

ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel



Incidens-menedzsment gyakorlat

Hadarics Kálmán



Nemzeti Közszerológati Egyetem



MAGYARY
PROGRAM

Budapest, 2014

Tartalom

Kivonat	5
1. Bevezetés.....	6
2. Az incidens-menedzsment helye az ITIL szolgáltatás-menedzsment modellben	7
2.1. Az ITIL v3 szolgáltatási életciklus szakaszai	7
2.2. Szolgáltatás üzemeltetése	9
2.3. Esemény, incidens vagy probléma megkülönböztetése gyakorlati szempontból	11
2.3.1. <i>Az esemény menedzsment</i>	11
2.3.2. <i>Az incidens-menedzsment</i>	13
2.3.3. <i>A probléma menedzsment</i>	14
2.4. Az incidens menedzsmenthez közvetlenül kapcsolódó törvényi szabályozás	14
2.5. Az incidens és incidens menedzsment definíciója az ITIL terminológia szerint	15
2.6. Az incidens menedzsmenthez fontossága.....	17
3. Az incidens-menedzsmenthez kapcsolódó csoportok és feladataik	19
3.1. Az IRT létrehozása	19
3.1.1. <i>Az IRT hatásköre</i>	20
3.1.2. <i>Az IRT felső szintű menedzsment támogatása</i>	21
3.1.3. <i>Az IRT megfelelő finanszírozása</i>	22
3.2. Az IRT helye a szervezetben	25
3.3. Központi, Elosztott és Virtuális csapatok.....	26
3.4. Szabályok és eljárások fejlesztése	27
3.4.1. <i>Az incidensek osztályozása és kezelése szabályzat</i>	29
3.4.2. <i>Információosztályozás és védelem</i>	31
3.4.3. <i>Információk terjesztése (disszeminációja)</i>	32

3.4.4.	<i>Információk megtartása és megszüntetése</i>	32
3.4.5.	<i>Titkosítás használata</i>	34
3.4.6.	<i>Együtműködés külső szervezetekkel</i>	35
4.	Teendők egy támadás esetén	36
4.1.	Az incidens kezelés lépései	36
4.1.1.	<i>Személy hozzárendelése az incidenshez</i>	37
4.1.2.	<i>Külső hatóság bevonása</i>	37
4.1.3.	<i>Az incidens komolyságának a meghatározása</i>	38
4.1.4.	<i>Az incidens hatókörének meghatározása</i>	41
4.1.5.	<i>Távoli diagnózis és telefonos beszélgetés</i>	43
4.1.6.	<i>A probléma megoldása</i>	44
4.1.7.	<i>POST-MORTEM analízis</i>	47
5.	Az incidens-menedzsmenthez kapcsolódó alkalmazások	50
5.1.	A naplózási szolgáltatás.....	50
5.2.	Számítógépes „nyomelemzés” (forensics)	52
5.3.	Incidens-menedzsmenthez fejlesztett szoftver	53
6.	Összefoglalás, összegzés	56
	Irodalomjegyzék	57

Kivonat

Jelen jegyzet a Nemzeti Közszerológáti Egyetem (NKE) Elektronikus Információbiztonsági Vezető (EIV) szakirányú továbbképzés keretében, az Incidens-menedzsment gyakorlat nevű tárgy keretében elsajátítandó ismereteket foglalja össze.

A képzés során az elektronikus információs rendszer biztonságáért felelős személyek megismerhetik azokat a problémákat, amelyekkel az incidens-menedzsmenttel kapcsolatban a gyakorlatban jelentkeznek.

A jegyzet felépítése, fő fejezetei:

- Az incidens-menedzsment helye az ITIL szolgáltatás-menedzsment modellben
- Az incidens-menedzsmenthez kapcsolódó csoportok és feladataik
- Teendők egy támadás esetén
- Az incidens-menedzsmenthez kapcsolódó alkalmazások

A jegyzet szervesen kapcsolódik az „Incidens-menedzsment, BCP, DRP integráció” nevű tárgy tartalmához. Ebben olvashatunk az Incidens-menedzsment elméletéről, jelen jegyzet gyakorlati szempontból közelíti meg a témakört. Segít abban, hogy az incidens-menedzsment bevezetéséhez szükséges gyakorlati szempontokat megértsük és ez alapján képesek legyünk az incidensek kezelését végző csapatban dolgozni, működésüket felügyelni, irányítani.

1. Bevezetés

Ahogy az információs rendszerek az élet minden területén megjelennek, kiemelt figyelmet kell fordítani e rendszerek biztonságára, az egyes szolgáltatások üzemeltetésére. Bármely ember alkotta rendszer működése során jelentkezhetnek hibák, problémák, amelyek sokrétűek lehetnek. Tisztában kell lennünk azzal, hogy manapság egyre inkább rá vagyunk kényszerítve/kényszerülve ezen szolgáltatások használatára. A rendszerek komplexitása megköveteli, hogy rengeteg különféle probléma elfordulására és megoldására fel kell készülnünk. Ezen problémák egy része a normál használat során jelentkezik (Például: program hibák), míg mások valamilyen konfigurálási hiba vagy támadás eredményeképpen. Szükség van egy olyan informatikai rendszerre, amely képes az incidensek érzékelésére, kezelésükre, és nyomon követésükre. Fontos, hogy egy incidens ne készületlenül érjen bennünket. A megoldási, helyreállítási folyamat során sokat segít, hogyha megértjük a probléma okát, és a problémával kapcsolatos döntést kellő körültekintéssel végezzük.

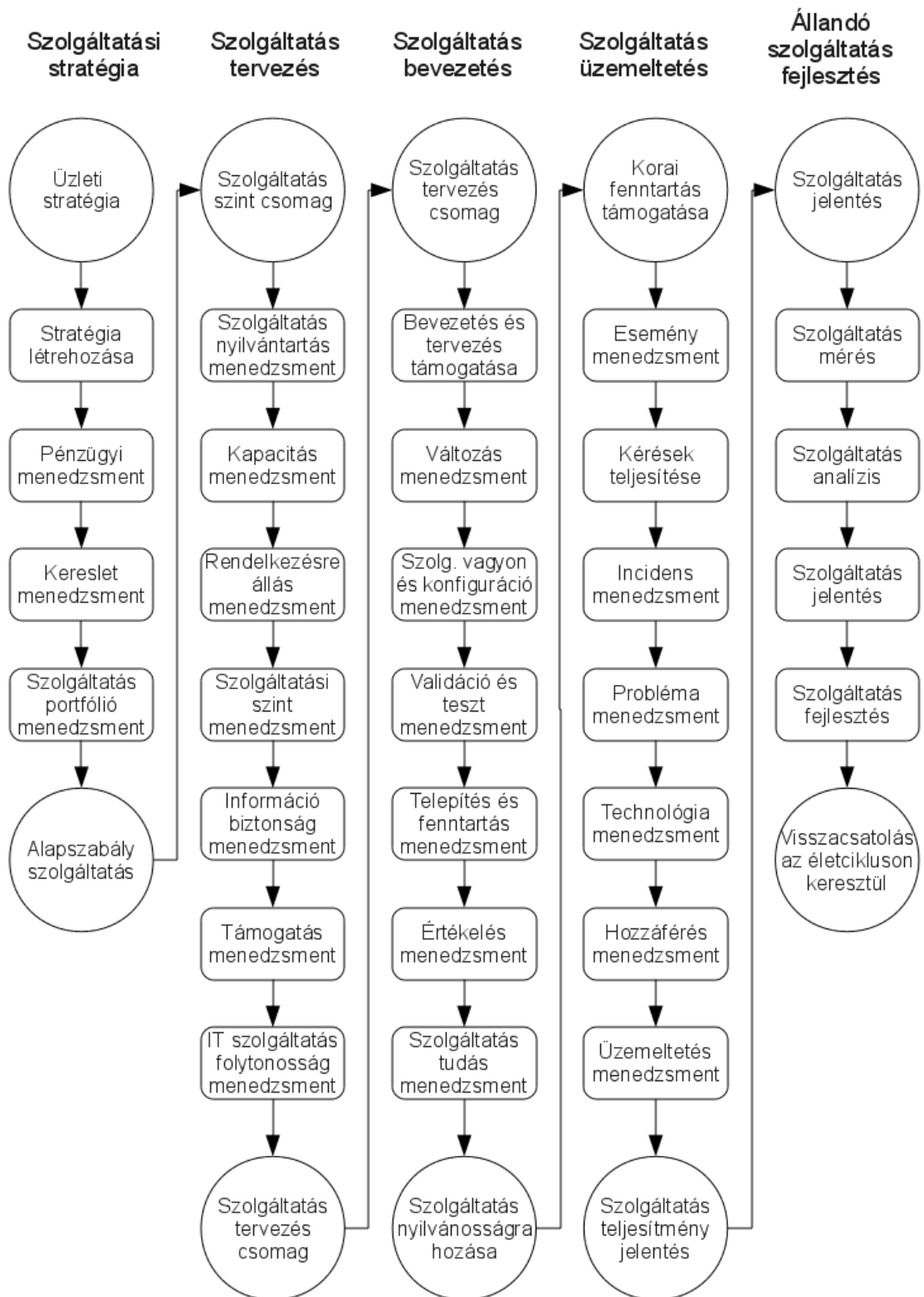
2. Az incidens-menedzsment helye az ITIL szolgáltatás-menedzsment modellben

Az Information Technology Infrastructure Library (ITIL) a szolgáltatás-menedzsment bevált gyakorlatának gyűjteményeként fogható fel. Az úgynevezett szolgáltatási életciklus egy jól körülhatárolt keretrendszert biztosít a szolgáltatás-menedzsment szervezéséhez. Ezen módszertan megismerése szükséges ahhoz, hogy el tudjuk helyezni az incidens-menedzsmentet a szolgáltatás-menedzsmenten belül, és lássuk, hogy miért is fontos ez egy intézmény vagy vállalat életében.

