Aruba Cloud Solution

Információbiztonsági kockázatkezelés

TARTALOMJEGYZÉK

BlazeArts Kft.
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu

1 FOGALMAK ÉS MEGHATÁROZÁSOK

Ez a fejezet az információbiztonsági kockázatszámítási és -kezelési modell ábrázolása szempontjából fontos meghatározásokat tartalmaz.

***BIA (Business Impact Analysis, vagyis üzleti hatásvizsgálat)*:**

Az adott folyamathoz/szolgáltatáshoz kapcsolódó információk bizalmas jellegének, integritásának és rendelkezésre állásának elvesztésével és annak megszakadásával kapcsolatos, az üzletágra gyakorolt gazdasági, szabályozási, illetve hírnévbeli hatások elemzése.

Rendelkezésre állás:

Annak biztosítása, hogy a szükséges információs rendszerek és adatok rendelkezésre álljanak, amikor szükséges.

Információbiztonsági kockázatkezelés

Olyan tevékenységek és üzleti folyamatok összessége, amelyek célja az adatok és szolgáltatások bizalmasságának, integritásának és rendelkezésre állásának (CIA) elvesztésével kapcsolatos kockázatok azonosítása, mérése, csökkentése és nyomon követése.

Hatás:

Egy vagy több fenyegetés előfordulásának negatív következménye.

Incidens:

Olyan kiberbiztonsági esemény, amely jelentős valószínűséggel veszélyezteti az üzleti tevékenységet és az információbiztonságot.

Integritás:

Ez az adatok és információk védelmét jelenti azok véletlen vagy szándékos tartalmi módosításaival szemben.

Fenyegetés:

Egy olyan (szándékos vagy véletlen) esemény lehetséges oka, amely károsíthatja a rendszert vagy a szervezetet, és hatással van az információk **t**itkosságára, **i**ntegritására és **e**lérhetőségére.

A fenyegetések lehetnek:

- „Kiberfenyegetések” – ezek negatívan hatnak a vállalatra:
    - az információs rendszer vagy annak elemei használata által (pl. hekkertámadás);
    - az információs rendszer kezelése által (pl. belső személyzet által okozott kár);
- „Nem kiberfenyetések” – ezek negatívan hatnak a vállalat informatikai rendszerére:
    - mert közvetlen hatással vannak az információs rendszer szolgáltatásnyújtására (pl. természeti katasztrófák, a támogató szolgáltatások megszakítása);

- mert befolyásolják az információs rendszer irányítását (pl. az informatikai feladatok végrehajtásának módját).

Az egyes fenyegetésekkel kapcsolatos kockázatok jellemzéséhez a következőkkel kell tisztában lennünk:

- Az információs rendszer elemeinek sebezhetősége, vagy ahol a fenyegetések megvalósulhatnak;
- Az elemek fenyegetettségnek való kitettsége, vagyis a fenyegetés megvalósulásának egyszerűsége (például egy olyan szerver, amely webszolgáltatást nyújt az ügyfelek számára, jobban ki van téve az internet által végrehajtott támadásoknak);
- A következmények típusai, figyelembe véve, hogy bizonyos fenyegetések más fenyegetések „hordozói" lehetnek (például a webszerverhez való jogosulatlan hozzáférés lehetővé teheti a behatoló számára az adatok ellopását, de lehetővé teheti azok törlését, módosítását, csalás elkövetését stb.).

Az előfordulás lehetősége vagy valószínűsége:

Annak a valószínűsége, hogy egy vagy több IT-elemet érintő fenyegetés egy adott időszakon belül negatív hatást gyakorol a vállalkozásra.

