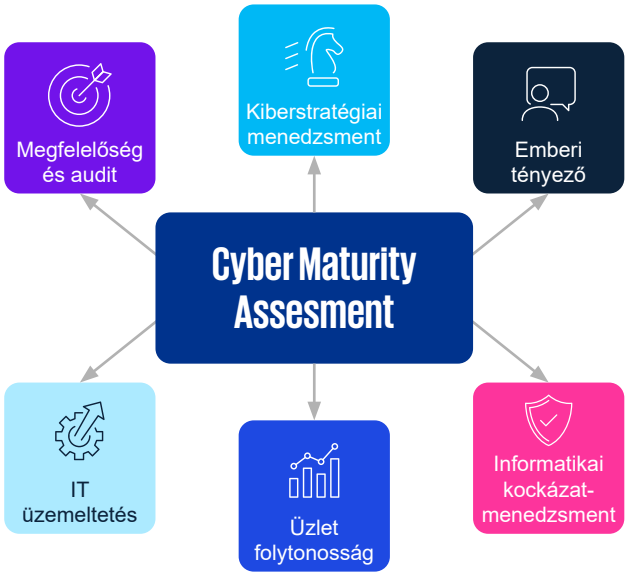
Kiberbiztonsági érettség vizsgálata

KPMG Technology Assurance

Tudta, hogy egy kiberbűnözők által végrehajtott informatikai támadás kezelése, az adatok helyreállítása akár több száz millió forint költséggel járhat? A nemrég elfogadott európai adatvédelmi rendelet miatt ráadásul az adatvédelmi bírságok ugrásszerű emelkedése is várható. Vállalatuk megfelelően felkészült a kiberbiztonsági kockázatok kezelésére?

A kiberbiztonsági kockázatok nem új keletűek, ugyanakkor egyre gyorsuló ütemben változnak. A vállalatoknak és közintézményeknek egyre több törvényi, felügyeleti előírásnak és belső szabályzatnak kell megfelelniük az adatkezelés és adatvédelem terén. Az EU 2016-ban elfogadott általános adatvédelmi rendelete nyomán a felügyeleti bírságok 2018-tól elérhetik akár az árbevétel 2-4 százalékát is. A kiberbűnözők és hackerek mindeközben egyre kifinomultabb módszereket alkalmaznak és a végrehajtott támadások száma évről-évre emelkedik.



A kibervédelmi képességeket ezért folyamatosan fejleszteni kell, mindig követve a „digitális környezet” aktuális változásait. Ma már nem elég reagálni az egyes kiberbiztonsági eseményekre: proaktív, a biztonság minden dimenzióját és a szervezet egészét lefedő megközelítésre van szükség.

Ismerősek Önnek az alábbi problémák?

- Szeretné tovább növelni a társaság informatikai kockázatkezelési rendszerének hatékonyságát, és számos javaslatot, ötletet kapni a fejlesztési lehetőségekről. Nincs ugyanakkor pontos képe kibervédelemi rendszerük jelenlegi érettségéről, és a kiindulási helyzet megfelelő ismerete nélkül nehéz meghatározni, hogy milyen fejlesztéseket és védelmi szintet tűzzenek ki stratégiai célként.
- Nem áll rendelkezésükre gyors és hatékony diagnosztikai eszköz a kibervédelmi érettség kimutatásához, a fejlődés ütemének méréséhez. Emiatt csak félévente, évente kapnak visszajelzést a fejlesztések eredményéről.
- Munkatársaik sokszor hanyagok, nem tartják be az információbiztonsági szabályokat, és az eddigi biztonságtudatossági tréningek, figyelemfelkeltő akciók nem hozták meg az elvárt eredményeket.