2.1. Az ITIL v3 szolgáltatási életciklus szakaszai

Az ITIL v3 esetében öt szolgáltatási életciklus szakaszt különböztethetünk meg (1. ábra):

- szolgáltatási stratégia (service strategy)
- szolgáltatás tervezése (service design)
- szolgáltatás bevezetése (service transition)
- szolgáltatás üzemeltetése (service operation)
- szolgáltatás állandó fejlesztése (continual service improvement)



1. ábra ITIL v3 Szolgáltatási életciklusok

Szolgáltatás stratégia: A szolgáltatásokat üzleti szempontból kell megközelíteni. Az üzlet az elsődleges, amelyet az informatika, informatikai rendszerek kiszolgálják, elősegítenek. Bármely szervezetnek vannak céljai, amelyeket szeretne elérni. A szolgáltatás stratégiának tartalmaznia kell azt, hogy ezt a célt hogyan lehet elérni. Ezen túl fontos szerepet tölt be a szolgáltatás stratégia abban is, hogy miként lehet az üzleti stratégiát IT stratégiává átfordítani.

Szolgáltatás tervezése: Az IT szolgáltatási megoldás tervezés az IT policy és architektúra létrehozási és kezelési vezérelveit tartalmazza. Ide tartozik például, hogy adott feladatok milyen módon (insourcing, outsourcing, cosourcing) legyenek megvalósítva.

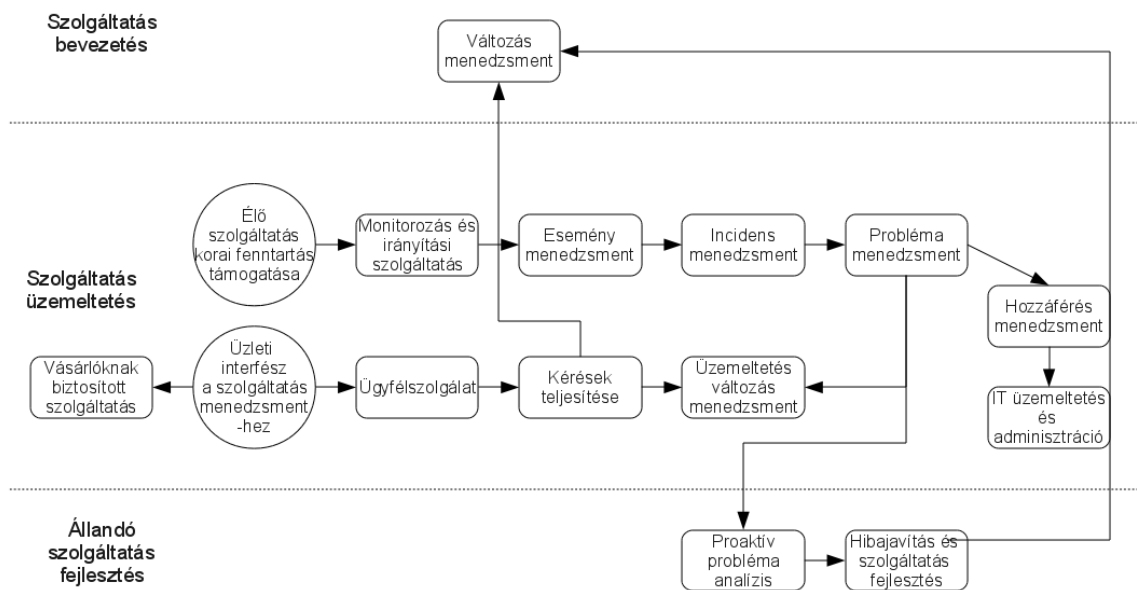
Szolgáltatás bevezetése: A szolgáltatás bevezetése tartalmazza a hosszú távú változáskezelés és a verziókkal kapcsolatos gyakorlatot. Ezen túl fontos, hogy egy adott szolgáltatást le kell képezni egy konkrét üzleti (termelési) környezetbe.

Szolgáltatás üzemeltetése: Az adott szolgáltatás biztosításával és a szolgáltatás stabilitásával foglalkozik. Ez a későbbiekben bővebben ismertetésre kerül, mivel az incidensmenedzsment ennek a részeként értelmezhető.

Szolgáltatás állandó fejlesztése: Az üzleti szolgáltatás menedzsment fejlesztésével foglalkozik. Ezen kívül a bevezetett szolgáltatások tökéletesítésével.

2.2. Szolgáltatás üzemeltetése

A szolgáltatás üzemeltetés célja, hogy koordinálja és valósítsa meg azokat a tevékenységeket és folyamatokat, amelyek lehetővé teszik, hogy az üzleti felhasználók megfelelő szolgáltatási szintnek megfelelően (SLA: Service Level Agreement) igénybe vegyék a szolgáltatást.



2. ábra ITIL v3 Szolgáltatás üzemeltetés

A szolgáltatás üzemeltetés folyamat esetében az alábbi elemeket különböztethetjük meg:

- eseménymenedzsment (event management)
- incidensmenedzsment (incident management)
- problémamenedzsment (problem management)
- szolgáltatási kérések teljesítése (request fulfilment)
- hozzáférés-menedzsment (access management)

A korábbiakban felsorolt folyamatok önmagukban nem jelentik a szolgáltatás üzemeltetés hatékony működését. Egy stabil infrastruktúra és megfelelően képzett személyzetre is természetesen szükség van. A személyzet esetében több csoportot definiálhatunk, amelyek adott célfeladatra koncentrálnak.

Ezek mindegyike szükséges a megfelelő szolgáltatás üzemeltetéséhez:

- Ügyfélszolgálat (Service desk vagy Help desk)
- Technikai menedzsment (Technical management)
- IT műveletek menedzsmentje (IT operations management)

- Alkalmazás-menedzsment (Application management)

A szolgáltatás üzemeltetésének ezen kívül kell, hogy kapcsolódjon a szolgáltatási életciklus többi lépéséhez.

- Változás-menedzsment (Change Management)
- Kapacitás- és Hozzáférhetőség-menedzsment (Capacity and Availability management)

2.3. Esemény, incidens vagy probléma megkülönböztetése gyakorlati szempontból

A köznapi szóhasználatban gyakran keverednek az alábbi fogalmak: esemény, incidens és probléma. Fontos azonban, hogy ezeket meg tudjuk különböztetni egymástól, és lássuk azt is, hogy ezek milyen módon kapcsolódnak egymáshoz.

2.3.1. Az esemény menedzsment

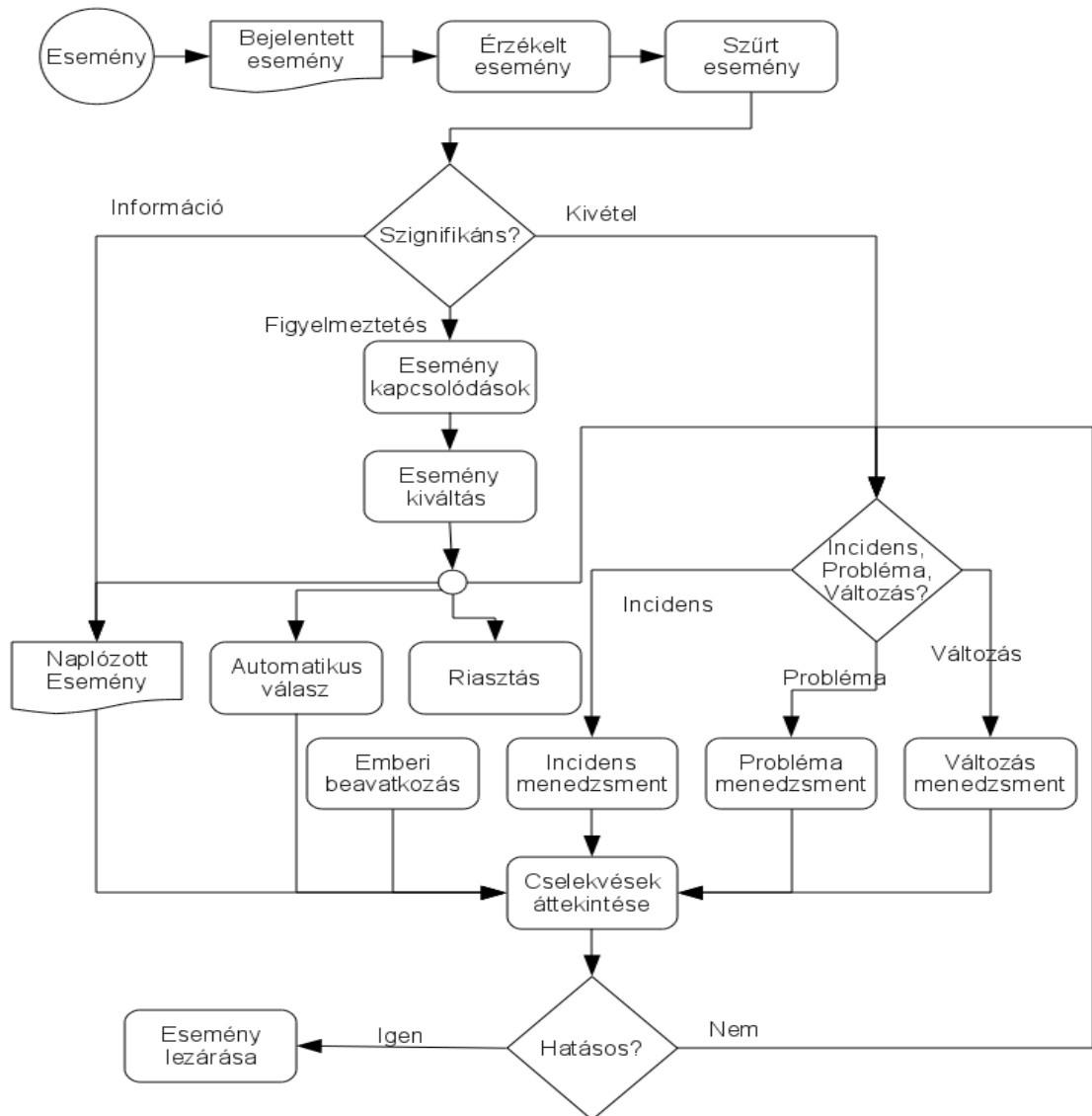
Az informatikai szolgáltatás üzemeltetésre tekinthetünk egyrészt a szolgáltató, másrészt pedig az ügyfél szempontjából. A kettő más-más szempontból közelíti meg a szolgáltatás-üzemeltetést.

