ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Kockázatmenedzsment gyakorlat

Som Zoltán

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalomjegyzék

Mottó:

„Az egyetértés - minden. A közvélemény támogatásával minden sikerül. Nélküle semmi."[1]

I. fejezet: A kockázatmenedzsment gyakorlat elméleti háttere, felépítése

1. *'Gap' elemzési technikák.*

A szó jelentését röviden elemezve valamilyen rés, szakadék, hézag vagy nyílás, amely egy objektumon található, vagy két objektum között. Érdemes röviden megvizsgálni, a keletkezését, információbiztonsági szempontból. Az információbiztonsági és egyéb vonatkozó törvényi és szabályozási környezet előírásait a munkaszervezetben, jellemzően munkavállalók hajtják végre.[2] Ahhoz hogy ezen feladatot, a kockázatok, folyamatok feltérképezését, elemzését végrehajthassák birtokában kell, hogy legyenek annak a tudásnak, hogy átlátják és perspektivikus rálátásuk van a szervezet minden folyamatára. Ezen tudás és a szaktudás birtokában, esetleges további tényezők figyelembevételével elkészül a szervezetre szabott kockázatfelmérés, majd ennek kezelési terve. Az előbbi rövid áttekintésből tehát kitűnik, hogy a folyamatok és feladatok mögött emberek dolgoznak, saját tudásukat felhasználva és aktuális rálátásuk alapján a szervezeti folyamatokra, elvégezik a kockázatmenedzsment adott lépéseit. Tehát az első lehetséges eltérés[3] ott adódik, hogy ezen tudás és a valós helyzet nem feltétlenül esik tökéletesen egybe. Ez önmagában tény és ekként kezelve és elfogadva, mint potenciális kockázatot már kezelni is lehetséges. A rendszeres felülvizsgálatok, változáskezelés, életciklusba épített kontrollpontok és frameworkök használata hatékony támogatást jelenthet ebben a folyamatban, az eltérések felderítésének tekintetében.

Általánosságban tekintve a szó jelentését, a jelenlegi és az elérni kívánt állapot közötti eltérésekre is használja a szakirodalom. Egyes megközelítésben beleértik az eltérések felderítését és ezekre akcióterv kidolgozását is a gap analízisbe. A költség és várható üzleti előnyök, a szervezet kockázatkezelési stratégiája és kockázati étvágy mind befolyásolni

[1] Abraham Lincoln
[2] Beleértve egyes hardverelemek konfigurációját is a munkavállaló folyamataiba.
[3] Lehetséges rokon értelmű szavak még: csapda, hézag

fogják a kockázatmenedzsmentet is.[4] Azaz akár az is elképzelhető, hogy adott eltérés dokumentálásra és elfogadásra kerül, mert felszámolása nem gazdaságos, azon a ponton alacsonyabb biztonsági szint is elfogadhatóvá válik.[5] A változások miatt természetesen folyamatosan alakulhatnak ki rések az kontrollok és a kontroll célkitűzések, vagy biztonsági célok között. Éppen ezért a változáskezelésben ezt a területet is kezelni szükséges, valamint ettől függetlenül, periodikusan felül kell vizsgálni a folyamatokat, bevett gyakorlattá kell tenni. A kontrollok hatékonyságát oly mértékben kell tesztelni, hogy ha azok hatékonysága kívül esik a kockázattűrésen, akkor szükségesség válhat a módosítása, újratervezése, vagy kiegészítése további kontroll tevékenységgel.

1.1 Ellenőrzések és ellenőrzési célkitűzések, amik befolyásolják az információk biztonságát

Egy egészen egyszerű megközelítés azt mondja, hogy az alábbi fő szempontok figyelembevételével, alkalmazásával és betartásával, amit már számos ágazatban használnak, elérhető a megfelelőség és a kontrollált állapot. A módszer alapja, hogy függetlenül a több száz kontrollponttól és szabályzattól. Az alábbi megközelítés segít biztosítani, hogy az információgyűjtés teljesen objektív, teljes és megismételhető. [6]

R – Ki, vagy kik azok a személyek, akik Felelősek a teljesítési szempont definiálásáért?

I – A kockázat alapú kontrollok vagy a PCI alapú kontrollok végrehajtása hatékonyabb?

D – Megfelelőek-e a támogató eljárások és dokumentációs szabályzatok?

E – Lehet-e bizonyítékot rendelkezésre bocsátani a hatékony bevezetéshez?[7]

Az eddigiek alapján megállapítható, hogy az első lépés megtétele előtt olyan szervezeti folyamatokat is átlátni képes, rendszerezett tudásra van szükség. Amely csökkentheti a szabályozással és kontrollpontokkal nem lefedett területeket, növelheti a folyamatok

[4] ISO, NIST, COBIT mint lehetséges szakirodalom és ajánlások gyűjteménye.
[5] Residual risk: elfogadott, vagy megmaradó biztonsági kockázat.
[6] Wright, Steve. "Chapter 4 - Step 4 – Conduct Gap Analysis". PCI DSS: A Practical Guide to Implementing and Maintaining Compliance, Third Edition. IT Governance.
[7] R: Responsible, I: Implemented, D: Documented, E: Evidence

értékteremtési indexét. Jelentős előny a kockázatmenedzsment folyamán a szervezeti kultúra és szokások és szokásjog ismerete, ezek esetleges eltérése a szabályzatoktól. [8]

Az ellenőrzések és ellenőrzési pontok minősége, a beérkező adatok mennyisége és minősége[9] jelentősen befolyásolni képes általában véve a biztonságot és az ellenőrzés minőségén, eredményén keresztül. A beérkező adatokat, eseményeket fel kell dolgozni. Ezek egy része történhet automatikusan, technikai eszközök segítéségével, azonban mindig lesznek olyanok, amelyek emberi erőforrást igényelnek a kiértékelés szempontjából. Ha ezen humánerőforrást igénylő események számossága túllép egy kritikus, reálisan feldolgozható mennyiséget, akkor elkerülhetetlenül romlik a minősége a feldolgozásnak. Ez a romlás minőségromlás többféle dimenzióban megnyilvánulhat, növekedhet a feldolgozás és ezáltal a válaszadás ideje, vagy a romolhat a feldolgozás precizitása. Esetleg az eredetileg még kézi feldolgozásra javasolt esemény, a fenntarthatóság érdekében átkerül a gépi, technikai feldolgozásra.

1.2 Jelenlegi helyzet és a kívánatos vagy célállapot meghatározása

Az alcímből is látszódik, hogy nem csak két állapota a kockázatokkal kapcsolatos helyzetnek. Mindig figyelembe kell venni a kockázat besorolását, mik a legsürgetőbb teendők, mi az, amelyik legnagyobb (pénzügyi) hatással lehet a szervezetre, mi a legkönnyebben és/vagy leggyorsabb elérhető cél.[10] A szervezeti kultúra és szabályozási környezet mit tesz lehetővé. Mindezek alapján egy lehetséges menetrend a nagyságrendi feladatok és lépések meghatározása:

- a jelenlegi helyzet meghatározása,
- a távlati célállapot meghatározása (vizionálása, elképzelése, security roadmap készítése)
- egy rövid és egy középtávú célállapot meghatározása (a döntési szempontok dokumentálása)
- a rövidtávú célállapothoz szükséges kezdeti lépések megfogalmazása.

[8] Abban a tipikus esetben, amikor a szervezeti szokásjog és szabályzat eltér, érdemes megvizsgálni, hogyan közelíthető egymáshoz a kettő. Javasolt figyelembe venni, hogy az új megoldás valóban több értéket legyen képes szállítani, mint az előzőek. Azaz valósuljon meg az információbiztonságon keresztül az értékteremtés is.
[9] Valamint további számos tényező
[10] Sürgős és/vagy fontos dolgok mátrixára számos értelmezés található az interneten.

A gap-analízis kifejezést használva a jelenlegi és a célállapot helyzetek különbségét érti a szakirodalom. Fontos kiemelni, hogy ennek az analízisnek nem része a problémamegoldás, csupán a vizsgálat. A cél az, hogy ezt a szakadékot valamilyen műveletsorral át lehessen hidalni. Gyakran alkalmazzák a visszafelé kereséses technikát, a kíván állapotból logikailag visszavezetve. Azonban néhány probléma, vagy túl sok alternatív megoldás esetén ennek kevés gyakorlati haszna lehet, vagy nem használható.
Az aktuális, jelenlegi helyzet meghatározásához figyelembe kell venni a:

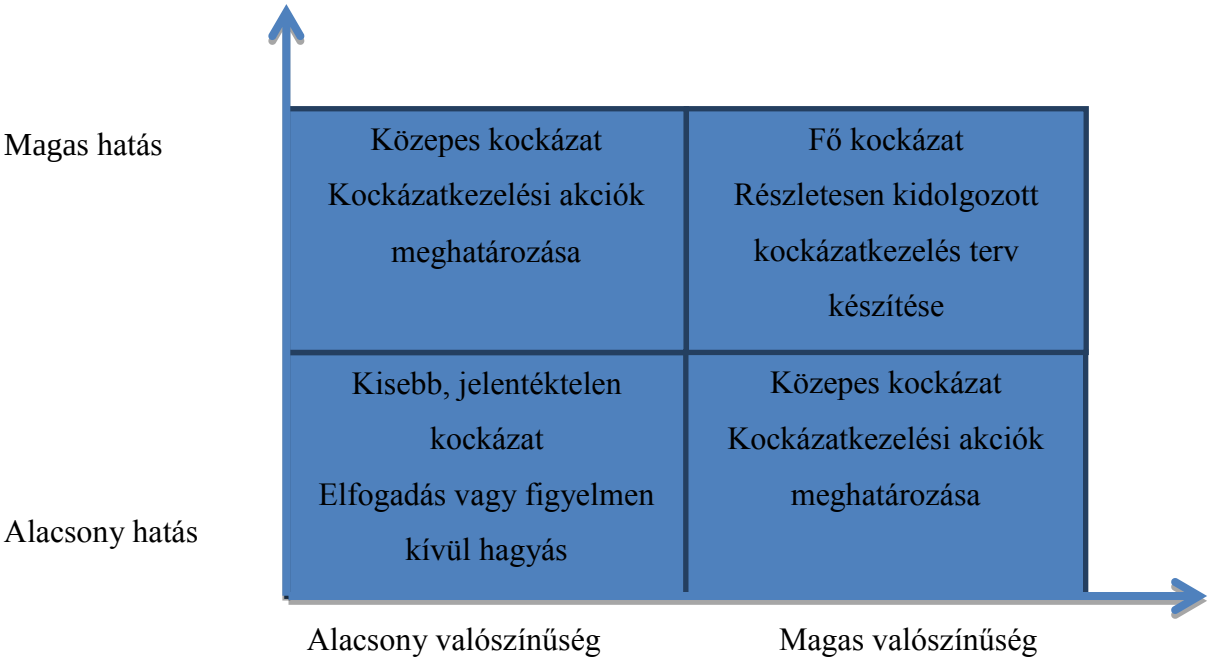
- nemzetközi sztenderdeket,
- törvényeket,
- belső szabályozásokat, eljárásrendet,

melyek képesek rámutatni, hogy mely szabványoknak, keretrendszereknek és vonatkozó egyéb feltételeknek kell majd megfelelni, vagy jelenleg megfelel-e a szervezet. Tehát a folyamat során megvalósul a feltérképezés is. Ez az analízis, elemzési folyamat betekintést nyújt, illetve pillanatképet ad a szervezet jelenlegi megfelelőségi szintjéről. Egy jól kivitelezett elemzés és az annak folyamán felmerülő információk hasznos segítségül szolgálhatnak a megfelelőség eléréséhez, az ütemterv létrehozásához. Ez a folyamat akkor teljes, ha sikerül azonosítani azokat a területeket, amivel foglalkozni szükséges és némi munkával a lista priorizálható, a következő lépés megtételéhez.
Az elemzés lefolytatásának talán első pontja az lehet, hogy be kell szerezni egy példányt minden vonatkozó szabályozásból. Ezen dokumentumok listája és hossza jelentős lehet. Természetesen ezen hazai, külföldi és szervezeti szabályozások, keretrendszerek ajánlások különböző súllyal esnek majd latba, de tisztában kell velük lenni. Szükséges egy példány az aktuális belső szabályozási és eljárási rendekből is, ezek le kell, hogy fedjék a szervezeti folyamatokat.[11] A gyakorlatban nagy segítség lehet valamilyen már meglévő keretrendszer, szabvány vagy ajánlás használata. Ennek kiválasztásához érdemes figyelembe venni hasonló szervezeteknél használtakat, ajánlásokat, vagy azt, hogy melyik modell hasonlít legjobban a jelenlegi szervezeti állapothoz.[12] Meg kell határozni az elemzés körét. Van pár megközelítés, hogy hogyan lehet elérni a megfelelőséget. Ez különösen könnyű akkor, ha valamilyen iparági szabvánnyal kell összevetni a meglévő állapotokat.

[11] Eljárások, szabályok, kontrollok, s a többi. Ne lehessen olyan kérdést feltenni, amely napi rutinnak számít, de nincs róla szó a dokumentumokban.
[12] A legnagyobb hasonlóságot mutató keretrendszert választva, a kevesebb változtatás révén több idő és energia jut a lényeges feladatokra.

1.3 Az aktuális kockázatok meghatározása

Az aktuális kockázatok meghatározásánál fontos megemlíteni, hogy a kockázatok meghatározása a legtöbb esetben nem esik egybe a „kezelt" kockázatokkal. Ennek az oka, hogy a kockázatok azonosításának a célja a rangsorolás, kategóriákba rendezés. Nem létezik olyan munkaszervezet, amelynek elegendő erőforrása lenne minden azonosított kockázat kontrolljára, kezelésére.[13] A kockázatkezelés jellemzően arra kap felhatalmazást, vagy arra tesz kísérletet, hogy hatékonyan, korlátozott források felhasználásával tegye meg a legtöbbet. Egy lehetséges egyszerű rangsorolási folyamat az alábbi ábrán[14] látható. Ennél természetesen sokkal összetettebb, az összefüggéseket is mutató mátrix is készíthető.



1. ábra[15] Lehetséges rangsorolási folyamathoz besorolási táblázat minta

Minden fenyegetés komoly aggodalomra ad okot, nincs olyan, amire elég legyinteni, hogy nem fontos, vagy ilyet már láttunk. Létre kell hozni egy olyan módszert, amely priorizálni képes (a már azonosított) kockázatokat kis, közepes és magas kategóriákba. Mivel a rendelkezésre álló erőforrások sokkal korlátozottabbak rendszerint, mint a fenyegetések, így a

[13] Természetesen kezelésnek tekinthetjük az elfogadást is, így ebben az esetben talán pontatlannak tűnhet a mondat.
[14] Peltier, Thomas R.. "Appendix K - Why Risk Assessments Fail". How to Complete a Risk Assessment in 5 Days or Less. Auerbach Publications. 2009.
[15] Peltier, Thomas R.. "Appendix K - Why Risk Assessments Fail". How to Complete a Risk Assessment in 5 Days or Less. Auerbach Publications. 2009 (K.1-es ábra, lehetséges rangsorolási folyamat)

korlátozott szervezeti erőforrások felhasználásával kell a lehető a lehető legtöbbet tenni, a legjobb eredményt elérni. Az 1. ábrán látható kategorizálásba minden fenyegetettséget besorolva már olyan kiindulási állapot nyerhető, amely (akár tovább vizsgálva és további kategóriákba rendezve) alkalmas lehet a fontos / sürgős, vagy az időben legelső teendők meghatározására.

Ezen meghatározások során, a szervezeti szabályozás áttekintésével is már kiderülhetnek olyan terültek, amelyek esetleg a szabályozási szcenárión kívül esnek. Az áttekintés során az adott keretrendszer függvényében tudjuk használni az ajánlott szempontokat. Ennek hiányában pedig a munkaszervezeti folyamatok feltérképezése során is kialakítható egy táblázat, akár az alábbi 2. ábrán látható minta alapján.

Kontroll	**Megfelelőség (Igen/Nem)**	**Megjegyzés**
A szervet informatikai biztonsági tisztségviselője vagy ezzel egyenértékű vezetői szintű hatóság ki van nevezve és felelős az információbiztonsági program végrehajtásáért és fenntartásáért, a hatékony programvégrehajtásért.		
Az információbiztonsági vezető csapatának vagy osztályának dedikált feladat és felelősség az információbiztonsági tevékenység folytatása a szervezetben, beleértve a biztonsági adminisztrációt, a tudatossági oktatást és tréninget, fejlesztést és esemény kivizsgálásokat.		
Az információbiztonsági program az üzleti, szervezeti célokat és a küldetésnyilatkozatot. Az egész szervezetre érvényes információbiztonsági program végrehajtását támogatja a felső vezetés.		
Átfogó információbiztonsági eljárások és irányelvek és leírások léteznek és az összes munkavállaló és harmadik fél (beszállítók) számára is elérhető.		

Átfogó információbiztonsági szabályok, sztenderdek és leírások léteznek és közzétételre kerültek az összes munkavállaló és harmadik fél (beszállítók) számára is elérhető a hálózaton.		
Az információbiztonsági program szerves része a szervezetben az általános irányítási gyakorlatnak.		
Az információbiztonsági program önálló költségvetési tétel (minimálisan 5-8%-a a teljes információs rendszer működésének).		
A felső vezetés tisztában van azzal, hogy az üzletnek szükséges van a hatékony információbiztonsági programra és demonstrálja elkötelezettségét, hogy ezzel is támogassa az információbiztonsági programot.		
A kockázatelemzési folyamat segít a menedzsmentnek azonosítani a potenciális veszélyeket és azok valószínűségét, a lehetséges ellenintézkedések és ez minden egyes rendszerfejlesztési folyamat része.		
Az információbiztonsági eszközök vásárlása és a szabályok és bevezetésük költség-haszon elemzés felhasználásával történik, ahol a kockázatelemzés az input tényező.		
Az információbiztonsági felelősség és elszámoltathatóság az összes alkalmazott és üzleti partner előtt egyértelmű és nyilvános, jól publikált.		
Minden szervezeti terület, osztály, iroda, s a többi rendelkezik kijelölt felelős személlyel, aki kommunikálja az információbiztonsági politikát és végrehajtásában rész vesz a szervezetben.		
Az információbiztonsági program integrált az összes területén a szervezetnek, belül és kívül egyaránt a számítógépes biztonság területén.		

A folyamatban lévő információbiztonsági tudatossági programot alkalmazzák minden alkalmazottra és üzleti partnerre.		
Pozitív és proaktív a kapcsolat az információbiztonsági program és az audit között. Rendszeres kommunikáció van a kettő között.		
Az alkalmazottak és üzleti partnerek tudatában vannak, hogy tevékenységüket ellenőrizni lehet, esetleg monitorozásra kerül.		
Egy hatékony program került bevezetésre az információbiztonsági programmal kapcsolatos tevékenységek nyomon követése és hatékonyságának értékelése érdekében.		
Az alkalmazottak megfelelőségének információbiztonsággal kapcsolatos értékelése rendszeres éves teendő.		
A rendszer fejlesztésének életciklusában az információbiztonsági követelmények minden fázisban jelen vannak, már a kezdeményezéstől, vagy az elemzés első fázisától.		
Az információbiztonsági programot legalább évente felülvizsgálják és szükség esetén módosításra kerül, ahol szükséges.		

2. ábra, Gap analízis meghatározására alkalmas táblázat minta[16]

A vizsgálat mélysége és szélessége is növelhető ezen minta alapján. Hiszen ezen kívül számos kérdésre kell még választ adni egy szervezetben, amelyek más-más területet érintenek, de mégis legalább ennyire fontosak abból a szempontból, hogy: minden folyamat szabályozott legyen, legyen egyértelműen hozzárendelt felelőse. Az alábbi minta dokumentum erre szolgáltat példát, hogy a folyamatok dokumentálása és egyértelmű feladat meghatározások a

[16] How to Complete a Risk Assessment in 5 Days or Less By Thomas R. Peltier, Copyright Taylor & Francis Group, LLC, 2009, Publisher: CRC Press

későbbi visszakereshetőség s a többi, a szabványoknak és ajánlásoknak való megfeleléshez az információbiztonsággal kapcsolatosan is el kell készíteni ezen feljegyzéseket.

Ellenőrzés	Megfelelés (Igen/Nem)	Megjegyzés
A vállalati informatikai biztonsági tisztviselőt (CISO) vagy ezzel egyenértékű vezetői szintű hatóságot kinevezésre került. Felelős a végrehajtásáért és fenntartásért a hatékony, teljes szervezetre érvényes információ védelemi program tekintetében.	Igen	Az információbiztonsági vezető, Tóth Jakab, 2013 július 1-vel munkába állt.
A CISO csapata vagy osztálya külön munkaköri feladataihoz hozzá van rendelve az információ biztonsági program a teljes szervezetre vonatkozólag, beleértve a védelmi igazgatás, a tudatosság és a képzés, az ezek és a program kutatás – fejlesztése és az incidens vizsgálatok is.	Igen	Az információbiztonsági küldetésnyilatkozat, dokumentum és szabályzat 2013. október 1-vel lépett hatályba és került kihirdetésre.

3. ábra, Gap analízis, a teljesítés folyamata.[17]

Az információbiztonsági programra vonatkozó lehetséges minta ellenőrzési táblázat látható az alábbi táblázatban megadva.

Információbiztonsági szabályzat	A felső vezetés irányultsága és támogatása az információbiztonsági program vonatkozásában egyértelműen megalapozott.	I…….. N……..

[17] How to Complete a Risk Assessment in 5 Days or Less, By Thomas R. Peltier, Copyright Taylor & Francis Group, LLC 2009, Table 5.4: Gap Analysis Example 1 Completion Process

Információbiztonsági szabályzat dokumentáció	Van-e a felső vezetés által jóváhagyott információbiztonsági program?	I…….. N……..
	Be van-e vezetve, végre van-e hajtva az információbiztonsági program?	I…….. N……..
	Az információbiztonsági szabályzatot megfelelően és kommunikálták-e minden alkalmazott felé?	I…….. N……..
Az információbiztonsági program felülvizsgálata	Az információbiztonsági program hozzá / egyértelműen össze van-e rendelve annak tulajdonosával?	I…….. N……..
	Létre van-e hozva / definiálva van-e a szabályzat felülvizsgálati folyamata?	I…….. N……..

4. ábra, Gap analízis, biztonsági szabályzat létrehozása, ellenőrzése (életciklus)

Mindezen ellenőrzési lehetőségek, kontrollpontok és a rájuk adott válaszok segíthetnek abban, hogy valós és mérhető képet alakítsunk ki a szervezet aktuális állapotáról. Ez lehet az a stabil alap, amely nagyrészt már definiálja is a rögzített kiindulási pontok tekintetében az útvonalat az ideális, de legalább a megcélzott állapot felé. Egyes ellenőrzési kérdésekhez akár súlyozott mértékben pontokat tudunk rendelni. Ezen pontszámokat, azok összességét skálához rendelve összehasonlíthatóvá válik a szervezeten belüli folyamatok, részegységek viszonya és eltérése. Továbbá a periodikus felülvizsgálatok által kimutathatóvá válik a változás, a fejlődés is. A

fentiekben bemutatott táblázatok terjedelemben és tartalomban is jelentősen egyszerűsített mintaként kerültek bemutatásra. [18]

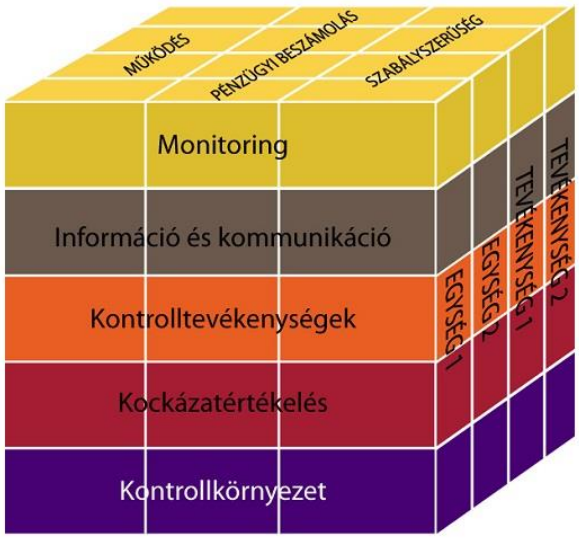
2 Szervezeti vagy ERM módszerek és technikák arra, hogy integráljuk az információs biztonság kockázatkezelését.