- Vállalatuknak, intézményüknek számos információbiztonsági előírásnak kell megfelelnie. Nehéz, időigényes feladat ugyanakkor szervezeti szinten áttekinteni, hogy a megfelelőség biztosítására kialakított eljárások mennyire hatékonyak, és milyen fejlesztésekre van szükség az esetleges felügyeleti bírságok elkerüléséhez.
- Kíváncsi arra, hogy a piac más hasonló résztvevőihez, vagy a nemzetközi információbiztonsági sztenderdekhez (pl. ISO 27001, NIST) viszonyítva társaságuk kibervédelme milyen fokú érettséget ért el, ugyanakkor nem állnak rendelkezésre jól hasznosítható benchmark adatok.;

Hogyan tudunk a segítségére lenni?

KPMG által kidolgozott Cyber Maturity Assessment módszertan révén gyorsan és hatékonyan fel tudjuk mérni mind gazdasági társaságok, mind állami vagy non-profit intézmények képességét az érzékeny adatok védelmére és a kibertámadások kezelésére. A szokásos információtechnológiai megközelítésen túl vizsgálatunk kiterjed a biztonság további dimenzióira: a biztonsági feladatokban részt vevő emberekre és a kibervédelmi rendszert támogató folyamatokra is. Újfajta értelmezési keretben mutatjuk be a sérülékenységeket, valamint a kezelésükhöz szükséges informatikai és szervezeti fejlesztéseket. Átlátható képet nyújtunk az adatvédelem terén vállalati, vagy törvényi szinten meghatározott követelményeknek való megfelelésről.

A Cyber Maturity Assessment vizsgálati módszer kidolgozása során a nemzetközi információbiztonsági sztenderdek előírásait kombináltuk a KPMG globális kiberbiztonsági, kockázatkezelési, vezetési tanácsadói és szervezetfejlesztési munkája során szerzett tapasztalatokkal. A felmérés a biztonság összesen hat dimenziójára terjed ki az alábbiak szerint:

- **Információbiztonsági irányítás:** Megvizsgáljuk azokat a folyamatokat, melyek révén a vállalat-, vagy intézményvezetés képes felelős és kezdeményező szerepet betölteni a szervezet kiberbiztonságának erősítésében.
- **Emberi tényező:** Kiértékeljük, hogy a szervezeti kultúra mennyire képes hatékonyan ötvözni a naprakész kibervédelmi tudást a megfelelő gyakorlati készségekkel és a biztonságtudatossággal.
- **Informatikai kockázatkezelés:** Feltárjuk, hogy az alkalmazott kockázatkezelési rendszer megfelelő védelmet biztosít-e az érzékeny üzleti információknak a szervezeten belül és a külső beszállítóknál egyaránt.
- **Üzletfolytonosság:** Felmérjük, hogy a kiberbiztonsági incidensek esetére kialakított eljárások képessé teszik-e a szervezetet a hatékony eseménykezelésre és a kárhatás minimalizálására.
- **Technológia és üzemeltetés:** Ellenőrizzük, hogy az IT-rendszer kialakítása és üzemeltetése terén alkalmazott biztonsági kontrollok szintje megfelel-e az azonosított kockázatok támasztotta követelményeknek.
- **Megfelelőség és audit:** Bemutatjuk, hogy a kialakított kibervédelem képes-e biztosítani a jogszabályon, vagy iparági szabványon alapuló követelményeknek való megfelelést.

Milyen előnyöket nyújtunk?

A Cyber Maturity Assessment egy egyedülállóan gyors, hatékony és átfogó diagnosztikai eszköz a kibervédelmi felkészültség mérésére és a fejlesztési szükségletek azonosítására. A KPMG Informatikai Kockázatkezelési Tanácsadása készen áll arra, hogy a vizsgálat során feltárt hiányosságok kezelésében közreműködjön a kiberbiztonság minden területén. Szakértőink támogatást biztosítanak a kibervédelmi rendszer stratégiai, folyamat- és technológiai szintű tervezésében, kialakításában, külső és belső sérülékenységi vizsgálatok, betörési tesztek végrehajtásában, az eseménykezelési és reagáló képesség fejlesztésében, valamint a proaktív, kockázatalapú biztonság-menedzsment szervezeti integrációjában.

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

KPMG.hu