
KÜRT
INFORMÁCIÓMENEDZSMENT
Az információ biztonsága

A KÜRTRŐL

Számos elemzés, tanulmány, felmérés jelent meg az elmúlt időszakban arról, hogy milyen változások mentek végbe a társadalomban és a gazdaságban. Ezek közül szinte mindegyik kiemeli azt, hogy a digitalizációban hónapok alatt többévnyi fejlődés zajlott le. Ez nem csak a használt eszközökön, szoftvereken és szolgáltatásokon látszik, de szemléletbeli változásnak is tanúi lehetünk. Ez nagyon komoly előrelépést jelent, elég csak belegondolnunk abba, hogy a digitális megoldásokkal mennyivel hatékonyabbá válhat a vállalkozások működése. Ezzel párhuzamosan rendkívüli módon megnövekedett az új kiberbiztonsági fenyegetések száma, legyen szó akár magánszemélyekről, akár vállalkozásokról vagy intézményekről- nos mind ezekkel kell napjaink vállalkozóinak szembenéznie.

A **KÜRT Információbiztonsági és Adatmentő Zrt.** lassan 40 éve, 1989-es indulásakor a megsérült számítógépes adatok helyreállítását tűzte ki célul és bátran kijelenthetem, hogy napjainkra elértük, hogy a nevünk összekapcsolódott ezzel a tevékenységgel nemcsak itthon, de nemzetközi szinten is. Évente közel 4000 adatmentési és -helyreállítási feladatot végzünk el, csak tavaly mintegy 2000 terabájtnyi adatmennyiséget sikerült helyreállítani laborunkban és úgy látjuk, a digitális fejlődésnek köszönhetően az igény folyamatosan nő szolgáltatásunkra.

Ma azonban már az adatok helyreállításánál sokkal többről szól a KÜRT, komplex információbiztonsági szolgáltatásokkal és megoldásokkal támogatjuk ügyfeleinket. Az adatmentés területén felhalmozott hatalmas tapasztalattal a birtokunkban egyedülálló szemlélettel állíthattuk fel a ma már nélkülözhetetlen adatok és információk biztonságát és hatékony kezelését támogató szolgáltatás portfóliónkat.

Információmenedzsment üzletágunk a hazai piac egyik meghatározó szereplője. A saját termékeink folyamatos fejlesztése mellett, főbb szakterületeink közé tartozik többek között a kockázatelemzés, projekt minőségbiztosítás, valamint széleskörű információbiztonsági tanácsadás. Incidensmenedzsment kompetencia központunk egyedülálló tudással és saját fejlesztésű megoldásokkal bír az etikus hackelés, vagyis az IT rendszerek sérülékenységvizsgálatának területén. Szakembereink a CEH képesítés mellett több hivatalos vizsgával is rendelkeznek. Kiemelkedő szaktudásunknak és saját fejlesztésű módszertanunknak köszönhetően az elmúlt években számos nagyvállalatnak, állami intézménynek és pénzintézetnek több száz sikeres információbiztonsági projektet hajtottunk végre.

A KÜRT portfóliója világszerte sikerrel állja meg a helyét. Adatmentés know-how-nkat megvásárolta a vietnámi és egyiptomi állam, információbiztonsági szolgáltatásainkat az EU tagállamoktól a Közel-Keletig igénybe veszik ügyfeleink. **SeCube** GRC szoftverünk, amely idén leányvállalatunkon keresztül már Németországban is elérhető, illetve szintén saját fejlesztésű **SeConical** logelemző szoftverrendszerünk a biztonságos és hatékony működésben támogatja ügyfeleinket.

A jelenlegi helyzet komoly kihívást jelent mindenki számára, amelyben az alkalmazkodóképesség, az ellenállóképesség és a stabil, megbízható működés minden eddiginél fontosabbá vált a piaci sikerekhez. Jómagam az elmúlt 30 évben, amit a Kürtnél töltöttem, részt vettem a cég szinte minden projektjében, dolgoztam a szervezet különböző szintjein. Ma vezérigazgatóként és többségi tulajdonosként a megbízhatóságot, a folyamatos stabil elérhetőséget és rendelkezésre állást, valamint a folyamatosan változó külső környezetre való reagálást tartom a legnagyobb erősségünknek.

A KÜRT több mint 30 éves tapasztalatával, folyamatosan fejlesztett szolgáltatásaival és termékeivel támogatja partnereit abban, hogy tovább haladhassanak azon az úton, amit elképzeltek maguknak és megvalósíthassák céljaikat.

Kmetty József
vezérigazgató

Tartalom

Informatikai és információbiztonsági átvilágítás

Az információ feldolgozása túlnyomórészt informatikai eszközökkel valósul meg, legyen szó akár szolgáltatás vagy termelésirányításról, elszámolásról vagy értékesítésről. Ezek és a hozzá tartozó folyamatok fenntartása, üzemeltetése, biztonságának megteremtése számos esetben nehézségekbe ütközhet, anyagi, humán vagy időbeli erőforráshiány miatt.

Teljes kép az informatikai rendszerekről

Az információbiztonsági helyzetfeltárás audit jellegű, célja, hogy olyan információkat szolgáltasson az informatikai infrastruktúra aktuális helyzetéről, amely alapján az informatikai rendszerek rendelkezésre állása, a lehetséges kockázati tényezők és biztonsági vagy üzemeltetési hiányosságok egyértelműen meghatározhatók. Az informatikai felülvizsgálatnál szempont, hogy az alkalmazott vizsgálati módszerek a teljes mértékben biztosítsák a tárgyszerűséget, és valósághű képet adjanak az informatikai rendszerek aktuális állapotáról.

Célzott vizsgálati esetek

Szolgáltatásunk célzott ügyfélspecifikus igények alapján történő felmérésről és kiértékelésről szól.

- Üzemzavar feltárás, kivizsgálás, elhárítás, megelőzés.
- Üzemeltetési hatékonyságnövelés-költségcsökkentés, szervezeti átszervezés.
- Biztonsági szint meghatározás, kockázatelemzés és kezelés, konszolidációs felmérés, migráció-szegregáció, implementáció, rendszerkivezetés.
- Kompetenciafelmérés, átszervezés, bővítés.
- Beruházástámogatás, tervkészítés, auditálás.

Az informatikai és információbiztonsági átvilágítás célja a szervezet információbiztonsági képességének felmérése és erősítése.

Módszertana

Az átvilágításhoz elsődlegesen az **ISO 27000** szabványcsaládot, továbbá a szakmai és gyártói ajánlásokat vesszük figyelembe, és ennek megfelelően vizsgáljuk Ügyfeleink informatikai rendszerét és annak szolgáltatásait.

Eredménytermékek

Az informatikai rendszerek felülvizsgálata után egy jelentést nyújtunk át Ügyfeleink számára, amelyben részletesen bemutatjuk az informatikai átvilágítás során feltárt problémákat, hiányosságokat, kockázatokat, illetve az ezekre tett megoldási javaslatainkat is.

Ide tartoznak:

- A javasolt intézkedések prioritásai, kritikussága és az ajánlott megvalósítási sorrend.
- Az elvégzendő feladatok és a végrehajtandó intézkedések.
- A feladatok elvégzéséhez kapcsolódó becsült időtávok és az időrendi terv, a javasolt intézkedések megvalósítására, ütemezésére.
- A javasolt intézkedések és megoldások becsült költsége.

Informatikai fejlesztéstámogatás

A fejlesztéstámogatás célja, hogy teljeskörű támogatást nyújtson azon szervezetek számára, amelyek új informatikai rendszereket, rendszerelemeket vezetnek be az üzleti működésük támogatására, illetve hatékonyságuk növelése érdekében.

Az informatikai rendszerek bevezetésére vonatkozó projektek lebonyolítása speciális szaktudást és tapasztalatot igényel, amely egy üzleti működésre fókuszáló szervezet esetében hiányozhat. A fejlesztéstámogatás több egymással összefüggő tevékenységből épül fel, amelyek akár önállóan is értelmezhetőek.

Mely szervezeteknek ajánljuk a szolgáltatásunkat?

Bármely olyan gazdasági szereplőnek, amely informatikai rendszer bevezetését végzi és ennek támogatására külsős szakértőt venne igénybe.

- Ha szeretné, hogy az informatikai projektje időben, a tervezetteknek megfelelően befejeződjön,
- ha szeretné, hogy az igényeknek megfelelő funkcionalitást nyújtsa a tervezett alkalmazás,
- ha szeretne segítséget igénybe venni a teljes projekt lebonyolítására,
- ha speciális informatikai szaktudásra lenne szüksége a projekt megvalósítása során,
- ha az informatikai rendszer bevezetését követően lenne szüksége informatikai támogatásra, vagy jogszabályi, rendeleti megfeleltetésben szorulna segítségre.

Mit ad a fejlesztéstámogatás?

- Fejlesztések átlátható és gyors bevezetésére szolgáló folyamatok kialakítása és bevezetése.
- Szabályozott release menedzsment folyamat kialakítása és bevezetése.
- Automatizált és kézi tesztek előkészítése és bevezetése.
- Az Informatikai rendszerek jogszabályi környezetnek (GDPR, IBTV, stb.) való megfelelésének támogatása.