A szolgáltatónak ez egy olyan felelősségteljes folyamat, amelynek a célja az ügyfél kiszolgálása a szolgáltatás menedzsment életciklus során úgy, hogy optimalizálja a költségeket és a szolgáltatási minőséget.

Az ügyfél számára pusztán a saját igényeinek a legmagasabb szintű kielégítése a cél a legkisebb ráfordítás árán.

Amennyiben a szolgáltatás nyújtás közben minőségi hiba történik, akkor az kihatással van a szolgáltatás-üzemeltetés céljára. Bekövetkezik egy úgynevezett esemény. Az esemény egy külső vagy belső hatás, amely miatt a szolgáltatás minőségében változás történik.

Természetesen az informatikai-szolgáltatás nyújtást is monitorozni lehet, amelyben a normális aktivitást megtörhetik bizonyos jelenségek. Például ha egy adott időpontban többen hívták a termék támogató központot, vagy többen keresték az ügyfélszolgálatot, ezt hívjuk eseménynek és az informatikai szolgáltatás ezen területével foglalkozó feladatokat összefoglalóan *esemény menedzsmentnek* (event management).



3. ábra Az esemény menedzsment folyamata

Az események bekövetkezésekor a következő tevékenységek elkerülhetetlenek:

- Esemény észlelése. Ez a legfőbb cél, hogy egyáltalán észlelni tudjuk az eseményeket. Ezért fontos a szolgáltatás monitorozása.
- Események csoportosítása, hatásfok szerint, rendszeresség szerint. Fontos tudni, hogy nem minden eseményből lesz incidens vagy probléma. Vannak események, amelyek csak informatív jellegűek, tudnunk kell róluk, de azonnali beavatkozást nem igényelnek.
- Esemény kiváltó okok vizsgálata.
- Események közti összefüggések vizsgálata.
- Valamilyen intézkedés, válaszadási procedúra.

2.3.2. Az incidens-menedzsment

Az események mögött általában valamilyen incidensek állnak. Az incidens lehet hiba, egy kérdés vagy új kérés is. Hagyományosan csak a hibákat szoktuk incidensnek nevezni, de ez egy téves szóhasználat. Egy incidens azonnali beavatkozást igényel. Olyan szinten kilengett a szolgáltatás minősége, hogy azt azonnal (a lehető legrövidebb idő alatt) helyre kell állítani, erről szól az incidens menedzsment (incident management).

Amikor incidens menedzsmentről beszélünk, a folyamatok már különböznek az esemény menedzsmenthez képest:

- Az incidens azonosítása.
- Az incidensről egy hibajegyet kell rögzíteni
- Az incidensek osztályozása (hiba, kérdés, kérés, módosítás, s a többi).
- Az incidensek fontossági rangsorolása (normál, sürgős, SOS).
- Előzetes diagnózis.
- Feladatok kiosztása, eskaláció (1st line support, technical support, s a többi). Ez az eskaláció történhet funkcionálisan, de hierarchikus eskaláció is lehet, lényegében menedzsmenti szinten kell tudni ezekről az incidensekről, mert lehet, hogy nem csak technikai, hanem vezetői szintű beavatkozás is szükséges

- Megoldás és lezárás.
- Post-mortem analízis.

2.3.3. A probléma menedzsment

A *probléma* viszont az incidens mögötti ok, amit egy incidensből nem is feltétlenül lehet kideríteni. Az informatikai szolgáltatás nyújtása során fellép egy hiba (incidens), a hibát a support (1st line, 2nd line, 3rd line) javítja is, de nem tudják garantálni, hogy máskor nem fog előfordulni. Ha nem sikerült feltárni az okát az incidensnek, elfedték a következményt, azaz kijavították a hibát, de lehet, hogy másnap ismét előjön. Egy adott probléma felderítéséhez nagyon sok körülményt kell ismerni és közel sem biztos, hogy a probléma teljesen feltárható. A problémák feltárásának van egy másodlagos haszna is, létrejön egy adatbázis az úgynevezett ismert hibákról, amelyek segítséget nyújthatnak a 1st line supportnak abban, hogy az incidensekre még gyorsabb választ adhassanak.

Amikor úgynevezett *probléma-menedzsmentről* (problem management) beszélünk, akkor legalább két folyamatról beszélünk:

- Reactive (visszaható) Problem Management: amikor a rendelkezésre információk alapján utólag tárjuk fel és elemezzük a problémát.
- Proactive (kezdemenyező) Problem Management: előzetes elemzése a lehetséges problémáknak.

2.4. Az incidens menedzsmenthez közvetlenül kapcsolódó törvényi szabályozás

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról definiálja a biztonsági esemény fogalmát:

biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;

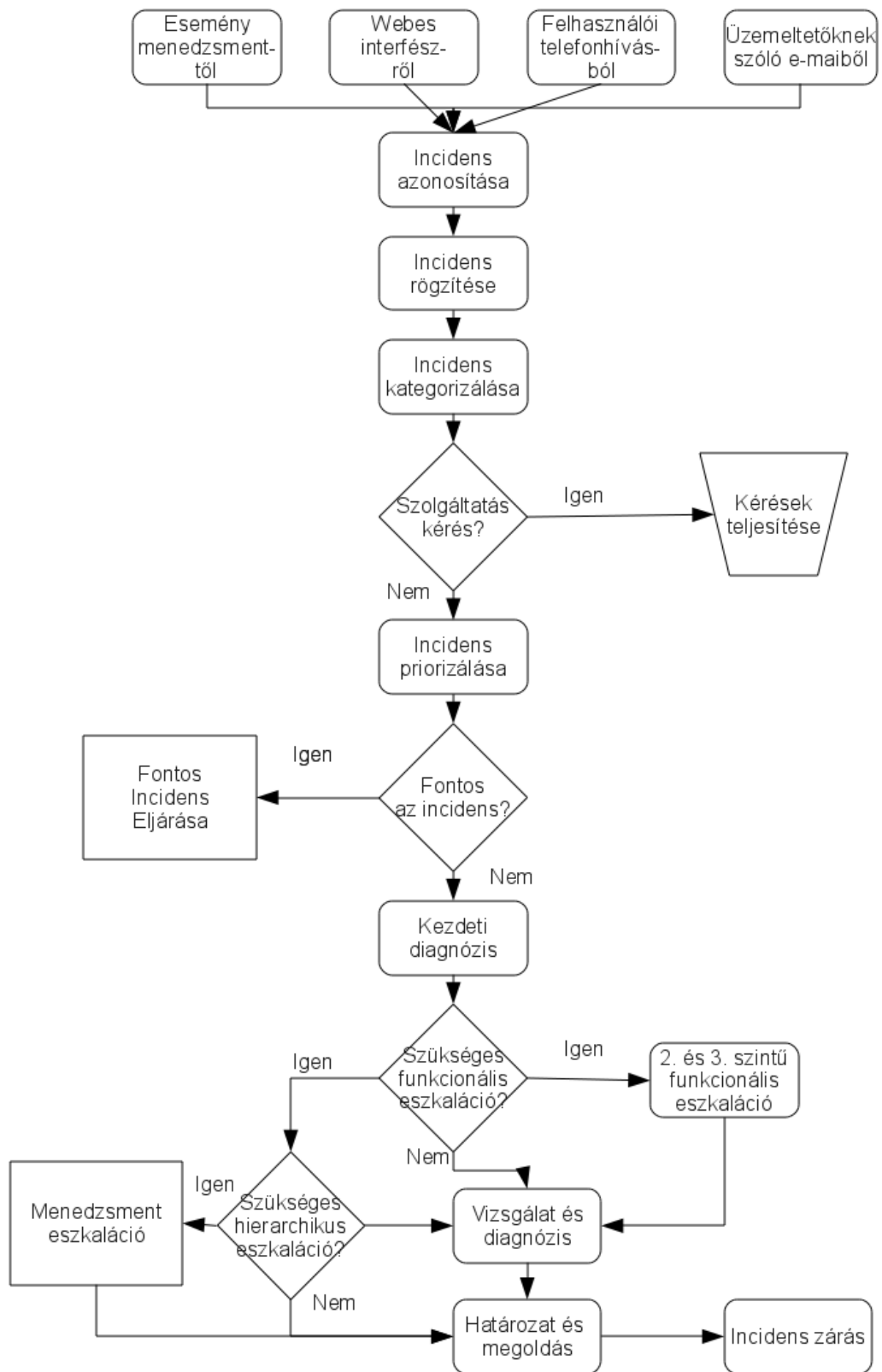
számítógépes incidenskezelő központ: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, számítástechnikai vészhelyzetekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal és akkreditációval rendelkezik (európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team));