Az Enterprise Risk Management módszerek, azaz a nagyvállalati kockázatkezelés jellemzően valamilyen keretrendszer alapján működik, amelyet többé-kevésbé az adott szervezetre szabva kis mértékben módosítanak. Az egyik ilyen lehetséges, széles körben használt megoldás a COSO[19] amely teljes körű megoldásként értelmezhető. Vizualizálására leggyakrabban egy kockát használnak, amely választ ad a Miért, Ki, Mit és Hogyan kérdésekre. A kontrollfolyamatokat, azok viszonyát a szervezeti célokhoz, valamint a célok eléréséhez rendelt felelősöket is képes egyetlen komplex rendszerbe összerendelni. A rendszerellenőrzés – a COSO modell mentén – felfogható úgy, mint a belső kontrollrendszer egyes elemeinek vizsgálata a szervezet egészére vagy egyes szervezeti egységeire vonatkozóan, a törvényi megfelelés, a működési hatékonyság és a pénzügyi megfelelés szempontjából. Természetesen a folyamatok tervezése ettől eltérő is lehet, az adott projekt folyamataiba és minden egyes folyamatába beépíthető a kockázatkezelés, akár csak a beszállítók értékelése. Ennek eldöntése a szervezeti méret és a szervezet döntésének a kérdése. A közszféra számára is létezik már számos ajánlást, irányelveket megfogalmazó dokumentum a belső kontroll folyamatok vonatkozásában.[20]

A COSO módszertannal kapcsolatosan jelentős szakirodalom áll rendelkezésre. A módszer nem csak az információbiztonság, hanem ennél jóval szélesebb körben elterjedt a

[18] A 77 / 2013 NFM rendelet http://njt.hu/cgi_bin/njt_doc.cgi?docid=165667.254105 mellékleteiben megadott táblázatok is jól felhasználhatóak a mélység és szélesség tekintetében is a felmérések elvégzésére.
[19] Commite of Sponsoring Organisation of the Treadway Commission) – modell
[20] Irányelvek a belső kontroll standardokhoz a közszférában. A legfőbb ellenőrzési intézmények nemzetközi standardjai (ISSAI); kiadja a legfőbb ellenőrzési intézmények nemzetközi szakmai szervezete (INTOSAI). További információ: www.issai.org, Letölthető: http://www.asz.hu/modszertan/iranyelvek-a-belso-kontroll-standardokhoz-a-kozszferaban-intosai-gov-9100/issai-9100.pdf

nagyvállalati környezetben. [21] Az alábbi ábrán egy mintát láthatunk a COSO kocka vizuális reprezentálására.[22]



5. ábra COSO kocka [23] [24]

A kockázatkezelési módszerek az adott szervezet függvényében minden logikai, fizikai és adminisztratív tényező ki kell, hogy terjedjenek. Például:

- konfigurációkezelés
- üzletmenet (ügymenet) folytonosság tervezése
- karbantartás
- adathordozók védelme
- azonosítás, hitelesítés

[21] Moeller, Robert R.: "Chapter 4 - COSO ERM Framework".COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance, Second Edition. John Wiley & Sons. © 2011. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=44326>
[22] Ivanyos János: A vállalati kockázatkezelés (2013) http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e3_kockazatmenedzsment_scorm/coso_belso_kontroll_IyzpDEu6yLwJHA1g.html
[23]Ivanyos János: A vállalati kockázatkezelés, 2013, http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e3_kockazatmenedzsment_scorm/coso_belso_kontroll_IyzpDEu6yLwJHA1g.html
[24] Moeller, Robert R.. COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance, Second Edition. John Wiley & Sons. 2011. ("Chapter 4 - COSO ERM Framework".)

- hozzáférés ellenőrzés
- rendszer- és információsértetlenség
- naplózás és elszámoltathatóság
- rendszer és kommunikációvédelem
- reagálás biztonsági eseményekre
- rendszer és szolgáltatás beszerzés.

Amelyek természetesen további, részletes kifejtését az adott szervezet profiljához, használati környezethez kell igazítani.

Kiemelt fontosságú, hogy az eseménykezelő rendszerek:

- egyrészt rögzítsenek mindent (minél több) eseményt,
- minél részletesebben kerüljenek rögzítésre az események
- az események kerüljenek minél gyorsabban feldolgozásra
- az események minél hosszabb ideig legyenek letárolva.

Azonban ki kell tudni választani, lehetőleg minél automatizáltabb módon azokat az eseményeket, információkat, amelyek tényleg annyira fontosak, hogy valóban gépi feldolgozásuk, hosszú idejű letárolásuk szükséges, vagy akár kézi vizsgálat alá kell venni. Tehát minél több esemény kerüljön automatikus feldolgozásra. Ellenkező esetben a kézi vizsgálat alá javasolt események nagy száma miatt:

- lassú lehet a reakcióidő,
- fontos, lényeges információk sikkadhatnak el a nagy tömegű adathalmazban,
- észrevétlen maradhat lényeges esemény.

Az, hogy mekkora a feldolgozható mennyiségű információ, esemény nem csak a szervezet méretétől és a ráfordítható kapacitástól, hanem a rendszerek konfigurációjától is függ.

Példák eseményekre:

- rendszeresemények, alkalmazások, operációs rendszerek eseménynaplói,
- sikeres / sikertelen belépés,
- többszöri sikertelen belépési kísérlet,
- nyomtatás hálózati nyomtatóra,
- hozzáférés hálózati meghajtóhoz, (sikeres, sikertelen, többszöri)[25]
- távoli bejelentkezés,
- bekapcsolva hagyott erőforrások munkaidőn kívül,
- munkaidőn kívüli aktivitások,
- a szokásostól valamilyen szempontrendszer alapján eltérő tevékenység,
- folyamatos „zaj”,[26]
- jelentések, beszámolók, környezeti események, hírek,
- a céges policy által tiltott forgalom észlelése (tartalom, irány, egyéb szempontból)
- ismeretlen, nem regisztrált eszköz megjelenése a hálózaton,
- egyéb események.

Az eseményt továbbító, fogadó, rögzítő, feldolgozó, elemző rendszer, amely ezeket az elemi eseményeket és összefüggéseket feldolgozni képes, jelentősen csökkentheti az elemzésre fordított emberi időráfordítást. Statisztika készítésre, összefüggések automatikus kimutatására lehet alkalmas. Riasztást, automatikus eseménykezelést, akár egyéb funkciók beállítására is

[25] A rendszerek konfigurációs és a figyelni kívánt események ennél részletesebb is lehet, de teljesen más szempontok is érvényesülhetnek.
[26] Olyan tevékenység, amely valamilyen eszközön vagy eszközökön folyamatosan logókat generál.

alkalmas lehet. Az egyik kiemelt elvárás egy ilyen rendszerrel kapcsolatban, hogy képes legyen a biztonsági szempontból valóban fontos események kiemelésére, amelyeket már valóban kezelni szükséges. Ez a kezelés lehet az, hogy valamilyen új kategória vagy szabály kerül létrehozásra, tehát valamilyen besorolást címkézést kap egy új vagy meglévő esemény, de elképzelhető, hogy ennél nagyobb beavatkozásra is szükség lehet az események összefüggéseit feltárva.

A szervezetben a tevékenységet nagy részét munkavállalók végzik, ők állnak minden egyes folyamat mögött, ezért is különösen fontos a képzésük mind informatikai, mind információbiztonsági, tudatossági szempontból. Kockázati szempontból, miközben megvizsgálásra kerül a szervezetben felismerhető minden folyamat, ki kell választani azokat, amelyeknek különösen nagy jelentősége, kockázata lehet. Ezeket a folyamatokat felismerve, a kezelésükre eljárást kell kidolgozni. Az egyik ilyen különösen nagy kockázattal járó folyamat lehet a munkavállalók belépése – távozása a munkaszervezettől. Vizsgálódásunkat most kizárólag a távozásra, azon belül is a kulcsember pozíciók vizsgálatára korlátozzuk. A megfelelően feltérképezett és dokumentált folyamatok döntően erre is megoldást kínálnak. Ehhez érdemes hozzávenni a kiemelt jogosultságú felhasználók tevékenységének valamilyen részletesebb rögzítését. Valamint a hozzáférések jelszószéfben vagy más megoldással történő tárolását, amely alkalmas arra, hogy távozás esetén azok gyorsan hozzáférhetőek és cserélhetők legyenek. A kulcsember pozíciók kialakulásának és az ebből fakadó kockázatok kialakulásának lehetőségét csökkentik, ha létezik jól működő vállalatirányítási rendszer[27], feltérképezettek és jól dokumentáltak a folyamatok, a kockázatkezelési tervben számolnak az ehhez kapcsolódó veszélyekkel, valamint a szervezeti folyamatok átláthatóak. Kulcsember pozíció több területen is keletkezhet, felsorolásszerűen az okok és lehetséges következmények:

- egyedül rendelkezik valamilyen ismerettel (folyamat, eljárás; nem dokumentált a folyamat, vagy nem elég részletesen)
- ezen tudás olyan szakismeret, amely túl bonyolult az átadáshoz, azaz magas szakmai végzettséget igényel
- pozícióból, beosztásból fakadóan (hiányzó kontrollok, nem visszakövethető döntésmechanizmus, nem kiszámítható belső működés, s a többi)

[27] ERP

- fizikai vagy logikai hozzáférésből fakadóan: a fizikai hozzáférés kulcskérdés az információs rendszerek esetén. A pozícióból, beosztásból fakadó kiemelt jogosultságok mindig kockázatot jelentenek. Javasolt a kiemelt felhasználók megfelelő monitoringja és csak a szükséges mértékű hozzáférés biztosítása.

Számos más tényező is vezethet kulcsember pozíciók kialakulásához. Egy ilyen kialakult helyzetnek több szempontból is van kockázata. A dokumentálatlan szervezeti tudás reprodukciója költségigényes lehet, konkurenciához kerülhet, s a többi. Az adott folyamat dokumentálatlanság révén olyan rés[28] alakul ki, amelyben nincsenek jelen a kontrollok, annak változására, és minőségére nincs objektív rálátás. Ennek következtében a változáskezelés sem valósulhat meg, vagy esetlegessé válhat. Nem visszakereshető és nem reprodukálható a döntési folyamat. Lehetséges példák:

- informatikai osztály dolgozói, akik adott területen, funkciók és rendszerek fölött teljes hozzáféréssel rendelkeznek,
- a saját területén egyedi végzettséggel és tudással rendelkező kolléga, aki egyedül, egy személyben látja el a funkciót,
- szervezeti vezetői pozíciók,
- beszállítók, akik egyedi szolgáltatást nyújtanak, egyedi rendszert fejlesztenek,
- egyéb.

Általános törekvés kell, hogy legyen a dokumentálás, a folyamtokba épített kontrollpontokon keresztül a változások kezelése, a kulcsember pozíciókból fakadó kockázatok minimalizálása. Csak arra lehet felkészülni, amiről tudunk, ha már tisztában vagyunk (beláttuk a valószínűségét) az ebből fakadó kockázatokkal, akkor megtettük az első lépést a kezelés érdekében.

[28] Gap, nem szabályozott, nem kezelt terület.

3 Kockázat figyelési technikák és hogyan integráljuk az incidenskezelési technikákkal.

A kockázat figyelési technikákra számos technikai válasz, megoldás létezik.[29] Alapvetően ezen technikák például arra alkalmasak, hogy a nagy tömegű eseményt redukálják és a valódi incidensgyanús eseményekre hívják fel a figyelmet. Illetve az események számának csökkentésével és rangsorolásával segítséget nyújt, hogy jusson megfelelő mennyiségű humánerőforrás azok átnézésére. Ez a mielőbbi beavatkozás érdekében praktikusan közel valós időben kell, hogy megvalósuljon. Az általános információgyűjtés révén hatékonyan lehet érzékelni a normál működéstől történő eltéréseket. A fentiekre alkalmas például egy SIEM[30] rendszer, amelynek célja a szoftver és hardver eszközök által generált riportok, riasztások, figyelmeztetések naplózása, analízise. A szakirodalomban megjelenik a SIM[31] és SEM[32] rövidítések is, amiket össze szoktak keverni a SIEM-mel, mivel hasonló[33] célokra használják ezeket is. A SIEM és hozzá hasonló rendszerek célja, hogy az eseményeket központilag tárolják el és elemezzék ki, ezáltal biztosítva azt, hogy a biztonságot veszélyeztető események, tevékenységek felfedezésre kerüljenek. További technikai eszközök támogathatják az emberi erőforrást, ezek alapját azonban erős kontrollok és szabályozott folyamatok kell, hogy képezzék. Logikai, szabályzat szinten szükséges elsősorban definiálni, hogy adott esemény bekövetkeztekor mi a teendő és az kinek a felelőssége. Tehát az incidens menedzsment folyamat választ kell, hogy adjon arra, hogy mit kell csinálni eseményvezérelt környezetben. Ezen riasztás aktiválódása esetén pedig (például az incidens menedzsmentnek, vagy) valamilyen válaszreakciónak el kell indulnia. Természetesen számos további folyamattal kell összhangban lenni, ilyenek lehetnek az üzletmenet folytonossági terv[34], vagy a katasztrófa helyreállítási terv[35]. Ezek és természetesen további folyamatok összessége és összhangja képes hatékonyan támogatni az incidenskezelést a folyamatok és technikai eszközök segítségével. A SIEM rendszerrel kapcsolatos stratégiával kapcsolatban és az audit megfelelőségről a SANS oldalain[36] bővebb információ található.

[29] Meg kell jegyezni, hogy mindennek az alapját a szabályozott, kidolgozott tervszerű működési elvek kell, hogy jelentsék.
[30] Security Information And Event Manager
[31] Security Information Manager
[32] Security Event Manager
[33] A SIEM gyakorlatilag a két szoftver típus ötvözése, jellemzően nem is szokták külön-külön alkalmazni már őket
[34] BCP: business continuity plan
[35] DRP: disaster recovery plan
[36] http://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528

3.1 Kulcsfontosságú ellenőrzések felügyelete

Az események szempontjából 7 dimenziót szokás vizsgálni, úgyis lehet fogalmazni, hogy ezekre a kérdésekre választ kell, hogy tudjon adni egy SIEM vagy más log gyűjtő rendszer.

- WHEN - Mikor történt az esemény
- WHO – Ki az aki az eseményt kiváltotta?
- WHAT – Mi az esemény (mit csinál?)
- WHERE – Melyik eszközön, gépen történt az esemény
- ON WHAT – Megadja, hogy melyik gépen, fájlon, s a többi történt az esemény.
- WHERE FROM – Honnan került kiváltásra az esemény?
- WHERE TO – Hová ment az esemény

Ez alapfunkciónak tekinthető, hiszen a logok normalizálásán túl, bizonyos események összekapcsolására is képes lehet, ezek már szoftveres, funkcionális, beállítási kérdések.

A szervezet működésének szempontjából vannak kiemelt jelentőségű tényezők, adatok, szolgáltatások. Ezekre vonatkozó működési (BCP, DRP), felügyeleti kérdések (események részletesebb rögzítése, elemzése, visszakereshetősége) jellemzően nagyobb súllyal kerülhetnek feldolgozásra. Az üzletmenet, vagy működőképesség fenntartásához elengedhetetlenül szükséges szoftver / hardver elemek mentése, eseményeinek rögzítése, s a többi az ezekkel kapcsolatos tényezőkhöz jellemzően több tekintetből is nagyobb erőforrásokat szoktak allokálni. Külön ellenőrzésre szolgáló folyamatokat is lehetséges ezekhez definiálni. Fontos kiemelni, hogy az események nagy száma, a napi rutin, a nem hatékony folyamatok, a szokásjog kialakulása és egyéb tényezők, oda vezethetnek, hogy ezen tevékenység olyan rutinná válik, amely nem kapja meg a kellő figyelmet, vagy erőforrást. Információs rendszereinkhez számos felhasználó fér hozzá folyamatosan. Ezen felhasználók csoportosítása jogosultsági szint tekintetében jelentősen eltérhet, azonban a munkájához szükséges adatok fölött jellemzően adminisztrátori jogosultsággal rendelkezik. A kiemelt hozzáférésekkel rendelkező felhasználók azonban több, vagy az összes adatcsoport fölött rendelkezhetnek kiemelt jogosultsággal. Ezen tevékenység figyelése, az események rögzítése

épp ezért kiemelt jelentőségű. Megfontolásra érdemes cél lehet az, hogy a kiemelt jogosultsággal rendelkező felhasználók tevékenysége akár automatikusan megakadályozásra kerüljön vagy a későbbiekben visszajátszható, részletekbe menően visszakereshető, értelmezhető legyen.

Az adatok, a rögzített események tárolásának időintervallumára számos ajánlás létezik. A pro és kontra érvek a minél hosszabb, a lehető legtovább történő tárolás és az erőforrások például tárhely kapacitás rendelkezésre állása. Ilyen jellegű döntéseknél azt érdemes mérlegelni, hogy mi az az intervallum, amelyen belüli esemény (például egy adatszivárgást indító esemény) észrevétlen maradhat és lényeges lehet az eredeti kiindulási állapotra történő visszaálláshoz a kezdeti esemény időpontjának felderítése.[37]

3.2 Fizikai és műszaki felügyeleti technikáknak megfontolása

A felügyeleti technikák és eszközök jelentősen képesek csökkenteni a humánerőforrás szükségességét. Azonban egy ilyen rendszer beüzemelésére úgymond betanítására, a betanítási folyamatra, ennek jellemzően a fordítottja igaz.

Az alábbiakban bemutatott táblázat, nagy segítség, a kiválasztás alapja lehet az egyes megoldásszállítók tekintetében. Azaz tisztában kell lennünk a szervezet funkció és kapacitás igényeivel egy erre irányuló vizsgálat eredményeképpen, például: a keletkező eseménymennyiség, annak feldolgozására vonatkozó igények (valós, késleltetett) a keletkező adatok tárolásának igénye. Fel kell készülni rá, hogy ezen adatmennyiség eseményvezérelt környezetben és időben jellemzően növekvő tendenciát mutat. Valamint érdemes 1-5 évre előre tervezni. Mindezen mérlegelési és kiválasztási szempontok a szervezet és a rendelkezésre álló források tekintetében jelentősen eltérőek is lehetnek.

3.3 Felügyeleti megközelítések (mit kell ellenőrizni)

A mit kell ellenőrizni kérdésre adott választ sokkal inkább azon tényezők befolyásolják, hogy meddig és milyen részletességgel képes tárolni (vagy meddig tárolhatja) a szervezet az adatokat, eseménynaplókat.

[37] Az események rögzítése, figyelése kapcsán olyan tényezőkre is gondolni kell, mint a kártyás, biometrikus egyéb elektronikusan rögzíthető belépések. A CCTV – zárt láncú videó megfigyelő, rögzítő rendszerek által felvett hang és képanyagra, s a többi. Mindezen információk tárolására is ki kell, hogy terjedjen a szabályzat és a felügyelet.

Jelen jegyzetben is részletezett kockázat felmérési táblázatok hosszúsága és változatai variánsa szinte végtelen. Egyik szakirodalom 5 fő kategóriára osztja a fenyegetéseket egy 426 elemű[38] checklista alapján.

- Vis major kategória: 15 db.
- Szervezési hiányosságok kategória: 101 db.
- Emberi hiba kategória: 76 db.
- Műszaki fenyegetés kategória: 52 db.
- Szándékos cselekmények kategória: 126 db.

Az alábbi bemutatásra kerülő minta táblázat előtt fontos megjegyezni, hogy szervezetenként ettől jelentősen eltérő is lehet, ez az adott szervezet, annak profiljai, területi elhelyezkedése, s a többi számtalan tényező befolyásolhatja.

Fenyegetés		***Alkalmazandó (Igen/Nem)***
Integritás		
Az adatfolyam lehet elfogtak, lehallgatták.		
Hibás programozás révén (véletlenül) módosultak az adatokat.		
Írott vagy elektronikus készített beszámolókhoz férhettek hozzá illetéktelen személyek nem szándékosan.		
Adatokat lehet beírni helytelenül, adatbevitel ellenőrzésének kérdése.		
Szándékosan helytelen adatbevitel.		
Elavult programok használata veszélyeztetné az információk integritása.		
Hibás hardver eredményezhet pontatlan adatbevitelt és elemzést.		

[38] IT-Grundschutz, http://www.bsi.de/English/gshb/index.htm

A harmadik fel módosíthatja az adatokat.		
Fájlok véletlenül törlésre kerülhetnek.		
Hackerek megváltoztathatták az adatokat.		
A belső felhasználók el tudnak indítani jogosulatlanul programokat, hozzáférni és módosítani banki adatokat.		
A jelentések hamisak, hamisítottak lehetnek.		
Belső lopás következtében megszerzett információkat alkalmazottak módosíthatják és később felhasználhatják.		
Hálózat lehallgatás révén elfoghatnak felhasználóneveket és jelszavakat és ez lehetővé teszi a jogosulatlan módosítását információnak.		
Az információ elavult lehet.		
Hackerek juthattak jogosulatlan hozzáféréshez a hálózaton és rendszer erőforrásokat kompromittáltak.		
Fizikai behatolás illetéktelen személyek által.		
Hamisított dokumentumok jelennek meg, amik hivatalos vállalati dokumentumnak tűnnek.		
Jogosulatlan vagy fiktív értékesítési művelet kerülhet jóváhagyásra.		
Információt lehet félreértelmezni nyelvi korlátok miatt.		
Csaló programozási eszközökkel lehet az adatok integritását veszélyeztetni, például rejtett vagy megtévesztő tartalommal.		
A számítógépes vírusok módosíthatják az adatokat.		
Információ lehet rosszul irányított.		

Tranzakciók lehet, hogy szándékosan nem futnak le , vagy eltérítésre kerülnek.		
Az újabb vagy frissített szoftver okozhat a dokumentumok vagy fájlok esetében lehetőséget a visszaélésre.		
Nem szabványos eljárásokat okozhatják információk téves értelmezését.		
Illetéktelen személyek használhatják a felügyelet nélkül hagyott munkaállomásokat.		
Tájékoztatás során és harmadik féltől nem megfelelő, korrupt adatok érkeznek.		
Fiók, hozzáférési információt meg lehet osztani.		
Egy áramszünet okozhatott korrupt, sérült információkat.		
Információ lehet benyújtani, továbbítani, bevinni homályos vagy félrevezető módon.		
Valaki képes megszemélyesíteni egy ügyfelet, a nyilvántartást meghamisítani (személyazonosság-lopás).		
Információkat lehet elhelyezni a vállalaton kívül.		
Információk integritása veszélybe kerülhet az adathordozó média miatt.		
Valaki megszemélyesíteni a munkavállalót korrupt információk felhasználásával.		
Az elbocsátott alkalmazottja képes szándékosan hibás adatokkal visszaélni.		
A szervezet célpontja lehet egy hackernek vagy elégedetlen ügyfélnek.		

