KPMG

Technikai informatikai biztonsági vizsgálatok

Informatikai Kockázatkezelési Tanácsadás

Tudta, hogy a hagyományos, megfelelőségi szemléletben kialakított információbiztonsági megoldások önmagukban nem jelentenek kielégítő védelmet a fejlett szervezeti és pénzügyi háttérrel bíró támadókkal, illetve egyes belső kockázatokkal szemben? Társaságuk készen áll hatékony kibervédelmi képességek kialakítására?

A világszerte egyre nagyobb számban észlelt, kiemelt kárértékkel járó incidensek is jól mutatják, hogy a nemzetközi információbiztonsági szabványoknak és a törvényi előírásoknak való, időszakonként felülvizsgált megfelelés önmagában nem jelent teljes körű védelmet a felkészült és célzott módszereket alkalmazó támadók ellen. A kihívás kezelésére alkalmas kockázatmenedzsment-rendszerek kiépítése során megalapozottan kell tudnunk dönteni arról, hogy túl a megfelelési követelményeken milyen megoldásokra célszerű pénzt áldozni a még hatékonyabb adatvédelem érdekében. Ez nem lehetséges az adott üzleti környezet és infrastruktúra szempontjából kiemelt fenyegetések és az érintett rendszerek sérülékenységeinek alapos ismeretére nélkül.

Ismerősek Önnek az alábbi problémák?

- Rengeteg hír érkezik újabb és újabb információbiztonsági kockázatokról, de nem jut naprakész adatokhoz arról, hogy a konkrét ágazatukat és gazdasági környezetüket illetően milyen specifikus fenyegetésekkel kell számolnia. Nincs megoldásuk arra sem, hogy az informatikai rendszereikben történt biztonsági eseményekről keletkező adattömeget rendszerezzék, kielemezzék. Mindezek miatt nem képesek információbiztonsági erőfeszítéseiket a tényleges fenyegetésekre fókuszálni.
- Kétségei vannak afelől, hogy az informatikai védelemért felelős megoldásaik képesek-e a gyakorlatban is megfelelni az infrastruktúra folyamatos változása okozta kihívásoknak.
- Habár belső hálózatuk védelme a külső betörések ellen eredményes, a belső kockázati tényezők (pl. rendszergazdai jogosultságokkal való visszaélés) elleni intézkedések hatékonyságáról nem kap objektív képet munkatársaitól.
- A hálózatukon korábban végzett betörési tesztek az infrastruktúra egészét lefedve automatizált módszerekre támaszkodtak. A legkritikusabb infrastruktúra-elemekről (pl. pénzügyi folyamatokat kiszolgáló szerverekről) nem rendelkeznek célzott, manuális betörési teszteredményekkel, így nincsenek megfelelő gyakorlati ismereteik ezek védettségéről sem.
- Társaságuk egyre több hordozható eszközön (pl. mobiltelefonon, tableten) működő üzleti alkalmazást használ. Ezek kliens oldali védelmében azonban nem alkalmaznak a mobil platformok generálta egyedi kihívásoknak megfelelő megoldásokat.

KPMG

Hogyan tudunk segítségére lenni?

Napjaink kihívásai komplex kibervédelem kialakítását teszik szükségessé. Alábbi szolgáltatásaink révén társaságuk képessé válik a leginkább költséghatékony megoldások kiválasztására.

Kockázati környezet vizsgálata: társaságuk munkatársaival együttműködve felmérjük az információbiztonság terén jelentkező szektorspecifikus technikai, üzleti és szabályozói kockázatokat, valamint megvizsgáljuk az általános kockázatelemzés során, illetve a biztonsági események kapcsán korábban keletkezett dokumentációkat. A vizsgálat eredményeit hasznosító elemzésünk támogatást biztosít társaságuk információbiztonsági megoldásainak kiemelt kockázatokra fókuszáló fejlesztéséhez.

Sérülékenység-vizsgálat: társaságuk munkatársaival együttműködve, aktív és passzív információgyűjtési módszerekkel feltérképezzük a társaság hálózatát, beazonosítjuk a külső peremhálózaton elhelyezkedő rendszereket, és a rajtuk futó sérülékeny szolgáltatásokat. Vizsgálatunk szükség szerint kiterjed a kliens–szerver alkalmazások, a webalkalmazások (pl. munkamenet-kezelés, titkosítási megoldások), a munkaállomások és a szerverek (pl. rendszerkonfiguráció, vírusvédelem), valamint a hálózatbiztonság (pl. távoli hozzáférési kontrollok, tűzfalak) tesztelésére.

Betörési teszt: a betörési teszteket a KPMG PTM módszertana alapján, a környezeti és a sérülékenységi vizsgálatok nyomán kialakított, társaságukkal egyeztetett célokat tartalmazó és közösen meghatározott rendszerelemekre kiterjedő terv alapján hajtjuk végre. Négy kidolgozott forgatókönyv egyedi igényekre szabott megvalósítására kerülhet sor az azonosított kockázatoknak megfelelően:

- külső betörési teszt hozzáférés nélkül (a „naiv" hacker szemszögéből);
- külső betörési teszt hozzáféréssel (egy ellenérdekűvé vált ügyfél, beszállító szemszögéből);
- belső betörési teszt hozzáférés nélkül (a társasághoz bejáratos külső támadó szemszögéből);
- belső betörési teszt hozzáféréssel (egy ellenérdekűvé vált munkatárs szemszögéből).

Részleges vizsgálatok és kiegészítő szolgáltatások: a fentieken túl vállaljuk rendszerinfrastruktúrájuk egy-egy részelemére (pl. a vezeték nélkül hálózatra, a mobil-platformokra, a kritikus alkalmazások forráskódjára) vonatkozó technikai tesztek elvégzését, valamint az informatikai erőforrásokon túlmutató alábbi támogató szolgáltatások biztosítását:

- „social engineering" vizsgálat munkatársaik gyakorlati biztonságtudatosságának felmérése céljából;
- biztonságtudatossági tréning a KPMG 3C módszertana alapján;.
- a rendszerinfrastruktúra fizikai környezeti biztonságának megfelelőségi vizsgálata;

Milyen előnyöket nyújtunk?

A KPMG Security Lab csoportja széles körű tapasztalattal bír informatikai rendszerek technikai vizsgálata terén az üzleti és a kormányzati szektorban egyaránt. Szolgáltatásaink módszertani megalapozottsága, vizsgálataink átlátható szerkezete és globális minőségbiztosítási rendszerünk jelenti a garanciát arra, hogy a társaságuknak szállítandó vizsgálati jelentések, valamint az azonnali beavatkozást igénylő sérülékenységek valós idejű, közös kezelése érdemben hozzájáruljon kibervédelmi képességeik költséghatékony, és napjaink kihívásainak megfelelő fejlesztéséhez.

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