2.5. Az incidens és incidens menedzsment definíciója az ITIL terminológia szerint

Az incidens egy előre nem tervezett megszakítása az IT szolgáltatásnak vagy az IT szolgáltatás minőségének csökkenése. Egy hardver elem működési hibája, amely még nincsen hatással a szolgáltatásra, az is incidensnek tekinthető. Ilyen például, amikor egy RAID1 kötet egyik lemeze meghibásodik.

Az incidens menedzsment az a folyamat, amely az összes incidenssel foglalkozik:

- ez tartalmazza a hardver/szoftver hibákat
- a felhasználói kérdéseket/kéréseket (amelyek az ügyfélszolgálaton keresztül érkeznek)
- a technikai személyzet általi kérések/kérdéseket
- az automatikusan érzékelt és jelzett eseményeket, amelyek az eseménymonitorozó eszközöktől érkeznek



4. ábra Az incidens menedzsment folyamata

2.6. Az incidens menedzsmenthez fontossága

Néhány cég és szervezet az gondolja, hogyha megvásárolják a jelenleg a piacon elérhető legjobb biztonsági eszközöket, tűzfalakat, akkor az informatikai biztonsággal kapcsolatban egyéb tennivalójuk nincsen. Ez természetesen nem így van. A technológia nem csodaszer, bár kétség kívül a különböző gyártók, különböző termékei között biztonsági szempontból jelentős különbségek vannak. Az informatikai rendszerekben előforduló események analizálásához, megértéséhez, következtetések levonásához feltétlenül szükséges a megfelelő szaktudás és tapasztalat. A megfelelő feladatkörök definiálása és leosztása nélkül nem képzelhető el az incidens-menedzsment.

Gyakorlati szempontból az alábbi okok miatt szükséges különös figyelmet fordítani az incidens-menedzsmentre:

Üzleti hatások:

Manapság az internet elterjedésével egyre több kommunikáció elektronikus az interneten keresztül történik. Mondhatjuk azt, hogy a normál ügymenetnek, a különféle folyamatoknak az internet használata szerves részét képezi. Bármilyen nem várt kimaradásnak, szolgáltatás kiesésnek komoly anyagi következményei lehetnek. A cég üzleti titkainak kiszivárgása, vagy az ügyféladatbázisához való illetéktelen hozzáférés egy cég szempontjából különösen veszélyes lehet. Az utóbbi néhány évben szinte minden nagyobb vállalat esetében történt már biztonsági incidens. Valahol ez napvilágra került és tanultak belőle, levonták a következményeket, míg mások esetleg abban a hitben élnek, hogy velük ilyen nem történhet, miközben érzékeny adataikat folyamatosan eltulajdonítják. Ha létezik incidens-menedzsment, akkor egy-egy nem várt esemény kapcsán hamarabb helyre állhat a rend, a várható kár jóval kisebb lesz.

Jogi szabályozás:

Különböző állami és önkormányzati szervezeteknél a hatályos törvények és rendeletek (Például: 73/2013 (XII.4) NFM rendelet, 301/2013 (VII.29.) Korm. rendelet) megkövetelik, hogy rendelkezzen a szervezet incidens-menedzsmenttel, és köteles ezeket jelenteni a 2013. évi L. törvénynek megfelelően.

„Megáll az élet”:

Nagyon sok cég esetében az ügyfelekkel való kapcsolattartás gyakran a cég honlapján keresztül történik. Ha ez valami miatt elérhetetlenné válik akár ideiglenesen, akár hosszabb időre, akkor a cég egyes folyamatai megállnak. Ilyen történhet például DDoS típusú támadások esetében, amikor nagyon belassulhat, extrém esetben teljesen leállhat az adott honlap. Ilyen támadás esetében kiemelten fontos az országos és/vagy nemzetközi biztonsági szervezetekkel (CERT (Computer Emergency Response Team))-el való kapcsolattartás, akik képesek arra, hogy segítsenek a támadók felkutatásában és a támadás visszaszorításában, megszüntetésében.

3. Az incidens-menedzsmenthez kapcsolódó csoportok és feladataik

Akarva, akaratlan számítógépes támadások mindig is lesznek. Nem lesz mindig minden támadás sikeres, de az elkövetők keresik a lehetőségeket. Ahol lehetőség van adott rendszer kompromittálására, az előbb-utóbb be is fog következni. Miután valaki megtámadtak, szükséges valamiféle reakció az adott támadásra a további támadások és károk megelőzése érdekében. Ez a reakció nem lehet egy ad-hoc folyamat. A támadás súlyosságához mérten a korábbi tervek (BCP, DRP) figyelembe vételével kell a szükséges feladatokat elvégezni.

Azt a csapatot vagy csoportot hívjuk IRT-nek (Incident Response Team), akik a szervezeten kívülről vagy belülről érkező támadási kísérletekkel foglalkoznak. Az ő elsődleges feladatuk, hogy szembe szálljanak a számítógépes incidensekkel és kritikus helyzetekben képesek legyenek a megfelelően megalapozott döntések meghozatalára. Egy ilyen team állhat néhány főből, azonban nagyobb szervezetek esetében akár százas nagyságrendű taggal is rendelkezhet.

3.1. Az IRT létrehozása

Egy IRT létrehozási folyamatában az alábbi különböző lépéseket kell elvégeznünk:

1. Az IRT hatáskörének definiálása
2. Biztosítani kell a felső menedzsment támogatását
3. Megbízható költségvetésre van szükség
4. Az IRT-t a szervezeti hierarchia részévé kell tenni
5. Meg kell határozni, hogy a csapat központi, elosztott vagy virtuális legyen
6. Szabály és eljárás gyűjteményt kell fejleszteni

3.1.1. Az IRT hatásköre

Az IRT létrehozásának első lépése annak a meghatározása, hogy kiket fog az IRT képviselni, illetve kik lesznek a tagjai. Milyen támadásokkal foglalkozik? Csak belső tagjai vannak, vagy az adott szervezet szempontjából vannak külső tagjai is? Ha vannak külső tagok, hogyan történik a külső tagok kiválasztása?

Ezek alapján néhány létező megoldás IRT esetében:

- *Szervezeten belüli:* Csak az adott szervezet felé irányuló támadásokkal foglalkozik, illetve azokkal, amelyek kiindulási pontja az adott szervezet. Gyakran hívják egy szervezet esetében IT Security Team-nek.
- *Szervezeten kívüli:* Ebben az esetben a támadásokat egy külső cég, általában az adott eszköz/szoftver gyártója alkotja. A vizsgálataik pedig adott eszközre/szoftverre terjednek ki.
- A szervezet szempontjából az előzők keveréke:
 - *Adott AS (Autonomous System)-hez tartozó:* Minden olyan támadás, amely útválasztási szempontból adott adminisztratív tartományhoz tartozik.
 - *Adott felsőbb szintű domain névhez tartozó:* Minden olyan támadás, amely adott tartománynévvel lefedett hálózatba vagy innét érkezik. Egy ilyen hálózatban több különböző tipikusan oktatási, kutatási, kulturális intézmény tartozik.
- *Nemzeti:* Ebben az esetben adott nemzet tagjai, vagy adott országban működő cégek kérhetik a nemzeti CERT csapat segítségét.
- *Nemzeti kritikus infrastruktúra:* Csak adott országon belül a kritikus infrastruktúrával foglalkoznak.
- *Adott szolgáltatást megvásárló szervezetek:* Amely szervezet megvásárol egy bizonyos szolgáltatást, akkor azzal együtt a szolgáltatáshoz biztonsági támogatást is kap a szolgáltatást üzemeltető cégtől.

Elképzelhető, hogy adott hatáskör egyszerre több szervezet hatáskörébe is tartozhat. Ilyenkor hatáskör átfedésről beszélhetünk. Egy IRT hatáskörének a definiálása a felsőbb szintű menedzsment hatásköre. Az ő feladatuk, hogy igyekezzenek csökkenteni az IRT-k közti átfedéseket, így az egyes csapatok hitelesen tudják ellátni feladataikat és kialakulhasson a felhasználók általi bizalom.