BCM üzletmenet-folytonossági menedzsment

Tanácsadóink az üzleti fókuszú üzletmenet-folytonosság tervezés *(BCP)* kialakítása során, üzleti hatáselemzéshez kapcsolódó és kockázatkezelési feladatok ellátásában állnak ügyfeleink rendelkezésére.

Az üzletmenet-folytonossági tervek azzal a céllal készülnek, hogy segítséget nyújtsanak, ha az adott szervezet működésében erőforrás kiesése miatt zavar keletkezne, akár az informatikai rendszer leállásáról, akár telefonvonalak, kulcsmunkatársak kieséséről legyen szó.

Az üzletmenet-folytonosság tervezés alapvető céljai az alábbiak:

- Erőforrás kiesés esetén a kritikus üzleti folyamatok az előre meghatározott szinten működni tudjanak.
- Kritikus üzleti folyamatok kieséséhez tartozó kockázatok, károk csökkentése.
- Egy esetleges kiesés esetén a legkisebb veszteség mellett, költségek szempontjából a leghatékonyabb megoldás alkalmazását teszik lehetővé a karbantartott cselekvési tervek.

Szakértőink a szervezet üzletmenet-folytonossági terveinek elkészítéséhez komplex megoldást nyújtanak a folyamat alapú üzleti hatáselemzéstől (BIA - Business Impact Analysis), egészen az üzletmenet-folytonossági dokumentumok elkészítéséig.

Lehetőség van akár komplex *BCM (business continuity management)* megvalósításra *(BCP+DRP)* a KÜRT tapasztalt szakértőivel.

Mely szervezeteknek ajánljuk a szolgáltatásunkat?

Az üzletmenet-folytonosság tervezésre bármely gazdasági szereplőnek szüksége lehet, amelyek informatikai rendszereket alkalmaznak a napi üzletmenetük támogatására. Továbbá arra a krizishelyzetre nyújt megoldást, amikor az üzletmenetet támogató informatikai rendszer folyamatos működése megszakad. A szolgáltatás előre felkészíti a szervezetet a krizishelyzetek megfelelő kezelésére, alternatívát állít fel a kritikus üzleti folyamatok működtetésére és megfogalmazza a szervezet számára a prioritásokat és az időkereteket.

DRP - Katasztrófahelyzet utáni helyreállítás tervezés

Szolgáltatásunk keretében célunk olyan intézkedési keretrendszer készítése, fenntartása és oktatása, mely révén az ügyfél informatikai rendszerében bekövetkezett kritikus üzleti folyamatokra károsan ható incidens miatti üzleti katasztrófa elhárítható, megszüntethető. Ez által lehetőség nyílik az egyes kockázatok minimalizálására, illetve a rendszer kritikusabb pontjainak megerősítésére, annak érdekében, hogy az üzemfolytonosság ne sérüljön.

A normális üzemmenettől eltérő katasztrófahelyzetek esetén is elvárás az érintett szerverek és alkalmazások legrövidebb időn belüli újraindítása. Ennek megvalósításához azonban nem elegendő a megfelelő redundanciával bíró hardverelemek megléte, valamint a helyesen megtervezett mentési rendszer kialakítása. Ennek oka, hogy a katasztrófahelyzetek változatos módon és időszakokban jelennek meg. Ezért van szükség az informatikai rendszer tekintetében katasztrófahelyzet kezelési terv kidolgozására és körültekintően megtervezett megvalósítására.

A katasztrófahelyzet utáni helyreállítás tervezés *(DRP)* fő fókusz területe az üzleti / termelési folyamatok által használt szolgáltatások, IT rendszerek és fontosabb erőforrások helyreállításának és szolgáltatás folytonosságának a tervezése.

Feladatunk felkészíteni a szervezetet a katasztrófahelyzet kezelésére, illetve kialakítani és erősíteni az informatikai katasztrófahelyzet kezelési képességét.

A DRP tevékenységi körök

- Az informatikai folyamatok, infrastruktúra felmérése.
- Az informatikai katasztrófahelyzet kezelési tervek definiálása.
- A Katasztrófa Elhárító Csapat felépítésének és az informatikai katasztrófahelyzet kezelés menetének megtervezése.
- A katasztrófahelyzet kezeléshez kapcsolódó felelősségek és hatáskörök behatárolása.
- Az informatikai katasztrófahelyzet kezelési folyamat dokumentumrendszerének kidolgozása.
- A hibafeltárás folyamata és a helyreállítás, visszaállítás folyamata.

Eredménytermékek

- DR keretrendszer / szabályzat
- DR folyamatokhoz szükséges nyilvántartások
- DR csapat elérhetőségei:
  - Kulcsok, hozzáférések elérhetőségei
  - Tartalék eszközök elérhetőségei
  - Mentések elérhetőségei
  - Telepítő médiák elérhetőségei
  - Dokumentációk elérhetőségei
- Általános visszaállítási tervek
- Rendszerspecifikus visszaállítási tervek
- Legfontosabb rendszerspecifikus beállítási paraméterek
- DR oktatási anyagok
- DR és redundancia teszt tervek
- DR és redundancia tesztelési jegyzőkönyvek és jelentés

Sérülékenységvizsgálat

Az informatikai rendszerek sérülékenységvizsgálatának célja, hogy megelőzzük a bizalmas és nélkülözhetetlen vállalati adatok elvesztését, ellopását, illetve megakadályozzuk az ezekhez való illegális hozzáférést.

Miért létfontosságú a rendszeres sérülékenységvizsgálat?

Mert e vizsgálat adja a kiinduló információt a kockázatok kezeléséhez, a védekezéshez. A technológiai, szervezeti, strukturális változások, illetve a szükséges rendszer frissítések bármelyikének elmaradása, megváltoztatják a szervezet biztonság szintjét és folyamatosan új kockázatokat jelentenek. A KÜRT Zrt. sérülékenységvizsgálatának eredményeiből intézkedési javaslatcsomag készül, amely fontosságuk szerint priorizálva tartalmazza a hibák és biztonsági rések felszámolása érdekében végrehajtandó teendőket. Igény esetén a már kijavított hibák visszaellenőrzésével zárul a vizsgálat.

Etikus hacker

Nagyon fontos, hogy a sérülékenységvizsgálatot kizárólag megbízással rendelkező hackerek végzik, akik kifejezetten csak a megbízásban szereplő rendszereket vizsgálhatják.

Vizsgálati módszertanunk főbb paraméterei

A sérülékenységvizsgálatok irányai

- Internet felőli, külső-és belső hálózat felőli vizsgálatok.
- Webes alkalmazások és WiFi hálózatok vizsgálata.

Ügyféligény esetén szakmai támogatás nyújtása a hardening tevékenység során. A sérülékenységvizsgálat által feltárt hibák és megoldási javaslatok után a cég saját szakemberei javítják a feltárt hibákat.

Rámutat az informatikai rendszerek gyenge pontjaira, a biztonsági hiányosságokra, amelyeken keresztül a rosszindulatú támadók kárt okozhatnak.

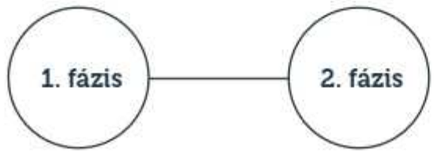
Jogosultsági szintek

Black-box: Jogosultságok nélküli vizsgálatok

Grey-box: Általános felhasználói jogosultságok birtokában végzett vizsgálatok

White-box: Kiemelt felhasználói jogosultságok birtokában végzett vizsgálatok

A sérülékenységvizsgálatok fázisai



Automata vizsgálatok

Kézi vizsgálatok

DORA/MNB IT megfelelés támogatása

A Pénzintézeti szektorra vonatkozó IT jellegű jogszabályi előírásoknak, EU rendeletnek, illetve az MNB informatikai felügyeleti ajánlásainak való megfelelés támogatása az IT prudens és megbízható működése érdekében. A szolgáltatáselem széles spektruma, akár kiterjedhet a pénzintézeti szolgáltatás nyújtásához szükséges MNB működési engedély megszerzéséhez informatikai szabályzási háttér és kockázatelemzés kialakításának támogatására, éppúgy, mint a DORA rendelet szerinti megfelelés értékelésre.

Ezen tevékenységek során a fő szempontrendszer a 2022/2554 pénzügyi ágazat digitális működési rezilienciájáról szóló (DORA) rendelethez kapcsolódó részletszabályoknak, a 42/2015. (III. 12.) Kormányrendeletnek, az MNB 1/2025. (I.13.) számú az informatikai rendszer védelméről szóló ajánlásnak, a MNB 12/2020 (XI.6.) számú távmunka és távoli hozzáférés informatikai biztonsági követelményeire vonatkozó ajánlásnak, az MNB 2/2025. (I.13.) számú a közösségi és publikus felhőszolgáltatások igénybevételére vonatkozó ajánlásnak való megfelelés. A tevékenység során kiemelten – SeCube GRC rendszerrel, kész megoldásokkal – támogatjuk az IKT kockázatkezelési keretrendszer és a fenyegetésalapú betörési tesztek (TLPT) követelményeinek való megfelelést.