Információbiztonsági kockázat (a továbbiakban: „kockázat")

A fenyegetés bekövetkezésének valószínűsége és a vállalatra gyakorolt hatás kombinációja az elemzésben érintett eszközökhöz képest. A felmérés idejétől függően a kockázatok a következőképpen határozhatók meg:

- Potenciális vagy eredendő kockázat (**rRp**):

  Ez azt a maximális kockázatot jelenti, amelynek egy adott eszköz ki van téve egy olyan fenyegetés létrehozásának lehetősége szempontjából, amely hatással lehet az információk bizalmasságának, integritásának vagy rendelkezésre állásának elvesztésére. A szolgáltatás elemzésében részt vevő összes komponens hozzájárul az eredendő kockázat meghatározásához: folyamatok, alkalmazások, adatok, infrastruktúrák és végül, de nem utolsósorban, emberi tényezők.

  Alapvetően egy, az adott módszertannak megfelelően kiszámított érték képviseli, az összes lehetséges fenyegetés összegén alapul, amelynek az eszköz ki van téve, figyelembe véve az előfordulás valószínűségét és hatását.

  Tehát, ez az a kockázat, amelynek egy eszköz ki lehet téve, egyszerűen a természete és a vele kapcsolatos veszélyek miatt. Például egy nyilvános hálózaton lévő számítógép, amely semmilyen védelmi intézkedést nem tartalmaz.

- Fennmaradó vagy végső kockázat (**rRf**):

  Ez azt a kockázatot jelenti, amelynek egy szolgáltatás ki lehet téve, miután az eredendő kockázat csökkentése érdekében ellenintézkedéseket alkalmaztak.

- Végső elfogadható kockázat (**rRfa**):

  Ez a szervezet számára elfogadható maximális kockázati küszöbértéket jelenti.

A fentiekben meghatározott valamennyi kockázati értéket dinamikusnak kell tekinteni, mivel azok az idő múlásával változnak, és például a következő elemek befolyásolják őket:

- A fenyegetések alakulása;
- A szükséges szolgáltatási szintek módosítása;
- A referenciamutató-szabályok jogi rendelkezéseinek módosítása;
- Olyan szervezeti változások, amelyek befolyásolhatják a gyengeségeket vagy a fenyegetések valószínűségét, vagy megváltoztathatják a hatásukat;
- A biztonsági ellenintézkedések megerősítése vagy gyengítése.

Alapvető kockázatok:

Ez az egyes eszközökhöz és kockázati forgatókönyvekhez kapcsolódó információbiztonsági kiberkockázatokra vonatkozik.

Titoktartás:

Ez az adatok és információk védelmére vonatkozik az információkhoz való jogosulatlan hozzáféréssel vagy azok felhasználásával kapcsolatos kockázatok csökkentése érdekében.

Kitűzött helyreállítási pont (RPO):

Ez az elfogadható adatvesztésre vonatkozik, és az a maximális időtartam, amely a folyamatból származó adatok utolsó mentése és a folyamatot leállító esemény között telik el.

Kitűzött helyreállítási idő (RTO):

Az incidens utáni időszak, amelyen belül:

- A terméket vagy szolgáltatást vissza kell állítani, vagy
- A tevékenységet folytatni kell, vagy
- Az erőforrásokat vissza kell állítani.

Kockázati forgatókönyv:

Két vagy több olyan fenyegetés kombinációja, amely lehetővé teszi azok osztályozását.

Sebezhetőség:

Egy folyamat, szolgáltatás vagy eszköz eredendő gyengesége, amely egy vagy több fenyegetés alatt lehetővé teszi az információbiztonsági célok (titoktartás, integritás és elérhetőség) megsértését.
Példák:

- Nem elkülönített hálózatok;
- Titkosítással nem védett protokollok alkalmazása;
- Nem rendszeresen frissített operációs rendszerek;

- Titkosítatlan „érzékeny” adatokat tartalmazó adatbázisok;
- Nem frissített vírusdefiníciók;
- Nem ellenőrzött fizikai hozzáférés;
- Automatikus tűzoltó rendszer hiánya;
- Nem megfelelő tartalék energiaellátó rendszerek, stb.

2 FŐ REFERENCIASZABVÁNYOK

A biztonság tekintetében a legjobb nemzetközi gyakorlatoknak való megfelelés biztosítása érdekében elfogadott fő normákat a következő bekezdések írják le.