Az alapértelmezett felhasználónévvel és jelszóval elérhető hálózati meghajtó. Ez felhasználható lehet a rendszer erőforrásait történő hozzáféréshez.		
Titoktartás, titkosság.		
Nem biztonságos e-mail tartalmazhat bizalmas információkat.		
Belső információlopás.		
Egy dolgozó nem képes ellenőrizni a személyazonosságát az ügyfélnek, például a telefon álcázás, megtévesztés.		
Bizalmas információ marad az asztalon elolvasható, leleshető módon.		
Társasági beszélgetések, társadalmi viták az irodán kívül vezethet érzékeny információk kitudódásához.		
Információ nyerhető vissza illetéktelen személyek által szemetes vagy más gyűjtőhelyekről.		
Harmadik félnek küldött információkkal lehet visszaélni.		
Felügyelet nélküli számítógép adhat lehetőséget jogosulatlan hozzáférésre a fájlokhoz.		
Nem szükséges jelszó minden munkaállomáshoz.		
Két vagy több különböző vevői nyilatkozatok / szerződés / dokumentumok egy borítékban / levélben.		
Jogosulatlan emberek bizalmas vagy korlátozott területeken lehetnek.		
A bizalmas információkat lehetnek, vagy maradhatnak a faxon vagy fénymásolón, lehetőséget adva a jogosulatlan megtekintésére a dokumentumoknak.		
Megtévesztő vagy hamis személyek		

telefonbeszélgetésekben.		
Válasz fax küldése ellenőrzés nélkül.		
Dokumentum került kiküldésre, azonosítással kapcsolatos információkkal, amely aztán visszapattant.		
Jogosulatlan hozzáférés az információhoz és dokumentumok munkavállaló mögül lelesve. (váll szörfözés - információ lelesés).		
Dokumentumokat lehet túlzottan duplikáltak.		
A munkavállalók megoszthatják a jelszavakat.		
Belső üzenetküldők kezelhetnek (kerülhetnek hozzá) bizalmas információkat.		
Munkavállalói és chat kapcsolatok által kicserélődhetnek kényes vagy bizalmas információk.		
Jogosulatlan adatközlést harmadik fél által.		
Nem megfelelő megsemmisítése elektronikus médiáknak, adathordozóknak. Maradhatnak médiákon visszanyerhető információk illetéktelen személyek által.		
A nem megfelelő tűzfal konfigurációt által véletlen információközlés.		
Aktuális ügyfél-információt fel lehet használni a sablonnak érzékeny információk megszerzéséhez.		
A munkavállalók megvitatják a bizalmas információkat az irodán kívül.		
Dokumentumokat kerülhetnek véletlen kézbesítés miatt rossz emberhez.		
Tartani a telefonbeszélgetést addig, amíg nem tudta ellenőrizni személyazonosságot.		

Társaságot ki lehet téve az elektronikus lehallgatásnak.		
Elbocsátott munkavállaló képes lehet elérni az épület vagy belső információkat.		
Takarító személyzet láthatja a bizalmas információkat.		
Szemetesek is tartalmazhatnak bizalmas információkat.		
Az alkalmazottak nem követi a kettős ellenőrzési eljárásokat.		
Ideiglenes vagy az új alkalmazottak nem eléggé képzettek.		
Korlátozott vagy tiltott területeket is elérhetnek a látogatók.		
A telefon, vagy a kihangosított telefon sértheti a titoktartást, információbizalmasságot.		
Információs és fájlokat lehet, hogy indokolatlanul is elérhetők a vállalati rendszerekben.		
A másodlagos site-on tárolt adatok veszélybe kerülhetnek, kompromittálódhatnak.		
A munkavállalók telepíthetnek illegális vagy nem jóváhagyott szoftvereket.		
Tanácsadók vagy egyéb szerződéses segítők, partnerek megtekinthetnek (megláthatnak) a bizalmas információkat.		
Elérhetőség		
A tárolt állományok személyes mappákban / gépen vannak és nem elérhetőek más alkalmazottak által, amikor szükséges.		
Hardver hibák hatással lehetnek a vállalati erőforrások rendelkezésre állására.		

A hiba esetén adatokhoz való hálózati hozzáférés is tiltásra kerül.		
„Cselekedeti kód:" tornádó, szökőár, hurrikán.		
Frissítések következtében a szoftver megakadályozhatja a hozzáférést.		
A céges rendszer elérhetetlenné válik vagy lekapcsol.		
Evés és ivás egy munkaállomáson közelében okozhat billentyűzet / beviteli hibát.		
Egy biztonságos, biztosított munkaterület veszélyeztetheti / kockáztathatja a bizalmas ügyfél-információkat.		
Az áramszünet létrejöhet valamilyen munkavállalói hozzáférés által.		
Szoftverfrissítések befolyásolhatnak más programokat.		
Lejárt felhasználói hozzáférés és / vagy nem megfelelő alkalmazotti képzés képes a számítógépes rendszer megzavarására.		
A rendelkezésre álló számítógépek megosztottak, közös használatban vannak több, nem hozzáértő felhasználó között.		
A beszállító vagy supportot biztosító személyzete nem elérhető vagy függ például időzóna eltérésektől.		
A kommunikációs hiba megzavarhatja a normál szervezeti, üzleti tevékenységet.		
Az alkalmazottak nem helyénvaló vagy nem megfelelő fájl hozzáféréssel rendelkezhet.		
Ha valaki ki (beteg / hiányzik / szabadságon / nem az irodában van) bizonyos kritikus fájlok nem érhető el, vagy nem hozzáférhetőek.		

A kérdések, amelyeket a harmadik fél által biztosított támogató szolgálathoz intéznek, amellyel próbálják megoldani a problémákat; oda vezethetnek, hogy eközben bizalmas információk kerülnek közlésre, hozzáférés adódik ezekhez.		
Egy hiányzó személy vagy eszköz akadályt jelenthet, ha nem áll rendelkezésre.		
A szervezet ki lehet téve bombák vagy bármilyen más terrorcselekmények általi fenyegetésnek.		
Berendezés vagy egyéb információ lopás.		
Elégtelen, nem megfelelő kereszt képzések a kritikus eljárásokban. Amely hatással lehet az üzleti folyamatokra.		
A rendelkezésre álló információs források (kontrollálása) által harmadik fél hatással lehet az üzleti folyamatokat.		
A sérült vagy megváltozott storage vagy hardver média.		
Nem minden munkaállomáson töltődnek be a programok, vagy nem minden program.		
A felhasználók elveszíthetik vagy rosszhelyre tehetik az állományaikat.		
A jelenlegi környezetben fennáll annak a kockázata, ember alkotta fenyegetéseknek kockázatot jelentenek.		
Földrajzi távolság és beszerzendő anyagok nagy távolsága.		
Vandalizmus és szabotázs kísérletet a hálózaton.		
Szoftverlicencek száma lehet, hogy nem elegendő.		
Az elégtelen személyi erőforrások hatással lehetnek		

az üzleti folyamatokra.		
Egy számítógépes vírust be lehet hozni e-mailben vagy a más adathordozón.		
Szolgáltatás megtagadásos támadások rosszindulatú internet felhasználóktól a szervezeten kívülről.		
Munkavállalói okokból kifolyólag ideiglenesen nem elérhető valamilyen dokumentum, átmeneti emberi mulasztás következtében.		
Természeti fenyegetés		
Elektromos vihar		
Jégvihar		
Hóvihar		
Jelentős földcsuszamlás		
Földcsuszamlás		
Cunami		
Tornádó		
Hurrikán / tájfun		
Nagy szél (70+ mph)		
Trópusi vihar		
Árvíz		
Szezonális árvíz		
Helyi árvíz		
Fő gát / tározó hiba		
Homokvihar		
A vulkáni tevékenység		
Földrengés (2-4 a Richter skála)		
Földrengés (5 vagy több, a Richter-skála)		
Járvány		
Emberi – véletlenszerű		
Tűz: Belső-kicsi		
Tűz: Belső-jelentősebb		
Tűz: Belső katasztrofális		

Tűz: külső		
Véletlen robbanás - a helyszínen		
Véletlen robbanás - a másodlagos site-on		
Repülőgép baleset		
Vonat baleset		
Kisiklás		
Auto / kamion baleset helyszínen		
Emberi hiba - karbantartás		
Emberi hiba - működési		
Emberi hiba - programozási		
Emberi hiba - a felhasználók		
Mérgező szennyezés		
Sürgősségi orvosi ügyelet		
Kulcsfontosságú munkatársak elvesztése		
Human - szándékos		
Környezeti		
Teljesítmény fluxus		
Áramszünet - belső		
Áramszünet - külső		
Víz szivárgás / Víz-hiba		
HVAC hiba[39]		
A hőmérséklet nem megfelelő		
Távközlési hiba		
Mérgező szennyezés		

6. ábra: Ellenőrzési lista minta[40]

Ezen közreadott minta alapján az adott szervezetben lehetséges rövidebb, vagy hossza, akár részletesebb felmérési táblázatot is összeállítani. Első lépcsőfokban tehát a felmérés, eljárási

[39] Hűtő, fűtő, szellőztető rendszerek, egyes esetekben a páratartalmat és más tényezőket is szabályozzák ezen ipari berendezések.
[40] Peltier, Thomas R.. "Appendix G - Sample Threat Checklist".How to Complete a Risk Assessment in 5 Days or Less.Auerbach Publications. 2009. Table G.1: Sample Threat Checklist

rend kialakítása, ezeken belül pedig a kontroll megvalósulásának érdekében ellenőrzési, visszacsatolási pontok létrehozása. Eltérő mértékben, de szervezet minden folyamatába és területén meg kell, hogy jelenjen az információbiztonsági megfelelőség érdekében a kontroll. Ennek belátásához elegendő azt végiggondolni, hogy jellemzően nincs a munkaszervezetekben független, semmilyen más eljárással össze nem függő folyamat. Ennél fogva, mivel köztük kapcsolat van, befolyásolni képes a másikat. Az így kifejtett hatás révén pedig képes csökkenteni az információbiztonsági szintet.

4 A kockázatkezelési program fejlesztése

A kezdeti lépések voltaképpen nem a program kidolgozásával kezdődnek. A program hatékony kidolgozásához, pontosabban a hatékony program kidolgozáshoz számtalan tényezőt érdemes figyelembe venni, ahhoz, hogy a program valóban jól működjön az adott szervezetben.[41] Az aktuális helyzet felmérése és a menedzsment elkötelezettségét követően a kommunikáció legalább ennyire fontos tényező a program hatékonyságához.

A kezdeti lépéseknek tartalmaznia kell a kidolgozáshoz:

- a program hátterét és céljait,
- a hatályát, alapszabályát és engedélyeit,
- a végrehajtási csoportot.

4.1 A program hátterének és céljainak megalapozás

Minden szervezetnek folyamatosan szembe kell néznie különböző kockázatokkal és folyamatosan foglalkoznia kell velük akár formálisan, akár alkalmanként, bizonyos esetekben akár figyelmen kívül hagyva azokat. Tehát az is lehet egy kockázat kezelési stratégia, hogy az adott kockázati szint, vagy a várható veszteség elfogadható, vagy a kockázat csökkentésének költsége nagyobb, mint a kockázat bekövetkeztekor felmerülő (helyreállítási és egyéb) költségek. Az információ biztonsági kockázatok kezelése kisebb – nagyobb mértékben általában az információ biztonsági vezető feladata. Az elsődleges feladat[42] a szervezet kockázatkezelési stratégiájának, egész pontosan s program céljainak a meghatározása, különös tekintettel kitérve a kívánt eredmények és célkitűzések tisztázására,

[41] Lásd a fenyegetettségek feltérképezését célzó táblázatok.
[42] Az aktuális helyzet felmérését követően.

definiálására. A stratégia kidolgozását követően a rövid és középtávú célok kijelölésére alkalmas a kockázatkezelési program kidolgozása. Lehetséges, hogy a programot egy korlátozott hatásra vagy célra kell kidolgozni, figyelve arra, hogy a környezet (szervezeti, jogi, szabályozási) követelményeknek megfeleljen. Elképzelhető olyan eset, hogy valamely kockázati tényező akkora súllyal, befolyással bír, hogy a terv első verziója mindössze ennek az egynek a befolyásolását tűzi ki célul. Amennyiben nem jön létre formálisan ilyen szabályozás vagy program, akkor elképzelhető, hogy a programot tágabban értelmezve, a felelősség is több szervezeti egység között kerüljön megosztásra. A biztonsági stratégia meghatározásának elsődleges feladata, a szervezet, folyamatok, projekt vagy tevékenység, hatókör és a megalapozott közép és hosszú távú célok definiálása. A hatékony programnak lényeges eleme annak meghatározása, hogy mekkora a szervezet elfogadott kockázat tolerancia szintje, vagy kockázati étvágya, mi a menedzsment által elfogadott kockázati szint. Minden szervezetben különböző kockázatot és kockázati szintet tekintenek elfogadhatónak és ez valószínűleg szervezeten belül az egyes részlegek, szervezeti egységek tekintetében is eltérő. Ennek felmérése, dokumentálása a szervezeti folyamatok áttekintésekor meg kell, hogy valósuljon, hiszen ekkor az információbiztonsági vezető kapcsolatba kell, hogy lépjen minden szervezeti egységvezetővel. Az, hogy az adott egység, adott folyamata milyen kockázattűréssel rendelkezik általában üzleti döntés, nem mindig kvantitatív értékeken alapul.[43] Fontos megemlíteni, hogy ilyenkor sokszor születik olyan válasz, hogy nem engedhető meg egyetlen másodperc kiesés sem éves szinten. Ilyen esetben ezen, kritériumhoz alkalmazkodva be kell áraztatni az illetékes egységekkel (IT, üzemeltetés, épületüzemeltetés, s a többi) ennek költségvonzatát. Előfordulhat, hogy az így előterjesztett információk mentén nagyobb lesz az érintettek hibatűrése, vagy megnő az üzemszerű működés helyreállítására fordítható időablak.

Jellemzően a felső vezetés adja meg a kockázatkezelési program alaphangját a stratégia és program hivatalos elfogadásával, támogatásával. Ez az alapvonal fontos eleme a felső vezetés felelősségvállalásának az irányításban. A szakirodalom szerint, mint minden más szempontból a felülről lefelé történő megközelítés lényegesen hatékonyabb, mint az alulról felfelé történő megközelítés, ahol alacsonyabb szintű vezetők kísérlik meg befolyásolni a szervezetet. Hiszen a munkavállalóknak általában a felsővezetők határozzák meg, mi az kérdés, feladat, ami magasabb prioritást érdemel. Fontos megjegyezni azonban, hogy a program sikeressége érdekében alacsonyabb vezetői elköteleződés mellett számos

[43] Bár a BCP és DRP esetén jól meghatározhatóak ezen időintervallumok, hogy mit tolerál a szervezet vagy adott egység.

egyéb lehetőség adódig. A már említett kommunikáció nem csak a meglévő csatornákon gyakoribb kommunikációt jelent, hanem meg kell találni azokat a formákat is, amelyek rendelkezésre állnak a munkaszervezetben, de még nem kerültek kihasználásra, vagy akár újszerű eszközöket is be lehet vezetni. További lehetőség mintacsoportok létrehozása középvezetők vagy alsóbb szintű vezetők segítségével, minta tréningek tartása, vagy véleményvezérek érintettségének növelése a programban. Kooperációban megvalósulhat olyan oktatás tartása, amelynek csak valamelyik modulja, egy része fókuszál a biztonságra. Ez különösen indokolt abban az esetben, ha bizonyos informatikai vagy ehhez kapcsolódó alapismeretek is fejlesztésre szorulnak. Általánosan vizsgálva, az információbiztonsági program hátterének megteremtéséhez a fentebb felsorolt tényezők többsége szükséges. Az információbiztonsági program létrehozása, a célok és feladatok definiálása és transzparenssé tétele annak érdekében, hogy minden egyes munkavállaló (és partner) tisztában legyen a benne felmerülő feladataival és kötelezettségével, ez a belépő a kockázatkezelési program stabil alapjának megteremtéséhez.

4.2 A kommunikáció szempontjából vizsgálandó tényezők

A sikeresen végrehajtott programhoz, projekthez egyik kulcstényező a projektmarketing, azaz a projekt megfelelő kommunikációja. A projekttulajdonos szempontjából a hangsúly jellemzően arra helyeződik, hogy a megvalósuló eredmény az érintett érdekcsoportok számára elfogadhatóvá váljon. Ez az elfogadás a teljes folyamatra, annak minden szempontból (idő, egyéb erőforrások) igaz kell, hogy legyen. A közreműködők szempontjából a projektmarketing értelmezése: a megfelelő üzleti célok elérésére miként és milyen hatékony marketing eszköztár áll rendelkezésre, melyek alkalmazhatóak a helyi sajátosságoknak megfelelően. Jellemzően az elérendő projektcélban a címzett (vevő vagy végfelhasználó) is kooperáló résztvevő, így fontos, hogy annak teljes folyamatában, minél nagyobb részében résztvevő közreműködő legyen. Ilyen szempontból vizsgálva a kommunikációt támogató marketing nem csak eladja a projektet (programot) az érintett érdekcsoportoknak (belső, külső, érdekeltek, partnerek) hanem a menedzsment érdeke, hogy olyan támogatás vegye körül, amely a program céljait segíti, növeli az egyes érdekcsoportok támogatási hajlandóságát, ezáltal a szükségtelen konfliktusokat csökkenti. Érdekcsoportnak tekinthető minden olyan alkalmi, vagy akár a szervezeti struktúra keretein belül működő egység (közösség) amelynek, ezen csoporton belül azonos vagy közel azonos érdekei vannak az adott projektszakaszban, vagy a projekt egészével, vagy céljaival

kapcsolatban. Ez a megnyilvánulás az előbbi célrendszer vonatkozásában lehet ellenséges vagy támogató, de időben (például: aktuális projektciklus tekintetében) változó is.

Fontos lehet egy olyan lépéssorozat megtervezése, amely hatékonyan képes támogatni a program kivitelezését megfelelő információk megszerzésével. Tehát hatékony és folytonos kommunikációval nem csak a programmal kapcsolatos tudnivalók átadására, a kockázatokra, egyéni felelősségvállalásra, s a többi egyéb tényezőkre lehet felhívni a figyelmet, hanem az érdekcsoportok meghatározása, az általuk képviselt érdekek azonosítására is lehetőség nyílik a visszajelzések alapján. Emlékezve az alapkoncepcióra, hogy a biztonsági program értéket teremt és be kell, hogy épüljön minden folyamatba, így nem is működhet másképp hatékonyan, mint hogy az információbiztonsági vezető megismeri az adott csoport, illetve a szervezet egészének érdekeit. Az érdekcsoportok szervezettségi szintjének megismerése (véleményvezérek, szervezeti vezetők azonosítása), az egyes érdekcsoportok projekttel, a célrendszerrel és a létrehozandó projekteredménnyel kapcsolatban várható magatartásának felmérése, a szervezeten belül alkalmazható marketing eszközök kialakítása mind olyan információk, amelyek a stratégia lokális implementációját támogatni képesek. A részletes információk megszerzése alapján, azt követően elkerülhetőek olyan csapdák, amely akár az egész projekt sikertelenségét vonhatná maga után. Az egyes érdekcsoportok szervezettségi szintjének megismerésén kívül fontos tényező lehet, annak megismerése, hogy ezt tudják-e valamilyen formában vagy csatornán hatékonyan kommunikálni és milyen mértékben képesek érdekeiket érvényesíteni, milyen okokra vezethető vissza és milyen intenzitással nyilvánul meg, ez mind fontos információ. Ezen információk gyakran csak személyes megbeszélések, szóbeli tájékozódás keretében szerezhetőek be. Általánosan elmondható, hogy ezen információk felmérése és az adatok feldolgozását követően van lehetőség olyan kommunikáció kialakítására, amely minden lehetséges érdek kapcsán ad valamekkora lehetőséget az érdekcsoportok befolyásolására, támogatásuk elnyerésére.

Különösen fontos ez akkor, amikor a gyakorlatban valamilyen SIEM rendszer, vagy bármely más a biztonságot technikai eszközökkel támogató rendszer bevezetéséről és fejlesztéséről van szó, hiszen a keletkező információk sok esetben nem tisztán műszaki jellegű értelmezést kívánnak, hanem az adott szakterület tudása is szükséges lehet hozzá. Az adott szakterületen, vagy adott speciális szoftver, hardver komponens által előállított események értelmezéséhez a területen dolgozók tudása is szükséges.

4.3 A kockázatkezelési program hatályát, alapszabályát és engedélyeit tekintve

Mivel minden részleg és működési egység a szervezetben valamilyen szinten felelős a kockázatkezelésért, épp ezért kiemelten fontos jelentőségű, hogy egyértelműen meghatározott legyen a felelősség és a jogkor különösen az információbiztonsági vezető, de az egyéb érdekelt felek vonatkozásában is. A hatály és felelősség vonatkozásában egy olyan ideális állapotig kell eljutni, ahol minden egyes személy tisztában van a saját egyéni felelősségével. Az ennek elérésére irányuló törekvés révén elkerülhetőek a párhuzamos folyamatok, egyes folyamatok közötti rések, továbbá párhuzamos, vagy szükségtelen folyamatok felderítésére, kiküszöbölésére is sor kerülhet.[44] Meg kell jegyezni, hogy mivel az összes információbiztonsági tevékenység kapcsolódik a kockázatkezeléshez, ennek tevékenységi térképe szorosan kapcsolódik a biztonsági vezető feladatköréhez, felelősségéhez. Függetlenül attól, hogy a felelősségnek ez a területe kihez tartozik a szervezet biztonsági menedzsmentjét úgy szükséges meghatározni, hogy a teljes szervezeti kockázatkezelés egészére, átfogó célokat határozzon meg. Amíg több egység feladata lesz a biztonság egyes aspektusainak kezelése, addig az információbiztonság lehetséges fő területei: a fizikai biztonság, az általános kockázat, és a működési, üzemeltetési kockázat kezelése.

Például definiálni szükséges, hogy ki a felelős azért, hogy bizalmas kinyomtatott dokumentumok ne maradhassanak a központi nyomtató (környékén) a megfelelő megsemmisítési eljárás bekövetkezzen (megakadályozva az esetleges papírkosár átvizsgálásából történő visszanyerést is). Esetleg olyan eljárásrendet kell tervezni, amelyben ilyen és ehhez hasonló lehetőségek kizárásra kerülnek. Bár a példa triviálisnak tűnhet, mégis fontos annak érdekében, hogy megértsük az információ biztonság szempontrendszerét. Hiszen a szervezetekben rengeteg metszéspontja van az információ biztonságnak, informatikai biztonság, épület (üzemeltetési) és fizikai biztonság, és egyéb beszállítók által biztosított szolgáltatások tekintetében fontos meghatározni és egyértelműen definiálni:

- eszközök azonosításával osztályozásával és tulajdonosi jogkor meghatározásával,
- a célok meghatározásával,
- módszerek meghatározásával,

[44] A szabályozásban, folyamatokban jelentkező gap, szintén kimutathatóvá válik.

