ÜZLETMENET-FOLYTONOSSÁGI ÉS KATASZTRÓFAELHÁRÍTÁSI TERV

A NIS 2 ÉS A KIBERTÖRVÉNY ÁLTAL ÉRINTETT SZERVEZETEK FELKÉSZÜLÉSE A TÖRVÉNYI MEGFELELÉSRE

BEVEZETÉS:

Üzletfolytonosság menedzsment

A legtöbb szervezet információs rendszerekre építi kritikus üzleti folyamatait. Ez a függőség elektronikus biztonsági fenyegetések formájában a kockázat egy új formájának megjelenéséhez vezetett, mint például a hackelés, adatvesztés, a titkosság megsértése vagy akár a terrorizmus. Az egyre kifinomultabb támadások érkezhetnek magánszemélyektől, magánvállalkozásoktól, vagy akár titkos külföldi hírszerző ügynökségektől is. Az ilyen támadásoknál információk vesznek el, bizalmas adatok kerülhetnek ki vagy kritikus rendszerek és dokumentumok sérülnek meg.

A biztonsági fenyegetések, támadások, váratlan incidensek miatt minden szervezet számára létfontosságú, hogy még a rendkívüli helyzetekben is legalább a minimálisan elvárható szinten fenn tudja tartani informatikai rendszerének és ezáltal működésének és szolgáltatásainak színvonalát. Az ilyen válsághelyzetekre való felkészülés érdekében az érintett szervezetek üzletmenetfolytonosság-menedzsment rendszert (BCM) alakítanak ki, mely a folyamatmenedzsment rendszerrel (BCP) és a kiesett erőforrások visszaállítását támogató rendszerrel (DRP) integráltan működik.

Célja, hogy rendkívüli helyzetekben is változatlan, de legalább a minimálisan elvárható szinten tartsa a szervezet informatikai rendszerét az incidens elhárításáig.

Érdemes külső tanácsadót bevonni, különösen akkor, ha a szervezet nem rendelkezik megfelelő belső szakértelemmel a NIS 2 vagy az érintett szervezetek számára meghatározott követelményrendszer teljesítése érdekében.

5N
Számítástechnikai és Szolgáltató Kft
Székhely : 1118 Bp., Beregszász út 4. A-B.
Telephely : 1106 Bp., Maglódi út 16.
Telefon : (36-1) 221-5419
(36-1) 221-5420
Telefax : (36-1) 383-2993
E-mail : 5N-Kft@5n.hu

DEFINÍCIÓK:

BCM – üzletmenet folytonosság menedzsment rendszer

- proaktív = békeidőben
- reaktív = krízishelyzetben
    - CrisCo - Krízis Bizottság, országos szint (proaktív és reaktív)
    - Helyi Krízis Bizottság, leányvállalati szint (reaktív és esetleg proaktív)
    - Helyi Krízis team (fiók szint; reaktív)
    - Krízis menedzser (csoport szint)

BCP – folyamatmenedzsment terv - kiesett erőforrások nélküli minimális funkcionalitást biztosító üzleti működés. A BCP viszont csak akkor indul el, ha az erőforrás várható visszaállítási ideje meghaladja a maximálisan tolerálható kiesési időt.

- hogyan kell eljárni, ha a normál üzleti működés nem folytatható
- milyen elkerülő megoldások léteznek.
    - BCP felelős
    - BCP koordinátor

BIA -üzleti hatástanulmány

DRP - kiesett erőforrások visszaállítása. A DRP minden esetben elindul, ha valamely, üzleti folyamatot támogató erőforrás kiesik.

GAP analízis – hiányanalízis. Lényege, hogy feltárja az eltéréseket (angolul: *gaps*) a szervezet jelenlegi gyakorlatai és a rendelet által előírt követelmények között. IT-ben: a jelenlegi és az optimális helyzet közötti eltéréseket térképezzük fel. A hiányanalízis elvégzésére az ISO 27001:2013 szabványt vesszük alapul, ahol az átvilágítás során pontos képet kapunk:

- a jelenlegi adatvédelmi és biztonsági intézkedésekről, megjelölve az esetleges hiányosságokat,
- az IT rendszerek és alkalmazások használatáról, működéséről, hatékonyságáról és megbízhatóságáról,
- azonosítjuk az IT rendszerek és folyamatok kockázatait, az adatvesztési vagy biztonsági réseket,
- az esetleges fejlődési lehetőségekről a biztonságos működés jegyében,
- valamint feltérképezzük, hogy milyen lépésekre van szüksége a vállalatnak egy kívánt tanúsítás elnyeréséhez, vagy pusztán az információbiztonság eléréséhez.