DORA/MNB IT szolgáltatásunk fő területei:

- Értékeljük a Pénzintézet IT jellegű jogszabályi, DORA rendelet szerinti megfelelésének szintjét.
- Felülvizsgáljuk, és elkészítjük az előírásoknak megfelelő informatikai szabályzó dokumentumokat.
- Végrehajtjuk az informatikai biztonsági kockázatelemzést, üzleti hatáselemzést.
- Támogatjuk a szolgáltatásfolytonossági szabályzatok (üzletmenet folytonosság, katasztrófa helyzet elhárítás) kialakítását.
- Igény esetén IT auditot végzünk a kialakított gyakorlat tekintetében, akár a zártsági feltételek teljesülése, akár az IT infrastruktúra fejlesztés érdekében.
- Támogatjuk a zártsági auditra való felkészülést.
- Belső ellenőri munkaterv IT jellegű ellenőrzésében való közreműködés.
- Kiszervezett tevékenységet végzőkre vonatkozó védelmi előírások betartásának ellenőrzése

Compliance támogatás célja

Elsődleges cél, hogy a hazai jogszabályoknak, a DORA rendeletnek és MNB IT ajánlásoknak megfelelő és a kockázatokkal arányos védelem kerüljön kialakításra partnerünknél, mind a már meglévő érintett szolgáltatások, mind az MNB működési engedély megszerzésére történő felkészülés tekintetében. Ezen túlmenően fontos, hogy egy olyan információbiztonsági környezet kialakításában támogassuk a partnerünk, mely egyértelmű iránymutatást ad a szervezet számára az információbiztonsági stratégiai irányok kialakításában, fenntartásában, működtetésében.

Eredménye

Pénzintézeti IT biztonsági megfelelés eltéréselemzésének módszerét a jogszabályi környezethez igazodóan, a gyakorlati útmutatókhoz (MNB ajánlások) illeszkedően alakítottuk ki. A megfelelési vizsgálat lefolytatása során GAP analysis keretein belül a DORA rendelet és az MNB 1/2025., 12/2020. és 2/2025 számú ajánlás követelményeinek való megfelelést, vagy annak eléréséhez szükséges feladatokat azonosítva biztosítjuk, hogy a Pénzintézet az MNB audit, zártsági audit megfelelés eléréséhez szükséges stratégiáját ki tudja alakítani.

Információbiztonsági kockázatmenedzsment

A KÜRT információbiztonsági kockázatmenedzsment szolgáltatása az adott szervezet információbiztonsági kockázatainak kezelésére koncentrál, illetve rávilágít, hogy az egyes információbiztonsági kockázatok milyen hatással varnak a különböző üzleti folyamatokra, szervezeti adatokra.

Az IT szolgáltatások mindegyikére hatnak a fenyegető tényezők, melyek az adatok bizalmasságának, integritásának sérülését okozhatják, illetve az IT rendszerek rendelkezésre állását veszélyeztethetik. A szervezetek működését fenyegető tényezők közül talán az IT infrastruktúra kockázata a legnagyobb. Ide tartoznak a létesítmények, az IT technológia, az eljárások, az adatok, valamint a humánerőforrás is. Elvárandó, hogy a szinte végtelen számú fenyegetés miatt legyen esélye a védekezésnek, sőt mindez hatékonyan, a megfelelő helyen és a megfelelő mértékben legyen bevetve.

Miért a KÜRT?

Információbiztonsági kockázatelemzési módszertanunk a hazai és nemzetközi ajánlások, szabványok, iránymutatások elvárásai alapján került kidolgozásra szem előtt tartva az adott szervezetre vonatkozó jogszabályi elvárásoknak a teljesítését.

A kockázatmenedzsment folyamat főbb lépései:

1. **Módszertan** kialakítása, mely biztositja, hogy az információbiztonsági kockázatfelmérés során összehasonlítható és megismételhető eredmények álljanak elő.
2. **Üzleti hatáselemzés** elvégzése, mely meghatározza az üzleti mutatók mentén mérve az adatok kompromittálódása, integritás sérülése, illetve az informatikai rendszerek rendelkezésre állás sérülése esetén várható kárhatásokat.
3. Információbiztonsági **kockázatok feltérképezése** a fenyegetések bekövetkezési valószínűségének és lehetséges hatásainak felkutatása.
4. Az információbiztonsági **kockázatok összehasonlítható** és objektív értékelése, rangsorolása.
5. Kezelendő információbiztonsági kockázatok kiválasztása, **kockázatcsökkentő intézkedések** kidolgozása.

Milyen eredmények várhatók az információbiztonsági kockázatmenedzsmenttől?

Rövidtávon várható eredmények:

- Világossá és priorizálhatóvá válnak a környezetben, az alkalmazott technológiában, az infrastruktúrában, illetve a humánerőforrásban rejlő információbiztonsági kockázatok.
- Az információbiztonság irányithatóvá, tervezhetővé, visszacsatolhatóvá válik.

Hosszútávon várható eredmények:

- Az információs rendszer működési kockázatai kockázatarányos szinten tarthatók.
- A fenyegető tényezők bekövetkezéséből fakadó veszteségek csökkennek.

ISO 27001 felkészítés

Akár első alkalommal szeretné megszerezni Információbiztonsági Irányitási Rendszerének (IBIR) ISO 27001-es tanúsitását, akár a már meglevő tanúsitását szeretné megújitani vagy kiterjeszteni, bizalommal fordulhat több évtizedes múlttal és szakmai tapasztalattal rendelkező szakértői csapatunkhoz.

Az általunk végzett felkészítés során átfogó üzleti hatáselemzést készitünk az ügyfél üzleti folyamatairól, kockázatelemzést és részletes cselekvési tervet állitunk össze a feltárt hiányosságokra és kockázatokra, valamint a gyakorlatban is jól működő, mindenki által betartható, a hatályos jogszabályokkal összhangban lévő szabályzókörnyezetet készitünk, az adott ügyfélre jellemző egyediségek és igényeinek maximális figyelembevétele mellett.

Szakértőinkre az alábbi feladatokban számithat:

- Helyzetfelmérés, eltérés (GAP) elemzés.
- Üzleti hatáselemzés és kockázatelemzés.
- Szabályzatok (szervezeti és üzemeltetési) készitése.
- Alkalmazhatósági nyilatkozat elkészitése.
- Gyakorlatban történő bevezetés (próbaidőszak).
- Tanúsitást megelőző belső audit elvégzése, támogatása

Mely szervezeteknek ajánljuk a szolgáltatásunkat?

Minden olyan szervezetnek, amely szeretné az informatikai biztonságát kiszámithatóvá és átláthatóvá tenni, továbbá meg kiván felelni egy olyan nemzetközi szabványnak *(ISO 27001)*, melyet az egész világon ismernek és elfogadnak.

Kapcsolódó rendelkezések, szabványok, ajánlások

MSZ ISO/IEC 27001:2023 Információbiztonsági Irányitási Rendszer (IBIR) és követelményei.

MSZ ISO/IEC 27002:2023 Gyakorlati útmutató az információbiztonsági, kiberbiztonsági és adatvédelmi kontrollokhoz/intézkedésekhez.

Igény esetén cégünk az informatikai infrastruktúra kialakitását, bővitését, valamint sérülékenységvizsgálatok elvégzését is vállalja.

Kiberbiztonsági audit (NIS2 / Kiberbiztonsági törvény)

Az elmúlt években világszerte jelentősen megszaporodtak az internetes támadások mind a kormányzati, mind a magánszféra rendszereivel szemben. Az online térben zajló küzdelem eszközrendszerében és hatékonyságában is jelentősen átalakult, ezért a védekezési stratégiákat rendszeresen felül kell vizsgálni.

A Network and Information Systems (NIS) direktiva, amelyet 2016-ban vezettek be, biztonsági és jelentési kötelezettségeket irt elő az Európai Unió kritikus nemzeti infrastruktúrái számára. Ezt követően, a NIS 2 irányelv 2022-ben további célokat tűzött ki a kiberbiztonság javítása érdekében az EU-ban. Az irányelv célja, hogy minden tagállam rendelkezzen a szükséges képességekkel, intézményekkel és szabályokkal a hatékony kiberbiztonság érdekében.

A KÜRT Zrt. mint *„a kiberbiztonsági audit végrehajtására jogosult auditorok nyilvántartásáról és az auditorral szemben támasztott követelményekről szóló 7/2024. (VI. 24.) SZTFH rendelet"* alapján nyilvántartásba vett auditor, így felhatalmazásra került **„Alap"** és **„Jelentős"** biztonsági osztályba besorolt elektronikus információs rendszereket működtető szervezetekre vonatkozó kiberbiztonsági audit lefolytatására.

Cél

A kiberbiztonsági audit alkalmával az evidenciák begyűjtése és objektív érékelése során ellenőrizzük az elektronikus információs rendszerek biztonsági osztályba sorolását és az elektronikus információs rendszerek biztonsági osztályba sorolásának megfelelő védelmi intézkedések alkalmazását.

Mely szervezeteknek ajánljuk a szolgáltatásunkat?