A kockázatkezelési információs biztonsági program fontos pontja kell, hogy legyen a tevékenységek és területek meghatározásán túl az a felelősségi körök egyértelmű kijelölése. A felelősségi körök kijelölésének lebontása meg kell, hogy valósuljon a szervezeti egység szinteken keresztül egészen a munkavállalói, személyes szintig.

5 A kidolgozásért felelős személy vagy csapat (végrehajtási csoport)

Jellemző ajánlás, hogy egy csapat dolgozza, fejlessze ki kockázatkezelési programot. Hiszen a sikeres program integritást igényel, a kockázatkezelés keretében a szervezet minden szintjén és minden folyamatában. Ebbe beletartozik az üzemeltető személyzet, az igazgatósági tagok, s a többi. Ennek a programot kidolgozó bizottságnak a munkáját kell segíteni azzal, hogy azonosítani kell a kockázatokat, meghatározni az elfogadható (jóváhagyott) kockázati szinteket olyan fejlesztési programot kidolgozni, amely az aktuális szintről az elfogadott (vagy tervezett) szint felé vezető utat stratégiailag, és a beavatkozási pontokat is kijelöli. Mivel pedig a kockázatkezelési program szervezeti és üzleti célokat szolgál, így rendkívül fontos, hogy minden releváns egység képviseltesse magát a programbizottságban. Bár említésre került már, de kiemelten fontos, hogy a kidolgozás folyamata egyértelműen folyamat vezérelt és nem technológiai elven kerül meghatározásra. Így ezen a szinten a szakmai csoport nem feltétlenül szükséges, hogy nagy súllyal figyelembe vegye a rendelkezésre álló technikai környezetet.

5.1.1 Szerepek és felelősségek

Az információs biztonsági kockázatmenedzsment szerves része a biztonsági irányításnak és jellemzően ennek vezetője felelős a felső vezetés felé a hatékony erőfeszítések megtételéért, annak megfelelő bemutatásával.[45] Időszakos jelentések segítségével visszajelzést kell adni, annak biztosítása érdekében, hogy a vezetés szándéka hogyan valósul meg a programban. Ez jó alkalom tisztázni a rendelkezésre álló forrásokat, a támogatás formáit, a kockázatkezelési tevékenységet, továbbá lehetőséget biztosít apróbb módosításokra. A jelentés lehet időszakos vagy esemény orientált is. Eseményvezérelt jelentésnél meg kell határozni a jellegét és súlyosságát az eseménynek, amely kiválthatja a jelentést. Írásban el kell fogadtatni a vezetéssel az elfogadható biztonsági szinteket definiáló

[45] A aktuális helyzet rövid, lényegre törő bemutatásán kívül fontos a beárazott döntési alternatívák bemutatása is.

dokumentumot és a kockázatkezelési célokat. A vezetésnek tehát nem csak a fő érintetteket és felelősöket, de a prioritásokat a kockázatkezelési célokat is meg kell határozni (el kell fogadnia) az szervezeti célokat támogató stratégiában. Ezt követően az informatikai biztonsági menedzser felelős a kidolgozásért ebben való együttműködésért, hogy a program elérje a meghatározott célokat. Szintén az információbiztonsági vezető felelős a kapcsolatok fenntartásáért a többi kockázatkezelési fejlesztő csoport között, sőt biztosítania kell program hatékonysága érdekében a program kommunikációját, hatékony koordinációját, az üzleti folyamatokkal való összhangját. Az amerikai National Institute of Science and Technology (NIST) által közzétett SP 800-30 ajánlás ismerteti a legfontosabb szerepeket a kockázatkezelési folyamat résztvevőivel, támogatóival kapcsolatban. [46]

Az információbiztonsági vezető tehát nagyrészt koordinátor olyan értelemben, hogy össze kell fognia a szervezet különböző részeit érintő kockázatok tekintetében azok felelőseit, együtt kell velük működnie és az egyes egységek közötti kommunikációba is be kell kapcsolódnia.

6 Változó környezetek

A kockázat feljegyzésével, értékelésével, kezelésével vaskos szakirodalom foglalkozik, így a fentiekben annak értékteremtő módon történő bemutatására szorítkoztam. Nemzetközi példák mutatják, hogy biztonsági hibákból kifolyólag nemzetközi cégek online reputációja sérülhet akár olyan mértékben is, hogy az adott üzletág, vagy teljes szervezet felszámolásához vezethet. Természetesen hatékony és jól kivitelezett információbiztonsági stratégiák, példák is nagy számban bizonyítják, a küldetés nem lehetetlen. Az elmúlt években, évtizedben jelentős átalakuláson ment keresztül a szervezetek életében az információbiztonság. A változás nagyjából ezt az életutat járta be: helyreállítás: incidensre reagálás, megelőzés:

- detektálás: behatolás detektálás
- biztosítás: sérülékenység analízis, logelemzés
- elkerülés: tűzfalak, PKI, szabályok, eljárások és sztenderdek

[46] NIST 800-30 ajánlása. http://csrc.nist.gov/publications/PubsSPs.html#800-30

Ez azt is jelzi, hogy a szervezetek egyre kisebb időablakot engedhetnek meg maguknak, amikor valamely szolgáltatás nem érhető el, teret nyert az üzletfolytonossági menedzsment.[47] Valamint a biztonsági szakma és szakirodalom, keretrendszer is folyamatos fejlődésen megy keresztül.

6.1 Szakirodalom és rövidítések

Az információbiztonság nemzetközi szinten is gyorsan fejlődik, változik. Ahogy a fentiekben is hivatkoztam rá, bár egyes szavak fordítása itt-ott felüti a fejét, de ez gyakran csak félreértésekre ad okot. Vannak olyan esetek, amikor egész egyszerűen nem érdemes magyarítani bizonyos kifejezéseket. Jelenleg a magyar közigazgatásban még nincs olyan régi hagyománya az információbiztonságnak, így az ezzel kapcsolatos elnevezések, fogalmak még nem egységesek. A helyzetet jól érzékelteti, hogy ahol van is már ilyen szakember, ott sem feltétlenül az ajánlásoknak megfelelően a legfelső szervezeti alá tartozik. Az információbiztonsági vezető, menedzser, CIO kifejezések munkaszervezet függvényében ugyan azt a pozíciót, feladatkört jelölhetik.

6.2 Az irányító testületek és a felső vezetés

A felső vezetés felelőssége a munkaszervezet sztenderdjeihez alakítva, hogy biztosítsa a szükséges forrásokat, valamint hogy ezen erőforrások valóban hatékonyan legyenek felhasználva annak érdekében, hogy a szükséges célokat elérjék a fejleszteni kívánt területeken. Fontos tényező maga a döntéshozatali mechanizmus, így az értékelési, döntéshozatali folyamatot is szerepeltetni kell a kockázatok között, hiszen a hatékony kockázatkezelési program értékelése és a kockázatok csökkentésére igényelt támogatás szempontrendszere igényli a felső vezetés támogatását és bevonását. [48]

Az informatikai vezető (CIO) felelőssége az IT rendszer tervezése, költségvetés és teljesítmény szempontjából. Beleérve az informatikai biztonságért felelős (hardver) komponenseket is. Hiszen ezeken a döntéseken is kell alapulnia a hatékony kockázatkezelési programnak. Az információ biztonsági vezető (CISO) felelőssége a szervezet biztonsági programja, általában beleértve a kockázatkezelés menedzselését, programját. Ezért is játszik

[47] BCP: Business Continuity Planning
[48] Általában véve igaz, hogy a döntéshozatalnak visszakövethetőnek kell lennie, azaz dokumentálni szükséges a kiindulási információkat és a döntést is.

vezető szerepet a megfelelő strukturált módszertan, hiszen segít azonosítani, értékelni (felmérni) és minimalizálni a kockázatokat az IT rendszerek vonatkozásában, amelyek a szervezetet támogatják céljainak elérésében. Tehát a CISO egy fő konzultánsnak kell, hogy legyen a felső vezető számára, vagy a felső vezetői körökben, voltaképpen vezető tanácsadó annak érdekében, hogy a felső vezetés biztos legyen abban, biztosítva legyen afelől, hogy a megfelelő tevékenység folyamatosan és rendeltetésszerűen zajlik.

6.3 A rendszer tulajdonosai és az információ tulajdonosai

A szakirodalomban a vagyontárgy vagy vagyonelem kifejezés egyszerre jelentheti a rendszer (hardver, szoftver) és az információ (adatok) összességét. Ezek tulajdonosai felelősek azért, hogy a megfelelő ellenőrzési kontrollok garantálják a rendszer és adatok integritását, sértetlenségét és bizalmasságát. Jellemzően ez a kör a felelős, az IT rendszerekben (tervezetten) bekövetkező változásokért, éppen ezért a tervezett feladatokat (átállásokat, rendszerfejlesztést, nagyobb vagy főbb hardver szoftver változtatásokat) azt megelőzően írásban be kell terjeszteniük. Ez különösen fontos annak érdekében, hogy maga a folyamat is teljesen szabályozott, nyomon követhető, utólag is visszakereshető és minden érintett számára világos legyen a felelősség szempontjából is. A folyamat (kidolgozás, kockázatelemzés, beterjesztés, elfogadás) során pedig lehetőség van a kockázatok kezelésére, változásuk nyomon követésére is. Az változások esetén pedig be kell, hogy induljanak a változáskezelés, kockázatkezelés és értékelés, gap analízis, s a többi folyamatok is.

A vagyonelem részletesebb tagolásával, egységekre bontásával lehetőség van tételesen meghatározni a tulajdonosokat és felelősségi köröket. Például egy adott számlázó szoftver egy külső vállalkozó fejleszti, de egy hostingban lévő szerveren található, amelyet a cég alkalmazottai üzemeltetnek. Ebben az esetben a hardver, az internetkapcsolat, az operációs rendszer és patch menedzsment valamint a számlázó program, mind külön komponensek és eltérő személyekhez tartozik az egyes rétegek tekintetében a felelősség.

6.4 Üzleti vezetők, funkcionális menedzserek, egységvezetők (és véleményvezérek)

A felelős szervezeti és üzleti vezetők részt kell, hogy vállaljanak aktívan az informatikai beszerzési folyamatokban az elvárások definiálásával, ennek kapcsán aktívan be kell kapcsolódniuk a kockázatkezelési folyamatokba is. Részvételükkel optimalizálható a

kiadások mértéke, mivel az a szükséges üzleti folyamtokhoz lesz hangolva és ehhez lesz kialakítva a kockázatkezelési program is. Ennek a folyamatnak és modellnek az előnye, hogy a hatékonyság mellett a kiadások alacsony szinten tathatóak. Ezért is kiemelten fontos, hogy már a tervezési fázisban, az első megbeszéléseken képviselve legyen a biztonsági szempont is. Ez csak akkor lehetséges, ha a munkahelyi szabályzat, kultúra és a szervezeti vezetők ezt támogatják, tisztában vannak ennek fontosságával.

6.5 Az informatikai szakemberek

Bizonyos szakszavak nem váltak el annyira élesen a magyar nyelvben, mint az angol szakirodalomban. Az viszont ettől függetlenül is belátható, hogy az informatikus szakma számtalan további, alkalmanként teljesen eltérő szakirányra, szakterületre bontható. Ilyenek például a hálózati rendszergazdák, az alkalmazás vagy adatbázis adminisztrátorok, a számítógép specialisták, biztonsági elemzők, tanácsadók és helpdesk munkatársak.[49] Mindezen szakterületeken, azaz általánosan az informatikai területen dolgozók felelőssége is, hogy az információbiztonsági program és a biztonsági előírásokat végrehajtsa az információs rendszerekben. A változásoknak, amelyeknek számos oka lehet, például: hálózati kiterjesztés, meglévő infrastruktúra vagy szervezeti szabályok átalakítása, áttérés új technológiára, frissítések, sérülékenységek derülnek ki, egyéb. Mindezek vonatkozásában az IT biztonsági területén érintett szakembereknek támogatnia kell a kockázatkezelési folyamatokat annak érdekében, hogy azonosítani és értékelni lehessen az új potenciális kockázatot és implementálni egy új biztonsági kontrollt az IT rendszerek biztonságának garantálásához.

6.6 A biztonságtudatossági oktatók

Az IT rendszer felhasználói lehet a szervezet személyzete, a beszállítók, a kiszervezett munkaerő, olyan munkavállalók is akik csak áttételesen kerülnek kapcsolatba ezen rendszerekkel, vagy áttételesen gyakorolnak hatást a biztonságra. Erre jó példa a fizikai biztonságért felelős, gyakran kiszervezettként foglalkoztatott személy, például a portás, vagy

[49] Az itt felsoroltaknál természetesen lényegesen több területre bontható az információs rendszerekkel kapcsolatos szakterületek száma.

az a beszállító, akinek bejárása van az épületbe.[50] Bárki, aki tehát érintett a szervezet információs és informatikai rendszereinek biztonságában, aki szervezeti adatvagyon megóvására befolyással lehet, tisztában kell, hogy legyen azokkal az alapvető viselkedési normákkal és szabályokkal, amelyeknek célja a kockázatok mérséklése. Ezen kockázati tényezők mérséklésével a szervezet elsődleges célja a szervezeti információ és tudásvagyon, további értékek, például: az IT erőforrások védelme. A hatékonyan működő biztonsági kontrollok része kell, hogy legyen a biztonságtudatossági szint emelése, a biztonságtudatossági oktatások. Ennek érdekében IT biztonsági képzésben jártas információbiztonsági trénernek olyan, a szervezet által elfogadott biztonsági szabályrendszeren alapuló képzési anyagokat és oktatásokat kell kifejleszteni és tartania, amelynek révén egyrészt csökkenthető a kockázat, mérhetővé és értékelhetővé válik a tudatossági szint, oktatással pedig tovább fejleszthető.

Jól láthatóan ebben a részben az információbiztonságról inkább az IT, informatikai biztonságra került a hangsúly. Ennek az az oka, hogy az oktatás hatékonyságához a megfelelő szintű (például: informatikai, számítógép kezelői) alapkompetenciákra is szükség van. Az oktatási program hatékonyságát befolyásoló tényezők munkaszervezetenként változhatnak, olyan koncepció is lehetséges, hogy más oktatási modulokhoz kölcsönösen betársulni a biztonságtudatossági szekcióval. Mindezek kivitelezése, lebonyolítása jelentős szervezési és kommunikációs munkát igényel. Az oktatási anyagokat minden esetben a célközönségre kell szabni és a szabályzatban foglalt rendszeres időközönként megismételni a közben eltelt időszak tapasztalatait is beépítve a programba. Erre jellemzően a megfelelő szakmai ismeretek mellett jó oktatási, módszertani, kommunikációs készségekkel rendelkező, azt hitelesen előadni képes kolléga ajánlott, hogy az általa átadott ismeretek minél inkább elérjék a kívánt hatást, növelve a tudatossági szintet.

6.7 Információ biztonsági kockázatra vonatkozó koncepciók

A legtöbb szervezetben biztosítva van a kockázatkezelési menedzsmenttel foglakozó önálló osztály, ami a forprofit világban a nagyvállalatokra érvényes lehet, azonban kisebb cégek vagy közigazgatásban jellemzően napjainkban még nincs olyan kiképzett szakember gárda réteg, illetve nincs meg az előzménye annak a szervezeti hagyományokon alapuló koncepciónak, hogy külön ilyen önálló osztályok létezzenek. Hangsúlyozom, hogy ez csak

[50] A beszállító, aki hetente újratölti az ásványvizes kioszkokat, takarítást, egyéb tevékenységet végző munkavállalók, elektromos hálózat, klíma karbantartó s a többi.

általánosságban igaz, ettől bármely irányban lehetnek és vannak is eltérések. Amire rá kívánok világítani, hogy nem elegendő egy adott személy kinevezése, egy adott tisztség létrehozása, hiszen a szervezet aktuális folyamatainak nagy többségébe és a szervezeti kultúrába, szokásokba is bele kell, hogy épüljön a kockázatkezelési stratégia, eljárásrend ezáltal valósulhatnak meg az üzleti, szervezeti célok támogatása.

Ahhoz, hogy az információ biztonsági menedzser által létrehozott program hatékonyan tudja csökkenteni a kockázatokat, ehhez szükséges ajánlásokat, javaslatokat tudjon kidolgozni, beterjeszteni, magában kell foglalnia számos folyamatnak a kockázatkezelési értékelést, úgy mint:

- technikai,
- stratégiai,
- taktikai,
- adminisztratív és
- operatív

elemeket is. A kidolgozott ajánlások elfogadása, beépülése a folyamatokba, az idő, amíg a munkavállalók többsége megfelelő tudatossági tudásszintet ér el, nem érhető el egyik napról a másikra. Tehát kicsit sarkítva a kérdés, ha végtelen erőforrással rendelkeznénk, akkor sem lehetne egyik napról a másikra megváltoztatni és optimális állapotot elérni, egészen egyszerűen azért, mert időre van szüksége az embereknek, hogy magukévá tudják tenni ezen információkat, hozzáállást, gondolatokat, szabályzatokat, beépülhessen a napi rutinba, szokássá váljon.

6.8 Koncepció

A hatékony kockázatcsökkentés érdekében meg kell ismerni legalább általánosságban azokat a koncepciókat és fogalmakat melynek segítségével a kockázatcsökkentési programban jól különválaszthatóak a felelősségi körök, teendők, egyéb szempontrendszerek alapján.

- veszélyek,
- sérülékenységek,

- kitettségek,
- kockázatok,
- hatások,
- kontrollok,
- ellenintézkedések,
- erőforrások értékelése,
- információs kockázat menedzsment,
- információs eszközök besorolása,
- kritikusság,
- érzékenység,
- a helyreállításhoz szükséges idő (RTO),
- helyreállítási pont,
- szolgáltatás szállítási célok,
- elfogadható megszakítási ablak, vagy időkeret,
- redundancia.

Üzletfolytonosság szempontjából további kockázat menedzselési kapcsolódó fogalmakat is meg kell érteni:

- szolgáltatási szint megállapodások (SLA-k)
- a rendszer robusztussága és rugalmassága,
- üzletfolytonosság és katasztrófa elhárítás,
- üzleti folyamatok újratervezése,
- projektmenedzsment határidők (mérföldkövek) és komplexitás,
- vállalati és biztonsági architektúrák,
- IT és információs biztonsági irányítás,
- rendszer életciklus menedzsment,
- szabályzatok, szabályok, szabványok és eljárások.

6.9 Technológiák

Sokféle, különböző információbiztonsági technológia érhető el a piacon, ezek műszaki és egyéb koncepciók tekintetében is eltérőek lehetnek. A szervezet számára

alkalmas technika és technológia kiválasztásához fontos ismerni alapvető fogalmakat, néhány ezek közül:

- alkalmazás biztonsági mérés, értékelés, intézkedés,
- fizikai biztonságra vonatkozó mérés, értékelés, intézkedés,
- környezeti ellenőrzés és szabályok,
- logikai hozzáférés szabályok,
- hálózati hozzáférés szabályok,
- routerek, tűzfalak, és egyéb hálózati komponensek,
- behatolás detektálás és megelőzés,
- vezeték nélküli technológiákkal kapcsolatos védelem,
- platformok védelme, biztonsága,
- titkosítás és nyilvános kulcsú infrastruktúra (PKI),
- antivírus, malware egyéb kártevők,
- spyware és adware,
- antispam alkalmazások és eszközök,
- telekommunikációs általános ismeretek és voice-over IP (VoIP).

Ezen kívül bár a személyi és létesítmény biztonság talán nem része az információ biztonsági menedzsmentnek fő területének, vagy a kockázatkezelési programnak, de ezen területek kockázatát is figyelembe kell venni a kockázatkezelési terv kialakításakor[51]. (Erre egy lehetséges, időben közeli példa Edward Snowden ügye).[52] Tehát az információ biztonsági menedzser muszáj, hogy tisztában legyen személyi és személyzeti biztonsági kérdésekkel, ellenőrzésekkel, feljegyzésekkel, szabályzatokkal. Továbbá a környezeti és létesítmény szabályzatokat egyaránt figyelembe kell venni a kockázat értékelési tevékenység során. Ilyenek lehetnek: az épület elektromos betáplálása, az épületen belüli elektromos tervrajzok, kapcsolatok a szolgáltatóval, kapcsolószekrények és elektromos eszközök használatára vonatkozó szabályzatok az épületben, szünetmentes, áthidalási idő, személyi és jogi kérdések, s a többi.

[51] Minden folyamatot azonosítani szükséges és mindegyiken végre kell hajtani a kockázatértékelést. Ez alól a tervezési, döntési folyamatok sem képeznek kivételt.
[52] Edward Snowden, amerikai számítógépes szakember, az amerikai Nemzetbiztonsági Ügynökség alkalmazottja volt és azzal vált ismertté, hogy nyilvánosságra hozott szigorúan titkos dokumentumokat.

6.10 A kockázatkezelési terv végrehajtása

A tervezési folyamat, a kockázatkezelési terv részeként az információ biztonsági menedzsernek azonosítani kell minden egyéb, a szervezet összes kockázatkezelési tevékenységét. Igyekezve integrálni ezeket a funkciókat és az információ biztonsági terv kontextusában értelmezni. Szervezetenként eltérő lehet a kockázatkezelési funkciók felosztása, tehát ahogy egy földrajzilag nagy kiterjedésű, több telephelyen rendelkező cégeknél a fizikai védelem lehet elsődleges, addig finanszírozással, pénzügyekkel foglalkozó szervezeteknél külön osztály létezhet a pénzügyi, hitelezési kockázatok kezelésére, más szervezeteknél más szempont szerinti kockázatkezelési osztályok is létezhetnek. Mindezen kockázatok gyors és hatékony kezelésére, olyan mechanizmusok szükségesek, amelyek biztosítják egyes kockázatkezeléssel foglalkozó egységek között a jó kommunikációt biztosító funkciókat. A jó kockázatkezelési program eredményeképpen összhangba kerülnek az egyes területeken működő folyamatok, megszűnnek a párhuzamosítások, minimalizálódik a le nem fedett területek nagysága. Ez hatékonyan befolyásolja az információvédelmi tevékenységet valamint a többi területen is csökkenti a működési és üzleti kockázatokat.

6.11 A kockázatmenedzselési folyamat

A kockázatmenedzsment a folyamatokban eltér a kockázat értékelésétől. Sokkal inkább a lehetőségek és alternatívák mérlegelése az érdekelt felekkel való konzultáció, figyelembe véve a kockázat értékelés és egyéb tényezőket és kiválasztva a megfelelő megelőző és ellenőrzési lehetőségeket az elfogadható költségek figyelembevételével. A kockázat menedzsment általában az alábbi folyamatokat tartalmazza:

- létrehozza a körét és határait (akár kijelöli a nem vizsgált területeket is),
- kockázat értékelés,
- kockázat kezelés,
- az elfogadható fennmaradó kockázat kijelölése.

Ezen folyamatok definíciója:

Létrehozza a körét és határait: A teljes szervezetre vonatkozólag meghatározásra, megállapításra kerülnek azok a paraméterek és teljesítménymutatók, amik a kockázat kezelési menedzsmentet érintik. Ez vonatkozik minden tényezőre (külső, belső).

Kockázat értékelés: Ez egy metodikai eljárás, amely három lépésből áll: a kockázat azonosítása, elemzése és értékelése.

