**Már csak azt nem tudja az Olvasó, mit is fog ténylegesen csinálni a szakdolgozat írója? Honnan hová miért hogyan akar eljutni majd a szerző lépésről lépésre?**

**Ha a chatGPT-t kérdezzük ügyesen, kb. ilyen jellegű dokumentumot kapunk, s a feladat ennek MEGHALADÁSA ember szakértelemmel, munkával.**

**Milyen címet adna a ma érintőleg említett szakdolgozati témájának?**

Komplex rendszertervek kialakítása az informatikai biztonság szakterületén

**2. Mi lenne az alcím?**

Rendszerarchitektúra fő komponensei és azok közötti kapcsolatoknak a kialakítása

**3. Hogyan nézzen ki a cím angolul?**

Designing Complex System Plans in the Field of IT Security

**4. Mi legyen az alcím fordítása angolra?**

Designing the main components of system architecture and their interrelationships

**5. Miként írná le kb. 1000 karakterben a dolgozat lényegét (vö. kivonat) = célok, célcsoportok, hasznosság, feladatok, motiváció**

**Célok:**

Az IT biztonság területén rohamos fejlődés mutatkozik, aminek a napra készen tartása eléggé nagy kihívást jelent a felhasználó számára, valamint cégek védelmének is egyaránt. Egyre szofisztikáltabb módszerekkel próbálnak a támadók rendszereket támadni, illetve adathalász tevékenységeket folytatni, továbbá ezzel visszaélni. Fontos, hogy rétegelt védelmet kell kialakítani, megfelelő eszközparkot létrehozni, ami megfelel a kihívás kritériumainak. Erősen javasolt az eszközök időszerű fejlesztése és az adott "trend" -hez való idomulása, finomhangolása.

**Célcsoportok:**A célcsoportok kissebb-nagyobb cégek és állami intézmények és hozzátartozó infrastruktúrák is érintettek egyaránt.

**Hasznosság:**Ezekkel a fejlett technológiákkal tudjuk szűrni és redukálni a beérkező támadásokat, nem kívánt káros tartalmakat. Óvni tudják a működő rendszerek folyamatosságát, és felhasználók napi munkájának körülményit megkönnyítik a zavartalan munkavégzés érdekében.

Kibervédelmi szempontból a fejlesztési költségek realizálása és a praktikum sok tényezőtől függ, és nem könnyű pontos számokat megadni. Az információ maradványértékének kiszámíthatósága is összetett, sok tényezőtől függő kérdés.

Veszélyek és kockázatok: A kibervédelem költsége és hatékonysága a fenyegetések és kockázatok típusától függ. Például egy nagyvállalatnak több erőforrást kell fordítania a védelemre, mert sebezhetőbb a kiberbűnözéssel és a kibertámadásokkal szemben.

Rendszerkomplexitás: A vállalatok és szervezetek informatikai rendszereinek mérete és összetettsége jelentős hatással van a fejlesztési költségekre. Minél nagyobb és összetettebb a rendszer, annál nagyobb erőforrásokra és finanszírozásra van szükség a megfelelő védelem kialakításához és fenntartásához.

Védelmi intézkedések típusa: A kibervédelmi stratégiában alkalmazott védelmi intézkedések típusa és szintje szintén befolyásolja a költségeket és a hatékonyságot. Például az egyszerűbb tűzfalak és víruskereső szoftverek olcsóbbak lehetnek, mint az összetett, kifinomult fenyegetésvédelmi rendszerek.

Az információ hozzáadott értéke: Az információ hozzáadott értéke az a képesség, hogy az információk és adatok védelmének javításával pozitívan befolyásolják egy vállalat vagy szervezet működését. Ez az érték lehet pénzügyi (például adataink elvesztésének vagy ellopásának megakadályozása), hírnevünk megőrzése, vagy az ügyfelek bizalmának növelése. Az információ hozzáadott értéke nehezen mérhető, és csak idővel észlelhető.

Folyamatos fejlesztés: A kibervédelem soha nem lehet teljesen statikus. A fenyegetések és a támadási minták folyamatosan változnak, ezért a védekezéssel kapcsolatos költségeket és intézkedéseket folyamatosan frissíteni és fejleszteni kell. Ez további költségekkel jár.

Végső soron nem lehet egyértelmű választ adni arra, hogy mekkora fejlesztési költségekkel mennyi hasznosság realizálható a kibervédelem terén, mivel minden szervezet más és más, és egyedi körülményekkel rendelkezik. Az információs többletérték előre tervezhetősége is változó lehet, és a hatásokat idővel lehet csak észlelni. Fontos azonban megérteni, hogy a kibervédelemre való beruházások hosszú távon kifizetődhetnek adataink és rendszereink biztonságának megőrzése és a potenciális veszteségek minimalizálása révén. Az előre tervezett beruházások és a folyamatos felülvizsgálatok segíthetnek az információs többletérték maximalizálásában.

