen?

Számos informatikai megoldás létezik már a probléma megoldására, viszont önmagában egyik sem elég. Minden megoldás mellé elengedhetetlen egy jól kiépített módszertan, és a védelmi vonalak együttműködése.

II.1. Adatok osztályozása

Mielőtt bármiféle védelmet bevezetünk elengedhetetlen lépés, hogy tudjuk, mit kell megvédenünk. Mik azok az adatok, amik fontosak, milyen formában (fizikai példány papír alapon, digitális dokumentum, adatbázis stb.), és hol tároljuk azokat.

Az adatok osztályozására vonatkozó protokoll kidolgozása egy egész vállalatot megmozgató folyamat, és fontos, hogy a meglévő adatok besorolása mellett az új adatok besorolhatóságának a rendszerét és folyamatát is kialakítsuk.

II.2. Belső folyamatok megismerése

A számunkra legmegfelelőbb megoldás kiválasztásához ismernünk kell belső folyamatainkat. Tudnunk kell egyes munkakörök milyen adatokat használnak munkájuk során, mi az, amivel aktív feladatuk van, és mi az, amit csak ismernie, „olvasnia" kell a munkavállalónak feladata végrehajtásához.

Ennek feltérképezése után a kockázati étvágynak megfelelően kialakíthatóvá válik egy elérési struktúra (*„jogosultsági mátrix"*).

II.3. Ellenőrzési, védekezési módszertanok

A tudásbázisunk megvédésére szolgáló ellenőrzések módszertanának is alkalmazkodnia kell a belső működésünkhöz. A védelmi vonalak együttműködése ez esetben is elengedhetetlen, azaz az információbiztonság, a csalásmegelőzés, a compliance, a belső ellenőrzés mind ki kell, hogy vegye a részét a feladatból.

<u>Ellenőrzési módszerek</u>

Az ellenőrzési feladatok ellátásában sokat segítenek az erre a célra fejlesztett informatikai rendszerek, de már a megfelelő rendszernaplózás kialakításával és az arra épülő elemzések bevezetésével is jelentős sikereket érhetünk el.
Egy jól kialakított naplórendszer segítségével könnyen kiszűrhetővé válnak a munkavégzéstől eltérő tevékenységek. Ilyen lehet például a tömeges adatkimentés, de gyanúra adhat okot a tömeges dokumentum megnyitás is, hiszen az információ nem csak a tárolt verziójában lehet érték, hanem az abban megjelenített adat is.

<u>Védekezési módszerek</u>

A belső működésünk feltérképezése során megismerhetőek az adatok továbbítására használt csatornák is, ezek racionalizálása nagyban hozzájárul tudásbázisunk védelméhez.

A dokumentumok munkakörök egymás közötti rendszeres, és folyamatos e-mail csatolmányként továbbítása helyett a fájlmegosztó programok kontrollált használata jelentős hasznot hozhat nem csak a biztonság szempontjából, hanem a tárhelyfelhasználás szempontjából is, hiszen megszüntetheti a levelező szoftver „dokumentumtár" funkcióját, ezáltal a megszűnik a fájlok végtelen mennyiségű példányainak tárolása.

Fontos eszköz lehet külsős adathordozókra, nem kontrollált fájlmegosztókra való kimentés lehetőségének korlátozása, vagy a lényeges adatok (osztályozási kategória szerint) e-mailhez való csatolásának korlátozása is (pl: kizárólag belsős címzett esetén).
Továbbá mára már lehetőség van a kiküldött dokumentum tulajdonságokkal való ellátásra is, amivel korlátozni tudjuk azt, ki ismerheti meg annak tartalmát.

Building a better working world

III. Mire figyeljünk még?

Mint minden ellenőrzési folyamat bevezetése előtt ez esetben is kiemelten fontos a szabályozó környezet kialakítása és az érintettek megfelelő szintű tájékoztatása.

Az adatvédelmi és a munkajogi szabályok betartása és betartatása kiemelten fontos, hiszen egy észlelt üzleti titok megsértése esetén az eljárás sikeresége múlik ezen.

IV. Összefoglalás

Vállalkozásunk, cégünk tudásbázisa egyik legféltettebb kincsünk, aminek védelme elengedhetetlen a mai világban. A kintről érkező, külsős támadások elhárítása mellett kiemelten fontos, hogy ezt a tudást az üzemmenet és a belső folyamatok zökkenőmentes fenntartása mellett falainkon belül tudjuk tartani.

Ahhoz, hogy ezt sikerrel tegyünk, három pontra kell megtalálnunk a választ:

1. Miből áll a tudásbázisunk?
2. Kik férnek hozzá és miért?
3. Hogyan tudom és akarom ellenőrizni a tudásbázisom biztonságát?

Ha ezt a három kérdést meg tudjuk válaszolni, a megoldás már félig a kezünkben van!