A NIS 2 irányelv szerinti GAP elemzés egy módszertan, amely segít azonosítani az adott szervezet jelenlegi megfelelőségi szintjét az Európai Unió új, kiberbiztonsági követelményeket meghatározó NIS 2 irányelvével szemben.

ISO 27001 - Az ISO/IEC 27001 az információ biztonság irányítás (IBIR) nemzetközi szabványa. Kereskedelmi, kormányzati és non-profit szervezetekre vonatkozik és meghatározza az Információbiztonság Irányítási Rendszerek létrehozásának, megvalósításának, folyamatos ellenőrzésének a módját.

PDCA modell (Plan-Do-Check-Act) - egy szervezet potenciális kockázatai a PDCA modell segítségével állapíthatók meg és elemezhetőek. Meghatározhatók általa a szükséges tevékenységek, intézkedések, lehetővé teszi a kockázatok folyamatos felügyeletét, mértékük optimalizálását és a lényeges biztonsági célok folyamatos monitorozását.

I. KRITIKUS TÉNYEZŐK AZONOSÍTÁSA (ELŐKÉSZÍTÉS)

A vállalat működése, prosperitásának fenntartása nagyban függ az üzleti folyamatokat támogató IT infrastruktúra rendelkezésre állásától. Így a katasztrófahelyzet elhárítás első lépéseként fel kell készülni azon esetekre, ha ez valamilyen hatásra megváltozik.

- Üzleti hatáselemzés (BIA)
- Fenyegetettségek felmérése (külső és belső)
- Kockázat(fenyegetettség) elemzés
    - Szolgáltatások teljes körű felmérése
        - Beazonosított (releváns) üzleti folyamatok és a hozzájuk használt
            - Releváns erőforrások kiválasztása és kockázatelemzése (humán, IT, szerződött partnerek, külső szolgáltatók, egyéb)
        - Minimum szolgáltatások/kritikus folyamatok kiszűrése
        - Az időkritikus folyamatokhoz igénybevett erőforrások és azok időkritikusságának beazonosítása

II. VÁLSÁGSTÁB KIJELÖLÉSE

A kibertv. értelmében a szervezet vezetője saját hatáskörében hatáselemző és kockázatmenedzsment keretrendszert hoz létre és működtet, az elektronikus információs rendszerekre és azok környezetére vonatkozóan. Ehhez kapcsolódóan meghatározza az elektronikus információs rendszerek védelmével kapcsolatos szerepköröket, felelősöket, feladatokat és az ehhez szükséges hatásköröket, kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt, és kijelöli a szervezet üzletmenet folytonosságáért felelős személyeket (válságstáb) a szervezet minden szintjén.
Proaktív és reaktív

III. INFRASTRUKTÚRA FELMÉRÉSE

Az információs környezetet átvizsgálva fel lehet tárni azon potenciális gócpontokat, melyek beavatkozás nélkül várhatóan problémákat fognak produkálni.

- IT rendszer áttekintő
- IT szolgáltatáskatalógus
    - Szolgáltatások teljes körű felmérése
        - Beazonosított (releváns) üzleti folyamatok és a hozzájuk használt
            - Releváns erőforrások kiválasztása és kockázatelemzése
    - Minimum szolgáltatások/kritikus folyamatok kiszűrése
    - Az időkritikus folyamatokhoz igénybevett erőforrások és azok időkritikusságának beazonosítása
- Adatvagyon leltár