3.1.2. Az IRT felső szintű menedzsment támogatása

Kritikus lépés az IRT létrehozásakor, hogy rendelkezzen a felsőbb szintű menedzsment támogatásával. Ez szükséges többek között a csapat hitelességének elnyeréséhez. A legjobb, hogyha van valaki a felsőbb menedzsmentben, aki hisz az IRT és szolgáltatásainak fontosságában, és egyidejűleg az IRT tagja is. Így könnyebb a kommunikáció és az IRT problémáinak a megértése a felsőbb menedzsmenttel. Ezen személy sok esetben megegyezik a CIO (Chief Information Officer)-val, aki az adott szervezet informatikai vezetőjének tekinthető.

Az IRT team azon tagját, aki a felsőbb menedzsmenttel való kapcsolattartást a továbbiakban IRT szponzornak hívjuk. Egy ilyen szponzor legfontosabb feladatai:

- A team hitelességének a fenntartása és képviselete a felsőbb menedzsment irányába. Az IRT képviselete a különböző bizottságokban.
- Krízis esetében a menedzsmenttel való kapcsolat tartása, az egyes krízissel kapcsolatos döntések előkészítése. A menedzsment megnyugtatása krízis esetében, a túlreagálások tompítása. Lehetővé tenni, hogy az IRT megfelelően tudja kezelni a krízist.
- Szakértői vélemény készítése az új stratégiák és szolgáltatások biztonságával kapcsolatban. Mit jelentenek adott új kezdeményezések biztonsági incidensek szempontjából? Például szeretnénk azt, hogy a munkavállalók otthonról is elérhessenek bizonyos vállalati erőforrásokat. Ennek milyen incidenskezeléssel kapcsolatos kockázatainak vannak?
- Az IRT költségének megfelelő szinten tartása.

3.1.3. Az IRT megfelelő finanszírozása

A megfelelő költségvetés feltétlenül fontos és szükséges egy IRT működéséhez. Az IRT működéséhez szükség van biztonságos helyszínre, megfelelő felszerelésekre, könyvekre, és arra, hogy a tagok tudjanak új ismereteket elsajátítani és utazni, hogy tapasztalatokat cseréljenek. Mondhatjuk azt, hogy egy sikeres IRT működéséhez sok erőforrásra van szükség.

Amíg például a legtöbb dolgozó munkájához elég egy számítógép, addig egy IRT tagnak minimum kettő vagy három számítógépre van szüksége. Ezen felül kellene különféle hálózati eszközök (switch, router, tűzfal, s a többi), amelyek segítségével izolált környezetben tudnak különféle kártevőket megfigyelni és analizálni. Ezen kívül naprakésznek kell lenniük, ami csak könyvek és képzések segítségével valósítható meg. Az utazások száma manapság jelentősen csökkenthető amennyiben videokonferencia rendszereken keresztül kommunikálnak más IRT-vel vagy vesznek részt különböző konferenciákon.

A cégen belüli költségek figyelembe vételével az alábbi finanszírozási módszereket különböztethetjük meg:

1. Az IRT mint költség központ

Egy vállalat szempontjából az IRT nem hoz pénzt a szervezetnek, csak szükséges, és emiatt viszi a pénzt. Nem könnyű annak a megállapítása, hogy mennyi legyen a megfelelő költségösszege. Itt elsősorban ezt célszerű figyelembe venni, hogy mennyi pénz maradt meg a cégnél amiatt, hogy IRT-t működtet, és az incidensek megfelelő kezelése révén sikerült az incidenseket minimalizálni. Tehát az IRT megakadályozta, hogy bizonyos incidensek bekövetkezzenek, illetve a lehető legkisebb anyagi veszteséggel kezelte a bekövetkezett incidenseket.

Az IRT működésében megkülönböztethetünk direkt költségeket és indirekt költségeket.

Direkt költségként jelentkeznek például:

- A munkaórák száma, amit adott incidens kezelésével kellett eltöltenie az IRT tagjainak.
- A munkaidő kiesés, ami bekövetkezett adott számítógép vagy alkalmazás esetében, amit egy incidens miatt nem lehetett használni.
- Egy kiesés miatt milyen hiányok jelentkeztek a késedelmes fizetések miatt, illetve az emiatt történő szállítások csúszásából adódóan.
- Az incidens miatt meghibásodott berendezések.

Indirekt költségként jelentkeznek például:

- A szervezet megítélésében, „imázsában” történt negatív változások.
- Adott lehetőség elvesztése. Például: új ügyfél megszerzése nem valósul meg a nem működő rendszerek miatt.
- A szervezeten belül morál csökkenése, ami negatív mértékben befolyásolhatja az egész szervezet hatékonyságát.
- Új hardverek és eszközök, szoftverek beszerzése, hogy a későbbiekben hatékonyabban megbirkózhasson a cég a későbbi támadásokkal.
- Érzékeny információk elvesztése. Ami a versenytársakat helyzeti előnybe hozhatja.

Mindezeket a költségeket pontosan megbecsülni nagyon nehéz, szinte lehetetlen.

Az incidensekkel kapcsolatos közvetlen költségbecslést segíti, hogyha az incidensekkel kapcsolatban az alábbi információk rendelkezésre állnak:

- azon órák száma, amelyeket adott incidenssel kapcsolatban kellett eltölteni
- azon dolgozók óránkénti munkadíja, akik részt vettek az incidens kezelésében
- azon személyek száma, akiket érintett az incidens
- azon személyek óránkénti munkadíja, akiket érintett az incidens
- azon időtartam, ameddig az érintettek nem tudták használni a megfelelő számítógépes erőforrásokat
- a túlórák száma és azon eszközök és szoftverek beszerzésének költsége, amelyeket az adott incidens miatt kellett megvásárolni

2. Az IRT szolgáltatások belső értékesítése

Ebben a modellben egy szervezet többi szervezeti egysége alkalmazza az IRT-t, hogy különféle incidensekkel kapcsolatban eljárjon. Ezek a szervezeti egységek az IRT-től kapott szolgáltatásokért fizetnek, és ebből áll össze az IRT büdzséje. Ez felfogható a korábbi költség központ modell egyfajta változatának, amikor az adott szervezeti egység a büdzséjének egy részét odaadja az IRT-nek.

Ebben az esetben a következő feltételeknek kell teljesülnie:

- Az IRT-nek rendelkeznie kell egy árlistával, hogy adott szolgáltatásért milyen összeget számol fel.
- Szerződésben kell rögzíteni a szabályokat a félreértések elkerülése végett.
- Az IRT-nek lehetséges, hogy problémái adódnak a kötelező feladatai elvégzésében. Ezek tipikusan jogosultsági problémák miatt történhetnek.

3. Az IRT szolgáltatások külső értékesítése

Ezen modell esetében az IRT a szolgáltatásait külső ügyfelek számára értékesíti. Ebben a modellben még fokozottabban jelentkezik a szolgáltatások pontos leírásával kapcsolatos dolgok. Vagyis egy SLA-ban rögzíteni kell, hogy ki milyen szerepet tölt be a folyamatban, és adott feladatoknak ki a felelőse. Szintén előfordulhat, hogy adott vállalat esetében nincsen például hozzáférés adott szolgáltatásokhoz, amelyek egy harmadik cég üzemeltet. Ezért nagyon fontos annak a rögzítése, hogy mit lehet megoldani, és mit nem lehet megoldani egy incidens esetében.

Ami szintén fontos, hogy az ügyfél számára mely szolgáltatások jelentik a prioritást. Ugyanis, hogyha egy incidens bekövetkezik, akkor már nem áll rendelkezésre megfelelő idő ennek megvitatására és a helyreállítás e szerinti ütemezésére. Az IRT részéről általában egy vagy több személy tartja a kapcsolatot adott céggel. Így a 24x7-es alapon történő rendelkezésre állás az IRT részéről megvalósítható.

3.2. Az IRT helye a szervezetben

Bizonyos szituációkban elképzelhető, hogy egy IRT működési modellje a korábbiakban bemutatottak közül egyik sem teljesen, hanem az előzőek keveréke. Főleg ilyen helyzetekben jöhet elő az a kérdés, hogy milyen szervezeti egységen belülré helyezzük az IRT-t. Ezt egyrészt befolyásolja a szervezeti hierarchia mélysége. Ha sokszintű, mély szervezeti hierarchia létezik, akkor általánosságban elmondható, hogy nem célszerű mélyre tenni a hierarchiában. Minél mélyebbre rakjuk az IRT-t, annál fokozottabban jelentkeznek a működési, hatékonysági problémák. Amikor egy IRT helyét keressük egy szervezetben a legfontosabb szempontnak annak kell lennie, hogy megfelelő hatékonysággal el tudja látni a feladatait az adott keretek között.

A gyakorlatban általában az alábbi szervezeti egységekkel együtt található:

- IT részleg (IT department)
- Hálózati támogatás (Network support)
- Ügyfélszolgálati központ (Help desk center)
- Belső biztonsággal foglalkozó csoport (Internal security)

A Hálózati támogatás és az Ügyfélszolgálati központ általában az IT részlegen belül található. Így a továbbiakban ezeket együttesen említem.

Az IT részleghez való tartozás legfőbb előnyei:

- A biztonsági incidensek kötődnek operációs rendszerekhez, alkalmazásokhoz, hálózati infrastruktúrához. Ezekhez pedig az IT részlegnek van hozzáférése.
- Az IT részleg birtokolja a szükséges tudást és tapasztalatot az infrastruktúra egyes komponenseinek telepítésére és konfigurálására.
- A felhasználók általában az IT részleg felé jelzik a tapasztalt incidenseket, vagy „furcsaságokat” a rendszer működésében. Ezért az IRT közvetlenül megkaphatja az incidens jelentéseket.