2.1 ISO/IEC 27001 szabvány

Az ISO/IEC 27001 szabvány egy nemzetközi biztonsági szabvány és egy valódi referenciaérték az információbiztonság szintjének értékeléséhez, amely képes elemezni mind azokat a technológiai, mind szervezeti összetevőket, amelyek hozzájárulnak az Információbiztonsági Irányítási Rendszer (ISMS) meghatározásához.
A szabvány meghatározza az ISMS-re vonatkozó követelményeket, és segít azonosítani, kezelni és minimalizálni azokat fenyegetéseket, amelyeknek az információk rendszeresen ki vannak téve. Ez a szabvány azokat a biztonsági ellenőrzéseket is meghatározza, melyeket az információk védelme érdekében el kell fogadni, és az érdekelt felek, köztük a szervezet ügyfelei számára is biztonságossá kell tenni.

2.2 ISO/IEC 27002 szabvány

Az ISO/IEC 27002 szabvány meghatározza a szervezeten belüli megfelelő információbiztonsági irányítási rendszer bevezetésének irányelveit és általános elveit.
Az ISO/IEC 27002 szabvány egy nemzetközi biztonsági szabvány és egy valódi viszonyítási alap az információs rendszer biztonságának szervezeti, eljárási, technológiai és szabályozási szempontjainak értékeléséhez annak érdekében, hogy:

- A szóban forgó rendszer által már biztosított vagy biztosítandó szolgáltatások és funkciók kritikai vizsgálata elvégzésre kerüljön;
- A rendszer sebezhetősége feltárásra kerüljön;
- A célkitűzésekben meghatározott biztonsági szint eléréséhez szükséges megfelelő intézkedések feltüntetésre kerüljenek.

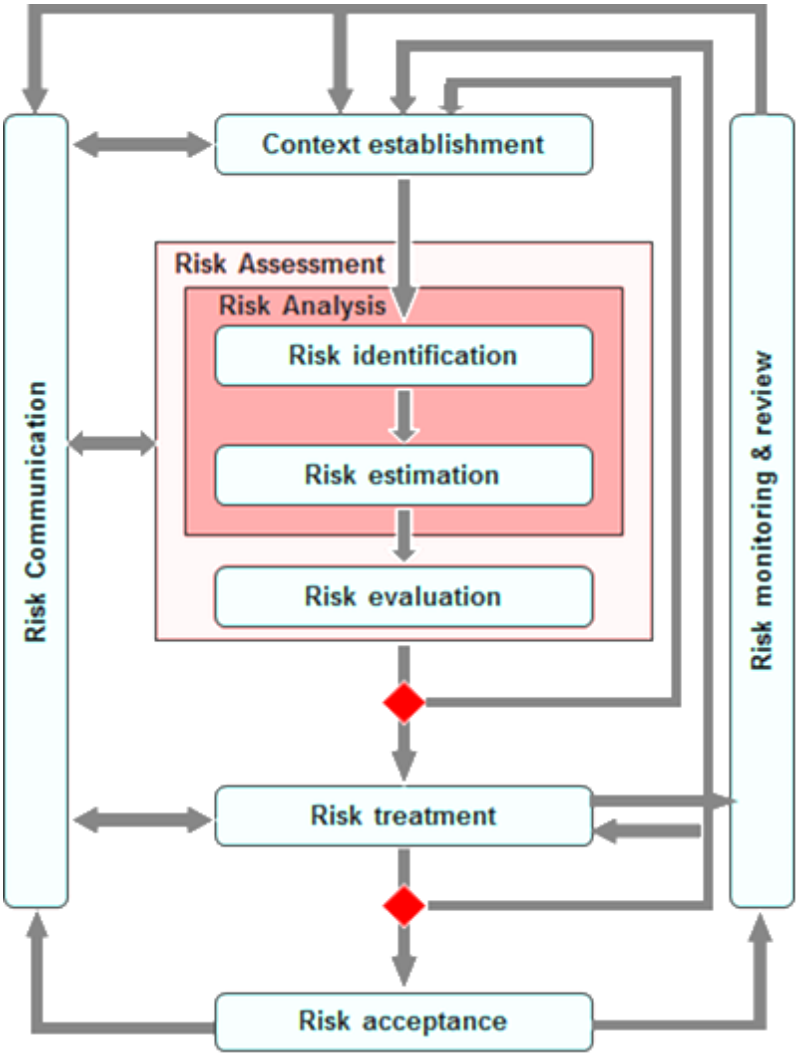
Meg kell jegyezni, hogy az ISO/IEC 27002 meghatározza azokat a biztonsági ellenőrzéseket, amelyeket a szervezetnek figyelembe kell vennie, de nem helyettesíti magát a kockázatelemzést.

