Sérülékenységvizsgálat

A vizsgálat rámutat az informatikai rendszerek gyenge pontjaira, a biztonsági hiányosságokra, amelyeken keresztül a rosszindulatú támadók kárt okozhatnak. Célja, hogy megelőzzük a bizalmas és nélkülözhetetlen vállalati adatok elvesztését, ellopását, illetve megakadályozzuk az ezekhez való illegális hozzáférést.

Kiberbiztonsági audit (NIS2/Kiberbiztonsági törvény)

Kiberbiztonsági audit szolgáltatásunkat kifejezetten az auditkötelezett, NIS2 irányelv és a Kiberbiztonsági törvény által érintett szervezetek számára ajánljuk. Az érintett szervezetnek kötelezően kétévente el kell végeztetnie a kiberbiztonsági auditot, hogy biztosítsa az információs rendszereik védelmét és megfelelőségét.

A KÜRT Zrt. audit csapata készen áll arra, hogy teljes körű támogatást nyújtson minden „Alap" és „Jelentős" biztonsági osztályba sorolt elektronikus információs rendszert üzemeltető szervezet számára. Szolgáltatásunk magában foglalja a Szabályozott Tevékenységek Felügyeleti Hatósága által elvárt kiberbiztonsági audit teljes körű lebonyolítását.

BCM üzletmenet-folytonossági menedzsment

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. A témakör legfontosabb eredménye, hogy prezentálni tudjuk főbb kritikus folyamatokat, amelyekre egy estleges informatika kiesés során a üzleti helyettesítési eljárások pótolni tudják az üzleti folyamatok folytonosságát.

Kritikus szervezetek ellenállóképességének növelése

A CER irányelv magyarországi átültetésével érvénybe lépett kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény hatálya alá eső Szervezetek részére kínálunk megoldásokat. A szolgáltatás keretein belül a 474/2024. (XII. 31.) Kormány rendeletben meghatározott tartalmi és formai követelményeknek megfelelő Ellenálló Képességi Terv készítésében nyújtunk segítséget, továbbá a szükséges mértékig támogatjuk az Ellenálló képességért felelős vezető munkáját. Igény esetén részt veszünk a szabályzási környezet kialakításában, a kockázatértékelés és ellenálló képességi mátrix elkészítésében, vagy egyéb ellenállóképeség fejlesztésére vonatkozó intézkedések kidolgozásában visszaellenőrzésében.

Tesztelés és tesztmenedzsment

A tesztelés a rendszerfejlesztési életciklus szerves része, melynek célja, hogy validálásra kerüljön a szoftver vagy informatikai rendszer megfelelősége. Sok esetben a tesztmenedzsment feladatkörébe tartozik a követelményrendszer felállítása és megfogalmazása is. A tesztelés során elsősorban a funkcionális minőségi jellemzőkre koncentrálunk és visszajelzést adunk a rendszerben tapasztalt eltérésekről.

Szoftverfejlesztés minőségbiztosítása

A KÜRT minőségbiztosítói portfóliójának egyik kiemelt eleme a komplex szoftverfejlesztési projektek minőségbiztosítása. Lényege a fejlesztési projekt eredményességének biztosítása, a költség- és időráfordítások megfelelő korlátok között tartásával. Itt nem csupán a követelmények teljesülését és hasznosságát vizsgáljuk, hanem best practice alapján a fejlesztési költségeket/napszámokat is minimalizálni tudjuk.

Informatikai fejlesztéstámogatás

Átvilágítjuk a szervezet fejlesztési folyamatait és javaslatokat teszünk azok átalakítására. Segítünk a változások gyakorlati bevezetésében is, ha arra lenne szükség. A legfontosabb érintett folyamatok a következők: Fejlesztési igények befogadása és kezelése, Release-k hatékony előállítása és Üzembe helyezése, Változáskezelési folyamatok, Tesztelési folyamatok. Konkrét segítséget is tudunk adni ezen folyamatok működtetéséhez mind koordinátori (Release menedzser, Teszt menedzser stb.), mind végrehajtói szinteken (Tesztelő, adminisztrátor, elemző stb.).

Kiberbiztonsági törvényi (NIS2) megfelelés támogatása

A NIS2 irányelvnek való megfelelés értékelésére és a követelményeknek való megfeleléshez komplex megoldásokat kínálunk. A NIS2 irányelvet a magyar jogba átültető Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényi megfelelés támogatás során elvégezzük az érintett elektronikus információs rendszerek azonosítását, biztonsági osztályba sorolását, továbbá a 7/2024. (VI. 24.) MK rendelet mentén végzett védelmi intézkedés GAP elemzés eredményéről értékelési jelentést készítünk. Igény esetén a megfelelés értékelésén túl elvégezzük a rendszerek kockázatelemzését, a szabályozási környezet kialakítását, a rendszerbiztonsági tervek elkészítését, egészen az érintett rendszerek használatbavételének/folytatásának jegyzőkönyvezéséig részt veszünk a megfelelés támogatásban.

Információbiztonsági kockázatmenedzsment

A KÜRT információbiztonsági kockázat-menedzsment szolgáltatása az adott szervezet információbiztonsági kockázatainak kezelésére koncentrál, illetve rávilágít, hogy az egyes információbiztonsági kockázatok milyen hatással vannak a különböző üzleti folyamatokra, szervezeti adatokra. Információbiztonsági kockázatértékelési módszertanunkat a szervezetre vonatkozó jogszabályi környezetnek megfelelően alakítjuk ki.

