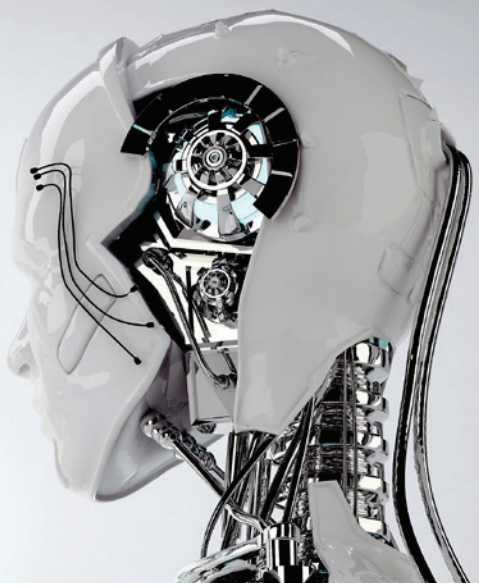
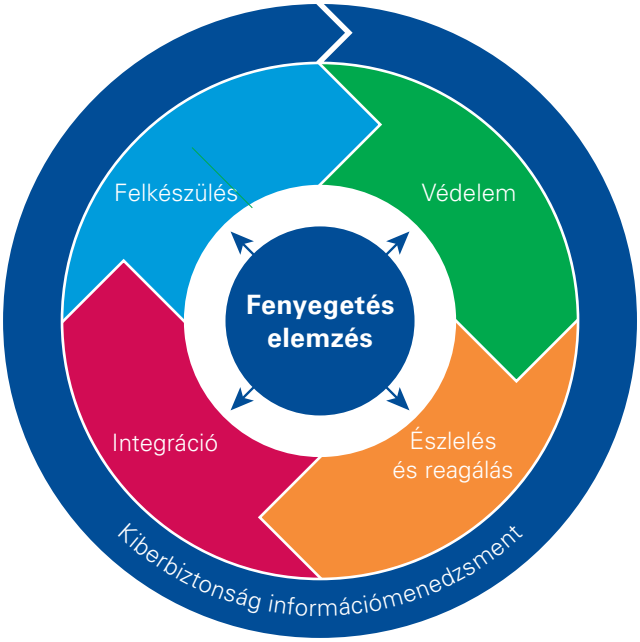
Kiberbiztonsági fenyegetéselemzés



Informatikai Kockázatkezelési Tanácsadás

Tudta Ön, hogy öt év alatt háromszorosára nőtt a kiberbűnözők által elkövetett adatbetörések száma? A vállalatvezetők több mint harmada úgy véli, a hackerek olyankor is jelen vannak az informatikai rendszereikben, amikor erről nincs tudomásuk. Az Önök társasága tisztában van azzal, hogy kibervédelmét milyen támadókkal és fenyegetésekkel szemben kell erősítenie?

Az elmúlt években egyre nagyobb károkat okoznak a vállalatok, közintézmények informatikai rendszereit érő támadások. A három leggyakoribb fenyegetés az IT-rendszerek „gyári", vagy hibás konfigurálásából eredő sérülékenységeinek kihasználása, a rosszindulatú programok telepítése, és a felhasználók biztonsági fegyelmének kijátszása. Igen változatos képet mutat ugyanakkor, hogy kik a támadók, milyen konkrét módszereket használnak, milyen időpontban, mely célpontok ellen lépnek fel, továbbá, hogy mi a támadásuk végső célja. Anélkül, hogy ezeket az információkat az adott térségre, szektorra és a hasonló működésű társaságokra vonatkozóan részletesen ismernénk, nem lehet proaktív és hatékony kibervédelmi rendszert kialakítani. A fenyegetésekre és incidensekre vonatkozó adatok elemzésén túl egyre nagyobb jelentősége van annak is, hogy az információk valós időben eljussanak a megfelelő szereplőkhöz. Így biztosítható, hogy a kibervédelem életciklusának mind a négy fázisában (lásd alábbi ábránkat) rendelkezésre álljon a gyors és eredményes cselekvéshez szükséges tudás.



Ismerősek Önnek az alábbi problémák?

Szeretne a társaságukra szabott kiberbiztonsági fenyegetéselemzési összefoglalót kapni, ugyanakkor a szükséges információk összegyűjtése időigényes feladat, illetve társaságuk nem rendelkezik az adatok feldolgozásához és elemzéséhez szükséges kompetenciákkal.

