KPMG

SAP biztonsági szolgáltatások

Kiberbiztonsági Tanácsadás

KPMG Tanácsadó Kft.

Szeretné felmérni, hogy mennyire biztonságos az SAP rendszere? Mi tudunk segíteni – a megvalósításban is.

A kibertámadások fokozott veszélye miatt a meglévő biztonsági és irányítási stratégiák egyszerűen már nem megfelelőek a SAP rendszerkörnyezet védelmében. A szervezeteknek meg kell változtatniuk az ezzel kapcsolatos szemléletüket és átfogó SAP biztonsági és irányítási stratégiát kell elfogadniuk, amely megvédi a teljes rendszerkörnyezetet. Ez megköveteli a SAP rendszereket érintő kiberbiztonsági fenyegetések proaktív azonosításának képességét, valamint egy biztonsági és irányítási stratégia végrehajtását a változó kockázatok kezelésére.

Hogy tudunk segítségükre lenni?

A főbb szolgáltatásaink alábbi rövid összefoglalóiból megtudhatja, hogy milyen területeken tudunk szakértői támogatást nyújtani az Ön vállalkozásának egyedi igényei szerint.

SAP jogosultsági koncepció

Egy megfelelően kialakított jogosultsági koncepció lehetővé teszi kollégáinak, hogy hatékonyan és időben teljesítsék feladataikat, ugyanakkor megakadályozza a csalárd cselekedeteket, és betartatja a különböző törvényeket és szabályozásokat. Szolgáltatásunk révén átfogó képet kaphat arról, hogy jelenleg milyen a jogosultsági struktúrájuk. A felmérés alapján javaslatot teszünk a hiányosságok orvoslása és a megfelelés biztosítása érdekében megteendő intézkedésekre. Ha igényli, szakértőink az egyes intézkedések megvalósításában is képesek teljes körűen közreműködni..

Összeférhetetlenségi (SoD) vizsgálatok

Meghatározzuk a meglévő jogosultsági struktúrából és a rendszer beállításaiból fakadó problémákat, különösen a feladatok nem megfelelő elkülönítését, az ütköző tevékenységeket lehetővé tevő, kockázatokhoz vezető szerepeket. Kiemelkedő szakértelemmel és eszközökkel rendelkezünk a SAP rendszerek jogosultsági struktúrájának és a SoD felülvizsgálatához. Ha még nem rendelkezik SoD Mátrixszal, mi segíthetünk annak létrehozásában is.

Vészhelyzeti hozzáférés-kezelés

Alapvető fontosságú a megfelelő vészhelyzeti hozzáférés-kezelés, amely lehetővé teszi a felhasználók számára a kritikus incidensek azonnali megoldását anélkül, hogy a napi hozzáférésük kiterjesztése miatt további kockázatok keletkeznének. Függetlenül attól, hogy használja-e a SAP GRC rendszerhez tartozó Emergency Access Management modul funkcióit, vagy létrehozott egy alternatív folyamatot, mi képesek vagyunk felmérni és értékelni az eljárás hatékonyságát. Ha jelenleg nincs kielégítő megoldása, úgy számíthat a segítségünkre a tervezés és megvalósítás során is.

Biztonsági események naplózása

A rendszer biztonságának biztosításához elengedhetetlen, hogy engedélyezzük a naplózási lehetőségeket. Az SAP Security Audit Log (SAL) megoldást biztosít a biztonsági események rögzítésére a rendszerben. Értékelésünk részeként felülvizsgáljuk a beállításokat, és szükség esetén javaslatot teszünk a megfelelő biztonsági intézkedések végrehajtására, beleértve a rendszeren belüli további naplózási lehetőségeket. Ezenkívül segítséget nyújthatunk Önnek abban, hogy ezeket az adatforrásokat beépítse a biztonsági incidensek és események kezelésére szakosodott szoftvermegoldásába (SIEM) azáltal, hogy az Ön vállalatára szabott használati eseteket biztosítunk.

ABAP programozási szabványok

Áttekintjük meglévő dokumentumaikat, amelyek útmutatást nyújtanak az ABAP fejlesztéséhez és meghatározzák a programozási szabványokat. Az értékelés során ellenőrizzük, hogy a szervezet fejlesztési politikája biztosítja-e a biztonsági követelmények figyelembe vételét, tervezését és megvalósulását a fejlesztés teljes életciklusa során.