A kockázatkezelés egy kiválasztási eljárás, amelynek során a szervezet kockázati étvágyához igazítják az azonosított kockázatot. Ilyenek lehetnek az elkerülés, a kockázatos tevékenységes megszűntetése, a kockázatos tevékenység csökkentése, eljárások kifejlesztése és bevezetése, kockázat áthelyezése vagy kiszervezetése harmadik félhez, biztosítás. A szakirodalom ezt a kiszervezetést nem minden esetben különálló szervezetre érti, hanem a szervezeten belül lehet egy másik részleg is. A kockázat általában megmarad, ha nincs költséghatékony módja a csökkentésnek, ha kevés vagy kicsire értékelik a potenciális hatását, vagy valamilyen okból nem lehetséges vele hatékonyan foglalkozni.

A fennmaradó (elfogadható) kockázat definiálása esetén, lehetséges annak elfogadása döntés és jóváhagyást követően. A vezetés elfogadhatja a kockázatértékelés során kapott kockázati eredményt. A kockázatkezelési folyamatban kell vele a továbbiakban foglalkozni.

A kockázat kommunikációja és monitoringja olyan folyamat melynek során kicserélik és megosztják a kockázattal kapcsolatos információkat és felülvizsgálják a teljes kockázatkezelési folyamat hatékonyságát. Ez a kommunikáció jellemzően a döntéshozók és az egyéb érdekeltek között történik, és nem feltétlenül korlátozódik a szervezetre. A kommunikáción és monitoringon keresztül van biztosítva a hatálya, a határa a kockázatértékelésnek, a cselekvési tervnek és folyamatoknak, ezek frissítésének.

6.12 A kockázat kezelési menedzselési folyamat

Egy ilyen folyamat nem tekinthető állandónak, folyamatos és szisztematikus fejlesztése elengedhetetlen. Ennek külső és belső okait és tényezőit talán felesleges is bőven kifejteni, de röviden a belső tényezők vonatkozásában fontos tényezők: a szoftver és hardver komponensek a szervezeti célok és a munkavállalói fluktuáció mind ide sorolható. A külső tényezők közül párat megemlítve: a beszállítók, árverseny, a konkurencia és a technikai változások, a munkavállalói attitűd, amelyre jelentős hatással vannak a társadalmi, politikai viszonyok, melyek önmagukban is ide sorolhatóak. Egy hatékony biztonsági program megvalósítását hivatalos keretek közé kell helyezni. Meghatározva a hozzávetőleges biztonsági szintet, a lehetséges biztonsági kockázatokat, ezek függvényében potenciális hatásokat és a szervezet kockázatcsökkentési képességét. Ezek a tényezők jellemzően szervezetenként eltérőek. Az információbiztonsági menedzser fel kell, hogy állítsa azokat a folyamatokat, amelyek segítségével rendszeresen végezhető a kockázatértékelés, szervezeti,

rendszer és alkalmazások szintjén. Hatékony mérési mutatók kidolgozására van szükség nem csak a kockázatok megállapítása miatt, hanem a biztonsági intézkedések hatékonyságának mérése miatt is, mely folyamatnak az információbiztonsági menedzser a felelőse. Egyszerű példával érzékeltetve, bármely változtatás után újra kell mérni, hogy annak következtében hogyan változott a biztonsági kockázat, hiszen nem biztos, hogy csökkent. Folyamatosan fel kell derítenie és javaslatot kell tennie adott felelősnek / tulajdonosnak. Ezek során manuális és automata technikákat is használhat. Ez a kockázatértékelés azért fontos és szükséges, mert közben meg kell határozni a szervezet biztonsági tevékenységére vonatkozó legnagyobb hatást is. A kockázatkezelésnek egy folyamatos és dinamikus folyamatnak kell lennie annak érdekében, hogy a változó fenyegetéseket és sérülékenységeket kezelni tudja egy időben.

Szükség van a folyamatos kockázat menedzselési lépésekre, a kidolgozott folyamatok állapotának és biztonsági ellenőrzések nyomon követéséhez. A folyamatok tekintetében kontrollpontok segítségével lehet menetközben hatékonyságot mérni. A szabályok és ellenőrzési kontrollok hatásfoka idővel jellemzően romlik, célját téveszti, vagy elveszti. Ezért folyamatos nyomon követésre és periodikus tesztelésre van szükség.

Általánosan használtak az alábbi folyamatok a szükséges kockázat menedzsment meghatározásához:

- meg kell határozni a szervezet kockázati profilját,
- meg kell érteni és dokumentálni kell a kockázati kitettség jellegét és mértékét,
- meg kell határozni a kockázatkezelési prioritásokat, amelyhez segítséget adnak a
    - a valószínűségi fenyegetések azonosítása
    - meghatározni a mennyiségi (pénzügyi) és minőségi (hatás) értékeket a kritikus információs rendszereken és eszközökön, amelyeket a biztonsági programban a helyén van, meg tud védeni:
    - annak a meghatározása, hogy milyen hatása lenne az üzletre / a szervezetre ha a sérülékenységet sikeresen kihasználnák.

6.13 A biztonsági értékesítése

Az információbiztonság és a kockázat voltaképpen termékek, melyeket az információ biztonsági szakembernek, el kell tudnia adni a menedzsment és a teljes munkaszervezet felé is. Más-más nyelvezet szükséges a célközönség függvényében ez egyértelmű. A legnagyobb

kihívás a „Miért?” kérdésre való válaszadás, annak menedzser nyelven, menedzserek vezetők által érthető módon történő indoklása. Miért kell erre ennyit költeni, miért van erre szükség? A szükséges program és indoklás felépítése a fogalmak, informális egyeztetések, a szaknyelv tisztázása rengeteg időt, energiát emészthet fel. Azonban a sztenderdek lefektetése nélkül nincs biztonsági program. A sztenderdek, szabályzatok elfogadására a legfelsőbb szinten kell, hogy sor kerüljön. Ennek eléréséhez folyamatos kommunikációra van szükség. Ezen kommunikációnak ki kell térni a helyzetfelmérés eredményeire, a kockázati tényezőkre valamint bizonyos megtérülési kalkulációkra is. A napi gyakorlat azt mutatja, hogy a munkavállalók, vezetők egyaránt túlterheltek. Azonban a napi rutinon túl az információbiztonsági vezető feladata a kitekintés is, a jövőt kémlelve a trendeket figyelve a jövő szabványaira és fenyegetéseire már ma választ kell adnia a választ, oly módon, hogy a menedzsment felé javaslatokat, alternatívákat terjeszt be. Tehát nem elég a meglévő rendszerek naprakészen tartása. A felhasználói szokások, a környezet, további tényezők változása állandó mozgásban tartja, fejlődési spirálba kényszeríti a szervezetet, a kockázat elfogadható szinten tartása érdekében.

Ezekből következik, hogy számos nem csak szigorúan vett szakmai kompetenciával kell rendelkezni:

- Fontos, hogy megértse a szervezeti kultúra értékelését,
- Tudnia kell, hogyan értékelje a szervezeti kultúrát,
- Ismerje a saját helyét és világosan egyértelműen definiálja a szervezetben elfoglalt helyét, szerepét,
- Szenvedéllyel végezze a munkáját,
- Tisztában kell lennie, hogy nem újra és újra szélmalomharcot vív, mindig vannak részeredmények,
- Szövetségesek azonosítása elengedhetetlen a sikerhez,
- Tudja értékelni az üzleti kockázatokat és halasztani a technikai megoldást.

Nem olyan régen még az információbiztonság inkább informatikai biztonságot jelentett még és az is leszűkült a vírusvédelmi rendszerek, tűzfalak telepítésére és implementálása, napjainkra azonban gyökeresen megváltozott a helyzet. Az alkalmazások és a szervezeti információ felhasználás (informatizálódás) által olyan dolgozói rétegre mutatkozik igény, amely nem csak technikai, hanem jogi, adatvédelmi, üzleti célokra,

kérdésekre is képes választ adni. A szervezetek sikeres működéséhez napjainkra elengedhetetlen:

- az információs folyamatok üzleti tervekhez történő igazítása,
- a költségek és a kockázatok egyensúlyban tartása,
- folyamatos kommunikáció az IT és az üzleti irányítás között,
- folyamatos kommunikáció az IT és az IT beszállítók között,
- olyan szervezeti kihívások kezelése, mint a technológia vagy szolgáltatás centrikus üzemeltetés kérdése,
- valamint a humán faktor, azaz a munkavállalók képességeinek fejlesztése, tudásbázis létrehozás, tudástranszfer és mentorálás.

A Gartner Group 2004-es felmérése alapján a megkérdezett informatikai vezetők az alábbiakat nevezték meg főbb problémaként:

- Nehéz értéket szolgáltatni az informatikával.
- Nem ismertek (nem egyértelműek) az üzleti elvárások (szervezeti célok).
- Hiányzik az összehangolás az IT erőfeszítések és az üzleti célok között.

Mindezek, abba az irányba mutatnak, hogy folyamatos és többirányú kommunikációra van szükség. Ez a kommunikációs feladat az egyik legnagyobb kihívás az információbiztonsági vezető életében.

7 Összegzés (I. fejezet)

A munkaszervezetek napi működésük során kapcsolatot létesítenek ügyfeleikkel, ezen kapcsolatok közben változnak az ügyféligények, környezeti tényezők. Ebből kifolyólag a legtöbb munkaszervet arra kényszerül, hogy a változó környezethez alakítsa folyamatait. Ezen változások mind lehetséges információbiztonsági kockázatot hordoznak. A gap analízis olyan eltéréseket keres, amely a tervezett és a jelenlegi állapot között található, szabályozásban, vagy valamely folyamatban jelen van. Ez a kockázatkezelési folyamat sztenderd része. Ennek elvégzésére nem csak változás esetén, hanem periodikusan is szükség van. A modern technika természetesen számos lehetőséget, cél szoftvert és hardvert kínál annak érdekében, hogy az

emberi tényezőt támogassa az ajánlásokon és keretrendszereken kívül, amik szintén támogatást nyújtanak.[53] A kockázatok hatékony kezeléséhez azonban elsősorban a megfelelő keretrendszer kiválasztása, a szabályozási környezet kialakítása és elhivatott, tudatos munkavállalók szükségesek, ehhez lehetséges további hatékonyságnövelő tényező a technikai megoldás. Ezek nélkül bármilyen jó is a technikai megoldás, jellemzően nem képesek betölteni funkcióját. Szükséges bizonyos időnként olyan gyakorlatok elvégzése adott célcsoporton, vagy az egész munkaszervezeten, amely valós visszajelzést tud adni, hogy eseményvezérelt helyzetben mi történne, hogyan működnének a folyamatok, hogyan reagálnának a munkavállalók. Ilyen gyakorlatoknak általános éberség fenntartó funkciója is van, de ezen kívül a gyakorlat lehetőségét is biztosítja az információbiztonsági vezető és a többi munkavállaló számára is.

8 Irodalomjegyzék (I. fejezet)

- Moeller, Robert R.. COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance, Second Edition. John Wiley & Sons. 2011. ("Chapter 4 - COSO ERM Framework".)
- Peltier, Thomas R.. How to Complete a Risk Assessment in 5 Days or Less. Auerbach Publications. 2009. "Appendix G - Sample Threat Checklist".
- Wong, Caroline. Security Metrics: A Beginners Guide. McGraw-Hill/Osborne. 2012.
- Wright, Steve. PCI DSS: A Practical Guide to Implementing and Maintaining Compliance, Third Edition. IT Governance. 2011
- Stackpole, Bill, and Eric Oksendahl. Security Strategy: From Requirements to Reality. Auerbach Publications. 2011.
- Tipton, Harold F., and Micki Krause. Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications. 2007
- Peltier, Thomas R.. Information Security Risk Analysis, Third Edition. Auerbach Publications. 2010.
- Wright, Steve. PCI DSS: A Practical Guide to Implementing and Maintaining Compliance, Third Edition. IT Governance. 2011 "Chapter 4 - Step 4 – Conduct Gap Analysis".

[53] Léteznek a folyamatok vizuális ábrázolására alkalmas célszoftverek, melyekben beállíthatók összefüggések, felelősök, egyéb függőségi viszonyok is.

- CISM Review Manual 2013, ISACA (2013)
- Informatikai projektek vezetése, Görög Mihály, Ternyik László. – Budapest : Kossuth K., 2001. – ISBN 963 09 4227 5
- Nemzeti Infokommunikációs Stratégia 2014-2020
- Ivanyos János: A vállalati kockázatkezelés, 2013, http://www.tankonyvtar.hu/hu/tartalom/tamop412A/0007_e3_kockazatmenedzsment_scorm/coso_belso_kontroll_IyzpDEu6yLwJHA1g.html

9 Ábrajegyzék (I. fejezet)

II. fejezet. Kockázatmenedzsment a gyakorlatban, minták és megoldások

1 A munkaszervezeteket érő hatások

Napjainkban jellemző, hogy a munkaszervezeteket gyakran érik külső-belső, különböző hatások. Ezek következnek a:

- piaci változásokból,
- az adott ország és a nemzetközi környezeti változásokból,
- jogszabályi változásokból,
- munkavállalók fluktuációjából,
- technikai (szoftver, hardver) változásokból,
- egyéb adott szervezetre specifikusan jellemző tényezőből.

A változás jelen van a legtöbb szervezet legtöbb folyamatában, ez az egy jelent állandóságot, hogy változás van. Ezen változásokra, jelentős részükre természetüknél fogva fel lehet készülni és tervet lehet készíteni. Egy részük pedig olyan típusú, amelyre annak előfordulásáig valószínűleg senki sem gondolt.[54] Azon kockázatok és változások hatása, amelyre előzetesen sikerült felkészülni, várhatólag rövidebb, könnyebben lokalizálható és kezelhetőbb lesz, mintha forgatókönyv nélkül érné a szervezetet az esemény.[55] Tekintettel arra, hogy civilizált életünk minden területén elektronikus, információs rendszerek dolgoznak a háttérben, így kiemelt jelentősége van ezen rendszerek védelmének, illetve ezen rendszerek védelmére történő felkészülésnek. Számos nemzetközi példa mutatja, hogy az információs hadviselés korát éljük, komoly tényezőként kell számolni az információs rendszereket ért

[54] USA 911, http://hu.wikipedia.org/wiki/2001._szeptember_11-ei_terrort%C3%A1mad%C3%A1sok
[55] Ezen felkészülés mértéke lehet pusztán logikai, a szabályozásban, szabályzatokban, vagy a kockázatkezelési tervben logikailag megjelenő. Vagy lehet olyan is, amely valamilyen tesztcsoporton az eseményvezérelt helyzet mintájára tesztelésre is kerül.

támadásokkal. Nagy különbség azonban a hagyományos pusztítást célzó támadásokkal szemben, hogy az információs rendszerekbe történő bejutás akár hosszú ideig[56] is észrevétlen maradhat. Valamint, hogy az információ megszerzése révén a hagyományos lopással ellentétben az adat, információ tovább létezik mindkét helyen. Természetesen a pusztításra, erő demonstrációra is vannak példák az elmúlt évekből.[57]

Ennek érdekében javasolt olyan forgatókönyvek elkészítése, amelyek ilyen a kockázatokra történő felkészülésnél még csak a képzeletben léteznek. A kockázatok elemzéséhez és kezeléséhez szükséges gyakorlatok, hipotetikus szcenáriók által azonban nem csak elkészülhetnek ezek a forgatókönyvek, hanem értékes tapasztalatokkal gazdagodhatnak a kidolgozásában részt vevők, olyan területek is felmerülhetnek[58] a kockázati területek felderítése közben, amely addig valamilyen gap területen helyezkedett el. Elkészítésükhöz pedig ugyan azok a bemeneti dokumentumok szükségesek, amelyeknek egyébként is rendelkezésre kell állniuk az osztályba sorolás, leltár és kockázatkezelési eljárásokban. Javasolt, hogy a kockázatmenedzsment lépéseit, kidolgozását a biztonságért felelős csapat, vagy ha ilyen nincs akkor az információbiztonsági vezető más szervezeti vezető, bizottsági tagok, s a többi bevonásával, azaz ne egyedül végezze. Ennek oka, hogy a folyamatokra, az egyes területekre több embernek, adott területen dolgozónak nagyobb rálátása lehet.

2 Kockázatmenedzsment gyakorlati minta

Az alábbiakban ismertetésre kerül egy kockázatkezelési gyakorlat, amely a feladatból és arra készült lehetséges, minta megoldásból áll. A példából jól látható, hogy napi szinten merülhetnek fel olyan események, környezeti tényezők, amelyek jelentős hatással lehetnek a szervezet információbiztonságára, funkcionális működőképességének fenntartására. A feladat a tantárgyhoz kapcsolódó gyakorlati oktatáson kerül ismertetésre, megoldásra, a teljes befejezéshez szükséges természetesen további önálló munka.

2.1 Gyakorlati feladat általános leírása

[56] A Stuxnet vírus és az iráni atomprogram http://wwwold.kfki.hu/fszemle/archivum/fsz1105/CserhatiAndras.pdf
[57] Az oroszok visszabombázzák Észtországot az online kőkorszakba, http://index.hu/tech/net/eszt290507
[58] Egy lehetséges szcenárió kibertámadásra, Digitális Mohács, http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Az alábbiakban ismertetett forgatókönyv alapján több, kockázatelemzéshez és kockázatkezeléshez kapcsolódó feladatot kell megoldani

A feladatok javasolt papíron, vázlatszerűen kidolgozni a gyakorlaton, majd azt tisztázott formában, elektronikusan kell leadni, ez lesz a gyakorlati jegy egyik tényezője.

Mivel egy valós szituációban, egy működő munkaszervezetnél is több különálló területet figyelembe kell venni, együtt kell működni társosztályokkal, s a többi, így jelen gyakorlat is alkalmat kíván teremteni a csapatban való munkához. A csapat tagjai ugyanazt a jegyet fogják megkapni, így egymással és egymásért is dolgoznak!

A második nap végén minden csapat röviden összefoglalja, milyen megoldást választott a kérdések megoldására. Ez a csoport és csapatok előtti beszámoló és interaktív visszajelzés lehetőséget kíván teremteni a vezetőség előtti, vagy különböző meetingeken történő érdekérvényesítés gyakorlásához.

A gyakorlat azt a célt szolgálja, hogy a résztvevők egymástól is tanuljanak, lehetőséget kíván teremteni, hogy mindenki be tudjon hozni egy kiválasztott problémát, amely úgy gondolja, hogy a munkaszervezetében fennáll, de nem talált még rá megoldás. Ezen szakmai kérdések felvetése és rövid megbeszélése lehetőséget ad a tudástranszferre, a jó-megoldások átadására. Ezen kívül nem titkolt cél a hazai szakembergárda közötti kommunikációs csatornák kiépítése, megvalósítása.

2.1.1 A szervezettel kapcsolatos információk

Az alábbiakban ismertetésre kerülő lehetséges megoldási minta a fentiekben megadott fiktív munkaszervezet a Zab – és Búzahegyezési Közigazgatási és Engedélyezési Hivatal[59] által alkalmazott kockázatkezelési gyakorlat modellezése. A szervezet rendelkezik már bizonyos szabályzatokkal (IBSZ, SZMSZ)[60], de számos területen még vélhetően hiányosak a dokumentációk illetve az eljárásrend. Összesen 3 főállású informatikust foglalkoztat a szervezet. Az informatikai rendszer meghatározó elemei folyamatosan kerültek beszerzésre a múltban, folyamatosan foltozgatva azt. Ez alól két kivétel van, a jogelőd Banánhajlító és Pucoló Hivataltól megörökölt személyügyi rendszer valamint az Európai Uniós forrásból nemrégiben kialakított Oatsharpener rendszer.

[59] Zabhegyező Hivatal, a példa szempontjából kitalált szervezet. A The catcher in the rye – Zabhegyező című könyv címét alapul véve.
[60] Információbiztonsági szabályzat, Szervezeti és működési szabályzat

A korábbi intézmény egy megyeszékhelyen működött, majd néhány éve elköltözött a fővárosba. Ezzel párhuzamosan kialakításra kerültek a regionális kirendeltségek. A régi telephelyen minden aktív munkavégzés megszűnt, csak egyetlen helyiséget használ továbbra is a Hivatal – a korábbi géptermet. Itt a régi eszközök egy része biztosítja az off-site mentést, illetve ezt a helyiséget használják a Banánhajlító és Pucoló Hivatal papíralapú nyilvántartásának tárolására is.

2.1.2 A feltérképezett, nyilvántartott informatikai infrastruktúra

A budapesti telephelyen került kialakításra a gépterem, itt került elhelyezésre az Intézet teljes számítási kapacitása. A vidéki (off-site) telephelyen a korábbi szerverhelyiségben backup site került kialakításra.

Az infrastruktúra régebb óta működő elemei elöregedtek, de az Uniós projektben megvalósított OatSharpener projektben beszerzésre kerültek új, korszerű elemek is.

2.1.2.1 A gépterem fizikai biztonsági elemei:

- 8 ponton záródó fém ajtó nagy biztonságú hengerzárral
- kártyás beléptető rendszer, amely a mágneszárat nyitja (és logol)
- riasztó ajtónyitás érzékelővel, riasztás esetén sziréna szólal meg a szerverszobánál és a biztonsági őrségnél
- a helyiség ablaktalan
- tűzérzékelő, amely riasztás esetén, a portán jelez
- CO^2-es oltókészülék a bejárati ajtó mellett (a külső oldalon)
- hőmérséklet érzékelő, riasztás a portán és SMS-ben
- nem redundáns, de megfelelően méretezett klíma
- megfelelően karbantartott és méretezett UPS-ek (X perc után megkezdődik az infrastruktúra automatikus leállítása, az áthidalási ideje csak erre elégséges)

2.1.2.2 A korábbi gépterem (Miskolc) fizikai biztonsági elemei:

- 6 ponton záródó fém ajtó 2 hengerzárral
- kártyás beléptető rendszer, amely a mágneszárat nyitja (és logol)
- a helyiség ablaktalan
- nem redundáns, de megfelelően méretezett klíma

2.1.2.3 A budapesti gépteremben lévő hardverelemek:

- 3 db 5 éves 2 utas 2U rack szerver (2*4 coreproc, 48 GB RAM, 2*1G LAN uplink LACP trunk, 2*1G SAN uplink) (virtuális környezet host)
- 2 db 1 évnél újabb 2 utas 2U rack szerver (2*10 coreproc, 256 GB RAM, 2*1G LAN uplink LACP trunk, 2*10G SAN uplink) (virtuális környezet host)
- 1 db 8 éves 2 utas 1U rack szerver (1*2 coreproc, 2 GB RAM, 1G LANuplink, 2*36GB SCSI HDD RAID1) (HR szerver)
- 1 db 1 évnél újabb 2 utas 2U rack szerver (2*3 coreproc, 128 GB RAM, 4*1G LAN uplink LACP trunk, 12*900GB 2,5” 10k SAS HDD) (backup szerver)
- 1 db 1 évnél fiatalabb tapelibrary (3 drive, LTO5, 48 tape, FC)
- 2 db 1 évnél fiatalabb 16 port FC switch (switchenként 8 port licencelve)
- 2 db 24 port L2 switch 20 db 1G porttal, és 4 db 10G (DAC) porttal („SAN switch”)
- 1 db 24 port L3 switch („coreswitch”)
- 1 db 5 éves dual kontrolleres iSCSI SAN, kontrollerenként 2*1G csatolással (8 GB cache, 28*300GB 3,5” 15k SAS HDD, 14*1TB SATA HDD)
- 1 db 1 évnél újabb dual kontrolleres iSCSI SAN, kontrollerenként 2*10G csatolással (32 GB cache, 8*450 GB SSD, 40*900GB 2,5” 10k SAS HDD, 25*3TB SATA HDD)
- 1 db 1 évnél újabb UTM

- 1 db szolgáltatói router
- 2*10 KVA 3 fázisos UPS (az 5 éves a szervereket szolgálja ki, az 1 évnél fiatalabb a storage)

2.1.2.4 A miskolci gépteremben lévő hardverelemek:

- 1*3 KVA 1 fázisos UPS
- nem redundáns klíma
- 1 db 24 port L3 switch
- 1 db 5 éves tapelibrary (1 drive, LTO4, 24 tape, FC)
- 1 db 5 éves FC switch (8 port licencelve)
- 1 db 1 évnél újabb UTM
- 1 db szolgáltatói router

Az kiszolgálók és egyéb infrastruktúra elemek a rendelkezésre álló eszközökhöz mérten lehetőség szerint redundánsan kerültek összekötésre. A 3 régi, és a 2 új szerver a virtuális környezet hosztjai, ezek szolgáltatják a rendszerek működéséhez szükséges számítási kapacitást. A virtuális környezet hardver hiba esetén automatizáltan biztosítja a HA funkciókat.