Jelen szolgáltatásunkat a kiberbiztonsági auditra kötelezett szervezetek számára ajánljuk. *(Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági törvény) 16. (1) bekezdés).*

Módszertan

Az audit az 1/2025. (I. 31.) SZTFH rendelet és a kiberbiztonsági törvény alapján történik, figyelembevéve a 7/2024. (VI. 24.) MK rendeletet, biztosítva az előírásoknak megfelelő, strukturált és ellenőrizhető auditálási rendszert.

Vizsgálati módszerek:

- Interjú
- Dokumentum vizsgálat
- Teszt vagy a Kiberbiztonsági tv. 22. § (1) bekezdése szerinti vizsgálati tevékenységek

Eredménytermékek:

A kiberbiztonsági audit folyamatának formális lezárása során az auditorok az audit során szerzett megállapításokat, értékeléseket a hivatalos auditjelentés dokumentumban összegzik, amely átadásra került az érintett szervezetnek, valamint a Szabályozott Tevékenységek Felügyeleti Hatóságának. A kiberbiztonsági auditjelentés elkészítése mellett kiállításra kerül az auditigazolás is.

Kiberbiztonsági törvényi (NIS2) megfelelés támogatása

Szolgáltatásunk keretében megoldást kínálunk a NIS2 irányelv alapján hazai környezetben kialakított kiberbiztonsági jogszabályok megfeleléséhez, a támogatás keretében felmérésre kerül a szervezet jelenlegi felkészültsége, melynek figyelembevételével kialakításra kerülnek a jogszabályok által elvárt szabályzatok, folyamatok, kontroll környezet, kockázatelemzés, valamint javaslatot tesztünk az elektronikus információs rendszerek elvárt biztonsági osztályához szükséges intézkedési tervekre.

A NIS2 irányelvet a magyar jogba átültető Magyarország kiberbiztonságáról szóló 2024. évi LXIX. Törvénynek (Kiberbiztonsági törvény) való megfelelés támogatási munkánk célja, hogy a szervezet rendszerbiztonsági állapotára vonatkozó 7/2024. (VI. 24.) MK rendelet szerint elvárt dokumentumok (értékelési jelentés, EIR szintű kockázatelemzés, intézkedési terv, rendszerbiztonsági terv, szabályzatok) előálljanak, ezáltal kiállítható legyen a rendszer használatbavételéről vagy használatának folytatásáról szóló jegyzőkönyv.

Mely szervezeteknek ajánljuk a szolgáltatásunkat?

Minden érintett Szervezetnek, akik a Kiberbiztonsági törvény hatálya alá tartozik, illetve azon állami és piaci szereplőknek, akik támogatásra szorulnak a kiberbiztonsági jogszabályok érintettségének értékelésében, önazonosításában.

Felkészítési munka során előálló eredmények:

1. Az elektronikus információs rendszerek nyilvántartása, biztonsági osztályba sorolással.
2. Megfelelés elemzés eredményének bemutatását leíró értékelési jelentés, mely kiterjed:
   - Fizikai biztonsági környezetre
   - Szabályzói, dokumentációs környezetre
   - Elektronikus információs rendszerek specifikus biztonsági képességeire.
3. A kockázatelemzés eredményének bemutatását leíró jelentés, intézkedési terv javaslatok.
4. Rendszerbiztonsági tervek
5. Szervezetre szabott jogszabályok által elvárt szabályzat(ok)

Szakértői munkánk során a Szervezet kiberbiztonsági ellenállóképességének növelése mellett kiemelt cél az 1/2025. (I. 31.) SZTFH rendelet szerinti kiberbiztonsági audit lefolytatására való sikeres felkészítés.

A kiberbiztonsági felkészítési folyamat nem egyszeri tevékenység, folyamatosan fenn kell tartani, működtetni és fejleszteni kell a védelmi intézkedések körét jóságát, melyben a KÜRT által nyújtott kapcsolódó szolgáltatások, mint például a SeCube GRC rendszer kiemelt támogatást nyújtanak.

Kritikus szervezetek ellenállóképességének növelése

A hatályos 2024. évi LXXXIV. törvény és kapcsolódó rendeletek meghatározzák az érintett szervezetek felkészülési feladatait, de megkövetelik az ellenálló képességük átfogó fejlesztését is. Cégünk szakértői csapata segít, hogy az érintett Szervezet megfeleljen az előírásoknak, és biztosítsa az alapvető szolgáltatások zavartalan működését.

1. Ellenálló képességi terv elkészítése

- Elkészítjük a törvény által előírt Ellenálló Képességi Tervet, amely során fókuszban tartjuk:
  - A kockázatok azonosítását és kezelését.
  - A rendkívüli eseményekre való reagálási terveket.
  - Az alapvető szolgáltatások folytonosságának biztosítására vonatkozó intézkedéseket.
- Kidolgozzuk az Ellenálló Képességi Mátrixot, amely részletesen bemutatja a kockázatok kezelésének módját.

2. Ellenálló képességért felelős vezető támogatása

- Segítünk a megfelelő képesítéssel rendelkező szakember kiválasztásában vagy delegálásában.
- Támogatjuk a vezető feladatainak meghatározását és a hatóságokkal való kapcsolattartást.

3. Jogszabályi megfelelés biztosítása

- Gondoskodunk arról, hogy minden szükséges dokumentáció és terv megfeleljen a KSZE törvény és a kapcsolódó rendeletek előírásainak.
- Szükséges szabályzatokat elkészítjük.
- Felkészítjük szervezetét a hatósági ellenőrzésekre és auditokra.

4. Folyamatos támogatás és tanácsadás

- Az egyszeri felkészítési projekten túl, igény esetén hosszú távon is támogatjuk szervezetét a szabályozásoknak való megfelelés fenntartásában.
- Szakértőink rendelkezésre állnak a jogszabályi változások követésében és az új követelmények bevezetésében.

A kritikus szervezetek ellenálló képessége kulcsfontosságú Magyarország társadalmi és gazdasági stabilitásának fenntartásában. A jogi szabályozás célja, hogy a szervezetek képesek legyenek megelőzni, kezelni és helyreállítani a működésüket érintő zavarokat, legyen szó természeti katasztrófákról, technológiai problémákról vagy más váratlan eseményekről.

Szoftverfejlesztés minőségbiztosítása

Fejlesztési projekt eredményességének biztosítása, költség- és időráfordítások megfelelő korlátok között tartásával. A KÜRT minőségbiztosítói portfóliójának egyik kiemelt eleme a komplex szoftverfejlesztési projektek minőségbiztosítása.

Az ilyen, nagy költségvetésű projekteknél nagy jelentősége van a minőségbiztosítói jelenlétnek és aktivitásnak:

- Biztosítja a megrendelő elvárásainak optimális teljesülését.
- Lehetővé teszi a megrendelő és a fejlesztő közötti zökkenőmentes együttműködést.

A szoftverfejlesztési projektek kihívásai

A nagy szoftverrendszerek fejlesztésére és karbantartására rendelt erőforrások jelentős részét tesztelésre és hibajavításra fordítják, aminek oka a szoftverfejlesztési projektek nem megfelelő tervezése, a kompetenciahiány, valamint az előzetes felmérések hiánya. A folyamatos hibajavítások újabb problémákat generálnak, melyek a szoftver minőségének romlásához vezetnek.

A KÜRT Megoldása

A fentiek orvoslására kínálja a KÜRT a fejlesztés teljes életciklusát végig kísérő, saját eszközrendszerével kiegészített minőségbiztosítási módszertanát.

Egyedi minőségbiztosítási módszertan szoftverfejlesztési projektekhez

A KÜRT egyedi módszertanának segítségével a már megszokott minőségbiztosítási eredmények mellett lehetőség nyílik a kulcsparaméterek folyamatos mérésére, ellenőrzésére. Ennek köszönhetően az esetleges hibák korán felismerhetők és javíthatók lesznek, ellentétben a megszokott módszertannal, ahol a végtermék elkészülte utáni tesztek alapján történnek a javítások jóval nagyobb költség- és idővonzattal.

Szolgáltatásunk előnyei

- Több évtizedes tapasztalattal rendelkezünk az informatikai és az információbiztonsági minőségbiztosítás területén.
- Minden esetben Ügyfeleink igényeihez szabjuk az ajánlatunkat, ezáltal egyedi és költséghatékony megoldásokat kínálunk.
- A KÜRT egyedi minőségbiztosítási módszertana a komplex szoftverfejlesztések teljes életciklusában maximális szakmai támogatást nyújt.

Tesztelés és tesztmenedzsment

A tesztelés a rendszerfejlesztési életciklus szerves része, melynek célja, hogy validálásra kerüljön a szoftver/informatikai rendszer megfelelősége. Sok esetben a tesztmenedzsment feladatkörébe tartozik követelményrendszer felállítása és megfogalmazása is.

Ezen tevékenységek speciális szakmai képzettség és eszközigénye miatt célszerű ezek egy részét vagy egészét külső szakértők bevonásával végrehajtani. A speciális tesztelési megközelítések előtt fontos meghatározni a teszteléssel kapcsolatos tevékenység hatókörét, mert ez mind a szakértelmet, mind pedig az eszközöket meghatározó kritérium. Külön kell választanunk a tesztelés gyakorlati végrehajtását, a tevékenység keretrendszerének meghatározásától, a lebonyolítás irányításától, a tevékenység nyomon követésétől, melynek eredményeként két alapvető területet határozunk meg:

- **A Tesztelés maga:** Informatikai rendszer minőségének ellenőrzése.
- **A Tesztelés menedzsmentje:** a tesztelés folyamatának felügyelete, a tesztelési feladatok irányítása.