A belső biztonsággal foglalkozó csoporthoz tartozás legfőbb előnyei:

- Az összes egyéb incidenst a belső biztonsággal foglalkozó csoport kezeli, miért lennének kivételek a számítógépes incidensek?
- A számítógépes incidensek lehetséges, hogy fizikai támadással vannak kombinálva (vagy fordítva), éppen ezért ha egy eseményt egy csoport kezel, az jóval hatékonyabb lehet.
- A belső biztonsággal foglalkozó csoport tagjainak lehet arra jogosultsága, hogy őrizetbe vegyenek bizonyos tevékenységeket elkövető személyeket. Bár ez közvetlenül nem segíti az IRT működését, de közvetve segíthet az IRT elismertségében, fontosságának hangsúlyozásában.

3.3.Központi, Elosztott és Virtuális csapatok

A következő döntés, amit az IRT-vel kapcsolatban meg kell hozni, az hogy egy „valódi” csapat legyen, vagy pedig virtuális. Ezen túl pedig, hogy helyileg egy központi helyhez legyen kötve, vagy pedig több helyre szétszétva.

Az incidensek megoldásakor gyakran szükség van külső szakértő meghívására. Ilyen értelmezésben egy IRT minden esetben virtuálisként fogható fel.

Általánosságban elmondható az is, hogyha van választási lehetőségünk, akkor célszerű virtuálisként létrehozni az IRT-t.

Ebben az esetben a legfontosabb előnyök:

- kevésbé formális és kevésbé lesz bürokratikus akadályozva
- könnyen létrehozható, kevés papírmunka szükséges a létrehozásához
- a csapat mérete igény szerint dinamikusan változtatható

- a mindenkori legjobb szakembereket tartalmazhatja

A virtuális csapat legfontosabb hátrányai:

- a csapat tagjainak megvannak a napi munkáik, amiktől elszakadni a virtuális csapat kedvéért nem biztos, hogy lehetséges
- minden virtuális csapat tagnak meg kell tanulnia, a működési folyamatokat és eljárásokat, ahogyan a csapat az incidenseket kezelni fogja
- viszonylag sok ideig tarthat egy virtuális csapat összeülése
- a virtuális csapat nem biztos, hogy emlékszik a korábbi történésekre a tagok cserélődése miatt
- amennyiben az incidensek száma elér egy bizonyos szintet, a virtuális team tagjai nem lesznek képesek a normál munkájuk ellátására, mert annyira lefoglalja őket az incidensek kezelése

A virtuális csapat csak akkor lehet működőképes hosszabb távon, hogyha vannak állandó belső tagjai. Ezek a belső tagok képesek gyorsan összeülni és munkájuk során folyamatosan az incidensekkel foglalkozni. Amennyiben az incidensek száma egy bizonyos szintet elér, abban az esetben lehetséges a belső tagok számának növelése. A külső tagok pedig inkább egy-egy speciális téma szakértőjeként jelennek meg. Amennyiben szükség van az ő munkájukra, abban az esetben kell őket meghívni az egyes döntési helyzetekben, kikérni a véleményüket, javaslatukat.

Egy IRT felépítésének általában célszerű követni az adott cég felépítését. Amennyiben több helyszínen szükséges a szolgáltatás biztosítása, abban az esetben célszerű az IRT tagjait is földrajzilag különböző helyekről választani.

3.4.Szabályok és eljárások fejlesztése

Ahhoz, hogy az IRT megfelelően tudjon működni, szükséges, hogy az alap működés és eljárások megfelelő módon szabályozva legyenek.

A legfontosabbak, amelyek feltétlenül szükségesek:

- incidensosztályozás és kezelés
- információosztályozás és védelem
- információk elterjesztése (disszeminációja)
- információk megtartása és megszüntetése
- titkosítás használata
- együttműködés külső szervezetekkel (más IRT-k, törvényhozó és végrehajtási szervezetek)

A korábbiak felsorolt szabályokat egymástól függetlenül szükséges létrehozni és kezelni. Ezeken túl általában még szükséges szabályok definiálása az alábbi területeken:

- bérlések szabályozása
- külső cég bevonása incidensek kezelésébe (outsourcing jelleggel)
- különféle hatáskörök, szerepek meghatározása

Ezen szabályok létrehozásához segítséget jelentenek az alábbi ISO/IEC szabványok:

- ISO/IEC 2 7001:2 005, Information technology—Security techniques—Information security management systems—Requirements.
- ISO/IEC 27002:2005, Information technology—Security techniques—Code of practice for information security management.
- ISO/IEC 27005:2008, Information technology—Security techniques—Information security risk management.
- ISO/PAS 22399:2007, Societal Security—Guidelines for Incident Preparedness and Operational Continuity Management.
- ISO/IEC TR 18044:2004, Information technology—Security techniques— Information security incident management.

A téma bővebben részletezésre került az Incidens menedzsment elméletéhez készült jegyzetben.

3.4.1. Az incidensek osztályozása és kezelése szabályzat

Ez az első szabályzat amelyben válaszolni kell az alábbiakra:

- Hogyan lehetséges adott incidens felismerése?
- Milyen módon történik az incidensek prioritizálása?
- Hogyan történik az egyes incidensek azonosítása és megjelölése?
- Milyen kritériumok teljesülése esetén lehetséges egy incidens lezárása?
- Milyen információkat kell az incidensekről szóló jelentésbe elhelyezni?
- Ki kapja meg a jelentéseket, és milyen tevékenységeket fog végezni ezekkel?
- Ki az a személy, aki adott incidenshez hozzá lesz rendelve?
- Hogyan lehetséges egy incidens eszkalációja, hogyha a másik fél nem reagál a jelzett incidenssel kapcsolatban?
- Hogyan lehetséges egy incidens eszkalációja, hogyha az IRT-nek esetlegesen nem sikerült megfelelően kezelnie azt?
- Milyen információkat kell gyűjteni statisztikai célok miatt?
- Milyen statisztikai információkat szeretne az IRT létrehozni?

Az incidens fogalmát definiálni kell. Például: Bármilyen olyan esemény, amely az információs rendszer bizalmasságát, integritását és elérhetőségét sérti biztonsági incidensnek tekinthető.

A bejövő riportok (események) érkezését folyamatosan figyelni kell. Erre alkalmas 8 óras munkaidőben egy illetékes személy. Ezt folyamatosan kell végezni, az IRT illetékes (ügyeletes) tagjai végzik ezt a tevékenységet, egymást felváltva 8 óránként.

Az IRT-hez érkező riportokat egy illetékes személynek el kell fogadnia, azonosítót kell hozzárendelnie, és tárolnia kell azt egy adatbázisban. Mindegyik riportot el kell látni megjegyzéssel, ami az incidens jellegére utal, illetve hozzá kell rendelni egy prioritást.

Az illetékes IRT tagnak kell eldöntenie, hogy az adott riport egy incidenst jelent, vagy nem. Amennyiben nem minősült incidensnek, akkor visszajelzést küld a jelentés feladójának, hogy a riport hamarosan lezárásra kerül.

A riport beérkezését követően adott időn belül (Például 5 órán belül) nyugtát kell küldeni az incidens jelzőjének. A választ titkosított formában kell visszaküldeni az incidens jelentőjének.

Adott időn belül (Például: 24 órán belül), egy tulajdonost kell rendelni az incidenshez. Az incidens tulajdonosa az a személy, aki majd az incidenset kezelni fogja irányítani.

Speciális minősítésű incidensek esetében (például: gyermek pornográfia) rögtön értesíteni kell a megbízót és az illetékes jogi szerveket.

Amennyiben a harmadik fél nem együttműködő, vagy az eredeti riportot küldő fél vagy az a fél, aki okozza az incidenst, abban az esetben meg kell kísérelni a kapcsolat felvételt az adott szervezettel más publikusan elérhető módon is. Például a saját weboldalukon lévő fórumokon vagy a WHOIS adatbázisban lévő elérhetőségeken keresztül. Amennyiben az alternatív megkeresésre sem felelnek, akkor 5 különböző jelzést követően (melyeket egymástól 3-5 napos időintervallum kell megkísérelni), akkor az incidenst nem megoldottá kell nyilvánítani.

Egy incidens addig nyitva marad, amíg az nem kerül megoldásra, vagy nem kerül létrehozásra egy másik folyamat, és az aktuális pedig nem lesz megoldottá nyilvánítva.

A post-mortem értékelések az incidens végkifejletétől függetlenül végre fognak hajtódni. Ezek praktikusán akkor történnek, miután az incidensek lezárásra kerülnek. Minden olyan incidens, fontos lesz, amely valamilyen szempontból eltér a korábbiakban kezelt incidensektől.

Az eltérés történhet:

- kiterjedésben (más érintett csoportok)
- technikai részletekben (újfajta technológia megoldás)
- újdonság (újfajta típusú incidens)

Minden éjfélfkor készül egy jelentés, amely a korábbi 24 óra történéseit mutatja be. Ebben a jelentésben a következőknek kell szerepelnie:

- a beérkezett incidensek száma
- a lezárt incidensek száma
- azon incidensek száma, amelyek még nem lettek személyhez rendelve

- az IRT mindenegybes tagjára jutó incidensek száma

Hasonló jelentéseket nem csak napi szinten, hanem heti és havi rendszerességgel is kell készíteni. Itt már a jelentés tartalmazhatja az incidensekre adott válaszok minimális, átlagos és maximális időbeni értékét is.

