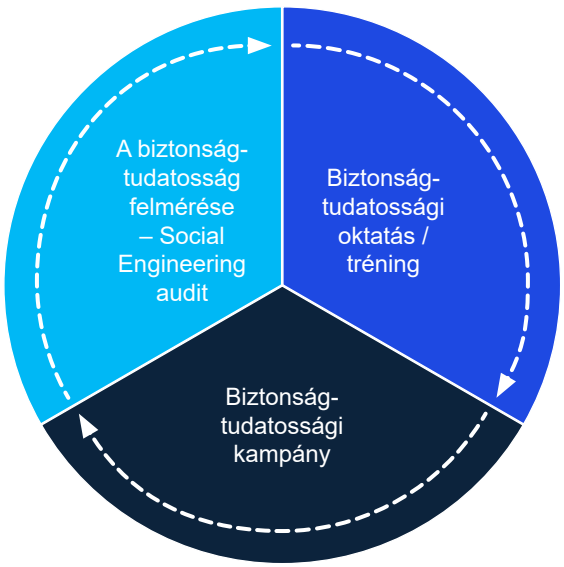
Social Engineering audit és biztonságtudatossági program

KPMG Technology Assurance

Tudta Ön, hogy az információbiztonság leggyengébb láncszeme általában az ember? Biztos abban, hogy a társaságánál dolgozó munkatársak tisztában vannak az információbiztonság-tudatosság fontosságával?

Legyen szó bármilyen vállalatról vagy intézményről, mindenhol található olyan adat, melynek nyilvánosságra kerülése vagy jogosulatlan módosítása nem kívánt hatással lehet a szervezet életére. Tapasztalataink szerint a felhasználók gyakran nincsenek tisztában azzal, hogy milyen megtévesztési technikáknak lehetnek áldozatai, illetve azzal sem, hogy akár jelentéktelennek tűnő információ kiadásával is hatalmas segítséget nyújthatnak egy, a szervezet ellen irányuló, célzott támadáshoz. Az emberi tényező jelentette kockázatok azonosítása, a biztonságtudatosság szintjének felmérése és megfelelő szinten tartása mindezek tükrében nem egyszerű feladat.



Ismerősek Önnek az alábbi problémák?

- Társaságánál a munkatársak információbiztonsági ismeretei hiányosak, vagy nem eléggé gyakorlatorientáltak. Fennáll a veszélye, hogy fertőzött fájlokat nyitnak meg, vagy adathalászat áldozataivá válnak;
- Tart tőle, hogy viszontlátja társasága bizalmas adatait a közösségi médiában;
- Nem tudja, hogyan előzhetné meg, hogy társasága munkatársai telefonon keresztül érzékeny adatokat, akár jelszavakat szivárogtassanak ki;
- Munkatársai sokszor bizalmas dokumentumokat is a kommunális szemetesbe dobnak;
- Tart attól, hogy illetéktelenek is bejuthatnak társasága telephelyére, és ott eltulajdoníthatnak eszközöket, vagy bizalmas információk kerülhetnek birtokukba.

Hogyan tudunk a segítségére lenni?

A KPMG alábbi, Social Engineering audit és biztonságtudatosság-fejlesztési szolgáltatásai segítik társaságát a belső informatikai biztonsági kontrollok hatékonyságának tesztelésében. Szolgáltatásaink külön-külön, illetve egyedi igényekre szabott csomagokban is megrendelhetőek.

Social Engineering audit: ez a vizsgálat, bevált módszer a munkavállalók biztonságtudatosságának felmérésére. Az audit során az emberi tényezőt kihasználva teszteljük a kialakított biztonsági kontrollokat. A leggyakoribb támadási formák, illetve az ezeket lehetővé tevő, leggyakrabban tapasztalt biztonságtudatossági hiányosságok alapján állítjuk össze személyre szabott auditprogramunkat.

Az ebben szereplő lehetséges feladatok a következők:

- általános információgyűjtés;
- az épületbe történő bejutás lehetőségeinek vizsgálata;
- az épületben való jogosulatlan tartózkodás során végrehajtható feladatok: eszköz eltulajdonítása, bizalmas információ megszerzése, billentyűleütést naplózó szoftver telepítése;
- telefonon keresztüli megszemélyesítéses támadások;
- hulladékátvizsgálás;
- helyszíni bejárás;
- adathalászat;
- fertőzött fájl beküldése;
- adathordozó-szétszórás.

Biztonságtudatossági oktatás, tréninganyag összeállítása: a biztonságtudatossági oktatás célja, hogy a munkatársak értesüljenek a rájuk vonatkozó, a szervezet által előírt szabályozásokról, biztonsági előírásokról, tisztában legyenek azok betartásának fontosságával, tudomást szerezzenek az őket fenyegető lehetséges veszélyekről, támadási technikákról, illetve egy esetleges Social Engineering audit során tapasztalt nem-megfelelőségekről. Diverzifikált oktatási programunknak köszönhetően az átlagfelhasználók, a menedzsment, és az üzemeltetésen dolgozó munkatársak is a számukra releváns oktatási anyagot kapják meg.

Biztonságtudatossági kampány kialakítása: a rendszeres oktatásokon túl fontos az alkalmazottak figyelmének folyamatos fenntartása is. Ennek leghatékonyabb módszere a kampányszervezés, melynek során a munkatársak nap mint nap, ismétlő jelleggel találkoznak a legfontosabb tudnivalókkal. Szolgáltatásunk keretében egyéni igényekre és szükségletekre szabott kampányt állítunk össze.

Milyen előnyöket nyújtunk?

- Valós körülmények között teszteljük a szabályozások gyakorlati működését, automatikus auditeszközök használata mellett Social Engineering támadást is szimulálunk;
- Miután a Social Engineering audit révén képet kaptunk a biztonsági érettségről, javaslatot teszünk a felzárkózáshoz, továbbfejlesztéshez szükséges lépésekre és azok prioritására vonatkozóan;
- Szolgáltatásaink kombinációjával nem csupán fel tudjuk mérni és megnyugtató szintre tudjuk emelni a biztonságtudatosság mértékét társaságánál, hanem annak szinten tarthatóságáról is gondoskodni tudunk;
- Szolgáltatásainknak köszönhetően jelentősen kisebb valószínűséggel kerül sor adatlopásra, illetve a hordozható eszközökön tárolt adatok eltulajdonítására;
- Diverzifikált oktatási programunknak köszönhetően a társaság minden munkatársát egyformán hasznos ismeretekkel látjuk el.

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

KPMG.hu