A tesztelés alatt legtöbbször értett funkcionális tesztelés helyett, mi elsősorban a nem funkcionális minőségi jellemzőkre koncentrálunk. Az általunk alkalmazott eljárás folyamata kiválóan illeszkedik a fejlesztési életciklusba, hiszen generikus lépésekből építettük fel:

1. **Tesztelés tervezése**
(célok tisztázása, a célok teljesítésének módjának meghatározása)

2. **Előfeltételek azonosítása**
(interjúk, megbeszélések, dokumentációk segítségével)

3. **Tesztelési forgatókönyv létrehozása**

4. **Tesztelés végrehajtása, tesztelési jegyzőkönyv elkészítése**

A függetlenség mellett követelmény a feladat ellátása során megismert adatok értelmezése és védelme is, amit meglátásunk szerint egy megbízható, hosszú távon is jelenlévő partner tud biztosítani. Az elmúlt évek során lehetőségünk volt számos nagy beruházás tesztelési feladatainak végrehajtásában részt vennünk, ezek tapasztalatait összegyűjtenünk.

Kiemelt tesztelési területek

- Biztonságtesztelés
- Performancia tesztelés

A nem funkcionális tesztelések elvégzése minden esetben elengedhetetlen, ha meg akarjuk előzni a negatív felhasználói élmény előfordulását, az ügyfélelégedetlenséget, a szerződésszegést eredményező működést, vagy nem várt működést, esetleg rendszerleállás kialakulását.

Kinek ajánljuk szolgáltatásunkat

Cégmérettől függetlenül bármilyen cégnek, szervezetnek, intézménynek, amely egyedi fejlesztésű szoftvert vagy informatikai rendszert:

- fejlesztet
- használ
- üzemeltet
- esetlegesen fejleszt

Adatosztályozás és biztonsági osztályba sorolás

Az elektronikus információs rendszerek biztonsági osztályba sorolása, az adatok osztályozása, akár egy teljes üzleti hatáselemzés elvégzése kulcsfontosságú a szervezetek számára, hogy megfeleljenek a 7/2024. MK rendelet és a 418/2024. Kormányrendelet előírásainak. Az adatok, folyamatok integritásának sérüléséből fakadó üzleti hatások elemzése elengedhetetlen input az elektronikus információs rendszerek kockázatarányos védelmének a kialakításához.

1. **Biztonsági osztályba sorolás támogatása MK rendelet szerint**

- Az elektronikus információs rendszerek „alap", „jelentős" vagy „magas" biztonsági osztályba sorolásának elvégzése a 7/2024. MK rendelet alapján, igény esetén a meglévő besorolás megfelelőségének validálása.
- A biztonsági osztályba sorolás dokumentált alátámasztásának támogatása, amely megfelel a jogszabályi előírásoknak.
- Segítünk a szervezet vezetőjének döntéselőkészítésében, hogy a biztonsági osztályba sorolás a kockázatokkal arányos legyen és a jogszabályi követelményeknek megfeleljen.

2. **Adatosztályozás végrehajtása vhr. alapján**

- Az adatok bizalmasság, sértetlenség és rendelkezésre állás szempontjából történő értékelése a 418/2024. Kormányrendelet előírási alapján.
- Az osztályozás eredménye alapján meghatározzuk a szükséges védelmi intézkedéseket, például titkosítási követelményeket vagy földrajzi korlátozásokat.

3. **Üzleti hatáselemzés elvégzése**

Az üzleti hatáselemzés célja, hogy meghatározhatók legyenek a EIR felé támasztott igények nem teljesítése esetén bekövetkező kárhatások, jellemzően üzleti mutatók mentén mérve (pl. anyagi, társadalmi, hírnév, jogi, működési, stb.). Teljeskörű hatáselemzés során meghatározásra kerülnek:

- A szervezet kritikus folyamatai
- RTO/RPO értékek
- A folyamatok és informatikai rendszerek kapcsolatai
- Informatikai rendszerek által kezelt adatkörök bizalmasság, sértetlenség és rendelkezésre állás értékei

A biztonsági osztályba sorolás, az adatosztályozás és az üzleti hatáselemzés célja, hogy a Szervezet elektronikus információs rendszereiben kezelt adatok védelme kockázatarányosan kerüljön kialakításra. Ez nemcsak a jogszabályi megfelelés szempontjából elengedhetetlen, hanem a Szervezet működésének biztonságát és a reputáció védelmét is szolgálja.

KÜRT Security Assurance - KSA

A KÜRT összes szakértőjének tudása az ön szolgálatában áll, hogy fejlesszük a szervezetének információbiztonságát. A *KÜRT Security Assurance* szolgáltatás keretein belül a Megrendelő a KÜRT portfóliójának bármely elemét megrendelheti. **Vállaljuk cége információbiztonsági fejlesztését és védelmét.**

A KSA szolgáltatás igénybevételének köszönhetően a Megrendelő egy folyamatosan felügyelt és karbantartott, valamint a szabványi és jogszabályi követelményeknek megfelelő információbiztonsági rendszert tudhat magáénak, mely megvalósítja a kockázatokkal arányos védelmet.

Költséghatékony megoldás. A KSA szolgáltatásra történő szerződés esetén a Megrendelő egy szakértő csapat tudását és szakértelmét állítja a saját szolgálatába, de mindig csak azokat a szolgáltatásokat, melyekre az adott időszakban szüksége van, ezzel rengeteg belső erőforrást megspórolva.

Információbiztonsági szükségletek felmérése

A csomag része és első lépése egy IT audit vizsgálat, amely feltárja a problémás területeket. Ennek eredményeként alakítjuk ki a Megrendelő számára legoptimálisabb szolgáltatáscsomag javaslatot. Az IT audit eredményét kiértékelve dönthet a Megrendelő, hogy milyen feladatok elvégzésére kívánja igénybe venni szakértői tevékenységünket, akár hosszú távon, folyamatos szolgáltatás keretében.

Egyedi szolgáltatáscsomag cégre szabva

Az IT audit elvégzése során talált problémás területek esetén lehetőség van célzott, részletes vizsgálatokra, illetve megkezdhetők a megállapítások alapján kijelölt további feladatok végrehajtása.

Kiknek ajánljuk?

Olyan cégeknek,

- ahol az informatikai szervezet méretéből fakadóan nem tudja ellátni a törvényi, szabványi és vezetői elvárások alapján elvégzendő feladatok sokaságát,
- ahol több szakterület kompetenciájára lenne szükség,
- ahol egy átfogó IT audit értékelésének segítségével kívánják továbbfejleszteni és optimalizálni a szervezet információbiztonsági képességeit.

Forensic – Digitális nyomozás szolgáltatás

Amennyiben egy cég számítógépes incidenst, visszaélést, csalást, adatmanipulációt vagy adatvesztést tapasztal, annak mindenképpen ajánlott egy átfogó képet kapnia az eseményről. Ezért minden ilyen esetben ajánlott olyan szakértő céget keresnie, akik rendelkeznek kellő szaktudással és tapasztalattal a bekövetkezett események teljeskörű kivizsgálásához.

A KÜRT *Digitális Forensic Vizsgálat* szolgáltatása épp az ilyen incidensekre, az informatikai rendszerekben bekövetkezett események felderítésére, utólagos rekonstrukciójára szolgál. Kiemelten fontos az incidens esemény bekövetkezéséhez legközelebbi állapot rögzítése és a begyűjtött bizonyítékok biztonságának és eredetiségének biztosítása, hogy a kapott eredmények és bizonyítékok egy esetleges hatósági vizsgálatnál is felhasználhatók legyenek.

A Forensic szolgáltatásunk a megtörtént incidens részleteit időrendi sorrendben képes újra összeállítani, ezen kívül bizonyítékkal tud szolgálni az incidenst alkotó események részleteiről is.

Vizsgálati tevékenység

- Számítógépes rendszerek, mobileszközök, hálózatforgalom vizsgálata.
- Naplóállományok, adattárolók elemzése.
- Események időrendi rekonstrukciója és korrelációs elemzésük.
- Informatikai rendszerekben leképzett folyamatok átvilágítása.
- Szervezetek forensic képességének megteremtése, erősítése.

Az audit módszertan lépései

1. Körülmények felmérése, hipotézis, gyanú felállítása
2. Szükséges alapadatok, adatállományok és eszközök begyűjtése
3. Adathordozókról biztonsági és az eredetivel megegyező bitazonos másolatok készítése
4. Események rekonstruálása, korrelációs elemzés
5. Incidens feltárása, esemény és hozzá tartozó adatállományok, bizonyítékok prezentálása
6. Javaslattétel a jelenlegi helyzet kezelésére, továbbá a jövőbeni hasonló incidensek elkerülése céljából
7. További intézkedések, vizsgálatok szakmai támogatása

Kinek ajánljuk szolgáltatásunkat

- Vállalatoknak
- Intézményeknek
- Szervezeteknek
- Hatóságoknak

KÜRT Adatmentés

A KÜRT Adatmentés 1989 óta van jelen az informatikai piacon, amely IT katasztrófák következményeinek felszámolására kínál világszínvonalú megoldásokat. Adatmentés üzletágunk a világ egyik vezető szaklaborja elismert adatmentési technológiával, évi közel 4000 adatmentéssel. 2003-ban Németországban megnyitottuk leányvállalatunkat, amely mostanra a német nyelvterület egyik legismertebb adatmentő cégévé vált. Magyarországon 2014-ben a KÜRT Adatmentés technológiája elnyerte a megtisztelő Hungarikum címet.