A kliens accesss witchek 10/100-as eszközök, 1G uplinkekkel, a szerverszobai „coreswitchbe” uplinkelve.

2.1.2.5 Alapvető kliens információk:

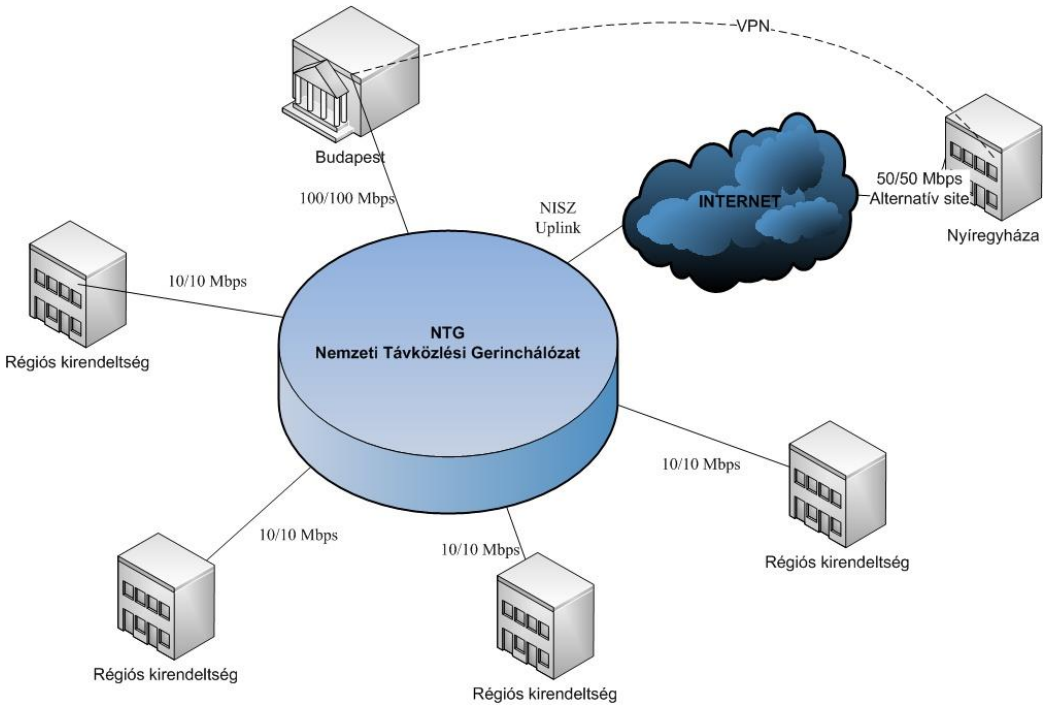
- vegyes életkorú (0-7 év) PC-k
- zömében Windows XP, kisebb számban Vista és Windows 7 licencek (OEM)[61]

[61] Általánosan megfogalmazva: az aktuálisan elterjed, de már kifutó operációs rendszer és az azt követő, leváltani képes operációs rendszerek aránya.

- a PC-k háza matricával leragasztott, hogy a háznyitásnak nyoma maradjon
- az operációs rendszerbe címtár alapú (LDAP) authentikációval lehet bejelentkezni
- viszonylag korszerű endpoint security megoldás (antivírus, HIPS, csatlakoztatható eszközök kontrollálása)
- multifunkciós eszközök PIN kódos nyomtatással

2.1.2.6 Hálózati kapcsolatok, eszközök

A hálózati diagram elkészítése és kapcsolatok ábrázolásának elkészítése tetszőleges mélységben készülhet. Általános tapasztalat, hogy ezek eseti jelleggel, eseményvezérelt környezetben kerülnek jellemzően felhasználásra. Ezen esetekben viszont a lehető leggyorsabban és legaprólékosabban kell, hogy rendelkezésre álljanak. Érdemes ezen szempontok figyelembevételével, több rétegben és többféle felhasználási célt szem előtt tartva, annak megfelelő részletezettséggel elkészíteni. Ezen megközelítések közül az egyik a telephelyek és internetkapcsolatok ábrázolása. Ezen kívül az alkalmazások, kiszolgálók, fizikai, hálózati eszközök ábrázolására is javasolt ábrát készíteni, az IP címek, egyéb fontos információk feltüntetésével.



7. ábra: Sematikus hálózati ábra

A hálózati határvédelmet, és a géptermek közötti VPN kapcsolatot az UTM-ek biztosítják. Az UTM által ellátott funkciók:

- L7 tűzfal
- alkalmazás azonosítás és alkalmazás szintű szabályok megadásának lehetősége
- címtár integráció, és user szintű szabályok megadásának lehetősége
- IPS/IDS
- SPAM szűrés
- vírusszűrés (SMTP, HTTP)
- sebezhetőség analízis és jelentés
- URL szűrés

2.1.2.7 Backup stratégia

- D2D2T mentési stratégia[62]
- az adatok és kritikus operációs rendszer adatok[63] örök inkremental mentése az operációs rendszerbe/alkalmazásba épülő pluginnal naponta
- a hypervisor és OS által biztosított eszközökkel a virtuális gépek heti image szintű mentése (DR mentés)
- a mentett adatok deduplikálása
- a mentett adatok miskolci telephelyre történő replikációja a site-to-site VPN kapcsolaton keresztül

[62] Disk-to-disk-to-tape (D2D2T) egy olyan megközelítés, a biztonsági mentés és archiválás során, amelyben az adatokat először egy biztonsági lemezes tároló rendszerre, majd ezt követően rendszeresen másolja a szalagos tároló rendszerre.
[63] Systemstate

2.1.2.8 Fontosabb alkalmazások

A hivatal az alábbi fontosabb alkalmazásokat használja:

Alkalmazás megnevezése	Megcélzott „rendelkezésre állás”	Egyéb megjegyzés
Oatsharpener	5/12	Webes, Oracle Linux és middleware, külön DB szerver
Iratkezelő	5/12	MSSQL
Gazdálkodási rendszer	5/12	MSSQL
Elektronikus levelezés	7/24	
File server	5/12	
Címtár szolgáltatás	7/24	
Jogtár	5/12	
Webserver	5/12	LAMP MySQL
Nyomtatószerver	5/12	MS / Cups
Patch management	5/12	
Antivírus mgmt szerver	7/24	
Tűzfal UTM	7/24	
Backup	5/12	
Felügyeleti rendszer / monitoring management	7/24	
LOG gyűjtés, elemzés, feldolgozás	7/24	
SMS küldő rendszer	7/24	Mobiltelefon, áramellátás, készülék, adatkábel
Elektra, elektronikus utalás	5/12	betárcsázós modem
Személyi rendszer	5/12	DOS, Epson FX-1050

8. ábra: Alkalmazás leltár minta

A fenti minta táblázat a feladat végrehajtása során tetszőlegesen változtatható, bővíthető. Cél, hogy a csapat tagjai saját tapasztalataik alapján minél jobban hozzák összhangba a valósággal. A felmerülő további kérdésekre közösen keressenek megoldást.

2.1.3 Feladatok részletesebb kibontása

1. feladat: A megadott információk alapján tervezze meg a Nemzeti Zab – és Búzahegyező Hivatal informatikai infrastruktúráját! A csoport alapvetően szabad

kezet kap kisebb módosítások, eltérések vonatkozásában, annak érdekében, hogy minél hitelesebb és saját munkaszervezetükben előforduló kérdéseket is szerepeltessenek anonim módon a kidolgozásban.

- 2. feladat: Készítsen egy 5-8 elemből álló adatvagyon-leltárt!
- 3. feladat: Határozzon meg minden leltárban szereplő elemhez 2-3 fenyegetést! A fenyegetések között legyenek személyi, fizikai és logikai jellegűek is és vegyesen érintse az egyes elemek bizalmasságát, sértetlenségét és rendelkezésre állását![64]
- 4. feladat: Elemezze az egyes fenyegetésekből következő sebezhetőségeket!
- 5. feladat: Határozzon meg egy kvalitatív kockázatelemzési módszertant!
- 6. feladat: A kockázatelemzési módszertan alapján határozza meg az egyes sebezhetőségből következő kockázatok mértékét!
- 7. feladat: A kockázatelemzési módszertan alapján tegyen javaslatot a kockázat kezelésének módjára!
- 8. feladat: A Hivatal egy szabadon választott elektronikus információs rendszerére vonatkozóan végezze el az adott rendszer kezdeti biztonsági osztályba sorolását![65]

2.1.4 Munka az elkészített dokumentumok alapján

- Az előzőekben elkészített dokumentumok alapján kell a feladatokkal továbbhaladni. A napi működés során felmerülő információk alapul véve további értelmezés és tennivalók válhatnak szükségesség.
- A nap folyamán hírek érkeznek, amikből következtetéseket kell levonni.
- A következtetések alapján új kockázatok jelenhetnek meg, esetleg már meglévő kockázatok módosulhatnak.
- A feladat a kockázati regiszter bővítése, módosítása az információk alapján.

[64] Bizalmasság (Confidentiality), Sértetlenség (Integrity), Rendelkezésre állás (Availability): A széles körben elfogadott megközelítés angol rövidítése: CIA.
[65] Vegye figyelembe a 2013. évi L. törvényt és az adott szervezetre vonatkozó végrehajtási rendeleteket, külső-belső szabályozási környezetet és a rendelkezésre álló határidőket. Fontos, hogy ezek alapján részletes, dátumokkal meghatározott ütemterv is készüljön.

- A leadott dolgozatban a döntések folyamatát szeretnénk látni! Különösen fontos, hogy megfelelő figyelmet kell szentelni a dokumentálásra, azaz a döntési mechanizmus visszakövethető legyen.

2.1.5 Hírek – 1 (I.)

Hat megyére adtak ki piros riasztást

Az özönvízszerű eső miatt hat megyére, szombatra is a legmagasabb fokú, vagyis a piros figyelmeztetést adta ki péntek este az Országos Meteorológiai Szolgálat.

Az özönvízszerű eső miatt az ország összes megyéjére első-, másod- vagy harmadfokú figyelmeztetést adtak ki péntekre. Ezek között a harmadfokú, vagyis piros figyelmeztetést Pest, Komárom-Esztergom, Somogy, Fejér, Hajdu-Bihar és Borsod-Abaúj-Zemplén megyére léptették életbe. A viharos erősségű széllökések miatt Nógrád és Békés megye kivételével az ország összes többi megyéjében első- vagy másodfokú figyelmeztetéseket adtak ki.

2.1.6 Hírek – 2 (II.)

Viruslab: rohamosan terjed a kiberbűnözés

Tavaly 42 százalékkal nőtt a célzott kibertámadások száma 2012-höz képest a Viruslab 18. internetbiztonsági jelentése szerint, ezen belül a kkv-k elleni támadások száma megháromszorozódott – közölte a cég csütörtökön, Budapesten, a sajtótájékoztatón.

A támadások leggyakrabban szellemi termékek eltulajdonítását célozták. A kiberbűnözők már nemcsak a kormányintézményeket veszik célba, hanem a termelő vállalatokat, és ezek között a kisebb cégeket is. Az alkalmazottak közül már nemcsak a felső vezetők, hanem a mérnökök, szakértők és kereskedelmi ügyintézők is ki vannak téve a támadás veszélyének – hangzott el.

2.1.7 Hírek – 3 (III.)

Vigyázat! Támadnak a kiberbűnözők!

A kibertér biztonságát szavatolni kell, de nem szabad engedni, hogy ez az internet szabadságát veszélyeztesse – hangzott el hétfőn egy, az informatikai rendszerek működésével kapcsolatos fővárosi konferencián.

Évről évre nő a kibertámadások száma Magyarországon, bár ezek nagyobb része még nagyon kezdetleges – mondta a Közigazgatási és Igazságügyi Minisztérium parlamenti államtitkára hétfőn a fővárosban egy konferencián.

Az államtitkár kijelentette: bár a támadások kezdetlegesek, de Magyarországon is megjelentek olyan nemzetközi – megfogalmazása szerint – kiberbűnözői csoportok, mint például az Anonymous. Az államnak energiát kell fordítania a probléma kezelésére, elsősorban a megelőzésére, ezért fel kell mérni az információbiztonság szintjét, a stratégiai pontokat pedig védeni kell – fűzte hozzá.

2.1.8 Jelentés – 1 (IV.)

Microsoft Windows VBScript memória kezelési sérülékenység

Angol cím: Microsoft Windows VBScript Memory Corruption Vulnerability

CERT-Hungary ID: CH-10532

Felfedezés dátuma: 2014-02-12

Összefoglaló: A Microsoft Windows sérülékenységét jelentették, amit kihasználva a támadók feltörhetik a felhasználó rendszerét.

Leírás: A sérülékenységet a VBScript scripting engine egy hibája okozza, és kihasználható a memória felülírására.

A sérülékenység sikeres kihasználása tetszőleges kód futtatását teszi lehetővé.

2.1.9 Informális tájékoztatás (V.)

A május 7-i KIBEV ülésen a résztvevők közül – jellemzően államigazgatási szektorból – többen jelezték, hogy az általuk felügyelt rendszerek ellen több DdoS jellegű támadást tapasztaltak. Megállapították, hogy ezen a területen fokozottabb figyelemre, illetve a tapasztalatok megosztására, esetleg a GovCERT bevonására lehet szükség.

2.1.10 Hírek – 4 (VI.)

Magyar politikusok teljes területi autonómiát követelnek a kárpátaljai magyar és ruszin kisebbségnek.

Egyes magyar politikusok teljes területi autonómiát követelnek a kárpátaljai magyar és ruszin kisebbségnek és arra szólították fel a nemzetközi közvéleményt, hogy szálljon síkra a Kárpátalján is megkezdődött katonai sorozások leállítása érdekében.

Képmutatónak nevezték a nyugatot amiatt, hogy a „válságot leghosszabb ideig visszafogottan szemlélő és önmérsékletet tanúsító, a kisebbségeinek a védelmére kelő Oroszországot teszi meg a válság bűnbakjává”. Bírálta, hogy eközben a nyugat által támogatott ellenzéki erők első hatalmi intézkedése az volt, hogy visszavonta a nyelvtörvényt, előrevetítve a „legdurvább ukrán sovinizmust” és a nemzeti kisebbségek – köztük a kárpátaljai magyar és ruszin, illetve orosz, lengyel, román és tatár kisebbségek – teljes jogfosztását.

2.1.11 Jelentés – 2 (VII.)

Jelentés

Jelentem, hogy május 9-én, 13:00-órától kezdődően az NZH weboldalának elérhetőségével kapcsolatos hibabejelentéseket kaptunk. A webszerver logjainak áttekintése során nagy mennyiségű, elosztott forrásból származó lekérdezést észleltünk, mely a kiszolgáló jelentős lassulására vezetett. A valószínűsíthető támadást a Kormányzati Eseménykezelő Központ és a NISZ Zrt részére bejelentettük, az elhárítása érdekében az

internetszolgáltatóval a kapcsolatot felvettük. A feltételezett támadás – eddig nem ismert okból – 16:10-kor véget ért.

Tóth János

rendszergazda

2.1.12 Hírek – 5 (VIII.)

Orosz kiberfegyver támadhatja Ukrajnát és más kelet-európai országot

A brit ABE Systems biztonsági szakértői szerint az ukrán és más kelet-európai hálózatokat támadja a Serpent (kígyó) vírus, amelyekkel a támadók teljes hozzáférést szerezhetnek a kompromittált rendszereken. Több hálózaton is beazonosították a kártevőt.

A kiberfegyvert egyre többet használják év eleje óta, de már használták Janukovics leváltása előtt is. A Serpent komplex összeállítása hasonlít az eredetileg iráni atomlétesítményeket támadó Sixnetre. Nagyon nehéz felismerni, akár napokig is teljesen inaktív lehet.

Nem tudni biztosan ki készítették, de a fejlesztők a moszkvaival megegyező időzóna szerint dolgoztak, és orosz szövegeket is találtak a kódban.

2.1.13 Jelentés – 3 (IX.)

Jelentés

Jelentem,

2014. május 10-én, a hajnali őrjárat során 05:47-kor ablak betörését észleltem a Miskolc, ismeretlen út 32. szám alatt lévő épület fsz.-i folyosó hátsó részén. A betört üvegek elhelyezkedéséből azt állapítottam meg, hogy az utca felől törték be az ablakot. A folyosón az üvegek között befelé irányuló lábnyomokat vettem észre. A létesítmény átvizsgálása során eszköz eltulajdonítását nem észleltem. A biztonsági szolgálat vezetőjét telefonon értesítettem, aki a rendőrségre bejelentést tett. A helyszint a rendőrség kiérkezéséig biztosítottam.

Miskolc, 2014. május 10.

Kovács János

biztonsági őr

2.1.14 Hivatalos államigazgatási jelzés (X.)

AH VIII/7-es Osztálya hivatalos jelzést küldött a NZH biztonsági vezetőjének, melyben jelezte, hogy információik szerint a zabhegyezési tevékenység az orosz és az ukrán hírszerzés fókuszterébe került, onnan szervezeti és technikai információkat igyekeznek megszerezni a politikai válsággal kapcsolatban, valamint igyekeznek olyan személyi kapcsolatokat nagyon gyorsan kialakítani, melyekkel ezt a hírszerző tevékenységüket a későbbiekben is támogathatják.

2.1.15 Jelentés – 4 (XI.)

Jelentés

Jelentem, hogy 2014. május 10-én a 7 órás váltásra Tóth János rendszergazda nem jelent meg, telefonon történő kapcsolatfelvétel sikertelen volt. Lakástelefonján feleségével beszéltünk, aki jelezte, hogy Tóth János már a hajnali órákban, a szokásosnál korábban elindult munkahelyére, azóta ő sem éri el mobiltelefonon.

Pótlásáról túlórában helyettesítő rendszergazdáról gondoskodtunk.

2014. május 10. 10:30

Nagy Péter

Informatikai vezető

2.1.16 Rendkívüli közlemény (XII.)

Az ukrán válság miatt operatív törzs létesül Magyarországon

Az ukrajnai helyzet miatt a régióban bekövetkező kibertámadások miatt a magyar miniszterelnök operatív törzs létrehozására kérte a belügyminisztert, írja az MTI. A

miniszterelnök ezt a visegrádi országok (V4) kormányfőinek pénteki budapesti munkavacsorája után jelentette be. Azt mondta, utasította a belügyminisztert, hogy

„Készítse fel az országot arra a helyzetre, hogyha Ukrajnában a dolgok nem a kedvező kibontakozás irányába mutatnak”.

Az ukrán válsággal foglalkozó rendkívüli találkozón a négy állam (hazánk mellett Szlovákia, Csehország és Lengyelország) kormányfői közös nyilatkozatot is elfogadtak. Ebben felsorolják az országok javaslatait a kiberkrízis kezelésére – hogy pontosan mik ezek a javaslatok, azt egyelőre nem tudni.

2.1.17 Napi jelentés (XIII.)

Tisztelt NZH Központi Főügyelet!

2014. július 1-én 00:00 – 23:59 között az Nemzeti Távközlési Gerinchálózaton az alábbi telephelyekkel kapcsolatban történt 15 percnél hosszabb időtartamú adathálózati kommunikációs zavar.

Telephely neve / Esemény	Időtartam	Intézkedések
Tóthjászkomlós, internetkapcsolat szakadás	9:56:15 - 10:41:55	Szolgáltatói hiba, bejelentés közben a kapcsolat helyreállt. Hibajegy száma: ABC-8952
Nagybérfalva, áramszünet	8:06:25 – 13:06:26	Bejelentett karbantartás, a helyi áramszolgáltató 9:30 és 14:00 óra között áramszünetet hirdetet.

Rövid idejű, 10 percen belüli leszakadások: Mezőlacháza, Soltszentlak, Kisbér, Mezőnagylak.

Az adathálózati vonalszakadás az említett telephelyek esetében érintették az informatikai főosztály által nyújtott informatikai szolgáltatások elérhetőségét, valamint az az alábbi rendszereket: levelezés, intranet, IP alapú telefónia működőképességét.

Tóth László
ügyeletes
NZH IT Ügyeleti Szolgálat

3 Megoldási útmutató

A fentiekben megadott és a csapat tagjai által kiegészített információk alapján az alábbiakban közreadott mintától eltérő megoldások is készülhetnek. Az alábbiakban ismertetésre kerülő megoldás, segítséget kíván adni ahhoz, hogy mi az a minimum szint és kockázatelemzési metódus, amelyet minden munkaszervezetben létre kell hozni.

