filter:max
az erőforrásbiztonsági cég

Bevezetés

A modern vállalatok mérettől és tevékenységtől függetlenül igényt tartanak a szabályozott működésre.

A tulajdonosi kockázatkezelési igényektől a külső megfelelési kényszereken és törvényi szabályozásokon át sok szempont figyelembevételével szükséges a megfelelő folyamatokat és technikai kontrollokat kialakítani.

Tanácsadói tevékenységünket azzal a céllal végezzük, hogy a vállalatokat egyre érettebb működés mellett segítsük a szabályozott működésben és kockázatkezelésben. Ezt a tulajdonosok és management számára is érthető kockázatkezelési és biztonsági stratégia kidolgozásával, a meglévő szabályzatok és megfelelőségek felülvizsgálatával, GAP elemzéssel, illetve IT biztonsági stratégia és kockázatkezelési javaslatok elkészítésével tudjuk támogatni.

Az ISO 27001 módszertana szerint az alábbi érettségi szintekre sorolhatóak a szervezetek. Természetesen ezek nem vegytiszta kategóriák, egyes területek vagy folyamatok más más érettségi szintet is mutathatnak.

Kompetenciáink

Alábbi kompetenciáink segítségével bármely kihívásban segíteni tudjuk partnereinket. Értékünk a gyorsaság és a hosszútávú gondolkodásmód, szolgáltatásainkat ezekre alapozzuk.

- Adatkezelés (DPO)
- Biztonsági műveleti központ (iSOC)
- Biztonságos rendszerfelügyelet
- (RDP, SSH, VPN, TV, LIN)
- Biztonságos vállalati WiFi
- Data Loss Protection / Prevention (DLP)
- Hálózatvédelem, hálózatbiztonság
- Incidenskezelési folyamatok kialakítása
- Incidenskezelő központ (SIEM, iSOC)
- ISO 27001:2016 auditori feladatok
- IT biztonsági műszaki audit
- Naplókezelés (Log Management)
- Objektumvédelem
- Identity Management (IDM)
- Privilegized Access Management (PAM)
- Sérülékenység vizsgálat (Voulnerability Test)
- Titkosított adattárolási megoldások
- Változáskezelés

filter:max
az erőforrásbiztonsági cég

Biztonsági stratégia, kockázat elemzés

A kockázat elemzés az legfontosabb lépés, amely segítségével stratégia készíthető és a management számára is átlátható, értelmezhető IT biztonsági irányítás valósítható meg. A kockázat elemzést a cég teljes működésére vetítve végezzük, nem csak IT folyamatokra, így lesz teljes értékű. A vizsgálatok megfelelő szervezése és mérhetősége érdekében a következő 5 ellenőrzési területen (ET1- ET5) a felosztás szerint végezzük a vizsgálatainkat:

A Fizikai Biztonsági vizsgálata (ET.1)

- kiszolgáló környezet szolgáltatásai;
- fizikai objektumok felmérése;
- tűzfal szeparáció;
- virtualizációs alapinfrastruktúra;
- storage alapinfrastruktúra;
- ugródeszka kiszolgálók;
- ugródeszka kiszolgálók központi menedzsmentje, felhasználó kezelés;
- központi frissítés és víruskeresés;
- adminisztrációs desktop kliensek;
- adatcsere szolgáltatás;
- e-mail szolgáltatás;
- adminisztratív hozzáférések audit alrendszere;
- távoli bejelentkezések azonosítása;
- központi naplógyűjtés;
- központi monitoring;
- mentési alrendszer;
- a fenti elemeket összekötő logikai hálózati kapcsolatok;
- Vagyontárgyakra vonatkozó szabályozók, és dokumentum követelmények vizsgálata;
- Felelősség a vagyontárgyakért felmérés;
- adatvagyonleltár vizsgálata;
- adatosztályozás vizsgálata;
- védelmi intézkedések felmérése.