A KÜRT Adatmentés az elromlott adattárolók javításával kezdte tevékenységét a 80-as évek végén. Akkor floppy, mágneslemez, majd merevlemez javítás volt a cég fő profilja, majd jött a szinte mindent elsöprő PC-áradat. A kihívás óriási volt, és most is az. Napjainkban a félvezető alapú adattárolók adatvesztési problémái állítják mérnökeinket újabb kihívások elé.

ÉRTÉKET MENTÜNK 1989 ÓTA

HUNGARIKUM

A KÜRT adatmentés magánszemélyeknek, kis- és nagyvállalatoknak, egészségügyi intézmények, valamint állami hivatalok számára kínál megoldást informatikai katasztrófa okozta adatvesztés elhárítására. Nagyvállalati környezetben leginkább szerverek, NAS-ok és virtuális gépek helyreállítását végezzük. Ezeknél a rendszereknél jellemzően a komplexitás és a nagy adatmennyiség az, ami igazán kihívás elé állítja az adatmentő mérnököket. Mivel egy adatvesztés okozta kiesés, vagy leállás komoly anyagi károkat is okozhat ezért elsősorban vállalatok számára kínáljuk SOS-Adatmentési szolgáltatásunkat, ahol az adathordozók laborunkba beérkezésétől kezdve soron kívül, 24 órában folyamatosan azon dolgozunk, hogy a keresett adatok eredeti formájukban kerüljenek vissza a megbízóhoz.

A KÜRT hazai mérnökcsapata kutatási és fejlesztési eredményeinek köszönhetően képes sikeresen megküzdeni a technológiai fejlődés újabb és újabb feladványaival.

Ma már legalább tízezer különböző típusú adattároló van forgalomban, és a gyártók folyamatosan dolgoznak újabb és újabb eszközök fejlesztésén. Az adattárolók pedig – a gyártók minden híresztelésével ellentétben – időnként elromlanak.

Ahhoz, hogy mérnökeink folyamatosan a legmagasabb szintű szolgáltatást tudják nyújtani, a hardverek ismerete mellett, a szoftverek ismerete is elengedhetetlen.

Az adatmentés olyan technológiai eljárás melynek lényege az adatvesztés jellegének feltárása és a hibás rész elemeinek (legyen az szoftver-, vagy hardverelem) pótlása, helyettesítése. A technológiai folyamat célja az adatok mentése egy helyesen működő eszközre, adattárolóra. Az eredeti adattartalom másolását követően kezdődik a valódi adat visszaállítás, azaz a kinyert adatok vizsgálata és újra használhatóvá tétele. Az adatmentési eljárásnak ugyanakkor nem célja a hiba okának felderítése, sem magának az eszköznek a megjavítása. A problémamegoldás nehézsége elsősorban abban rejlik, hogy a hiba az építőelemek szintjén jelentkezik. A hardverhiba szinte molekuláris méretű, a szoftverhiba pedig bit méretű is lehet, amelyikből több milliárdnyi található egy modern adattárolón.

Munkánk során a legfontosabb a titoktartás és adatbiztonság. Büszkék vagyunk arra, hogy számos európai nyomozóhatóság, valamint multinacionális vállalat is ránk bízta érzékeny adatokat tartalmazó sérült adathordozóit. A technológiánk szavatolja, hogy minden esetben az eredeti állapotot megőrizve, bitazonos másolatot készítsünk a sérült adathordozóról. Az adatmentési folyamatot már ezen a munkapéldányon végezzük el. Így mindig vissza tudunk nyúlni az eredeti állapothoz, és a létező legjobb eredményt érhetjük el. Adatmentési technológiánk világszerte ismert, *know-how*-nk egyes elemeit megvásárolta a vietnámi és az egyiptomi állam is.

Az elmúlt 30 év során az adathordozók kapacitása több mint 1.000-szeresére nőtt. Ezzel együtt nőnek az adatvesztések is. 2020-ban már 2 petabyte, ami 2000 terabyte adatmennyiséget sikerült adatmentő laborunkban helyreállítani, ahol további növekedés várható.

Ügyfeleink professzionális ügyfélszolgálatunkat és a több mint 80% hatékonyságú adatmentés szolgáltatásunkat emelik ki, amelyre büszkék vagyunk és továbbra is a legmagasabb szintű kiszolgálásra törekszünk.

A SeCube GRC egy egységes keretrendszerben modulárisan összeilleszthető biztonságirányítási, kockázat, compliance, audit és üzletmenet-folytonosság menedzsment szoftver

SeCube GRC

Célja egy vállalat különböző területeinek hatókörébe tartozó – BIA, RISK, TPRM, Compliance, Audit, IT DR és BCM - biztonsággal kapcsolatos elemzői, tervezői és fenntartási folyamatok integrált támogatása, ezáltal megteremtve a teljes vállalati biztonság átlátható és riportálható irányítását.

Kiknek készült a SeCube?

A SeCube GRC célfelhasználói az IT üzemeltetés, a biztonság, az üzleti folyamat felelősök, a belső ellenőrzés és a compliance területek szakértői és vezetői. Egységes rendszerben képes a különböző szakmai területek felhasználóinak a vállalat egészét átfogó, biztonsággal kapcsolatos tevékenységeit kezelni.

Mire nyújt megoldást a SeCube

- Kockázat, TPRM, BCM és Compliance menedzsment egységes rendszerben, kockázatarányos védelem kialakítása és fenntartása.
- NIS2 és DORA **kockázatmenedzsment keretrendszer, hatósági** (NKI, SZTFH, MNB) és **kiberbiztonsági audit megfelelés** támogatása.
- A szervezet működéséhez szükséges erőforrások, szolgáltatások, adatvagyon, üzleti folyamatok és ezek kapcsolatait leíró áttekinthető struktúra.
- A biztonságirányítás különböző folyamatainak és területeinek együttműködésének támogatása, egymás eredményeinek konzisztenciája, naprakész riportok biztosítása.
- Biztonsági döntések alátámasztása, biztonságirányítás erőforrás és költség optimalizálása.

USE CASE	SeCube GRC modulok: Inventory (CMDB)	Governance	RISK	Compliance (Audit)	BCM (BCP&DRP)	TPRM
Third Party Risk Management						
Kiberbiztonsági tv. NIS2 menedzsment			7/2024 MK rendelet információbiztonsági kockázatelemzés Kockázatmenedzsment keretrendszer	7/2024 MK rendelet védelmi intézkedés felmérés, 1/2025 SZTFH kiber audit felkészülés (VMI és SZEKI kimutatás), NKI CVI felmérés, riportálás, Értékelési Jelentés, Rendszerbiztonsági terv (RBT), Cselekvés tervezés		
ISMS ISO27001			Információbiztonsági kockázatelemzés és kockázatkezelés (ISO27005)	Alkalmazhatósági nyilatkozat Belső audit és jelentések	Működésfolytonosság-Üzletmenet (ügymenet) folytonosság tervezése; IT helyreállítás tervezés; Időcélok (RTO, RPO, MTPD); Felkészülési cselekvések menedzsmentje; Tesztelés;	
MNB megfelelés DORA IKT	Szervezeti felépítés Fizikai objektumok Erőforrások (IT és termelői) Rendszerek és szolgáltatások IKT szolgáltatások Elektronikus információs rendszerek (EIR) Third party és szolgáltatásaik Adatvagyon nyilvántartás GDPR Adatkezelési tevékenységek Üzleti folyamatok Termékek és vállalati szolgáltatások Adatvagyon nyilvántartás Vagyonelem leltár Vállalati működési modell, erőforrás függőségek Vizuális szimulációk	Üzleti hatáselemzés (BIA) BSR osztályozás Inventory felülvizsgálat menedzsment Védelmi intézkedések nyilvántartása Feladatkezelő Incidens nyilvántartás Biztonsági kivételek nyilvántartás Dokumentum menedzsment	DORA IKT kockázat elemzési és kezelési keretrendszer (IT, információbiztonság, fizikai és szervezeti)	MNB ajánlások és DORA IKT megfelelés felmérés Belső audit támogatás		Vendorok és Szolgáltatásaik nyilvántartása Kérdőív és TP risk módszertan Vendor felmérések workflow menedzsmentje Mitigációs feladatok menedzsmentje Dokumentum menedzsment Vendorok Adatvédelmi felmérése
BCM (ISO22301)			Szervezeti működési kockázatelemzés			
IT DRP			IT működési kockázatelemzés			
ERM vállalati kockázatmenedzsment			Üzleti/működési, információbiztonsági, humán, fizikai kockázatelemzés és kockázatkezelés			
GDPR			Adatkezelési tevékenységek kockázatelemzés	GDPR megfelelés vizsgálat		
Belső audit				Belső audit és eltérés tervezés Kontrol környezet		

Funkciók és modulok áttekintése

Vállalati biztonsági integrált irányítása:

- **Egy vállalat, egy biztonsági irányítás.** A szerteágazó biztonsági területek és folyamatok együttműködésének integrált támogatása, egységes és összeérő módszertanok, nyilvántartások mentén, biztositva a naprakész és konzisztens eredményeket (riportok, tervek, compliance és risk jelentések).
- **Leszámolás az egyszeri eredménytermékekkel.** A kockázatelemzési jelentés, a BCP, DRP, GDPR vagy a megfelelés jelentések már nem egyszeri eredmények, hanem könnyen karbantartható, kevesebb emberi erőforrást igénylő folyamatok, igény szerint generálható naprakész riportokkal.
- A korábban compliance kényszerből végrehajtott feladatok, a compliance megugráson túl, valós biztonsági irányitási folyamatokká és eredményekké válnak.