2.3 ISO/IEC 27005 szabvány

Az ISO/IEC 27005 leírja az információbiztonsági kockázatkezelési folyamatot és a kapcsolódó intézkedéseket, amelyek támogatják az ISO/IEC 27001 általános elveit.

A szabvány – az ISO 31000 szabványnak megfelelően – arra szolgál, hogy segítse a vállalatokat az információbiztonsági kockázatok kezelésében, hasonlóan ahhoz, ahogyan más típusú kockázatokat kezelnek.

Az 1. ábra az ISO/IEC 27005 által javasolt kockázatkezelési folyamatot mutatja be, amely az Aruba Csoport által elfogadott és kifejlesztett modellt ihlette.



1. ábra – ISO/IEC 27005: A kockázatkezelés folyamata

3 INFORMÁCIÓBIZTONSÁGI KOCKÁZATOK KEZELÉSÉNEK MÓDSZERTANA

Az Aruba S.p.A. Csoport számára az információ olyan eszközt jelent, amely gondos kezelést igényel, és stratégiai fontosságú a vállalat üzleti tevékenységének védelme és fejlesztése szempontjából.

Ebben az összefüggésben a kiberkockázat olyan bizonytalan eseményként határozható meg, amely a vállalat információs eszközeinek az alábbi három fő tulajdonsága közül egyet vagy többet veszélyeztethet:

- **T**itoktartás (az adatokhoz illetéktelen személyek is hozzáférhetnek);
- **I**ntegritás (az adatok jogosulatlan módosítás tárgyát képezhetik, és megváltoztathatók);
- **E**lérhetőség (a számítógépes rendszer nem használható);

a súlyosság szintjétől függően, amely szigorúan az érintett információ típusától függ.

A kockázatértékelés a következő lehetséges hatástípusokat veszi figyelembe:

- Gazdasági;
- Szabályozási;
- Hírnévbeli.

Az információbiztonsági kockázatkezelés a szervezet eszközei, kapott fenyegetései és sebezhetőségei közötti kölcsönhatások értékelésére szolgáló folyamat. Ezen elemzési folyamat célja, hogy azonosítsa az eszközökben található sebezhetőségekkel és fenyegetésekkel kapcsolatos kockázatokat, és alapot adjon egy hatékony biztonsági program meghatározásához.

A figyelembe vett kockázati kategóriáknak meg kell egyezniük az adott helyzetben alkalmazandó típusokkal. A figyelembe vett kockázatok tehát származhatnak belső, külső vagy környezeti fenyegetésekből, valamint szándékos cselekményekből, illetve a nem megfelelő szervezeti irányításból vagy gondatlanságból.

A kockázat értéke a kérdéses eszközök értékének, a fenyegetések értékének és a sebezhetőségeknek a függvénye.

A kockázatelemzés eredményeit a következőkkel együtt kell dokumentálni:

- A fő kockázatok egyértelmű azonosítása;
- Annak értékelése, hogy az azonosított kockázatok milyen potenciális hatással lehetnek az üzleti tevékenységre;
- Ajánlott intézkedési terv a kockázatok csökkentésére és elfogadható szintre való visszaállítására.

Az Aruba Csoport kvalitatív elemzési modellt alkalmaz, mivel azonnal magas szinten ismerteti a szóban forgó technológiai környezetet érintő főbb ICT-kockázatokat.

