VIVETECH
INFORMATION SECURITY

ViveSec

IT BIZTONSÁGI IRÁNYÍTÁSI RENDSZER KRITIKUS INFRASTRUKTÚRA SZOLGÁLTATÓKNAK

A KIHÍVÁS

Legacy kritikus infrastruktúrák

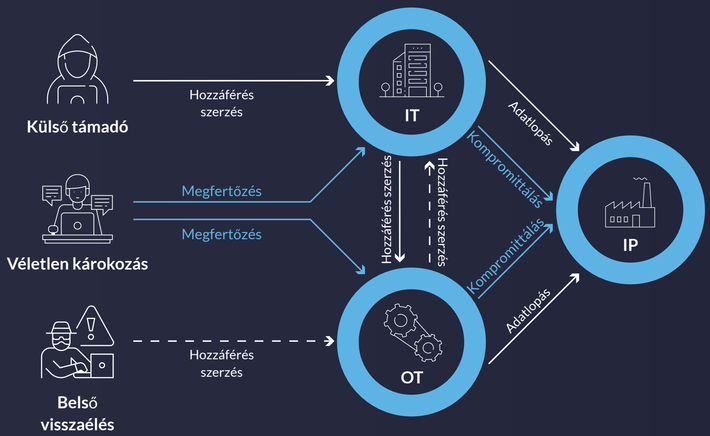
A közművállalatok, különösen a kritikus infrastruktúra-szolgáltatók hagyományosan védtelenek a kibertámadások ellen. Jellegüknél fogva nehezebb is ezeket a rendszereket védeni, hiszen üzemeltetési-beavatkozási célból gyors, távoli hozzáférést kell hozzájuk biztosítani. Ezen rendszerek életciklusa hosszú, így sokszor elavultak, tervezésüknél még nem volt szempont az IT biztonság. Az iparág sajátosságai miatt sok esetben nem is alkalmazhatóak itt a "hagyományos" informatikai biztonsági megoldások.

Kibertámadások keresztttüzében

A kritikus infrastruktúrák védelme azért is különösen fontos, mert egyre inkább a kiberhadviselés fő célpontjává válnak. Könnyen belátható, hogy egy stratégiai fontosságú áramszolgáltató elleni sikeres támadás mennyire romboló hatású lehet - a szolgáltatás teljes leállásához és személyi sérüléshez vezethet, sőt súlyos környezeti tragédiát okozhat.

Szakértelem hiánya és szabályozói követelmények

A kritikus infrastruktúrát üzemeltető szervezeteknél nem áll rendelkezésre a szükséges kibervédelmi kapacitás. Törvény kötelezi azonban őket, hogy vizsgálják felül folyamataikat, védelmi eszközeiket, és bizonyos információbiztonsági szabványoknak (pl. ISO 27001) feleljenek meg. Nagy szükség lehet tehát egy olyan automatizált szolgáltatásra, ami segít a közmű vállalatoknak az információbiztonsági irányítást kézben tartani.



1. Ábra: Iparvállalatok IT biztonsági fenyegetettségei

www.vivesec.com info@vivetech.com

A MEGOLDÁS

Iparág specifikus biztonsági irányítási rendszer

A ViVeSec egy olyan alkalmazásplatform, amely nagyfokú automatizáltságának és integráltságának köszönhetően egy rendszerben valósítja meg az információbiztonsági irányítási rendszer (IBIR) teljes körű és hatékony működtetését.

A ViVeSec egy **rugalmas, könnyen kezelhető platform**, amely minden szükséges építőelemet tartalmaz egy információbiztonsági irányítási rendszert támogató szoftver környezet összeállításához. A platform elemeinek konfigurálásával gyorsan és kockázatmentesen alakítható ki a szervezet igényeire szabott IBIR támogatás.

Hatékonyságának egyik alappillére a **nagyfokú automatizáltság**: a beépített tudásbázisra épülő elemzési képesség és a munkafolyamatok (workflow) aktívan támogatják a döntés előkészítést. A súlyozott, rendszerezett, értelmezett adatokon túl a rendszer **digitális szakértőként segíti a döntéshozatalt**. Automatizmusai és az adott iparágra szabott sablonjai lehetővé teszik akár egy egyszemélyes biztonsági szervezet által működtetett rendszer létrehozását is.

2. Ábra: Információbiztonsági minőségirányítási rendszer folyamatai

KIEMELT FUNKCIÓK

Információbiztonsági irányítás

A platform létrehozza és működteti azt az információbiztonsági irányítási keretet, amely az összes kapcsolódó feladatot és tevékenységet tartalmazza. Az irányítási rendszer elemeit a szabályozói követelmények határozzák meg, de maga a felhasználó is összeválogathatja. Az IT biztonsággal kapcsolatos valamennyi feladat tervszerűen, ütemezve, az érintett felelősökkel együttműködve kerül végrehajtásra.

Inventory és tudástár

Minden egy helyen: az adott szervezet felépítésének és működésének leírását tartalmazó adat és tudásbázis, ideértve az ehhez szükséges felmérő és adatrögzítő funkcionalitást is. Az adott iparágra jellemző, előre definiált sablonok és munkafolyamatok gyűjteménye csökkenti az IBIR rendszeren belüli feladatok erőforrás igényét, beleértve a drága és korlátozott szakértői kapacitás igényt.