Inventory - CMDB

A SeCube konfigurációs adatbázisában nyilvántartott erőforrásokat hierarchiába és kapcsolati viszonyba szervezhetjük, valamint definiálhatjuk a vállalat működési modelljét. Az adatbázisban többek között a vállalat szervezeti felépitését, telephelyi struktúráját, technológiai és humán erőforrásait, rendszereit, szolgáltatásait, adatvagyonát, GDPR adatkezelési tevékenységeit és üzleti folyamatait és termékeit rögzithetjük, illetve ezek összefüggéseit ábrázolhatjuk, modellezhetjük a működési függőségeket.

BIA - Üzleti hatáselemzés

Felméréseket készithetünk az üzleti tevékenységek / adatok / rendszerek lehetséges sérülése mentén fellépő anyagi és immateriális kárhatásokról. A hatáselemzések alapján besorolhatjuk és BSR osztályozhatjuk erőforrásainkat, illetve támogathatjuk a kockázat elemzési és üzletmenet-folytonosság tervezési feladatainkat.

RISK – Kockázatmenedzsment

A kockázatelemzés összekapcsolja vagyonelemeink sérülékenységeit és védelmi intézkedéseit a fenyegető veszélyekkel. Lehetséges bekövetkezésük esetén ok-okozati szimulációk mentén elemezhetjük a következményeket és a fellépő üzleti károkat. Egyszerre számos terület különböző tipusú (BSR információbiztonsági, IKT, humán, fizikai, üzleti, működési, adhoc, projekt alapú) kockázatelemzése is futhat párhuzamosan, melyek eredményei egységesen is kezelhetők, ezáltal megvalósitva és támogatva az integrált teljes vállalati kockázatmenedzsmentet (ERM – Enterprise risk management). Folyamatos kockázatkezelési és jelentés készitő funkciók támogatják a vállalat kockázatarányos védelmének folyamatos irányitását.

TPRM – Third Party Risk management

Külső felek és IKT szolgáltatásaik központi nyilvántartása. Kontroll, adat és kockázat felmérő kérdőivek összeállitása. A felméréshez kockázatelemzési módszertan illesztése. A third party szolgáltatások felmérésének részletes workflow támogatása. Vendorok számára részletes kérdőiv küldése, kérdőiv értékelése, üzleti és biztonsági jóváhagyása, esetleges assurance és mitigációs cselekvések meghatározása, monitorozása. A szállitói biztonsági kockázat szintjének értékelésére a begyüjtött adatok alapján, szolgáltatások kockázati szintjének kimutatása, követése. Certek és egyéb dokumentumom menedzsmentje.

Compliance & Audit

Rendszeres megfelelés és audit vizsgálatokat hajthatunk végre számos előre definiált nemzetközi szabvány, biztonsági ajánlás és jogszabály szerint, ugyanakkor tetszőleges audit/követelmény jegyzékeket is (pl. biztonsági szabályzatok, anyavállalati elvárások, belső audit követelmények) összeállithatunk. A különböző megfelelés/audit vizsgálatokat akár párhuzamosan is kezelhetjük, a hiányosságokat pedig integrált cselekvési tervekkel kezelhetjük, részletes, akár időgép szerű riportolási és jelentés generálási lehetőségekkel. A hazai jogszabályi **(kiberbiztonsági törvény)** felmérések és hatósági elvárások **(NKI - OVI, SZTFH, MNB – DORA RTS)** kifejezett támogatása.

BCM - Üzletmenet-folytonosság és IT helyreállítás menedzsment:

A BCM modul képes egységes módon kezelni mind az üzletmenet- folytonosság, mind a technológiai helyreállitás tervezést, közös visszaállitási időcélok (RTO, MTPD, RPO) mentén. Az üzletmenet-folytonosság tervezés (BCP) során az üzleti folyamatokat támogató erőforrások (legyen az technológia, humán, létesitmény stb.) kiesésére definiálhatunk helyettesitő és megkerülő megoldásokat. A helyreállitás (DRP) és szolgáltatásfolytonosság (SCM) tervezés során a technológia erőforrások, rendszerek, szolgáltatások részletes helyreállitási és áthidalási tervezését hajthatjuk végre.

GDPR

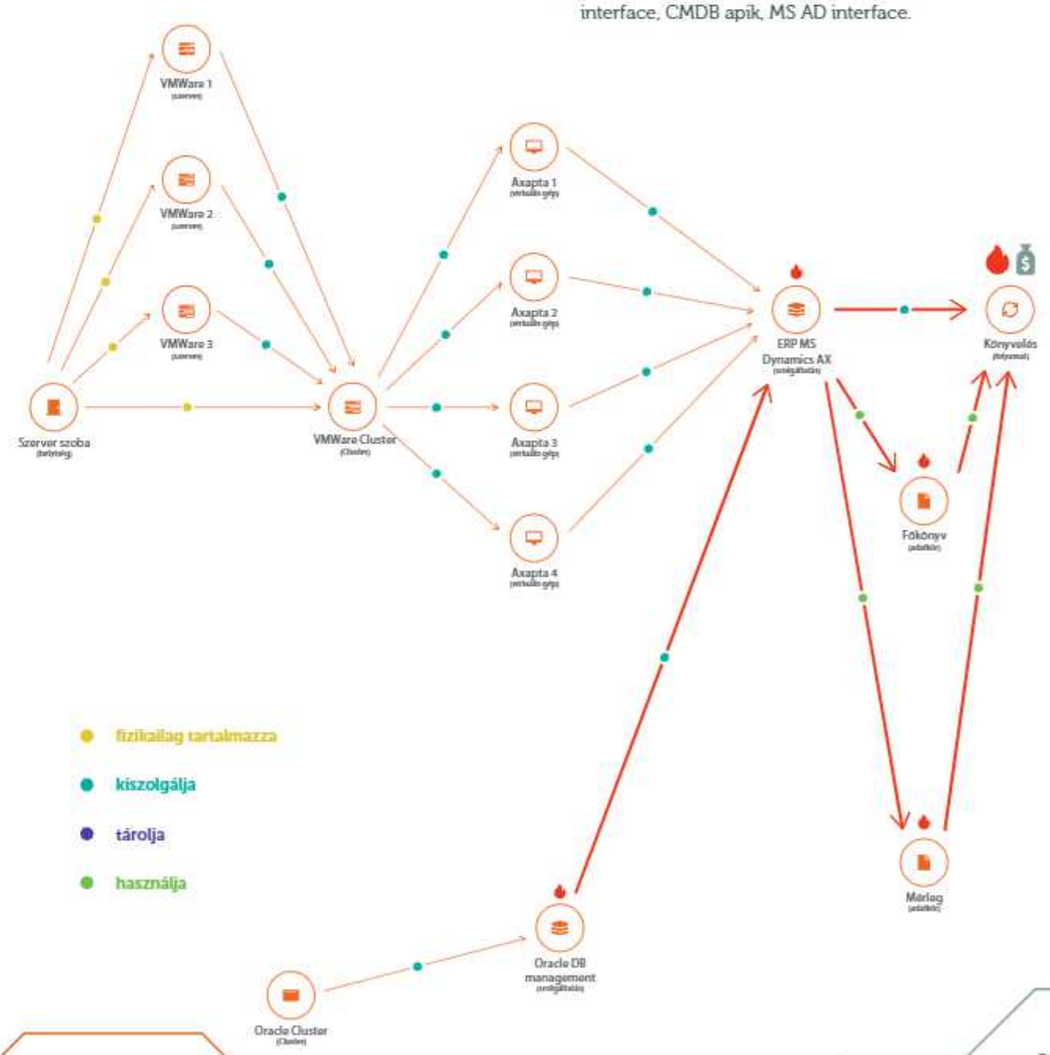
Az adatvédelemre fókuszáló funkciókkal támogatjuk az adatkezelési tevékenységek, személyes adatkörök, incidensek nyilvántartását, adatvédelmi compliance vizsgálatok és kockázatelemzések végrehajtását.