Az alkalmazott módszertan:

- A Csoport a vonatkozó folyamatokban szereplő információk értékének és az őket fenyegető kockázat szintjének becslésére alkalmazza, hogy megfelelő védintézkedéseket hajthasson végre;

- Akkor is alkalmazandó, ha olyan új infrastrukturális vagy alkalmazási megoldások kerülnek kifejlesztésre, amelyek hatással vannak a kezelt adatok biztonságára. Ebben az esetben a módszertan lehetővé teszi annak felmérését, hogy mennyire kritikusak az adatok és a rájuk leselkedő veszélyek, hogy a számítógépes rendszerek fejlesztése és beszerzése során a kockázatelemzésért felelős személyek megfelelő védelmi intézkedéseket hozhassanak a sebezhetőségek minimalizálása érdekében.

A kockázatértékelést, valamint az eszközök, a fenyegetések és az ellenintézkedések közötti összefüggések elemzése egy belső fejlesztésű eszköz segítségével kerül elvégzésre, az elemzett folyamatokban részt vevő különböző személyekkel folytatott konkrét találkozók során összegyűjtött információk felhasználásával.
A módszertan egy olyan üzleti modell létrehozását jelenti, amelyben leírásra kerülnek a későbbi elemzésekhez szükséges alapelemek, azok jellemzői, hierarchikus struktúrái és a kapcsolódó kapcsolatok.

4 A KOCKÁZATKEZELÉS FOLYAMATA

Az Aruba S.p.A. Csoport által elfogadott és alkalmazott, az információbiztonsággal kapcsolatos kockázatok kezelésére szolgáló elemzési modell fő fázisait az alábbiakban ismertetjük.

4.1 1. FÁZIS – A kontextus meghatározása

Az elemzés kontextusának meghatározása magában foglalja a vállalat helyzetének modellezését és az érintett fő üzleti szolgáltatások, folyamatok, makrofolyamatok és eszközök azonosítását.

Az ISO/IEC 27005 „Information technology – Security techniques – Information security risk management” által javasolt erőforrások azonosításakor két különböző típust kell figyelembe venni:

- **Elsődleges erőforrások** – információk, folyamatok, makro-folyamatok és üzleti szolgáltatások;
- **Másodlagos erőforrások vagy eszközök** – hardver, szoftver, személyzet, hálózat, helyszín és szervezet.

4.1.1 A szolgáltatások, folyamatok és makrofolyamatok azonosítása

A szervezet szolgáltatásainak és folyamatainak azonosításakor a belső vállalati kommunikációs eszközön keresztül közzétett és elérhetővé tett szervezeti struktúrákat használjuk kiindulási referenciaként.
Ezt követően az egyes folyamatokat, amelyek hozzájárulnak a szolgáltatások nyújtásához, az elemzett kontextusra jellemző makrofolyamatokba csoportosítjuk.

4.1.2 Az eszközök azonosítása

Az eszközök pontos azonosítása érdekében az alábbi lépéseket követjük:

1. Az információs eszközök **kategóriáinak (pl. hardver, szoftver, helyszín stb.) azonosítása** az ISO/IEC 27005 szabványban meghatározott osztályozási rendszer szerint;

2. Az információs eszközök **kategóriáinak súlyozása** a vállalat biztonsági stratégiájának és üzleti, jogi és szerződéses követelményeinek megfelelően;
3. A kategorizált eszközök kategóriái közötti **függőségek azonosítása**.

4.1.3 A makrofolyamatok és az eszközök közti kapcsolatok

Az eszközök azonosítása után meghatározásra kerülnek az eszközök és a makrofolyamatok közötti függőségek.

Ezek a függőségek azt jelentik, hogy a CIA hatásértékei az egyes eszközkategóriákhoz társíthatók (BIA interjúk által meghatározva), és ezáltal az egyes eszközökhöz kapcsolódó alapvető kiberkockázatok kiszámíthatók.