IV. GAP ANALÍZIS

A GAP analízis (eltéréselemzés / hiányanalízis / hiányfeltárás) célja az üzleti folyamatok rendszerszerű irányításának kialakítása. Betekintést nyújt egy cég folyamatiba, pillanatképet ad a vállalat aktuális megfelelőségi szintjéről. Átvilágítja az aktuális folyamatot, hogy rámutasson a jövő optimalizálási szükségleteire, lehetőségeire. IT területen a jelenlegi és az optimális helyzet közötti eltéréseket térképezzük fel, melyhez az **ISO 27001:2013 szabványt** vesszük alapul. (nemzetközi információbiztonsági rendszer működtetésére vonatkozó szabvány, alapja a PDCA modell) A GAP

analízis segít megérteni az IT működését és hatékonyságát, azonosítani a fejlődési területeket és problémákat, és javaslatokat tenni a fejlesztési irányokra, hogy a működés és az adatbiztonság a célállapothoz közeli legyen. Ezért a NIS 2 felkészülés első lépéseként jellemzően a *„GAP elemzést”* szokták javasolni, mely segít azonosítani az adott szervezet jelenlegi megfelelőségi szintjét a **NIS 2 irányelvével** szemben.

1. Szervezet tevékenységi körének elemzése

- Eldönteni, hogy a szervezet a NIS 2 által érintett szervezetek közé tartozik-e.
- Azonosítani a releváns kritériumokat, például méret, tevékenységi kör, kockázati profil.

2. NIS 2 követelmények feltérképezése

- Az irányelv elvárásai:
  - Kockázatkezelési elvárások: Biztonsági irányítás, incidenskezelés
  - Szabályozási követelmények: Jelentési kötelezettségek, auditálás.
  - Műszaki és szervezeti intézkedések: hálózati biztonság, adatszivárgás megelőzése, incidensérzékenység.

3. Meglévő állapot felmérése

- Meg kell vizsgálni a meglévő biztonsági és kockázatkezelési folyamatokat, technológiákat, és irányelveket.
- Fel kell mérni, hogy a meglévő szabályozások mennyire támogatják a NIS 2 megfelelést.

4. Eltérések (GAP-ek) azonosítása

- A fenti munkák után össze lehet vetni a meglévő állapotot a NIS 2 követelményekkel.
- Azonosítani kell a hiányosságokat mind technológiai, mind szervezeti szinten (pl. hiányzó biztonsági szabályzatok, nem megfelelő incidenskezelési folyamatok).

5. Kockázatelemzés

- Prioritás szerint kell osztályozni az azonosított eltéréseket a kockázati hatásuk és valószínűségük alapján.
- El kell dönteni, mely területek igényelnek azonnali beavatkozást.

6. Javító intézkedési terv kidolgozása

- Részletes akcióterv (cselekvési terv, ütemterv stb.) kidolgozása a hiányosságok megszüntetésére:
  - Felelősök kijelölése.
  - Határidők meghatározása.
  - Erőforrásigények kalkulálása.

7. Kommunikáció és tájékoztatás

- Tájékoztatni kell az érintett vezetőket és munkacsoportokat a GAP elemzés eredményeiről.
- Döntési szintenként, érintettségek alapján továbbképzéseket kell indítani az új elvárásokról és feladatokról (szabványokról).

8. Ellenőrzés és nyomon követés

- Rendszeres ellenőrzéseket, teszteket és felülvizsgálatokat kell végezni, ennek eredményeit pedig beépíteni a folyamatokba.

Eredmény

A GAP elemzés eredményeként világos kép alakul ki, hogy milyen hiányosságok vannak a jelenlegi és a NIS 2 megfelelési követelmények között. Konkrét akciótervvel, áthidaló lépésekkel meg lehet kezdeni a felzárkózást.