Társaságuk a rendszeres kockázatelemzések során számba veszi a lehetséges kiberfenyegetéseket, ezek az elemzések azonban nem adnak érdemi információt az alábbiakról:

- milyen külső és belső elkövetők állhatnak a fenyegetések (pl. malware bejuttatása, DDOS támadás, adatlopás, phishing) mögött,
- az elkövetők milyen célokat követnek,
- milyen gyakran hajtanak végre támadást az azonos szektorba tartozó, vagy a társaságukhoz hasonló működésű célpontok ellen,
- milyen konkrét technológia alkalmazásával és milyen forgatókönyvek mentén zajlanak a támadások.

© 2018 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.

Habár az elmúlt években társaságuk sokat fordított kiberbiztonságra, védelmi képességeik továbbra is az incidensek azonosítására és utólagos kezelésére szorítkoznak, nem alkalmasak a támadások előrejelzésére. Nehéz számszerűsítve bemutatni a kibervédelemre elkülönített források megtérülését.

Terveik között szerepel egy egységes, vállalati szintű Security Operations Center (SOC) létrehozása a biztonsági incidensek és események kezelése érdekében, melynek kialakításához külső szakértői támogatást kívánnak igénybe venni.

Hogyan tudunk segítségére lenni?

Kiberbiztonsági fenyegetéselemzés

Szakértőink rövid határidővel vállalják a nagy mennyiségű hazai és nemzetközi incidensinformáció jelentős erőforrást igénylő feldolgozását, és az Önök ágazatára, a társaságuk működésére jellemző kibertámadások adatbázisának és trendanalízisének elkészítését a KPMG globális Cyber Trends Index nevű tudástárának felhasználásával.

Törvényi megfelelőségi követelmények

A kibervédelmi stratégia és tervezés támogatása céljából a társaságukra szabott összefoglaló jelentést készítünk a törvényi előírásokról és a nemzetközi sztenderdek követelményeiről. Ennek során feltárjuk a nemzetközi szabályozók és szabványok, illetve a hazai jogszabályok Önök számára releváns kritériumait a kiberbiztonság és az adatvédelem terén. Feltérképezzük az előírások rövid- és középtávon várható változásait.

Kiberbiztonsági információmenedzsment

Szakértőink támogatják Önöket annak felmérésében, hogy kellően hatékonyak-e azok a folyamatok, melyeket társaságuk a fenyegetésekre, biztonsági eseményekre és incidensekre vonatkozó információk rögzítésére, feldolgozására és elemzésére, valamint az információk megosztására kialakított. E folyamatok optimalizálásával hozzásegítjük Önöket, hogy pontosabb előrejelzést adhassanak a kiberincidensek előfordulásáról és a támadások lefolyásáról, ami kulcsfontosságú a kiberincidensek minél hatékonyabb kezeléséhez.

Security Operations Center (SOC) kialakítása

Amennyiben társaságuk még nem rendelkezik egységes funkcióval és folyamatokkal a kiberbiztonsági információgyűjtéshez és -elemzéshez, tanácsadóink közreműködnek ezek társaságuk igényei és a legjobb nemzetközi gyakorlatok szerinti kialakításában. Amennyiben külső szolgáltatóhoz kívánja kiszervezni a SOC funkciót, segítünk a megfelelő partner kiválasztásában az ajánlattételi felhívás előkészítésétől a beadott ajánlatok szakmai értékelésén keresztül a külső szolgáltató munkájának minőségbiztosításáig.

Milyen előnyöket nyújtunk?

A KPMG globális tanácsadói hálózata és magyarországi információbiztonsági tanácsadása széles körű tapasztalattal rendelkezik a biztonsági célú adatgyűjtéshez és adatfeldolgozáshoz kötődő képességek, folyamatok kialakításában, hatékonyságának felmérésében és továbbfejlesztésében. Szakértőink együttműködnek mind magánvállalatokkal (pl. kritikus infrastruktúra működtetői), mind állami szervekkel a kibervédelemhez szükséges információelemzési funkciók és folyamatok optimalizálása terén. Tanácsadó csapatunk a szükséges információbiztonsági auditálási, technológiai, kockázatelemzési és hírszerzési kompetenciákat teljes körűen lefedi.

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

Kapcsolat:

Kórász Tamás
partner
T.: +(36) 1 887 7322
E.: tamas.korasz@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.

© 2018 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.