3.4.2. Információosztályozás és védelem

Meg kell határozni, hogy adott információk milyen kategóriába sorolhatók, és ennek megfelelően kell eljárni az incidens menedzsment folyamán.

Ilyenfajta osztályozás lehet például a következő (az alacsonyabbtól a magasabbig skálázva):

- *Publikus*: az információt szabadon meg lehet osztani az IRT-n és a szervezeten kívül is
- *Korlátozott*: az információt csak az adott szervezet munkavállalóival (teljes munkaidős, rész munkaidős, beszállítók) lehet megosztani
- *Bizalmas*: az információt csak az adott szervezet teljes munkaidős alkalmazottjaival lehet megosztani
- *Titkos*: az információt csak az arra illetékesekkel lehetséges megosztani

Az IRT alapértelmezésként minden információt titkosként osztályoz és kezel, kivéve akkor, amennyiben a küldő kifejezetten kéri, egy másik kategóriába sorolását. Az IRT összes tagjának fontos, hogy tisztában legyen azzal, hogy adott incidens milyen besorolás alá esik. Amennyiben egy incidens a korlátozott vagy magasabb kategóriába lett besorolva, abban az esetben egy számítógépen csak titkosított formában lehet tárolni. Amennyiben külső adathordozón történik a tárolása, abban az esetben gondoskodni kell a biztonságos tároláshoz. Az IRT adott incidens osztályozását menet közben megnövelheti, amennyiben az szükséges.

3.4.3. Információk terjesztése (disszeminációja)

Ahhoz, hogy egy incidenst lehessen kezelni, információkat kell megosztani az incidenssel kapcsolatban. Ez az információ megosztás nem lehet esetleges, hanem kontrolláltnak és céltudatosnak kell lennie. Az IRT-nek különféle csoportokkal kell megosztani információkat a szervezeten belül és kívül egyaránt. Viszont nem minden csoportnak van szüksége pontosan ugyanarra a részletes információra. Az időzítés és az információ megosztás célja is nagyon fontos.

<i>Csoport</i>	<i>Cél</i>	<i>Információk részletessége</i>	<i>Időzítés</i>
Külső IRT	Segítsen az incidens kezelésében.	A vonatkozó információk részletesen.	Mihelyt lehetséges.
Helyi menedzsmen	Statisztikák	Csak az összesített számadatokat.	Rendszeres időközönként (havonta, negyedévente, évente)
	Post-mortem analízis eredményei a fontos incidensekkel kapcsolatban	Az incidensek részletes leírása, ezek okai, a javasolt megelőzési lépések.	Az incidens zárását követően.
Helyi jogi szervezet	Az incidensek jogi aspektusai	A jogi vélelmezéshez szükséges információk.	Amikor jogi segítség szükséges.
Helyi nyomda, sajtó	Promóciós anyagok	Összesített eredmények, kevés technikai részlettel.	Rendszeres időközönként
	Érdeklődés adott incidenssel kapcsolatban.	Kevés részlet, személyek adatai nélkül	A PR részleg kérésének megfelelően.

5. ábra Az információk terjesztése

3.4.4. Információk megtartása és megszüntetése

Az információk megtartására és megszüntetésére vonatkozóan általában léteznek belső szabályozások és hatályos jogszabályok is.

Néhány általános irányelv:

- Az információt nem kellene hosszabb ideig megtartani, mint azt szükséges.
- Az EU-n belül az erre vonatkozó szabályok különösen szigorúak.

- Ne soroljuk titkosabb osztályba az adatainkat, mind azt szükséges lenne.
- Az adatok megszüntetésekor vegyük figyelembe az adott szinthez tartozó megsemmisítési szabályokat.

Az IRT által létrehozott információk megőrzésére is a szervezet általános megőrzési és megsemmisítési szabályai vonatkoznak. Amennyiben az adott incidens még nyitott állapotban van, akkor nem vonatkoznak rá a megőrzési szabályok. A megsemmisítésre vonatkozóan az IRT birtokolja annak a jogát, hogy megsemmisítsen bizonyos dokumentumokat.

Információ megőrzés:

Az információkat és dokumentumokat 6 évig kell a keletkezésüktől kezdve megőrizni. Ezt követően ezeket meg lehet szüntetni. Ez alól kivételek a következők:

- Amennyiben az információ még mindig aktív incidenshez tartozik
- Az információ szükséges az IRT működéséhez
- Az információ hasonlít egy aktív incidenshez, és ameddig az le nem zárul, addig azt meg kell tartani.

E-mail:

Amennyiben az e-mailek adott egyéni használatú eszközökön vannak tárolva, abban az esetben törölni kell őket, amikor már nem szükségesek vagy egy éven belül. A szervereken tárolt e-mailekre vonatkozik a hat éves megőrzési szabály.

Információk megszüntetése:

Minden információt biztonságosan és környezetbarát módon kell megszüntetni. Az IRT-nek teljes felelőssége van a megszüntetési folyamatban. Az információ megszüntetés módja függ attól, hogy az adott információ milyen módon lett osztályozva, és milyen adathordozón került tárolásra.

Publikus információk esetében: nem szükséges meghatározott eljárás definiálása

Korlátozott és bizalmas információk esetében a papír alapú dokumentumokat iratmegsemmisítővel kell megsemmisíteni, az optikai lemezeket, mágnes szalagokat szintén. Mágnes lemezek esetében az adatokat le kell törölni, felülírni a merevlemez egyes szektorait.

Titkos információk esetében minden papír dokumentumot és minden adathordozót, ami éghető anyagból áll – de nem tartalmaz mérgező anyagot – először íratmegsemmisítővel kell megsemmisíteni, majd elégetni. A merevlemezeket és optikai lemezeket fizikailag kell megsemmisíteni. A mágneslemezek esetében szét kell szedni az eszközt, és a benne lévő, az információt tartalmazó lemezeket kell eltávolítani és megsemmisíteni, a vezérlő elektronikát és a merevlemez keretet nem szükséges.

3.4.5. Titkosítás használata

Az IRT-nek képesnek kell lennie információk biztonságos küldésére és fogadására. Ez a gyakorlatban általában a kriptográfia alkalmazását jelenti. Lehetséges, hogy a támadók figyelik a kommunikációs csatornákat, ahonnan például értesülhetnek a felfedezésük tényéről, vagy az incidenssel kapcsolatos tervekről. Éppen ezért fontos, hogy az IRT-n belül a titkosítás módja és algoritmusai előre meghatározott legyenek. A gyakorlatban az GNU PG (Privacy Guard) használata jellemző. A GPG támogatja a szimmetrikus titkosítási módszereket, amelyekkel ugyanazon kulcs használatával képesek vagyunk szöveg titkosítására és visszafejtésére. Támogatja az aszimmetrikus kulcsú rejtjelezést, ahol privát és publikus kulcsunk felhasználásával dokumentumokat írhatunk alá vagy titkosíthatunk, illetve ellenőrizhetjük a kapott dokumentumokat.

A titkosítással kapcsolatban az alábbi kérdésekre kell tudnunk választ adni:

- Mikor kell titkosítást használni?
- Milyen titkosítási algoritmust, szoftvert, hardvert fogunk használni?
- Hány kulcsra van szükségünk?
- Adott kulcsokat mire akarunk használni?
- Hogyan biztosítjuk a kulcsaink „legitimizációját”? Mások honnan tudják meg, hogy ezek a kulcsok valójában az IRT-hez tartoznak?
- Hogyan történik a team kulcsának a belső terjesztése?
- Milyen hosszú ideig valós a kulcs?
- Milyen eljárást követően lehetséges egy kulcs visszavonása?

Példa:

- Minden egyes e-mailt, amit az IRT küld, digitálisan alá kell írni, azért, hogy a hitelességét ellenőrizni lehessen.
- Ha érkezik egy titkosított e-mail, akkor arra titkosított formában lehessen válaszolni.
- Az összes, nem publikus információt tartalmazó e-maileket titkosítottan kell elküldeni.
- Amennyiben egy kommunikáció titkosított e-mail formájában kezdődött el, akkor azt úgy is kell folytatni.
- Csak az információ tulajdonosa dönthet úgy, hogy nem szükséges a további párbeszéd folytatását titkosított formában végezni.

3.4.6. Együttműködés külső szervezetekkel

Sok esetben az IRT-nek igénybe kell venni más csapatok segítségét abban, hogy incidenseket tudjon megoldani. Ebben az esetben szabályozni kell, hogy milyen körülmények között lehetséges egy külső csapat bevonása, és őket milyen információkkal szabad ellátni.

Általában ha saját magunk nem tudunk megoldani egy incidenst, csak akkor szokás más IRT-ktől segítséget kérni. Ebben az esetben számítunk a másik IRT tapasztalatára: Ha ők vállalják az incidens megoldását, abban az esetben minden releváns információt meg kell velük osztani. Több IRT kooperálhat egymással, ilyen esetben NDA (NonDisclosure Agreement)-et kötnek, amiben definiálják az együttműködés területeit, feltételeit, célját.

Mondhatjuk azt, hogy az IRT-k egy oldalon állnak, és közös céljuk a biztonság növelése, és „rossz fiúk” tevékenységének meggátolása, minimalizálása. Éppen ezért nagyon fontos az együttműködés.