Governance

Az elemzési és tervezési funkciókon felül a szoftver kifejezett célja a biztonsági irányitási rendszer folyamatos felügyelete és fenntartása is (NIS2, DORA, ISMS). További támogatott téma területek: incidens és biztonsági kivételek nyilvántartása, szervezet védelmi intézkedéseinek nyilvántartása, feladatok és felelősségek kezelése, felülvizsgálatok vezetése.

Kiemelt képességek

- Multitenant keretrendszer és moduláris felépités.
- On-prem vagy Cloud használat.
- Szerepkör, feladat és felelősség alapú jogosultság kezelés.
- Kiosztható felmérési és eredmény karbantartási feladatok, email értesitőkkel.
- Valós testreszabhatóság, rugalmasság, meglévő vállalati gyakorlatokhoz, előirásokhoz való alkalmazkodást.
- Vizuális incidens szimulációs képességek, érzékeny és egyedi hibapontok (SPoF) feltérképezése, fenyegetések rendszerelemek közötti terjedésének, következményeinek, üzleti hatásainak elemzése.
- Nemzetközi ajánlásokon alapuló és folyamatosan frissülő know how (fenyegetés, védelmi intézkedések, sérülékenységek stb.).
- Kiterjedt adat import/export képességek, MS Excel interface, CMDB apik, MS AD interface.



Appliance megoldás az informatikai biztonsági események megfigyelésére és az incidensek felderítésére.

A SeConical logelemző appliance, naplóbejegyzések gyűjtését és feldolgozását végző szoftverrendszer, mely automatikus elemzést követően, hetente riportot készít az elmúlt hét biztonsági eseményeiről.

A riportok átvizsgálása során fény derülhet az informatikai rendszerben történt incidensekre, valamint olyan folyamatokra, melyek jelenleg még nem okoznak, de a jövőben problémát okozhatnak. Incidens esetén a szakértők további manuális logelemzést is végezhetnek az appliance-ben, az okok és problémák mélyebb felderítése céljából.

A heti jelentéseken kívül, a vezetők számára havonta készül egy átfogó riport az elmúlt hónap eseményeiről. Ez kumulálva és trendelemzésre alkalmas módon szemlélteti a szervezet informatikai infrastruktúrájában végbemenő biztonsági folyamatok változásait.

A szervezet naplózási rendszere a SeConical segítségével átláthatóvá, könnyen kezelhetővé válik, mert a felhasználók igényei alapján lett kialakítva.

A SeConical felépítése

A **SeConical** appliance egy webes workflow vezérelt alkalmazásrendszer, amely main és external szerverekből áll. A main szerveren található a **Felügyeleti** modul, mely az automatikus vezérlésen felül a felhasználók kényelmes kiszolgálásáért felel. Az external szerver, a rendszer lelke, melyen a **Logelemző** alkalmazás fut.

A **Felügyeleti** modul lehetővé teszi, hogy valós időben lehessen nyomon követni az appliance üzemállapotát. Segítségével módosíthatók a beállítások, illetve elérhetők a különböző logelemzési riportok, valamint ez a modul felelős a két szerver összehangolt működéséért.

A **Logelemző** modul a naplóbejegyzések gyűjtését és feldolgozását végző szoftverrendszer – előbbit **Flume**, utóbbit **LogDrill** nevű alegység végzi –, mely a naplóbejegyzések feldolgozása után hetente, automatikusan egy elemzési riportot készít az elmúlt hét eseményeiről. A riportok rugalmasan alakíthatók az ügyfél igényeinek megfelelően és a riportok alapján további személyes átvizsgálása során fény derülhet az informatikai rendszerben történt incidensek mélyebb okaira, melyek részletes kivizsgálása és korrigálása gyorsabbá és egyszerűbbé válik.

Az appliance nagy előnye, hogy nem igényel üzemeltetési személyzetet és logelemző szakértőket. A bevezetés után automatikusan működik, készíti a heti és havi jelentéseket, melyek értelmezéséhez nincs szükség speciális szaktudásra. Biztonsági incidens gyanúja esetén, eseti jelleggel szükséges csak logelemző vagy forensic szakértőhöz fordulni, aki egy külön (opcionálisan) illeszthető Forensic modul segítségével az összegyűjtött logokban manuális logelemzéssel az okok és problémák felderítése céljából mélyre tud hatolni.

Olyan szervezeteknek ajánljuk, ahol elvárás

- az IBTV által előírt tevékenységekről készült naplóállományok elemzéséről rendszeres riportok előállítása az adott elektronikus információs rendszer (EIR) besorolásának megfelelően,
- a nemzetközi szabványokban (NIST SP 800-53, COBIT 5, ISO/IEC 27001) megfogalmazott hatékony, biztonságos és automatizált logelemzési folyamat megvalósítása,
- hogy a loggyűjtés, logelemzés és jelentés készítés ne terhelje a szervezet humán erőforrásait, hanem azokat az illetékesek automatikusan, mindig határidőre kézhez kapják,
- hogy az informatikai rendszerek üzemeltetését támogató logelemzési jelentések készüljenek rendszeresen.

Saját fejlesztésű **SeCube** alkalmazásunk opcionális modulként illeszthető a SeConical rendszerhez. A SeCube IT GRC szoftver egy egységes keretrendszerben modulárisan összeilleszthető szoftver-komponensekből álló, workflow vezérelt, elemzési, tervezési és folyamatos karbantartási tevékenységeket támogató webes rendszer, mellyel a szervezet információbiztonsági irányítási rendszere (IBIR) megteremthetővé, átláthatóvá és kézben tarthatóvá válik. **A két rendszer összekapcsolásának nagy előnye az, hogy a SeConical riportokból kiolvasható fenyegetettségek rögtön beilleszthetők a SeCube kockázatmenedzsment folyamatába, ahol a felhasználók megkapják a kockázatkezelési terveket is.**

A SeConical fő jellemzői

- rack szekrénybe szerelhető appliance;
- **moduláris felépítésű, testre szabható rendszer;**
- könnyen telepíthető, egyszerűen üzemeltethető;
- rugalmasan illeszthető a már meglévő loggyűjtő megoldásokhoz;
- **egy rendszerben megvalósított adatgyűjtés, tárolás, feldolgozás és elemzés;**
- informatikai rendszerek felügyeletének ellátása;
- hierarchikus (jogosultság-függő) dashboard felületen kezelhető;
- törvényi megfelelőség támogatása azáltal, hogy az IBTV-ben előírt tevékenységekről készült naplóállományok elemzéséről rendszeres riportok készülnek;
- nemzetközi szabványokban (NIST SP 800-53, COBIT 5, ISO/IEC 27001) megfogalmazott hatékony, biztonságos és automatizált logelemzési folyamat megvalósítása;
- informatikai rendszerek felügyeletének ellátása;

Funkciók és modulok áttekintése

Központi loggyűjtés

A központi loggyűjtéssel a szervezet logforrásai által naplózott információk egy helyre, strukturáltan kerülnek összegyűjtésre, majd mentésre kiajánlásra, ezzel elősegítve az automatikus logelemzést és az esetleges manuális nyomozati vizsgálatokat is.

Automatizált logelemzés és riportkészítés

A logelemzés során a logállományok automatikus és ütemezett feldolgozása lehetővé teszi az IT rendszerek állapotának figyelemmel kísérését és riportokba foglalását, esetenként azok viselkedésének, problémáinak előrejelzését. A SeConical logelemző modulja nagy, különböző formátumú, struktúrájú és forrású adattömegek villámgyors elemzésére is képes. A logelemzés eredményeiből automatikus készül heti éshavi jelentés, valamint egy kattintással készíthetők ad-hoc jelentések, melyek a rendszerbe feltöltött információk alapján generálódnak.

Logtovábbítás

A logtovábbítás lehetővé teszi, hogy az adatokat más rendszerek is feldolgozhassák. A logtovábbítás szolgáltatás által a logforrásból nyert adatok a SeConical rendszeren keresztül jutnak el a Megrendelő által meghatározott helyekre.

Felügyelet

A felügyeleti modulban nyomon követhető a SeConical valós idejű állapota és loggyűjtő agentek állapota, elvégezhetők különböző beállítások és parancsok, illetve kezelhető és létrehozható többféle logelemzési riport, majd ezek megnézhetők itt.

Manuális logelemzés

A Forensic modul segítségével lehetőség van az összegyűjtött logokban manuális logelemzésre annak érdekében, hogy incidens esetén az okok és problémák felderítése céljából mélyre tudjanak fúrni a szakértők.

SeCube

Egy moduláris felépítésű IT GRC alkalmazás, melynek segítségével egy szervezet információbiztonsági irányítási rendszere, átláthatóvá és kézben tarthatóvá válik. Részletesen: *https://www.secube.hu/*

KÜRT INFORMÁCIÓMENEDZSMENT

+36 1 424 6666

www.kurt.hu

sales@kurt.hu

KÜRT ADATMENTÉS

+36 1 228 5410

www.adatmentes.kurt.hu

adatmentes@kurt.hu

Kiberbiztonsági audit: auditor@kurt.hu

KÜRT Információbiztonsági és Adatmentő Zrt.

H-1118 Budapest, Rétköz u. 5.

NATO BESZÁLLÍTÁSRA ALKALMAS

nqa ISO 9001 QUALITY MANAGEMENT

nqa ISO 27001 INFORMATION SECURITY MANAGEMENT