Kockázatmenedzsment

A kockázatmenedzsment modul az Inventory-ban tárolt sablonok segítségével támogatja a kockázatmenedzsment teljes folyamatát. Az Inventory és a beépített logika alapján képes a fenyegetettségek teljes láncolatát automatikusan felépíteni és szimulálni. A kockázatelemzések így pontosabbak és megismételhetők lesznek. A kockázatok kezelése dinamikus és vizualizálható.

www.vivesec.com info@vivetech.com

Megfelelés (Compliance)

A ViVeSec a compliance követelményeket lefedő, beépített kontrol jegyzék segítségével képes létrehozni egy teljeskörű szabályozási rendszert, melynek szabályozási szintjeit a kockázatelemzési eredmények is befolyásolják.

A megfelelés kulcsa a kétszintű audit rendszer.
A **“Compliance audit”** képes valós időben követni a külső követelményeknek való megfelelés állapotát, és dinamikusan változtatni az erről szóló riportokat.
A **“Belső audit”** a leképezett szabályzatokat és az alkalmazott szokásjogot hasonlítja össze, amelyhez információkat a hagyományos audit módszerek szolgáltatnak. A szoftver a fenti audit megtervezését, végrehajtását és kiértékelését is hatékonyan támogatja.

Védelmi technológia irányítása (OPSEC)

A ViVeSec képes a már meglévő IT biztonsági technológiákat (tűzfal, IPS, WAF, VM, stb.) elemezni, menedzselni, és védelmi szintjüket naprakészen tartani.

Üzletmenet folytonosság

A workflow vezérelt üzletmenet folytonossági (BCM) modul segítségével különböző vészhelyzet kezelési tervek és forgatókönyvek hozhatók létre annak érdekében, hogy egy esemény bekövetkezéséből fakadó szolgáltatás-kiesés hatása minimalizálható legyen. Magas szinten támogatja a tesztelési folyamatot, amely során szimulálhatók az egyes hatásláncolatok. A BCM teszteket képes hatékonyan irányítani és dokumentálni.

Incidenskezelés

A ViVeSec tartalmaz egy kifejezetten IT biztonsági feladatokra kifejlesztett incidenskezelő modult.
A hagyományos ticketing funkciók mellett a felhasználóktól és külső rendszerektől (SIEM, HD, stb.) beérkezett kérésekből és incidensekből - sablon folyamatok mentén - képes feladatokat létre hozni (IB taszkok, kockázatelemzés, BCM feladatok, audit, adatszolgáltatás stb.), azok életciklusát nyomon követni, és eredményeit emailben visszaküldeni.

Miért a ViVeSec?

- Tartalmazza az IBIR bevezetéséhez és működtetéséhez szükséges szakértői tudást, feleslegessé teszi a jelentős szakértői jelenlétet
- Az információbiztonsági irányítás teljes folyamatát lefedi, támogatja az elvégzendő összes operatív tevékenységet
- A bevezetést, minősítést, fenntartást és a folyamatos fejlesztést is tervezi és ütemezi
- A szervezetre vonatkozó iparági és országspecifikus megfelelési követelményrendszert teljes körűen lefedi (ISO 27001, BSI, 2008/114/EC, GDPR)
- Jelentős mértékben felgyorsítja az auditra való felkészülést, és csökkenti annak költségeit
- Automatikusan kezeli az összefüggéseket, a beállt változások hatását azonnal megjeleníti
  Könnyen megtanulható, egyszerűen kezelhető, nem igényel jelentős szakértelmet
- Jól skálázható és testreszabható szoftver, amely elérhető a felhőben vagy helyileg telepítve egyaránt

Kiknek ajánljuk?

- Kritikus infrastruktúrát üzemeltető vállalatoknak
- Közműszolgáltatóknak
- Nagy iparvállalatoknak
- BSI vagy ISO 27001 megfelelés alá tartozó szervezeteknek

A ViVeSec olyan szakértői rendszer, mely a szervezet IT biztonsági érettségi szintjétől függetlenül, teljeskörűen, az iparági és a belső szabályozási környezet alapján, jelentős helyszíni tanácsadói támogatás és belső speciális tudás igénye nélkül, BSI/ISO 27001 alapokon támogatja a szervezet Információbiztonsági Irányítási Rendszerének bevezetését, minősítését, fenntartását és az információ biztonság fokozását.

ViVeTech

A ViVeTech egy 2011 óta sikeresen működő informatikai tanácsadó és fejlesztő vállalkozás, melynek fókuszában az ember és a technológia együttműködése áll. Küldetésünk, hogy a nemzetközi és hazai iparvállalatoknak és infrastruktúra üzemeltetőknek szoftverünkbe épített elemzőképesség és szaktudásunk segítségével olyan szolgáltatásokat nyújtsunk, amelyek optimalizálják működésüket, és jelentősen felgyorsítják számukra az iparági és törvényi megfelelőséget. Küldetésünkkel összhangban az információbiztonsági üzletágunk által képviselt újszerű megközelítésben is kiemelt szerepet kapnak az ergonómiai szempontok a hozzáadott üzleti érték biztosítékaként.

www.vivesec.com info@vivetech.com