4 Adatvagyon leltár

Adatvagyon megnevezése	**Vonatkozó jogszabályok, rendelkezések**	**Adatvagyonért felelős szervezeti egység**	**Adatvagyon felhasználója**
Zabhegyezést végzők nyilvántartása	Ztv.	Nyilvántartási és Engedélyezési Főosztály	u.a., Kormány, EU, NAV
Személyügyi adatok	Kjt.	Személyügyi Főosztály	u.a., Bérszámfejtési O., KIM, KSH
Iratkezelési adatok	Levéltári tv.	Szervezési Osztály	A hivatal
Gazdálkodási adatok	Hatályos jogszabályok	Gazdálkodási Osztály	u.a., MAK, NGM, OEP, ONYF, KSH
Archív Banánhajlító nyilvántartás Működési adatok (logok, konfigurációk, beállítások)	A korábban hatályos Bhtv	Nyilvántartási és Engedélyezési Főosztály	u. a., Személyügyi Főosztály, ONYF Informatikai osztály, felhasználók.
Szervezeti tudás (eljárásokra, folyamatokra vonatkozó leírások)	Alapító dokumentum, szervezeti szabályzatok és vonatkozó törvények.	Információbiztonsági osztály, informatikai osztály, technológiai osztály, ahol a dokumentumok tárolódnak, felső vezetés – szabályozási környezet.	Tulajdonjog gyakorlója, a Magyar állam

Adatvagyon megnevezése	Adatbáziskezelő rendszer	Adatbázis neve	Külső adatszolgáltatás	Külső adatkapcsolat	Informatikai üzemeltetésért felelős
Zabhegyezést végzők nyilvántartása	Oracle	ZAB	NAV (tételes), Kormány és EU (aggregált, n.éves)	nincs	informatikai csoport
Személyügyi adatok	DBase	munkatars	bérszámfejtés (havi, tételes, eseti), KIM (eset), KSH (n. éves aggregált)	nincs	informatikai csoport
Iratkezelési adatok	MSSQL	iktat.dbf	Levéltár (éves, tételes)	nincs	informatikai csoport
Gazdálkodási adatok	MSSQL	FORRAS.dbf	MAK (havi, tételes), NGM (n.éves mérleg), OEP, ONYF (havi és eseti), KSH (éves, aggr.)	nincs	informatikai csoport
Archív Banánhajlító nyilvántartás	kézi visszakeresés	Banánhajlító nyilvántartás	ONYF, államplogárok számára munkaviszony igazolás kiadása	nincs	informatikai csoport

9. ábra: Adatvagyon leltár minta

5 Kockázat elemzési módszertan

A feladat során meghatároztunk egy kvalitatív kockázat-elemzési módszertant. A módszertan két tényezőt vesz figyelembe, az esemény várható bekövetkezését valamint a kár mértékét. Az egyes tényezők 1-től 5-ig terjedő skálán kerülnek besorolásra. A kockázat mértéket a két tényező szorzata adja. Ennél összetettebb rendszer esetében figyelembe lehet venni az adatvesztés anyagi, személyi és időbeli hatályát. A maximálisan megengedett kiesési, visszaállítási időablakot. A normál üzletmenet szempontjából percenként / óránként keletkező veszteséget, kiesést, termeléselmaradást. Nem utolsó sorban az online reputáció sérülésével járó bizalomvesztés hatását, tovább azt a tényezőt, hogy az előre elkészített kommunikációs stratégiával mennyire lehet az adott esemény következményeit tompítani.

Mivel a tevékenységet jogszabály írja elő, tevékenység felfüggesztése nem jöhet szóba. Adott esetben a kockázat elfogadása nem jelenti azt, hogy a kockázattal nem foglalkozik a szervezet, azonban az ezekre való felkészülést, illetve a kockázat csökkentését csak eseti jelleggel végzi. Valamint lehet olyan döntés, pénzügyi vagy más megfontolásból, hogy minimális mitigáció valósul csak meg az ügyben. Ezen kívül lehet más elemzési módszert is meghatározni, akár a fentiekben bemutatott táblázatok alapján.

Nemzeti Zabhegyező Hivatal

kvalitatív kockázatértékelés (kockázat = kár mértéke x kár valószínűsége)[66]

Jelmagyarázat:

Elfogadás (kockázat kisebb mint 8)

Áthárítás (kockázat egyenlő 8)

Csökkentés (kockázat nagyobb mint 8)

Kár mértéke	Kár valószínűsége	elhanyagolható esély 1	0,25 körüli valószínűség 2	0,5 körüli valószínűség 3	0,75 körüli valószínűség 4	(szinte) biztos esemény 5
nincs vagy elhanyagolható	1	1	2	3	4	5
2 embernappal pótolható, vagy ennek megfelelő érték elvesztése	2	2	4	6	8	10
2 emberhéttel pótolható, vagy ennek megfelelő érték elvesztése	3	3	6	9	12	15
2 emberhónappal pótolható, vagy ennek megfelelő érték elvesztése	4	4	8	12	16	20
súlyos, helyre nem állítható kár	5	5	10	15	20	25

10. ábra: Kockázatszámítási táblázat (kvantifikálás)

[66] Kvalitatív információkból kvantitatív információkat származtatunk, így lehetséges lesz a számszerűsítésen kívül az összehasonlításuk is. (Kvantifikálás).

Azonosított kockázatok

Érintett adatvagyon megnevezése	CIA[67]	Vonatkozás[68]	Fenyegetés	Sérülékenység	Kár mértéke	Kár valószínűsége	Kockázat	Intézkedés
Zabhegyezést végzők nyilvántartása	S	L	papír beadványok elfogadása	Rossz adatot küldenek be a hivatalnak.	1	3	3	-
Zabhegyezést végzők nyilvántartása	R	F	eszköz tönkremenetele	A LAN switch megsérül.	2	2	4	-
Zabhegyezést végzők nyilvántartása	S	L	jogszabályi hiba	Nem jelentik a megszűnő zabhegyezési tevékenységet.	5	3	15	jogszabály változtatási javaslat
Személyügyi adatok	R	F	eszköz tönkremenetele	meghibásodik az adatbázist kezelő hardver	3	2	6	-
Személyügyi adatok	B	L	illetéktelen adatbetekintés	nincs authentikáció	2	3	6	-
Iratkezelési adatok	S	Sz	hibásan kezelt program	oktatás hiánya	4	2	8	felelősségbiztosítás kötése
Iratkezelési adatok	R	L	fejlesztői hiba	visszakereshetőség hiánya	4	2	8	támogatási szerződés kötése
Gazdálkodási adatok	B	Sz	illetéktelen adatmódosítás	alkalmazott elbocsájtása	1	3	3	-
Gazdálkodási adatok	S	Sz	hibásan kezelt program	hibás adatrögzítés	2	2	4	-
Gazdálkodási adatok	R	F	alátámasztó adat elvesztése	a leltári címkék leesnek	2	1	2	-
Archív Banánhajlító nyilvántartás	R	F	adatvesztés	tűzeset	2	5	10	tűzoltó készülék elhelyezése
Archív Banánhajlító nyilvántartás	B	F	illetéktelen betekintés	arra járó személy belenéz az iratokba	2	1	2	-

11. ábra: Azonosított kockázatok

5.1 Azonosított kockázatok

Az előzetesen felállított módszertan a feladatban előírt mértékben került elvégzésre a kockázat elemzés. Számbavételre kerültek a fenyegetéseket és az azok alapján szóba jövő sérülékenységek. Az elemzést az 2. melléklet tartalmazza. (Lásd Excel tábla.) Az

[67] Sértetlenség, Rendelkezésre állás, Bizalmasság. Bizalmasság (Confidentiality), Sértetlenség (Integrity), Rendelkezésre állás (Availability): A széles körben elfogadott megközelítés angol rövidítése: CIA.
[68] Logikai, Fizikai, Személyi

Oatsharpener biztonsági osztályba sorolása megtörtént az Ibtv[69] alapján. Az Ibtv. végrehajtási rendelete, a 77/2013. (XII. 19.) NFM rendelet 1. mellékletének 2. biztonsági osztályokról szóló pontja alapján lett elvégezve a rendszer biztonsági osztályba sorolása.[70] Megvizsgálva a felsorolt szempontokat, elemezve a rendszerre vonatkozóan azokat bizalmasság, sértetlenség és rendelkezésre állás szempontjából. [71]

A legmagasabb biztonsági osztály az alábbi két szempont alapján állt elő: „2.5.3. az üzlet-, vagy ügymenet szempontjából nagy értékű, üzleti titkot, vagy az érintett szervezet szempontjából különösen érzékeny folyamatokat kezelő elektronikus információs rendszer, vagy információt képező adat tömegesen, vagy jelentősen sérülhet”.

A 2.5.3. alapján mind a bizalmasság, mind a sértetlenség, mind a rendelkezésre állás szempontjából igazolható az adott biztonsági osztály. Valamint a „2.5.4. a káresemény lehetséges társadalmi-politikai hatásaként a jogszabályok betartása, vagy végrehajtása elmaradhat, bekövetkezhet a bizalomvesztés a szervezeten belül, az érintett szervezet felső vezetésében, az érintett szervezet vezetésében személyi konzekvenciákat kell alkalmazni”. A 2.5.4. alapján különösen a sértetlenség és a rendelkezésre állás szempontjából igazolható az adott biztonsági osztály. Tekintettel arra, hogy a hivatal legfontosabb feladata a Ztv.-ből eredő feladatok végrehajtása, nem javasolt a rendszer besorolásának lefelé történő módosítása. A rendelet vonatkozó utasításai alapján, tekintve, hogy a Zabhegyezést végzők nyilvántartása a nemzeti adatvagyon részét képezi, a sértetlenség követelménye az elsődleges – azaz más követelmény, különösen, ha az alacsonyabb, alapján nem sorolható osztályba a rendszer. A fentiek alapján az Oatsharpener biztonsági osztálya: 4.

6 A szervezethez érkezett hírek és azok értékelése

A szervezethez érkezett hírek alapján megtörtént azok értékelése és adott esetben a kockázatelemzés módosítása, intézkedések foganatosítása. Összességében működésbe lépett az kockázatkezelési terv megfelelő vonatkozásban.

[69] 2013. évi L. törvény és végrehajtási rendeletei.
[70] 77/2013 NFM rendelet: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről. http://njt.hu/cgi_bin/njt_doc.cgi?docid=165667.254105
[71] 77/2013 NFM rendelet, 3. melléklet, Besorolási útmutató.

6.1 Információ – 1, minta megoldás

Hír1: országos eső (piros riasztás, országos hír a hírportálokon) „Annyi eső jön, mint máskor egész májusban”. A hír kapcsán két további fenyegetés került beazonosításra. Az egyik kolléga[72] jelezte, hogy a nyíregyházi épület teteje hajlamos lehet beázásra. Informatikus kollégák felhívták a figyelmünket a 2007-es nagy áramszünet tanulságaira is, mikor az üdítő és kávé automaták órákra leálltak.[73]

Valószínűség/kár mértéke: 4/4 és 3/1

Az azonosított sérülékenységek és a kezelési javaslatok:

Beázás: Nyíregyházán fóliával letakarni az iratokat, 30 percenként ellenőrizni. Megoldást tenni a hosszú távú megoldásra. A felhalmozódó víz ellen polcrendszerre helyezni a gépeket és iratokat. Meghatározni a maximálisan megengedhető legmagasabb vízszintet. Elvi szinten felkészülni az ennél magasabb vízszint esetén a teendőkre. Az épület áramellátásával kapcsolatos információkat begyűjteni. Ez lehet leállítás és evakuálás, valamin áram vagy dízelmotoros vízszivattyú üzembeállítása. A 2007-es nagy áramszünet és egyéb felmerülő releváns információk dokumentálása. A jelenlegi helyzet és döntési tényezők dokumentálása.

Áramszünet: elfogadás (2 gépteremben UPS, automatikus lekapcsolás áthidalási időn belül).

6.2 Információ – 2, minta megoldás

Erősödik kiberbűnözés. Támadják a kisebb cégeket is és a vezetőn túl az alkalmazottakat is. Fontos, hogy az alkalmazottak oktatása ne csak a munkahelyi, hanem az otthoni és személyes életükben esetlegesen előforduló helyzetekre is terjedjen ki.

Az erősödő kiberfenyegetések az adatainkhoz való illetéktelen hozzáféréssel, azok ellopásával vagy meghamisításával fenyeget.

Valószínűség/kár mértéke: 3/3

Bízunk a tűzfalunkban[74], de átvizsgálásra kerülnek a beállításai és eseménynaplók tüzetesen a felmerült új szempontokból. Az oktatási programban és időszakos hírlevelekben, kampányokban külön figyelmet szentelünk a kapcsolódó információknak. A tudatosítási program része, hogy olyan kampányt, versenyt hirdetünk a dolgozók között, amivel ők is bevonódnak és aktívan részt vállalnak.

[72] Csapatmunka, együttgondolkodás.
[73] Szabályozni szükséges az épületbe hozható elektromos készülékek körét is.
[74] Valamint, IDS/IPS/SIEM rendszerek összességében.

6.3 Információ – 3, minta megoldás

(Államtitkár sajtó tájékoztatója.) Fel kell mérni az informatikai biztonság szintjét és a stratégiai pontokat védeni kell!
Valószínűség/kár mértéke: 2/2
Fel kell készülnünk újabb kockázatelemzésre és jelentés írására a meghozott intézkedésekről. Az előző hír hivatalos megerősítése. Ugyanakkor várhatóan csak a késleltetett politikai figyelem megnyilvánulása.

6.4 Információ – 4, minta megoldás

(VB script sérülékenység)

Az Office dokumentumok makróival terjedő kártékony kód illetéktelen hozzáférést tesz lehetővé, ezzel a kezelt adatok integritása sérülhet.
Valószínűség/kár mértéke: 3/3
Meg kell nézni, hogy az Microsoft adott-e ki javítást. Adott ki javítást. Ellenőrizzük, hogy a WSUS frissült-e. Az Office makrókat letiltjuk a Group Policy-ben. Az intézkedések felhasználók számára releváns részét közzétesszük, kommunikáljuk.
Amennyiben nem adott ki javítást, akkor Group Policy segítségével a házirend releváns részei frissíthetőek. Tájékoztatás a kollégáknak képekkel illusztrálva, de maximum 2 oldal terjedelemben az elkerülési és megoldási lehetőségekről. Megoldás kidolgozása arra az esetre, ha valamely munkavállaló munkájához szükséges funkciók kerültek blokkolásra.
Fontos, hogy a megoldás soha ne akadályozza nagymértékben az adott munkafolyamatot, vagy adott munkavállaló feladatának végrehajtását.

6.5 Információ – 5, minta megoldás

(KIBEV értekezletről származó információ.) A DDoS támadások száma növekszik. Rendszertelen időközönként, webről, szórt IP tartományból. Ezzel elvehetik a szervezet web forgalmának sávszélességét és elérhetetlenné tehetik a hivatal weblapját. Az elektronikus iratbeadás/lekérdezés lehetetlenné válhat. Félő, hogy a médiavisszhangja nagyobb lesz az ügyben, mint az egyébként érintettek száma vagy az okozott kiesés, kár, azaz a legjobban az online reputáció sérülhet.
Valószínűség/kár mértéke: 3/1

A többi szervezettől és a hálózati szolgáltatótól / üzemeltetőtől elkértük az információk, mit lehet tudni támadásokról. A log fájlokat elemezzük. Tűzfal beállítást ellenőrizzük, hogy van-e olyan beállítás, hogy adott IP címről határértéken felüli kérés érkezik, 30 perc után letiltás. NISZ értesítése az összegyűjtött információkról. Adott címtartomány vagy minta letiltása, túl hosszú élettartamú csomagok eldobása, egy irányú vagy túlzott forgalomra csomagvesztési szabály létrehozása, egyéb technikai és logikai elemzése a megoldásoknak.

Technikai szakértő bevonásával elemzésre kerülnek a támadásban használt csomagok. Azaz olyan logikai, technikai lehetőségeket is számba kell venni, amely már hamarabb, a hálózat korábbi szakaszán kitilthatóvá teszi az adott forgalmat nem csak forrásip, hanem más jellemzők alapján akár. A támadás és a csomagok típusa sokféle lehet, jelen esetben egyszerű elárasztásos DDOS támadás van szó. Megoldás lehet a válaszidő kitolása. Ha elsősorban belföldi felhasználói vannak rendszerünknek, akkor a külföldről érkező kéréseket átirányítjuk egy másik oldalra, site-ra, szerverre, ip-tartományba, s a többi, ahol tájékoztatjuk, hogy szolgáltatásunk jelenleg csak belföldről elérhető. Ekkor a támadás intenzitása 25%-ra esik vissza. További elemzéssel, az érintett szolgáltatókat az ip címek alapján tájékoztatjuk és megkérjük a szükséges lépések megtételére, kiemelve a BTK vonatkozó rendelkezéseit. [75] Ilyen (alapszintű) támadások ellen hatékony lehet, ha pusztán a szerver front-end, ügyfeleket fogadó részét valamilyen másik, akár külső hosting szolgáltatóhoz költöztetjük, fixre vagy eseményvezérelt környezetben automatikus redirekteléssel. Ebben az esetben a front-end részen nem találhatóak cégspecifikus belső adatok, ezek és az adatbázisok továbbra is a munkaszervezet fizikai és logikai kontrollja alatt maradnak.

6.6 Információ – 6, minta megoldás

(Autonómia követelés Ukrajnában) „Kijevben bekérették a magyar nagykövetet” – országos hírportálon vezető cikk.

A hír ellenérzést válthat ki Ukrajnában, melynek hatására a legális tiltakozásokon kívül illegális módokon – informatikai eszközökkel – is kifejezhetik az érintettek nemtetszésüket.[76] Komoly esély van rá, hogy a kormányzati szervek kitüntetett helyet kapnak a támadás során. Saját vélelmezésünk alapján a hivatal, mivel nem elég frekventált,

[75] 2012. évi C. törvény a Büntető Törvénykönyvről, XLIII. fejezet, Tiltott adatszerzés és az információs rendszer elleni bűncselekmények 422. § - 424 §.
[76] Hasonlóan a 2007-es Észtországi eseményekhez.

valószínűleg nem esik a támadók látókörébe. Ezzel párhuzamosan a dolgozókat, partnereket a szükséges mértékben tájékoztatjuk.

Valószínűség/kár mértéke: 3/2

Támadás, forgalomnövekedés, gyanús tevékenység esetén egyrészt fokozott figyelmet kértünk a dolgozóktól. Másrészről, ha az általagostól eltérő tevékenységet, forgalmat észlel a szervezet, akkor azt a szokott csatornákon jelentjük, hiszen ez akár egy komplex támadássorozat kezdete is lehet, amelyben más szervezetek és érintettekké válnak.

6.7 Információ – 7, minta megoldás

(DDOS támadás) 05.09-én 13 órától a NZH weblapjának elérése akadozik. Nagy mennyiségű, elosztott (USA, Kanada, Ausztrália, s a többi) támadás következtében.

A hivatal weblapja fontos kapcsolat az ügyfelekkel. A rendelkezésre állásunk sérül.

Valószínűség/kár mértéke: 5/1 (bekövetkezett, de a kár elhanyagolható, az ügyfelek más módon is intézhetik ügyeiket). A fentiekben ismertetett másodlagos site-ra váltjuk át a webszerver front-end felületét, technikailag a támadás erejét veszti, mivel a hivatal weblapja csak belföldi forgalmat fogad onnantól. Ezt követően a belföldi támadás célú forgalom csökkentésére, megszüntetésére fókuszálunk a fentebb már részletezett módon. A támadás függvényében protokollokra[77] és egyéb jellemzőkre történő szegmentálás és ezekre adott különböző válaszokkal csökkenthetőek a hatások.

A korábbi 3/1-es besorolás módosul.

Mivel a kockázat mértéke a legmagasabb osztályban volt, ezért elemezzük a log fájlokat, amely eredményeként módosítunk a tűzfal beállításokon. A webszerver és egyéb loggyűjtő helyek erőforrás és tárterület kapacitását felül kell vizsgálni, ha szükséges módosítani kell. A kiszolgálók tárhely és egyéb kapacitás kiterheltségét folyamatosan monitorozni szükséges az esetleges túlterhelésből következő visszaélési lehetőségek elkerülése érdekében.

6.8 Információ – 8, minta megoldás

(Sajtóhír orosz kiberfegyverről: http://www.minuszos.hu/olyat-lattak-a-kaspersky-szakertoi-amitol-tatva-maradt-a-szajuk/) Most került nyilvánosságra információ, egy

[77] A támadás típusa és a támadó által használt protokollok lehetnek egységesek, vagy sokfélék. Például egyszerű esetben csak ICMP vagy UDP (dns) vagy TCP kapcsolatokat építenek fel. Valamint ezen belül is további jellegzetességek lelhetőek fel. Ebben az esetben – már csak – a szűkített szcenárióra kell hatékony választ kidolgozni.

valószínűsíthetően orosz kiberfegyverről, ami rootkitet használ rejtőzéshez és kifejezetten államigazgatási adatok eltulajdonítására tervezték. A támadó eszköz nagyon szofisztikált, fertőzése estén az intézmény adatvagyona komoly veszélybe kerülhet.
Valószínűség/kár mértéke: 2/3 (mivel nem tartjuk magunkat célpontnak)
A kártevő tulajdonságainak[78] jobb megismerése után a detektálási és szűrési lehetőséginket célirányosan meg kell erősíteni. A kiadott információk alapján szignatúra és ip cím tiltásokat, beállításokat eszközölünk a központi rendszerekben.

6.9 Információ – 9, minta megoldás

(Fizikai betörés Nyíregyházán.) 05.10. 05:47: A biztonsági őr észlelte, hogy az ablakon keresztül betörtek a nyíregyházi épületbe. Lábnyomok láthatók a törött üvegeken.

Az első információink alapján lopás nem történt, a rendőrségi helyszínelés folyik. A helyzet teljes elemzéséhez kevés az információ, nem tudni, hogy pontosan mi volt a teremben vagy jelenleg mi van ott.
Valószínűség/kár mértéke: 1/1 (mivel informatikai vonatkozása nem igazolható)

Mivel a jelenlegi információnk szerint lopás nem történt, a szerver szoba ajtaja zárt, ezért a nyíregyházi szerverek logjait átvizsgálva igyekszünk ez megerősíteni. További helyszíni információt kérünk a biztonsági őrtől. Elképzelhető, hogy le kell mennie egy kollégának ellenőrizni, az iratokat és a hálózatra csatlakoztatott eszközöket szemrevételezni.

6.10 Információ – 10, minta megoldás

(AH jelzése) 05.10. értesítés: Az AH VIII/7 osztály jelenti, hogy a zab – és búzahegyezési tevékenység az orosz és az ukrán hírszerzés fókuszába került. Szervezeti és technikai információkat próbálnak megszerezni, akár személyes kapcsolatok felhasználásával is. A támadás az eddigi ismeretek alapján az intézményben felhalmozódott adatvagyon ellen irányulhat, különösen a Zabhegyező nyilvántartás van veszélyben.
Valószínűség/kár mértéke: 5/4 (teljes körű megsemmisítéstől nem kell tartani, de észrevétlenül jelentős módosítást hajthatnak végre)
Nyíregyházát azonnal le kell választani a hálózatról, kezdődjön azonnali és teljes körű átvizsgálás szakértő bevonásával. A papír alapú anyagok tételes ellenőrzése. Az előzőekben a felhasználók oktatása már megtörtént, de nyomatékosításul rendkívüli vezetői tájékoztató kerül kiadásra. A kiadvány tudomásulvételét írásban kell másnap délig minden

[78] Szignatúra, működés, ip címtartomány, egyéb jellegzetességek.

munkavállalónak igazolnia az iktatóban elhelyezett aláíró íven. A helyzet súlyosságára való tekintettel újabb figyelmeztetéssel nyomatékosítjuk a tanultakat. Kidolgozzuk a mentési rendet Nyíregyháza nélkül.

6.11 Információ – 11, minta megoldás

(Eltűnt a rendszergazda) 05. 10. 10:30 : Tóth J. rendszergazda lement Nyíregyházára, jelentette, hogy minden rendben van. Hazajött, reggel korán munkába indult, majd eltűnt. Tóth J. rendszergazdai jogai és jelszavai illetéktelen kezekben a rendszerünk teljes kompromittálódását jelenthetik. Egyelőre vélelmezzük, hogy eltűnésének nincs köze a korábbi eseményekhez.
Valószínűség/kár mértéke: 5/3 (a kár mértéke az előző feltételezés miatt módosult lefelé, illetve intézkedéssel csökkenthetőnek tartottuk)
Azonnali beavatkozást igényel. A rendszergazdai jelszavak megváltoztatása, jogosultságainak felfüggesztése, logelemzés az elmúlt 48 óráról, az esemény jelentése az Alkotmányvédelmi Hivatal felé, a többi rendszergazda személye kapcsán kockázatcsökkentő intézkedések.