4.2 2. FÁZIS – Kockázatelemzés

4.2.1 Hatásvizsgálat

A hatásvizsgálatot (Business Impact Analysis, BIA) a főbb nemzetközi szabványok (ISO 27005, ISO 22301) kiegészítéseként elfogadott módszerrel összhangban, üzleti képviselők végzik.
A BIA interjú szakaszában egy belső információgyűjtésre kifejlesztett eszköz használatával a különböző vállalati részlegek vezetői értékelik a hatáskörükön belül kezelt információk bizalmasságának, integritásának és elérhetőségének elvesztését a gazdasági, szabályozási és jó hírnévre gyakorolt hatás szempontjából, jól meghatározott értékelési skálák szerint.

Az 1. FÁZISBAN leírtak szerint az egyes folyamatokat az elemzett kontextusra jellemző makrofolyamatokba csoportosítják. Az ezekhez a makrofolyamatokhoz kapcsolódó hatásokat az őket alkotó különböző folyamatok egyedi hatásainak *„legrosszabb eseteként”* számítják ki.

4.2.2 Az eszközök azonosítása és értékelése

Az eszközök azonosítása a kiindulópont, amely nélkül nem lehet megfelelően és hatékonyan kezelni a vállalat biztonságát. Valójában a leltár a kiindulópont a vállalat eszközeinek osztályozásához és a kockázati szint elemzéséhez.

Ennek az operatív szakasznak az a célja, hogy leltárt készítsünk az információs eszközökről, vagy hivatalossá tegyük a meglévő módszereket, amelyeket a vállalat „küldetéskritikusnak” tekint üzleti céljainak elérése, szerződéses kötelezettségeinek teljesítése és végül a tevékenységére vonatkozó szabályok és jogszabályok betartása érdekében.
Egy eszköz központi értékét általában azok az információk (vagy adatok) képviselik, amelyeket a rendszer feldolgoz, és a feldolgozás vagy a védelem feladatát más eszközökre hagyja.
Ebben az összefüggésben az értéket a BIA interjúk során hozzárendeljük az eszközökhöz és a CIA biztonsági dimenzióhoz (titoktartás, integritás és rendelkezésre állás).

Az interjúk során összegyűjtött információk felhasználásával tehát lehetőség van arra, hogy az egyes eszközökhöz hozzárendeljük azokat a makrofolyamatokból eredő hatásokat, amelyek során azokat használjuk.

4.2.3 A fenyegetések elemzése és valószínűségük vizsgálata

Az információbiztonsági kockázatkezelési folyamat során alkalmazott módszertan időszerű lépést határoz meg a szóban forgó eszközöket érintő fenyegetések meghatározásában. A fenyegetések mindazokat az elemeket vagy eseményeket képviselik, amelyek kárt okozhatnak egy eszközben.

E tevékenység célja az azonosított és a kockázatelemzési és -kezelési folyamat részét képező eszközöket érintő fenyegetések és sebezhetőségek azonosítása, valamint előfordulásuk valószínűségének felmérése.

Annak érdekében, hogy a fenyegetések listája teljes legyen, az ENISA által a témával kapcsolatos tanulmányait követően kidolgozott és közzétett megfontolásokon kívül hivatkozunk az ISO/IEC 27005 szabványban szereplő fenyegetések listájára is.

Az egyes fenyegetéseket ezt követően reális kockázati forgatókönyvek szerint csoportosítjuk az elemzés tárgyát képező kontextusra vonatkozóan.

4.2.4 Az ellenintézkedések elemzése

E tevékenység célja az előző lépésben azonosított eszközökre vonatkozó kockázati forgatókönyvek fedezéséhez szükségesnek ítélt ellenintézkedések azonosítása.

A lista teljességének biztosítása érdekében az Aruba Group S.p.A az ISO/IEC 27001 A. melléklet szerinti szabvány legjobb gyakorlatain alapuló ellenintézkedések listáját alkalmazza. Az elemzett szolgáltatás típusától függően az egyes tárgyak esetében az értékeléseket a hiteles források, például az ENISA, az AgID, a NIST stb. által javasolt további ellenőrzések elemzésével lehet bővíteni.