DORA/MNB IT megfelelés támogatása

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.

ISO 27001 felkészítés

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

Adatosztályozás és biztonsági osztályba sorolás

A 7/2024. MK rendelet és a 418/2024. kormányrendelet előírásainak megfelelően segítünk a szervezet elektronikus információs rendszereiben kezelt adatok biztonságának megteremtésében. Szolgáltatásaink keretében elvégezzük az adatok osztályozását, a rendszerek biztonsági osztályba sorolását, valamint igény esetén egyedi módszertan alapján üzleti hatáselemzést, hogy az üzleti mutatók mentén kerüljenek kialakítása az informatikai rendszerek kockázatarányos védelmi intézkedései. Szakértőink támogatásával biztosíthatja a jogszabályi megfelelést, miközben növeli szervezete működésének biztonságát és ellenálló képességét.

Az információ biztonsága

A KÜRT Információbiztonsági és Adatmentő Zrt. több mint 30 éve, 1989-es indulása óta már évente közel 4000 adatmentési és -helyreállítási feladatot végez el. 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 alakíthattuk ki a ma már nélkülözhetetlen adatok és információk biztonságát és hatékony kezelését támogató szolgáltatás portfóliónkat.

NATO BESZÁLLÍTÁSRA ALKALMAS

ISO 9001 ISO 27001 INTEGRATED MANAGEMENT

ISO 37001 ANTI-BRIBERY MANAGEMENT

FORENSIC – Digitális nyomozás szolgáltatás

A Forensic – Digitális nyomozás szolgáltatása digitális incidensek kivizsgálására, az informatikai rendszerekben bekövetkezett negatív események felderítésére, utólagos rekonstrukciójára szolgál. A Forensic szolgáltatásunk a megtörtént incidens részleteit időrendi sorrendben képes újra összeállítani, ezen kívül bizonyítékkal tud szolgálni az incidenst alkotó események részleteiről is.

DRP - Katasztrófahelyzet utáni helyreállítás tervezés

Feladatunk felkészíteni a szervezetet a katasztrófahelyzet kezelésére, illetve kialakítani és erősíteni az informatikai katasztrófahelyzet kezelési képességét. Eredménytermékeink megfelelnek a NIS2 jogszabályi és DORA rendelet szerinti elvárásoknak.

Informatikai és információbiztonsági átvilágítás

Az informatikai és információbiztonsági átvilágítás célja a szervezet információbiztonsági képességének felmérése, illetve javaslattétel kidolgozása annak erősítésére.

Saját fejlesztésű szoftverek és rendszerek

KÜRT ADATMENTÉS

HUNGARIKUM

Adatmentés üzletágunk a világ egyik vezető szaklaborja elismert adatmentési technológiával végez adatmentés 1989 óta. Magánszemélyeknek, kis- és nagyvállalatoknak, egészségügy intézmények, valamint állami hivatalok számára kínálunk megoldást informatikai katasztrófa okozta adatvesztés elhárítására. Nagyvállalati környezetben leginkább szerverek, NAS-ok és virtuális gépek helyreállítását végezzük. 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.

secube

GOVERN your RISK and COMPLIANCE think COMPLEX do EASY

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

Célja a szerteágazó biztonsági folyamatok integrált támogatásával megteremteni és fenntartani a teljes vállalati biztonság átlátható és riportálható irányítását. A SeCube GRC kockázatmenedzsment keretrendszerben felépíthetjük vállalatunk működési modelljét (erőforrások, rendszerek, adatvagyon, üzleti folyamatok), üzleti hatáselemzés (BIA) mentén értékelhetjük működésünk. Kockázatelemzések mentén (információbiztonsági, fizikai, humán, üzleti, third-party) kezelhetjük kockázatainkat. IT és üzletmenet folytonosságot tervezhetünk (BCM), valamint belső audit és compliance vizsgálatokat menedzselhetünk. A hazai kiberbiztonsági törvényi (NIS2) és DORA szerinti kockázatmenedzsment rendszer, illetve nemzetközi szabványok (ISO27001, Tisax) megfelelés támogatás. A SeCube GRC TPRM képessége támogatja a külső szolgáltatások kockázati felmérését és kiértékelését.

SeConical **Automatizált Biztonsági Elemzés**

A SeConical logelemző appliance megoldást biztosít az informatikai biztonsági események megfigyelésére és az incidensek felderítésére.

Naplóbejegyzések gyűjtését és feldolgozását végző szoftverrendszer, mely automatikus elemzést követően, hetente riportot készít az elmúlt hét biztonsági eseményeiről, melyek értelmezéséhez nincs szükség speciális szaktudásra. Az appliance nagy előnye, hogy nem igényel üzemeltetési és logelemző szakértőket, valamint a törvényi megfelelésben is támogatást nyújt. A szervezet incidenskezelése sokkal hatékonyabbá válik a SeConical segítségével, míg az üzemeltetésnek hathatós támogatást nyújt a rossz irányba mutató folyamatok kiemelésével.

Lépjen kapcsolatba velünk vagy Partnereinkkel:

WWW.KURT.HU

Adatmentés: **adatmentes@kurt.hu**
Információmenedzsment, KÜRT szolgáltatások: **sales@kurt.hu**
Kiberbiztonsági audit: **auditor@kurt.hu**

KÜRT Információbiztonsági és Adatmentő Zrt.
H-1118 Budapest, Rétköz u. 5.