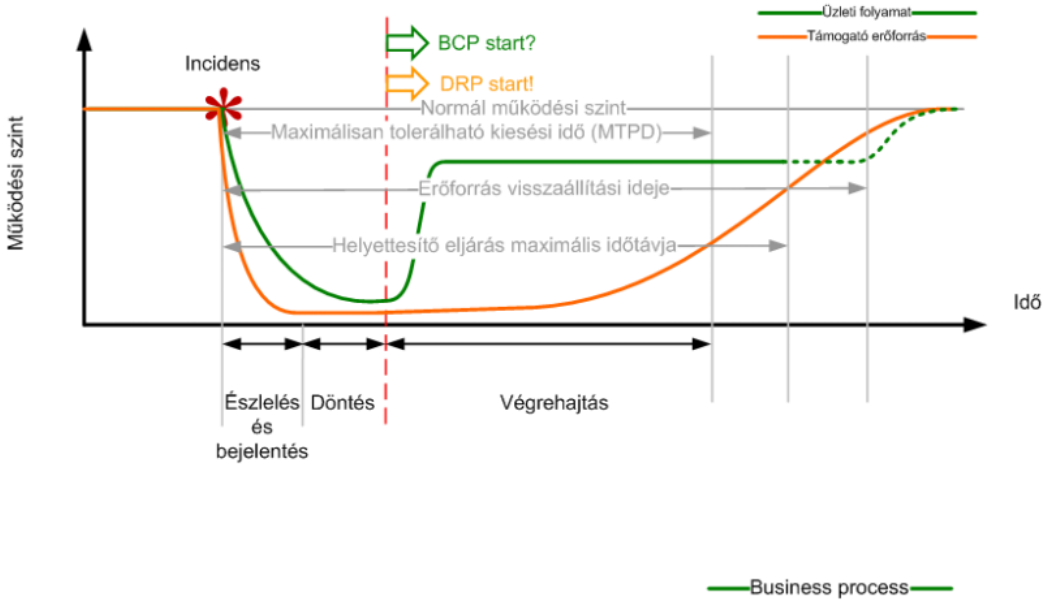
V. KOCKÁZAT ÉS HATÁSELEMZÉS

Nem kell minden kockázattal egyformán foglalkoznunk. Vannak köztük olyanok, melyek alig érzékelhető fennakadásokat okoznak és vannak, amik azonnali, kritikus rendszerleállást okozhatnak.

Értékeli és osztályozni az adott fenyegetés bekövetkezési valószínűségének és a várható kárnak a viszonyát vizsgálva kell. Ezt vizsgálva azonnal kitűnik, hogy mely fenyegetéseket kell komolyan venni és melyek azok melyek kezelése nyugodtan várhat . Ezzel a védelemszervezés ráfordításai optimalizálhatók a védelmi szint maximalizálása mellett.

VI. AKCIÓTERV ELKÉSZÍTÉSE

Miután feltérképeztük a hiányok áthidalásának lehetséges módjait, és eldöntöttük, melyik lenne a legjobb, fontos, hogy készítsünk egy megvalósítható célokat tartalmazó tervet. (idővonal, ütemezés, átfogó cselekvési terv, ami konkrét feladatokat rendel csapatokhoz vagy egyénekhez.)



VII. TESZTELÉS

- Tesztelés
- Cselekvési tervek közös tesztje
- Teszttapasztalatok beépítése

VIII. BCP/DRP KÉZIKÖNYV ELKÉSZÍTÉSE

A BCP és a DRP alapja a megfelelően elvégzett Üzleti hatáselemzés (BIA) illetve Kockázatelemzés. Ezek szolgáltatják a releváns erőforrások, releváns fenyegetések listáját, illetve a maximálisan tolerálható kiesési időt is.

A BCP és a DRP az alábbiak szerint viszonyul egymáshoz: A DRP minden esetben elindul, ha valamelyik üzleti folyamatot támogató erőforrás kiesik. A BCP viszont csak akkor indul el, ha az erőforrás várható visszaállítási ideje meghaladja a maximálisan tolerálható kiesési időt. Ha a maximálisan tolerálható kiesési időn belül vissza lehet állítani az erőforrást, akkor nincs szükség a

BCP aktiválására, hiszen az adott terület tolerálja a kiesést. Mivel a két területnek szorosan együtt kell működnie, erősen javasolt a két rendszert nem különválasztva megvalósítani.

IX. CSELEKVÉSI TERV ELKÉSZÍTÉSE

A cselekvési terv a fent leírt felmérések, hiányelemzések, kockázat-, és hatáselemzések, az akciótervek és azok tesztjeinek átfogó eredménye, mely biztosítja, hogy az informatikai védelmünket optimális ráfordításokkal, a feladatkörök pontos kijelölése mellett, maximális hatásfokkal tudjuk kialakítani a fenyegetések és támadások elhárítása érdekében.

X. KIEGÉSZÍTŐ EREDMÉNYTERMÉKEK

- IT rendszer áttekintő
- IT szolgáltatáskatalógus
- Releváns támogató erőforrások listája
- Adatvagyon leltár
- Kockázatelemzési jelentés
- Üzletmenet folytonossági stratégia és keretszabályzat
- Aktiválási kézikönyvek és cselekvési tervek
- Kockázatkezelési javaslatok és fejlesztési követelmények