A védelmi ellenőrzések listájának meghatározását követően feltérképezzük őket azon kockázati forgatókönyvek tekintetében, amelyek alapján csökkenthetők a releváns fenyegetések bekövetkezésének valószínűsége vagy hatása.

Az ellenintézkedések felépítése:

- **Reaktív** (r), amelynek célja a hatás csökkentése;
- **Preventív** (p), amelynek célja, hogy csökkentse a fenyegetés bekövetkezésének valószínűségét.

4.3 3. FÁZIS – Kockázatértékelés

4.3.1 Kockázati modell és módszertan

A kockázat értékét funkciónak kell tekinteni $R = f(A, M, V)$, ahol A a kérdéses eszközök értéke, M a fenyegetések értéke és V a sebezhetőségek.

Az információbiztonsági kockázatkezelési folyamat 2. FÁZISÁN keresztül meghatározható a kockázati modell (*veszélymodellezés*). Ez egy olyan folyamat, amelyet a potenciális fenyegetések és sebezhetőségek azonosítására, az adott körülmény bekövetkezésének valószínűségének felmérésére, rangsorolására és a bekövetkezésük kockázatának csökkentésére használnak a megfelelő ellenintézkedések végrehajtásával.

Miután az alapvető kontextus meghatározásra került, a *fenyegetésmodellezési* folyamat magában foglalja:

- A potenciális támadások/sebezhetőségek listájának összeállítását, amely tartalmazza az adatok bizalmasságának, integritásának és elérhetőségének veszélyeztetését;
- A legvalószínűbb támadások/sebezhetőségek értékelését, kivéve azokat, amelyek valószínűtlenek vagy orvoslásuk szinte lehetetlen, és az összes többi ellenőrzést vagy ellenintézkedést, amely technikai vagy eljárási jellegű.

4.3.2 Alkalmazandó biztonsági követelmények és megfelelőségi szint

Az elemzés keretében alkalmazandónak tekintett biztonsági követelmények meghatározását követően (lásd az „Ellenintézkedések elemzése" című szakaszt) az ISO/IEC 27001 szabvány A mellékletében meghatározott 14 területre vonatkozó követelmények teljesülésének mértéke kerül értékelésre.

Az egyes ellenintézkedések megfelelőségének mértékét jól meghatározott, 0-tól (ahol nincs ellenintézkedés) 4-ig terjedő értékskála szerint fejezzük ki, amennyiben az ellenintézkedés teljes mértékben végrehajtásra került.

Az ISO/IEC 27001 szabvány A mellékletében előírt ellenőrzések megfelelőségi szintjének elemzéséhez a belsőleg végzett konkrét értékelési tevékenységek során gyűjtött információkat és bizonyítékokat használjuk fel.

4.3.3 Az eredendő és fennmaradó alapkockázatok kiszámítása

Ebben a fázisban számítjuk ki az elemzés tárgyát képező szolgáltatással kapcsolatos alapvető CIA biztonsági kockázatok (JELENLEGI, tervezett és jövőbeli) értékét.

Az egyes eszközökre és forgatókönyvekre vonatkozó, a fent leírt logika szerint társított, eredendő alapkockázatokat az egyes kockázati forgatókönyvek bekövetkezésének valószínűsége és azok lehetséges hatása figyelembevételével számítjuk ki.

Az eredendő kockázatok meghatározását követően a fennmaradó kockázatok (JELENLEGI, tervezett és jövőbeli) elérése érdekében a belső ellenőrzési szakaszban figyelembe vesszük az azonosított kockázati forgatókönyvek ellensúlyozásához szükséges biztonsági ellenintézkedésekhez kapcsolódó értékeket, mind a veszélyek valószínűségének, mind a hatás csökkentése tekintetében.

