

Információbiztonsági kockázatelemzés

Informatikai kockázatkezelési tanácsadás



Tudja, mely adatok a legértékesebbek társasága számára? Van reális képe róla, hogy ezen adatok sérülése vagy elvesztése milyen jellegű és mértékű kárt okozhat? Segítségünkkel megismerheti az információk kezelésével kapcsolatos valamennyi fenyegetést és kapcsolódó üzleti hatást, így azokra lehetőségeihez mérten hatásos választ adhat.

A helyesen kezelt és megfelelően védett információk hozzájárulnak az üzlet hatékony és eredményes működéséhez, sokba kerülhet azonban, ha az információk elvesznek, vagy illetéktelenül módosítják őket – közvetlen módon a javítására vagy újbóli előállítására fordított idő miatt, közvetve pedig az elvesztett üzleti lehetőség vagy lekéselt határidő formájában. Az érzékeny információk kiszivárgása a versenylőny elvesztésével járhat, törvényszegést eredményezhet, vagy ahhoz vezethet, hogy elveszik az ügyfelek és a munkatársak körében

hosszú idő alatt kiérdemelt bizalom, és azon keresztül az üzleti lehetőségek egy része is. Segítségünkkel megismerheti, és ezáltal hatékonyan kezelheti az információbiztonsági kihívásokat, és amennyiben társaságuk pénzügyi szolgáltatásokat is nyújt, úgy megoldásunkkal a kétévente kötelező kockázatelemzés követelményének is eleget tesz.

Ismerősek Önnek az alábbi problémák?

- Nincsenek feltérképezve az adatok, az adatkezelő rendszerek és eszközök, így nem tudni, mi az, amit védeni kell;
- nem tudni, hogy a kiépített információvédelmi eszközök és eljárások elégségesek-e, arányosak-e a valós kockázatokkal;
- az elmaradt beruházások miatt az informatikai védelmi megoldások elavultak, ugyanakkor nem egyértelmű, hogy a korszerűsítést melyik területen, milyen sorrendben kell elkezdni;
- bár bizonyos időközönként készül kockázatelemzés a társaságnál, ezeket különböző módszertanok szerint, nem koherensen végzik el, így az eredmények sem összehasonlíthatóak.

Hogyan tudunk a segítségére lenni?

A KPMG által nyújtott, nemzetközi szabványokon alapuló, ugyanakkor gyakorlatias és a felügyeleti szervek által is elfogadott keretrendszerünk az alábbi szolgáltatásokkal segíti információinak hatékony védelmét.

Eszköz- és információvagyon-nyilvántartás kialakítása: Felmérjük a szervezet által használt informatikai rendszereket, az általuk kezelt és

Kockázatelemzés szempontjai





tárolt adatok körét, valamint jellegükből, üzleti fontosságukból és érzékenysükből kiindulva osztályozzuk őket. Munkánk eredményeképpen így egy olyan adatbázist állítunk elő, mely nem csak a nyilvánvaló informatikai rendszereket, hanem a teljes szoftver- és hardvervagyon, valamint az igénybe vett szolgáltatások (telekommunikáció, közüzemek) teljes körét is tartalmazza.

Fenyegetések és bekövetkezési valószínűségük felmérése: Feltérképezzük az azonosított eszköz- és információvagyonra jellemző fenyegetéseket, legyen az külső, belső, műszaki, vagy természeti. Ezt követően historikus adatok és korábbi tapasztalataink alapján, valamint az érintettek bevonásával meghatározzuk e fenyegetések jövőbeli bekövetkezési valószínűségét.

Üzleti hatások elemzése: Az üzleti hatás-elemzés (Business Impact Analysis – BIA) elvégzésével pontosan előre jelezzük egy teoretikus fenyegetés bekövetkezése esetén a társaságot érő kár jellegét, (bevételkiesés, működési fennakadások, jogi, vagy reputációs) és pénzben kifejezett mértékét. Az üzleti hatás-elemzés kiemelkedő fontosságú, hiszen segítségével láthatóvá válik, hogy mely vagyonelemek vagy folyamatok a legfontosabbak a szervezet számára, így nyilvánvalóvá válik az is, hogy melyek védelmére kell a leginkább fókuszálni.

Kockázatok kiértékelése: A fenyegetések bekövetkezési valószínűségének és az okozott károk mértékének függvényében a már meglévő védelmi intézkedések és műszaki megoldások figyelembe vételével meghatározzuk, és rangsoroljuk a társaság számára releváns valamennyi információbiztonsági kockázatot. Ezt követően az azonosított kockázatokhoz védelmi intézkedési tervet készítünk, melynek a mérföldköveit és időtávját az Önök igényeinek és lehetőségeinek figyelembe vételével állapítjuk meg.

Milyen előnyöket nyújtunk?

- Az általunk elvégzett információbiztonsági kockázatelemzést később bármikor, akár Önök saját maguk is megismételhetik, az eredmények összehasonlíthatóak maradnak;
- keretrendszerünk gyakorlati megközelítésű, megfelel a törvényi és felügyeleti elvárásoknak, valamint figyelembe veszi az információbiztonság üzleti, technológiai, és emberi tényezőit.
- a költségek figyelembevételével teszünk javaslatot arra, miként csökkenthetőek a kockázatok elfogadható szintre; így megközelítésünk biztosítja a belső erőforrások minimális igénybevételét.

Amennyiben felkeltettük érdeklődését, a részletekkel kapcsolatosan keressen bennünket az alábbi elérhetőségeinken.

Kapcsolat:

Sallai György

igazgató

T.: +(36) 1 887 6620

E.: gyorgy.sallai@kpmg.hu

KPMG.hu



Az itt megjelölt információk tájékoztató jellegűek, és nem vonatkoznak valamely meghatározott természetes vagy jogi személy, illetve jogi személyiség nélküli szervezet körülményeire. Társaságunk ugyan törekszik pontos és időszerű információkat közölni, ennek ellenére nem vállal felelősséget a közölt információk jelenlegi vagy jövőbeli hatályosságáért. Társaságunk nem vállal felelősséget az olyan tevékenységből eredő károkért, amelyek az itt közölt információk felhasználásából erednek, és nélkülözik társaságunknak az adott esetre vonatkozó teljes körű vizsgálatát és az azon alapuló megfelelő szaktanácsadást.

A KPMG név, a KPMG logó a KPMG International lajstromozott védjegye.

© 2016 KPMG Tanácsadó Kft., a magyar jog alapján bejegyzett korlátolt felelősségű társaság, és egyben a független tagtársaságokból álló KPMG-hálózat magyar tagja, amely hálózat a KPMG International Cooperative-hez ("KPMG International"), a Svájci Államszövetség joga alapján bejegyzett jogi személyhez kapcsolódik. Minden jog fenntartva.