Patch menedzsment

A biztonsági rések és a programhibák kijavításának biztosítása érdekében időnként szükséges, hogy átnézzük és szükség esetén implementáljunk a SAP által kiajánlott patcheket. Ezeknek elmulasztása esetén megnő a rendszer váratlan leállásának és a teljesítmény romlásának a kockázata. Támogathatjuk Önt egy átfogó, megbízható és költséghatékony javításkezelési folyamat létrehozásában.

Profilparaméterek

Az SAP NetWeaver biztonságának egyik első lépése a profilparaméterek beállítása. A profilparaméterek a rendszer viselkedésének és működésének számos aspektusát vezérlik. Felülvizsgálhatjuk ezeket a beállításokat, és ajánlhatunk megoldásokat a lehetséges problémákra.

Hálózati és szállítási réteg biztonsága

A rendszerek közötti interfészek komoly kockázatokkal járnak. Az adatok elveszhetnek, megváltozhatnak vagy akár duplikálódhatnak; az ilyen események pedig jelentősen befolyásolhatják a rendszerek működését vagy akár a vállalat főkönyvi adatait. Audit technikáink segítségével feltárjuk a funkcionális hibákat, és javaslatokat teszünk a fejlesztésekre. Például segíthetünk a Unified Connectivity (UCON) funkció beállításában, ami az RFC-modulok megfigyelését teszi lehetővé.

Felhasználókezelés és hitelesítés

Különböző típusú felhasználók hozhatók létre és ruházhatok fel jogosultsággal egy SAP rendszeren belül. Ellenőrizhetjük meglévő struktúráját és a kapcsolódó folyamatokat (pl. a felhasználói hozzáférések éves felülvizsgálatához kapcsolódóan), a felhasználói csoportok megfelelő használatát, valamint a biztonságos jelszó politikát és a kapcsolódó beállításokat.

Széleskörű tapasztalattal rendelkezünk a CUA eszközzel kapcsolatban is, és támogatni tudjuk Önt egy ilyen megoldás megvalósításában vagy üzemeltetésében.

SAP Health Check

Ha átfogó képet szeretne kapni a rendszereinek felkészültségéről, vagy nem tudja eldönteni, hogy mely SAP biztonsági szolgáltatásaink jelentenék a legtöbb értéket szervezete számára, kérjük, lépjen velünk kapcsolatba, hogy segíteni tudjunk Önnek. Létrehoztunk egy állapotfelmérési csomagot, amely gyors áttekintést kínál a fenti területekről, és támogatja Önt a döntéshozatali folyamatban.

Milyen előnyöket tudunk nyújtani az Ön számára?

- Kollégáink rendkívül tapasztalt szakemberek, és rendelkeznek SAP S / 4 HANA tudással is.
- Segítségünkkel világos és valós képet alkothat a SAP rendszereihez kapcsolódó gyengeségekről, lehetséges fejlesztésekről és jövőbeli kihívásokról.
- Szolgáltatásaink felkészítik az Ön vállalkozását az üzleti tevékenység során felmerülő kockázatok korai felismerésére és az előírásoknak megfelelő kezelésére.
- Csökkentheti a nem szándékosan elkövetett hibákból fakadó vagy a rosszindulatú külső és belső támadásokból eredő pénzügyi károkat és a reputációs kockázatokat.
- Szolgáltatásaink elősegítik az SAP biztonsági folyamatainak az ipari bevált gyakorlatokhoz történő igazítását, ami a jövőben jelentősen csökkenti az üzemeltetési és karbantartási költségeket.

Ha úgy érzi, hogy ezek a kérdések relevánsak a vállalkozása szempontjából, kérjük, forduljon hozzánk további részletekért.

Kapcsolat

Lukács Kornél
partner

T: +36 1 887 7472
E: kornel.lukacs@kpmg.hu

kpmg.hu

kpmg.com/socialmedia

BLOG

A jelen dokumentumban ismertetett szolgáltatások közül néhány vagy mindegyik lehet, hogy nem engedélyezett a KPMG könyvvizsgálattal érintett ügyfelei, valamint azok leányvállalatai vagy kapcsolt társaságai esetében.