4.4 4. FÁZIS – Kockázatkezelés

4.4.1 Az elfogadott kockázatok elemzése

A kockázatkezeléssel kapcsolatos egyik fogalom az elfogadott kockázatok fogalma. Ez a kifejezés általában azokra a kockázatokra vonatkozik, amelyeket valamilyen okból nem lehet praktikusan vagy egyáltalán kezelni, és amelyeket egyszerűen elfogadunk.

Ennek a tevékenységnek a célja tehát egy olyan kritérium meghatározása, amely szerint az alacsony kockázattal járó fenyegetettségi eszközpárok egyszerűen elfogadhatók. Az egyedi eseteken túl ezért egy küszöbértéket határozunk meg, amely alatt egy bizonyos kockázat egyszerűen költségnek minősül, és ezért nem foglalkozunk vele.

4.4.2 Az elemzés eredménye: fennmaradó JELENLEGI kockázat

A kockázatok elemzésével és értékelésével kapcsolatos munka, figyelembe véve az alkalmazott ellenintézkedéseket (fennmaradó kockázat), a következők végrehajtásával történik:

- A biztonsági ellenőrzések értékelése az ISO/IEC 27001 szabvány A mellékletének legjobb gyakorlata tekintetében;
- A kérdéses szolgáltatások tekintetében az információ rendelkezésre állásának, bizalmasságának és integritásának elvesztéséből eredő hatás elemzése;
- A sebezhetőségek és az eszközöket fenyegető veszélyek elemzése;
- A jelenlegi információbiztonsági kockázat felmérése és a fontossági sorrend megállapítása.

4.4.3 Hiányelemzés és a végrehajtandó ellenintézkedések kiválasztása

Az elvégzett elemzési munkát követően az Aruba Group S.p.A. által nyújtott szolgáltatások körébe tartozó releváns kockázatok/kérdések kezelése és az ISMS folyamatos javítása érdekében a kockázatelemzési eszközben elvégzett elemzésekből nyert adatokat feldolgozzuk azon kockázati területek azonosítása érdekében, amelyekre vonatkozóan megfelelő biztonsági intézkedéseket kell meghatározni.

A kockázatok javításához és csökkentéséhez szükségesnek ítélt intézkedések azonosítása érdekében ezért időről időre hiányelemzést kell készíteni a biztonsági ellenintézkedések jelenlegi alkalmazási szintje és a legmagasabb alkalmazandó szint közötti eltérés értékelésére.

4.4.4 Kockázatkezelési terv – A beavatkozás racionalizálása

A hiányelemzésben azonosított intézkedéseket ezután konkrét projektkezdeményezésekbe csoportosítjuk, és dokumentáljuk a kockázatkezelési tervben.

5 AZ ELEMZÉSEK GYAKORISÁGA

Az információbiztonsági kockázatkezelési folyamatot 12 havonta, illetve jelentős esemény bekövetkezése esetén gyakrabban kell elvégezni, beleértve, de nem kizárólagosan az alábbiakat:

- A kockázatkezelés hatálya alá tartozó új eszközök;
- A szervezeten belüli és kívüli olyan új fenyegetések, amelyeket még nem értékeltünk;
- Annak lehetősége, hogy az új vagy megnövekedett sebezhetőségeket kihasználják a fenyegetések;
- A már azonosított sebezhetőségek felülvizsgálata az új vagy újonnan felbukkanó fenyegetéseknek jobban kitettek meghatározása érdekében;
- Az eszközökre, sebezhetőségekre és kockázatokra gyakorolt fokozott hatások vagy következmények, amelyek együttesen elfogadhatatlan általános kockázati szintet eredményeznek;
- Különösen súlyos biztonsági esetek.

Ezenkívül az elemzések különböző gyakorisággal is elvégezhetők, például bizonyos szabványoknak vagy tanúsítási követelményeknek való megfeleléssel kapcsolatban.

BlazeArts Kft.
1096 Budapest, Thaly Kálmán utca 39. cégjegyzékszám: 01-09-389087
adószám: 12539833-2-43 közösségi adószám: HU12539833
https://www.arubacloud.hu