6.12 Információ – 12, minta megoldás

(Kibertámadások Ukrajnából) A Belügyminisztérium operatív bizottságot hoz létre, hogy felkészítse az országot az ukrajnai helyzetből adódó problémákra. Figyeljük az Bizottság közleményit és várjuk az információkat. A Zabhegyező adatbázist lementve páncélszekrényben őrizzük. Mivel a kiberhadviselés jelenleg kívül esik a konvencionális hadviselésen, ezért a már meglévő fenyegetettség vélhetően nem nő tovább.
Valószínűség/kár mértéke: 3/3 (a közlemény értékelése ennyi)
Mivel előzőleg már magasabb éberségi, besorolási állapotba került a szervezet, a fenti semmiképp nem enyhít, inkább kicsit erősíti a megelőző kockázatokat. Maga a bejelentés viszont nincs direkt hatással a Hivatalra.

Hírek hatására felvett kockázatok

Érintett adatvagyon megnevezése	CIA	Vonatkozás[79]	Fenyegetés	Sérülékenység	Kár mértéke	Kár valószínűsége	Kockázat	Intézkedés	Hír kapcsolat
Archív Banánhajlító nyilvántartás	Rendelkezésre állás	F	beázás	papír nyilvántartás megsérül	4	4	16	fólia takarás, egyéb lásd szöveges kifejtés	I.
Áramszünet a viharok, beázás miatt.	Rendelkezésre állás	F	Leállás áramszünet miatt.	SLA	3	1	3	elfogadott kockázat	I.
A kiberbűnözés erősödik.	Mindhárom	L	Illetéktelen hozzáférés, adatmódosítás	nyilvánosságra hozott alkalmazás sérülékenységek	3	3	9	védelem erősítése	II.
VB script	Mindhárom	L	Illetéktelen hozzáférés, adatmódosítás	Office sérülékenység kihasználásával kártékony kód futtatása	3	3	9	frissítés, makró tiltás	IV.
DDoS támadások	Rendelkezésre állás	L	Webes tájékoztatás és iratkezelés nem működik	Hálózati és kiszolgáló eszközök túlterhelése	3	1	3	elfogadott kockázat	V.
DDoS támadások	Rendelkezésre állás	L	Webes tájékoztatás és iratkezelés nem működik	Hálózati és kiszolgáló eszközök túlterhelése	5	1	5	elfogadott kockázat, logelemzés	VII.
Orosz kiberfegyver	Mindhárom	L	Illetéktelen hozzáférés, adatmódosítás	érzékeny adatok (személyes, Zabhegyező nyilvántartás, stb) eltulajdonítása	2	3	6	detektálási információk gyűjtése	VIII.
Az AH jelenti hírszerző tevékenység a zabhegyezés területén.	Bizalmasság	L	Illetéktelen hozzáférés, adatmódosítás	érzékeny adatok (személyes, Zabhegyező nyilvántartás, stb) eltulajdonítása	5	4	20	rendszer leválasztás, szakértő, teljes átvizsgálás	X.
Az AH jelenti hírszerző tevékenység a zabhegyezés területén.	Bizalmasság	F	Illetéktelen hozzáférés, adatmódosítás	érzékeny adatok (személyes, Zabhegyező nyilvántartás, stb) eltulajdonítása	5	4	20	rendszer leválasztás, szakértő, teljes átvizsgálás	X.
Napi jelentés (áramszünet, rövid idejű megszakadások)	Rendelkezésre állás	F	Lehetséges illetéktelen hozzáférés a felügyeleti kapcsolat megszakadása alatt.	További adatok, illetéktelen hozzáférés megszerzése.	2	2	4	nyilvántartásban nyomon követni az események időbeli és fizikai elhelyezkedését, ismétlődését.	XIII.
Tóth J. (24) budapesti lakos eltűnt	Mindhárom	Sz	Magas szintű hozzáférés/jogosultság illetéktelen megszerzése	Nehezen észlelhető módon történő adatok eltulajdonítása	5	3	15	jogosultságok felfüggesztése, jelszavak megváltoztatása, AH értesítése, eseménynaplók átnézése	XI.

12. ábra: Azonosított kockázatok [80]

[79] F: fizikai, L: Logikai, Sz: Személyi

[80] A 9. és 10. ábra és a beérkező információk alapján elkészítve.

7 Összegzés (II. fejezet)

A valóságban, egyes munkaszervezeteknél jellemzően a fentieknél több összetevő is előfordulhat, hiszen egy valós munkaszervezet folyamatinak számossága is jóval több lehet. A belső vagy gerinchálózati eszközök üzemeltetése és frissítése, a beszállítók kockázatértékelése, az aktuális szerződések[81], és SLA-k kapcsán nem vizsgálódtunk a jelenlegi példákban. Nem lett kitűzve cél és határidő a dokumentációkkal kapcsolatban és nem lettek meghatározva a kulcsember pozíciókból fakadó kockázatok sem. Azonban a fenti minta alapján mindez továbbgondolható és elkészíthető, alkalmas lehet arra, hogy a felső vezetés számára jól kommunikálható, bemutathatóvá váljon. Összességében a napi folyamatokban támogatni tudja azon törekvést, hogy a változások következtében módosuló kockázatok és a rájuk kidolgozott terv képes legyen valódi és megfelelő választ adni az adott kérdésre. Felderíthetőek legyenek a be nem jelentett változások, minden olyan folyamat, esemény, ami a célállapottól való eltérésként definiálható. Ezek feltárását követően pedig automatikusan indulnak a kockázatkezelési folyamatok. Ezek kezelése a gyakorlatban, a hétköznapi életben változó intenzitással jelentkezik. Általános projektmenedzseri tapasztalat sokat segíthet ebben a munkakörben, ahol fontos a megújulni tudás, képesség. Újat és megoldást kell tudni mondani, utat kell tudni mutatni nemcsak az aktuális kihívásokra, de azokra az új, talán még a munkaszervezetben nem jelentkező, de várhatólag oda is beszivárgó szokásokra, technikákra, eszközökre, melyek hatással lehetnek és lesznek a szervezeti információbiztonsági szintre.

Ehhez a munkához kívánunk sok sikert és reméljük hasznos segítséggel, kiindulóponttal tudtunk szolgálni a fentiekben.

8 Ábrajegyzék (II. fejezet)

[81] A partnerek, a szoftver, hardver beszállítók, garanciális cserére vonatkozó SLA-k, s a többi. Számos további részletesebb vizsgálatnak is alá lehet vetni a szervezetet, az infrastruktúrát és a folyamatokat.

9 Irodalomjegyzék (II. fejezet)

- Stackpole, Bill, and Eric Oksendahl. Security Strategy: From Requirements to Reality. Auerbach Publications. 2011.
- Tipton, Harold F., and Micki Krause. Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications. 2007
- Peltier, Thomas R.. Information Security Risk Analysis, Third Edition. Auerbach Publications. 2010.
- CISM Review Manual 2013, ISACA (2013)

III. fejezet, Kártevők által okozott veszélyeztetettségi mérték meghatározása (esettanulmány)

1 Bevezetés

A számítógép hálózatok biztonsága egyre nagyobb problémát jelent. A hálózati biztonság területén a manuálisan vagy célprogramok segítségével megvalósított támadások mellett az automatikusan terjedő kártevők is nagy veszélyt jelentenek. A támadók gyakran használják ki a kártevők hatását, esetenként szándékosan indítanak útjára kártevőket annak érdekében, hogy a fertőzött számítógépek távolról irányítható (botnet) hálózatát használják fel későbbi támadásokhoz. A kártevők alapvetően két fő tényezőre alapozzák terjedésüket: Kihasználhatják a felhasználó hiszékenységét, esetleg hozzá nem értését és ráveszik arra, hogy az általa biztonságosnak hitt objektumba rejtett kártékony kódot lefuttassa. Másrészről a kártevők építhetnek a számítógépen futó operációs rendszerek és alkalmazások biztonsági réseire és akár a felhasználó tudomása és engedélye nélkül automatikusan is vezérléshez juthatnak.

További problémát jelent a személyek közötti kapcsolat. A Social Engineering módszereit felhasználva egy támadó ráveheti egy általa el nem érhető számítógép felhasználóját, hogy hajtson végre néhány műveletet a számítógépén. Akár például, hogy látogasson meg egy weboldalt, ahol persze korábban egy olyan kódot helyezett el, amivel aztán átveheti a vezérlést a számítógép felett.

Az alábbiakban egy olyan K+F projekt módszerét mutatjuk be, amelynek célja, hogy egy informatikai infrastruktúrának az aktuálisan elterjedt kártevőkkel szembeni veszélyeztetettségi mértékét meghatározza.

2 A projekt célja, indokoltsága, előnyei

A megvalósítandó projekt célja egy olyan on-line elérhető **szimulációs rendszer prototípusának a fejlesztése, mely alkalmas a számítógépes kártevők kockázatának elemzésére**. A kockázatelemzés révén lehetőség nyílik - a kártevőkre vonatkozó - folyamatosan változó biztonsági szint nyomon követésére, a leggyengébb láncszem azonosítására, illetve a számítógépes hálózatok, illetve a használt operációs, hálózati rendszerek valamint protokollok optimális megtervezésére. A rendszer bemenetét jelenti a hálózati topológia, hálózati kapcsolatok, használt protokollok részletes leírása. A kockázatelemzés ezek után a rendelkezésre álló adatok alapján, a kártevők elterjedtségi statisztikáit is felhasználva képes a kockázat elemzésére, a hálózat legveszélyeztetettebb pontjainak az azonosítására. Természetesen lehetőség van a hálózatra jellemző adatok módosítására, illetve a kártevők körének változásával a kockázatelemzés eredményeinek folyamatos követésére.

3 A megvalósítandó technológia elméleti háttere

A számítógépes hálózatokon keresztül történő, a számítógépek és a felhasználók kommunikációját kihasználó támadások egyre nagyobb veszélyt jelentenek. Ide tartoznak a leggyakrabban az e-mail üzenetekben terjedő kártevők, a célzott támadások botnet hálózatok igénybevételével vagy anélkül, és ide sorolhatjuk a social engineering alapú, a személyes kommunikációra épülő támadásokat is. Az alábbiakban a kommunikáción alapuló támadások, elsősorban a kapcsolatokra vonatkozó matematikai modellje kerül bemutatásra. A kommunikáció egyrészt a számítógépek közötti kapcsolatot jelenti, másrészt a számítógépek felhasználói közötti kommunikációt, illetve a számítógépek és a felhasználók közötti kapcsolatot is. A megtárgyalandó biztonsági modell alkalmas arra, hogy modellezze a támadási lehetőségeket. Segítségével azonosíthatók a támadó által elérhető pontok. A modell segítségével megállapíthatjuk, hogy a támadó által elérhető pontok közül melyek a legveszélyesebbek, azonosíthatjuk a kritikus kommunikációs csatornákat, protokollokat, így a modell lehetőséget ad arra, hogy megkeressük a biztonsági rendszerünk gyenge pontjait.

A kommunikációs csatornák biztonsága két kérdéskört érint. A középkorban a futárral történő üzenetküldés legnagyobb kockázatát az út során történő információszerzés jelentette. Ezért az információt titkosították, rejtjelezték. Egy támadó két támadási módszer közül választhatott. Mint passzív támadó lehallgatja az üzenetet, megfejti, és saját céljaira felhasználja, de NEM akadályozza az eredeti üzenet célba érkezését. Másrészt, mint aktív támadó megteheti azt is, hogy a lehallgatott információt módosítva küldi tovább, esetleg válaszol az eredeti üzenet küldőjének.

A középkorban még nem volt jelentős az a probléma, amit az jelenti, hogy a támadó ellenőrzése alá vonja az egyik végpontot (küldő vagy fogadó). Manapság azonban a csatorna lehallgatása mellett ez egy sokkal jelentősebb veszélyforrást jelent. A kommunikációs eszközök, az Internet gyors fejlődésével egy támadó valós időben felügyelheti a megtámadott eszközeit, illetve saját céljainak megfelelően befolyásolhatja működésüket.

3.1 A modell elemei

A gyakorlatban megvalósítandó biztonsági modell segítségével a számítógépeket, a rajtuk futó folyamatokkal, a számítógépeket felhasználó személyeket (legyen az egy laikus felhasználó vagy akár egy hozzáértő támadó), valamint a köztük lévő kapcsolatokat szeretnénk modellezni. A számítógépeken alkalmazások, folyamatok futnak. Minden egyes olyan folyamatot, amely képes arra, hogy online vagy offline módon más folyamatokkal kommunikációt létesítsen, entitásnak definiáljuk.

Az entitások között kommunikációs csatornákat feltételezünk, melyek alkalmasak arra, hogy a kommunikációs csatorna működését leíró szabályoknak megfelelően biztosítsa az üzenetek küldését. Online módon történő kommunikációt jelent, ha az adott entitás az őt tartalmazó számítógép segítségével valamely kommunikációs csatornán keresztül kommunikációt folytat egy másik számítógép valamely entitásával. Ez tipikusan az Interneten keresztül valósulhat meg. Egy ilyen kommunikációs csatornán üzenetek folyama zajlik, mely üzenetek szabályait a kommunikációs csatornához rendelt protokoll írja le.

Offline módon történő kommunikáció esetén egy entitás az őt tartalmazó számítógép háttértárán elhelyezett adatfájlt tölti be és értelmezi. Ebben az esetben a másik folyamat, amellyel a kommunikáció zajlik, az a folyamat, amely az adott adatfájlt létrehozta. Ez a

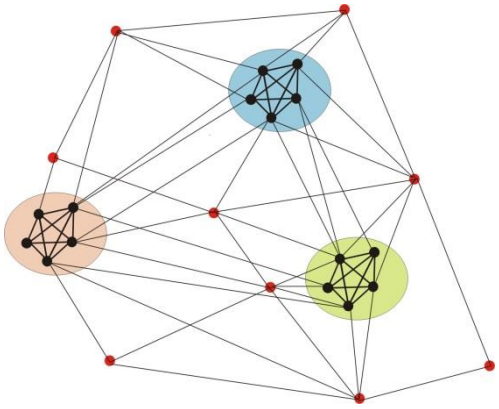
folyamat akár egy másik számítógépen is lehet és vagy valamilyen adathordozón vagy pedig valamely online kommunikációs csatornán juttatta el az adatfájlt a másik számítógépre. Ebben az esetben a kommunikációs csatorna szabályait az adatfájl formátumleírása jelenti.

A számítógépen futó folyamatok mellett az entitások körébe beleértjük magukat a számítógépet felhasználó személyeket is, ők is képesek arra, hogy más entitásokkal kommunikáljanak. A folyamatokkal való kommunikáció tipikusan a felhasználói bevitellel illetve az alkalmazások, folyamatok üzeneteivel valósulhat meg, de az is elképzelhető, hogy más felhasználóval alakítsanak ki kapcsolatot, vele kommunikáljanak (például: személyesen vagy telefonon).

Az egy számítógépen belül elhelyezkedő entitásokat, mint az entitások egy halmazát összetartozónak definiáljuk. Feltételezzük, hogy ha egy támadó sikeresen megtámadott egy entitást, akkor képes arra, hogy felügyelje, illetve befolyásolja az adott számítógéphez tartozó többi entitást is.

3.2 Gráf reprezentáció

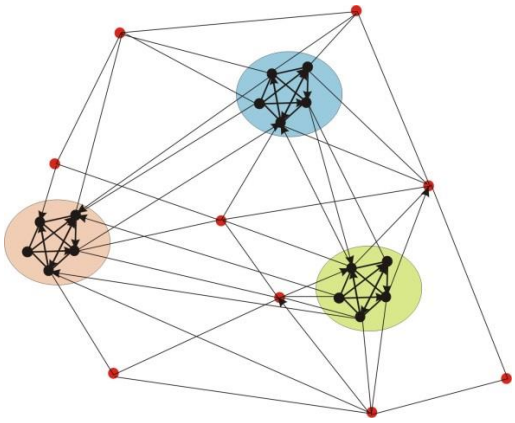
A biztonsági modell elemeit egy gráfként reprezentálhatjuk, ahol a csomópontokat az egyes entitások jelentik, melyek a számítógépeken futó folyamatokat, illetve magukat a számítógép felhasználó személyeket jelképezik. A csomópontok közötti élek jelképezik az entitások közötti kommunikációs csatornát. Két folyamat közötti kommunikáció valamilyen adatátvitelt jelent online vagy offline módon. Természetesen személyek között is lehet kapcsolat, hiszen bármely személy bármely más személlyel kapcsolatba kerülhet (például telefonon felhívja). A folyamatok és személyek közötti kapcsolat esetén lényeges megkülönböztetnünk a kommunikáció két irányát. Míg a számítógépek felhasználói a megfelelő beviteli mezők segítségével alakíthatják az egyes folyamatok működését, addig a folyamatok is küldhetnek üzenetet a felhasználónak.



13. ábra: Egy egyszerű gráfmodell

A piros pontok a felhasználókat a fekete pontok a számítógépeken belüli folyamatokat jelképezik. A színes ellipszisek az egy számítógépen belül, az összetartozó folyamatokat mutatják.

A kommunikációs csatorna irányainak a megkülönböztetésével a modell irányított gráffal történő reprezentálásához juthatunk. Ez sokkal élethűbben mutatja be a valós körülményeket, hiszen a protokollok esetén általában nem tekinthetjük egyformának a két irányt. Különösen igaz ez a szerver-kliens alapú kommunikáció esetén.



14. ábra: Irányított gráfmodell

Modellünk így azt mutatja, hogy mely entitások állnak egymással kapcsolatban. Az egyes irányított élekhez azonban súlyozást is rendelhetünk, attól függően, hogy az adott

kommunikációs csatorna megfelelő iránya mennyire alkalmas arra, hogy egy támadó megtámadjon egy másik entitást. Abban az esetben, ha ez az érték 0, akkor erre nincs lehetőség, és minél nagyobb, annál könnyebben kihasználható a csatorna.

3.3 Mátrix reprezentáció

A gráfmodell alapján elkészíthetjük modellünk mátrixreprezentációját is. Itt minden sornak és minden oszlopnak megfeleltetünk egy-egy entitást. A mátrixban lévő számok pedig a két csomópont közötti kommunikációs csatorna megfelelő irányához, mint a gráfbeli irányított élhez rendelt értéket jelentik.

Mindezek alapján, ha a mátrixban az értékeket úgy választjuk meg, hogy minden sorban az ott szereplő értékek összege pontosan 1 legyen, akkor a valószínűségszámítás bolyongási feladatainál ismert Markov-lánchoz juthatunk. Tekintsük ugyanis az entitások azon állapotvektorát, amely minden egyes entitáshoz tartalmazza azt az értéket, hogy az adott entitás mennyire támadható. Feltételezhetjük, hogy maga a támadó, mint személy is szerepel az entitások között, és kezdetben őt tekintjük egyedül veszélyesnek. Így a kezdeti állapotvektorban a támadónak megfelelő érték 1, a többi érték pedig 0.

Ekkor a kezdeti állapotvektor és az állapotátmenetet jelentő mátrix segítségével megkaphatjuk, hogy a támadó mely más entitásokat vonhat az ellenőrzése alá, illetve azt is, hogy ez milyen erőfeszítést jelent, mennyire könnyű ezt véghezvinnie.

Az állapot-átmeneti mátrixban szereplő a_{ij} érték tehát 0, ha nincs lehetőség arra, hogy az i. entitás felügyeletével rendelkező támadó megszerezze a j. entitás felügyeletét, egyébként $a_{ij} > 0$. Az a_{ij} érték a kommunikációs csatornára, a protokollra, illetve az i. és j. entitásra jellemző érték. Értékét több tényező befolyásolja:

- A kommunikációs csatorna, illetve kommunikáció szabályait leíró protokoll megbízhatósága, támadhatósága.
- A folyamatot jelentő j. entitás megbízhatósága, biztonsági rései, az azokra vonatkozó javítások. Nem mindegy például, hogy a Microsoft Outlook Express sok évvel ezelőtti

5-ös verzióját, vagy például a jóval biztonságosabb The Bat levelezőt használjuk. Az összehasonlítás alapja az ilyenkor az adott alkalmazásra vonatkozóan a napvilágot látott sérülékenységek száma, típusa, illetve ezek trendje.

- Amennyiben a j. entitás személy, úgy az ő hiszékenysége is befolyásolja az a_{ij} értéket.
- Befolyásoló tényező lehet maga az idő, hiszen egy biztonsági rés ismertté válásával a támadhatósági lehetőség is növekszik.

4 Biztonsági megfontolások

Az ismertetett biztonsági modell segítségével a támadó lehetőségei könnyen vizsgálhatóak. Ez nem csupán az informatikai jellegű támadásokat, hanem a social engineering adta módszereket is jelenti. Vegyük észre, hogy ha egy támadó a támadást egy belső személy segítségével szeretné véghezvinni, akkor az ő meggyőzésére számos módszer közül választhat:

- Megteheti, hogy például telefonon felhívja és egy megbízható személynek kiadva magát ráveszi a gyanútlan belső személy, hogy látogasson el egy weboldalra.
- Az átverő üzenetet akár emailben is elküldheti.
- Igénybe veheti egy kártevő segítségét, amely akár hasonló eszközzel próbál hatni a belső munkatársra.
- Személyesen is megpróbálhatja rávenni, hogy a támadó által megadott cselekvéssort hajtsa végre a számítógépén.

A modell segítségével jól vizsgálhatók azok a problémák, amelyek azon alapulnak, hogy egyes kommunikációs csatornákhoz tartozó protokollok más szabály szerinti formátumú adatfolyamot szállítanak valamely entitáshoz. Például egy JPEG képet az SMTP vagy a HTTP protokoll szállíthat a célszámítógép valamely képkezelő alkalmazása számára.

5 Összegzés (III. fejezet)

A III. fejezetben ismertetett modellezési eljárás segítségével lehetőség van egy informatikai infrastruktúra veszélyeztetettségi mértékének a meghatározására, illetve ennek folyamatos monitorozására. A modell szerinti eljárás fő bemeneti paramétercsoportjait képezik

(1) az infrastruktúra felépítése, topológiája, hardver és szoftver összetevői,
(2) a felhasználói (elsősorban a biztonságtudatosságra vonatkozó) magatartás paraméterei,
(3) az adott időpontban az elterjedt és valós fenyegetések működési elve, tulajdonságai.

A módszer nemcsak abban adhat segítséget, hogy felhívja a figyelmet a biztonsági szint fokozására, hanem hatékony támogatást is képes adni például az aktuális fenyegetésekkel szembeni leggyengébb láncszem azonosítására.

6 Ábrajegyzék (III. fejezet)

7 Irodalomjegyzék (III. fejezet)

[1] R., Szabó : "TCP/IP Networks and IP Telephony" in dr. G., Gordos ed. *Telecommunications Networks and Informatics Services,* , Scientific Association for Infocommunications Hungary, pp.394-402 http://www.hte.hu/ob/eng/hte_ob_eng.pdf

[2] *ITU-T Y 2011/(10/2004) Next Generation Networks – Frameworks and functional architecture models* ITU-T / ATIS Workshop "Next Generation Technology and

Standardization“ Las Vegas, 19-20 March 2006. http://www.itu.int/ITU-T/ngn/introduction.html

[3] *Microsoft Security Bulletin* MS04-028, http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx, 2006.

[4] Microsoft Security Advisory (912840), http://www.microsoft.com/technet/security/advisory/912840.mspx, 2006

[5] Microsoft Security Bulletin MS02-072, http://www.microsoft.com/technet/security/Bulletin/MS02-072.mspx, 2002

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.