**Feladatok:A f**elhasználókkal meg kell ismertetni a biztonságtudatos hozzáállást a munkavállalói állomány minden szintjén (kinek, hogyan?). Architektúra szempontjából fontos, hogy egy stabil rendszert tudjuk felállítani, és legyen másodlagos megoldás is.

A kiberbiztonsági feladatok indulástól az eljutásig és ezek számon kérhetősége egy fontos folyamatot jelent a kiberbiztonság területén. Az alábbiakban bemutatom a lépéseket és azt, hogyan lehet ellenőrizni vagy számon kérni ezeket a feladatokat:

Azonosítás: Az első lépés azonosítani a kiberbiztonsági feladatokat, amelyekre szükség van a vállalkozásban (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?). Ez lehet például a hálózati védelem, a tűzfal beállítások ellenőrzése, a biztonsági mentések végrehajtása stb. Fontos, hogy egyértelműen meghatározzuk ezeket a feladatokat és dokumentáljuk őket

Prioritás meghatározása: Fontos tudni, hogy melyik feladatok a legfontosabbak és melyek a kevésbé fontosak. Ezt a vállalkozás biztonsági kockázatai alapján lehet meghatározni. (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?)

Felelősök kinevezése: Minden feladathoz rendeljünk ki felelősöket, akik felelősek lesznek a feladat elvégzéséért és az eredményekért. A felelősöknek világos iránymutatást kell kapniuk a feladatokra vonatkozóan. (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?)

Rendszeres ellenőrzés: Fontos, hogy rendszeresen ellenőrizzük a kiberbiztonsági feladatok végrehajtását. Ez történhet manuálisan vagy automatizáltan, például biztonsági auditok vagy rendszeres jelentések formájában. Az ellenőrzések alkalmával ellenőrizzük, hogy a feladatokat megfelelően és időben elvégezték-e. (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?)

Eredmények dokumentálása: Dokumentáljuk az elvégzett kiberbiztonsági feladatok eredményeit. Ez segít nyomon követni a fejlődést, és biztosítja a nyomot az esetleges vizsgálatok vagy felülvizsgálatok esetére. (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?)

Szükség szerinti módosítások: Ha szükséges, módosítsuk és frissítsük a kiberbiztonsági feladatokat. A változó céges környezetben és biztonsági fenyegetések alapján folyamatosan felül kell vizsgálni és frissíteni a feladatokat. (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?)

Ezeknek a lépéseknek köszönhetően ellenőrizhetjük és számon kérhetjük a kiberbiztonsági feladatokat az indulástól az eljutásig. A dokumentáció és a rendszeres ellenőrzések kulcsfontosságúak annak biztosításához, hogy a vállalkozás számára kritikus feladatokat megfelelően elvégezzék és a biztonság megfelelő szintjét fenntartsák. (a szerző akar és ha igen, mit akar csinálni konkrétan ezen a területen?)

**Motiváció:**

Adatvédelem: Az információbiztonság elsődleges célja az érzékeny és bizalmas adatok védelme. Ezek az adatok lehetnek személyes adatok, pénzügyi információk, üzleti titkok vagy bármilyen más adat, amelynek jogi vagy üzleti következményei lehetnek, ha illetéktelenekhez jut.

Üzleti folytonosság: Az információbiztonság védelme hozzájárul az üzleti folytonossághoz. Adatainak elvesztése vagy sérülése komoly pénzügyi veszteségeket és hosszú távú károkat okozhat egy vállalkozásnak. A megfelelő védelem biztosítja, hogy az adatok rendelkezésre álljanak, amikor szükség van rájuk.

Ügyfélbizalom: Az ügyfeleknek és partnereknek bizalommal kell lenniük abban, hogy az adataikat megfelelően védik. Az információbiztonság hiánya vagy sérülése megkérdőjelezheti egy vállalkozás hitelességét és megszólítását.

Személyes felelősség: Az információbiztonság védelmének motivációjához hozzájárul az egyéni felelősség is. Az információbiztonság minden munkavállaló felelőssége, és mindenki hozzájárulhat a vállalkozás védelméhez azzal, hogy megfelelően kezeli az információkat és szabálykövető módon viselkedik.

Prevenció: Az információbiztonság védelme segít megelőzni a potenciális támadásokat és incidenseket, amelyek károkat és költségeket okozhatnak. A megelőző intézkedések hatékonyan csökkenthetik az információbiztonsági kockázatot.

**6. Hogyan néz ki angolul (abstract) a magyar kivonat?**

Helyes, hogy majd csak egy végleges magyar állapot fordítása fog megtörténni…

😊