Az adminisztratív biztonság vizsgálata (ET.2)

- Szervezeti körülmények;
- szereplők azonosítása;
- dokumentációs környezet;
- Külső felekre vonatkozó szabályozók, és dokumentum követelmények;
- A beszállító alvállalkozóinak kezelése;
- védelmi intézkedések azonosítása és bemutatása;
- titkosítás;
- Biztonsági jelentések vizsgálata;
- kockázatok ismertetése folyamat;
- kockázatok osztályozása folyamat;
- kockázatjavító intézkedések történnek;
- incidenskezelésre vonatkozó szabályozók, és dokumentum követelmények;
- incidensfolyamatok azonosítása, dokumentálása;
- riasztások kezelése;
- KPI alkalmazása;
- incidenskezelési központ;
- kivételkezelés;
- előíró dokumentumokra vonatkozó szabályozók, és dokumentum követelmények;
- előírt feladatok tervezett végrehajtásának koordinációja megvalósul e;
- nyilvántartások ellenőrzése;
- biztonságos tárolás ellenőrzése;
- „Emergency Key Management” rendszeres felülvizsgálata;
- utasítások módosítása, és annak követése,
- teljességvizsgálat belső ellenőrzési folyamatainak megvalósulása biztosított e.

filter:max
az erőforrásbiztonsági cég

A Logikai biztonság vizsgálata (ET.3)

- Az üzemeltetést a következő dokumentumok szabályozzák;
- Az üzemeltetést végzők azonosítása;
- kiemelt felhasználók azonosítása;
- különleges felelősségi körök;
- Üzemeltetési eljárások;
- Változáskezelés;
- Patch management és követés;
- Szolgáltatásnyújtás minősége;
- Tervezés és elfogadás;
- monitoringra vonatkozó szabályozók, és dokumentum követelmények;
- milyen monitoring megoldásokat alkalmaznak, saját és alvállalkozói;
- bemeneti és kimeneti pontok azonosítása;
- speciális szabályok (audit logging, UAC);
- felügyeleti rendszer vizsgálata;
- nyomok gyűjtése és tárolása hogyan valósul meg;
- összefüggésvizsgálat történik e;
- kezelési és eszkalációs folyamatok feltérképezése;
- SIEM;
- Üzletment-folytonosságra vonatkozó szabályozók, és dokumentum követelmények;
- BCP és DRP bekérése,
- tesztek azonosítása, és evidenciák (tesztjegyzőkönyvek) bekérése;
- BCP célértékek azonosítása és vizsgálata.

HUMÁN erőforrás vizsgálata (ET.4)

- Emberi erőforrásokra vonatkozó szabályozók, és dokumentum követelmények vizsgálata;
- Feladatok és felelősségi körök (szervezet rendje, munkáltatói jogkör gyakorlója);
- oktatások, képzések (terv, megvalósulás, evidenciák);
- Helyettesítés rendje (keresztkompetenciák, szabályozás);
- Munkaköri leírások, munkaszerződés, munkautasítás;
- Versenytilalmi, és jogi klauzulák;
- nyilvános szereplés és közösségi média szabályozása.

Adatvédelem, és személyes adat kezelése (ET.5)

- 2011. évi CXII. törvény (Továbbiakban: Infotv.) érintettség-vizsgálata;
- egyéb törvényi kötelezettségek érintettség-vizsgálata;
- 2016/697 EU-GDPR rendelet megfeleltetése;
- Tudatosság igazolása;
- Meglévő információk kezelése;
- Tájékoztatás biztosítása;
- Az érintettek jogainak megtartása;
- Az adatfeldolgozás jogalapja;
- Hozzájárulás megvalósulása;
- A gyermekek jogai;
- Jogsértések kezelése, folyamatai;
- Hatásvizsgálatok;
- Az adatvédelmi Tisztviselő (DPO); Nemzetközi kapcsolatok felügyelete