4. Teendők egy támadás esetén

Számítógépes és hálózati biztonsági incidensek folyamatosan történnek minden percben valahol a világban. Közülük sok észrevétlen marad, míg másokat valamilyen automatizált monitorozásnak köszönhetően, vagy pusztán a szerencse következtében sikerül érzékelni. A gyakorlatban a következő incidens fajtákkal nagy valószínűséggel találkozni fogunk:

- közvetlen hálózati támadás
- brute-force támadások hitelesítési információk megszerzésére
- szolgáltatás megtagadás (DoS) alapú támadások
- munkavállaló által elvesztett laptop
- biztonsági mentést tartalmazó mágnesszalag elvesztése
- bizalmas információk kiszivárgása
- zsarolások
- USB és egyéb hordozható médiákon keresztül történő támadások
- kémprogramok
- billentyüleütést figyelő alkalmazások
- vezeték nélküli hálózatok biztonsági problémái

Bármely támadás esetében készen kell állnunk arra, hogy ezeket valamilyen módon meg tudjuk válaszolni. Amikor egy adott incidens esetében keressük a megfelelő válaszlépéseket fontos, hogy ne essünk pánikba, ne reagáljunk túl a támadást, és ne vállaljunk fel szükségtelen kockázatokat.

4.1. Az incidens kezelés lépései

Amikor egy incidens bekövetkezik, akkor a válaszlépéseknek előre megtervezett intézkedések sorozatából kell állniuk. A legfontosabb lépések a gyakorlatban, amelyek el kell végezni:

- az incidenshez egy személyt kell hozzárendelni, aki az incidenssel kapcsolatos ügyeket fogja a továbbiakban elvégezni
- eldönteni, hogy az incidenssel kapcsolatban szükséges-e valamilyen külső hatóság bevonása
- meghatározni az incidens komolyságát
- megnézni az incidens hatókörét
- megoldani a problémát, a megoldás többféle lehet az incidens típusának függvényében.
- meghatározni, hogy szükséges-e más IRT-k bevonás
- meghatározni, hogy az incidens hatással van-e más rendszerre is
- elvégezni az incidens post-mortem analízisét

4.1.1. Személy hozzárendelése az incidenshez

Az első és legfontosabb feladat, hogy azonosítani, kell az incidens „tulajdonosát”. A tulajdonos lesz az, aki az incidens kezelésével foglalkozik, aki felelős az incidens koordinálásáért, a vezetéséért, és az incidenssel kapcsolatos döntések meghozásáért. Egyszerűbben megfogalmazva felelős a teljes incidensért. Ez nem azt jelenti, hogy neki egy személyben kell minden döntést meghoznia. Az ő felelőssége, hogy az incidenssel kapcsolatos minden nézőpont a döntések folyamán figyelembe legyen véve.

Lehetséges, hogy néha akarunk egy másodlagos személyt is hozzárendelni az incidenshez. Ez főleg nagy incidensek esetében fontos, amikor egy személy képtelen az incidenssel kapcsolatos dolgokat egy személyben elvégezni. Ez lehetőséget ad arra is, hogy a tapasztaltabb IRT tagok segítsék a kevésbé tapasztaltak munkáját, szakmai fejlődését.

4.1.2. Külső hatóság bevonása

Az incidensek korai szakaszában döntést kell hozni azzal kapcsolatban, hogy szükséges-e külső hatóság bevonása. Ez ugyanis befolyásolhatja annak a módját, ahogyan egy IRT az incidenst kezelni fogja és vele kapcsolatban milyen szintű jelentéseket készít. Ugyanis ebben az esetben várhatóan az incidens következtében jogi lépések megtétele is szükséges

lesz. Amennyiben az IRT-ről kiderül, hogy adott incidens esetében nem megfelelően járt el, ez rossz fényt vet az egész csapatra. Mivel ilyenkor általában bírósági ügy lesz az incidensből, ezért a megfelelő incidens kezelési eljárás elvégzése különösen hangsúlyos.

Amennyiben az IRT nem biztos abban, hogy szükséges külső hatóság bevonása, legbiztosabb, hogyha az incidenst „elszenvedő” félre bízva a döntést. Abban az esetben kötelező a külső hatóságok bevonása, hogyha „élet-halál” kérdéstről van szó, gyermekek elrablásáról vagy gyermek pornográfiával kapcsolatos az incidens. Mielőtt bármilyen bejelentés történne, feltétlenül konzultálni kell a csapat vezetőjével és a cég jogi szakértőjével.

4.1.3. Az incidens komolyságának a meghatározása

Az incidens kezelőjének kijelölését követően fontos megérteni a problémát és annak komolyságát. A fő cél, hogy meghatározzuk az incidens hatását a teljes szervezetre vonatkozóan. A hatás elemzését követően van arra lehetőség, hogy az incidenst besoroljuk fontosságát és sürgősségét tekintve. Az IRT-nek általában egy bizonyos időpontban több incidenst is kell egyszerre kezelnie, az incidens komolysága azt határozza meg, hogy mennyire fontos az új incidens mihamarabbi megoldása.

Az adott incidens bejelentői sok esetben érzékelnek egy bizonyos problémát, viszont a valóságban nem feltétlenül az általuk érzékelt dolog jelenti a valós okot. A bejelentők sok esetben nincsenek tisztában a probléma hatáskörével és az incidens komolyságával sem.

Az IRT részéről az incidens komolyságának eldöntéséhez információkat kell gyűjteni, nem elég megérteni a problémát, hanem a probléma megoldását is meg kell tervezni. Az információk gyűjtését úgy kell végezni, először az adott problémára kell koncentrálni kicsiben, majd fokozatosan általánosságban, nagyobb összefüggések figyelembe vételével vizsgálni azt.

Vagyis először kivizsgálni a bejelentő által tapasztaltakat, majd megvizsgálni, hogy az adott szervezetre milyen hatással lehet a bejelentett probléma.

Ahhoz, hogy ilyen jellegű információszerzést el lehessen végezni szükséges, hogy különböző dokumentációk rendelkezésre álljanak és segítsék az információszerzést:

- A hálózati topológia leírása. Segít abban, hogy melyik eszköz milyen más eszközökkel van közvetlen kapcsolatban. Mivel a támadások sokszor sérülékenységeket használnak fel, ezért azon eszközök listája, amelyek közvetlenül elérhetők, fontos lehet.

- A hálózat logikai topológiája, a létező VLAN-ok (Virtual Local Area Network). Milyen eszközök alkotnak logikailag egy egységet, amin keresztül bár fizikailag nem feltétlenül kapcsolódnak, logikailag mégis létezik közöttük kapcsolat.

- A fontosabb eszközök szerepe és feladata a hálózaton belül. Hol futnak különböző alkalmazások, hol vannak a hozzájuk tartozó adatbázisok, kik érhetik el ezeket az adatbázisokat. Adott eszközök feladata, illetve betöltött szerepe az informatikai infrastruktúrában.

- A szervezet hierarchiája. Sok esetben szükséges más személyek bevonása is a szervezet különböző részlegeiből. Ez elsősorban azért fontos, mivel szükséges lehet több információ gyűjtése az incidenssel kapcsolatban.

Amennyiben az előzőekben felsorolt dokumentációk nem állnak rendelkezésre, abban az esetben az incidens kivizsgálása lelassul, de nem lehetetlen. Ebben az esetben szükséges, hogy minden releváns információhoz hozzájussunk az incidenssel kapcsolatban.

Tipikus kérdések, amelyeket célszerű lehet megkérdezni ebben az esetben:

- Mit lát pontosan? Milyen szokatlan dolgot tapasztal? Miben különbözik a jelenlegi viselkedés a megszokottól?

Ezekből a kérdésekből a probléma tüneteit lehet megtudni. De vigyázzunk, ne vonjunk le túl gyorsan tapasztalatokat a hallottakból, mert ez könnyen tévútra terelheti az adott probléma megoldását.

- Az adott jelenség a bejelentőhöz kapcsolódik, vagy esetleg ő idézett elő valamit, ami mások számára okoz problémát?

Az adott esemény iránya fontos lehet.

Befelé jövő eseményről lehet szó:

- „Valaki csinál valamit a számítógépen.”

Vagy kifelé történő eseményről van szó:

- „A számítógépem valamit küldözget kifelé.”

Ezen bejelentések valóság tartalmának a kivizsgálásához mélyebb technikai analízis szükséges. Csak ezt követően állapítható meg, hogy az események pontos iránya.

- Mikor jelentkeztek az adott tünetek? Még mindig fennállnak, vagy csak időszakosan jelentkeznek? Meddig fordultak elő a tünetek? Társítható-e az adott tünet valamilyen változáshoz (Például: böngésző frissítés)?

Ahhoz, hogy az eseményeket pontosan rekonstruálni lehessen, az előfordulás ideje és körülményei nagyon fontosak. Az adott időpontban bekövetkezett egyéb eseményeket meg lehet vizsgálni, amelyek sok esetben magyarázatul szolgálhatnak az adott problémára vonatkozóan.

- Ismeri a hálózati topológiát? Hogyan kapcsolódik az eszköze az adott hálózati szegmenshez?

A hálózati topológiát valamilyen módon fel kell térképezni. Amennyiben a bejelentést tevő személy nem rendelkezik erre vonatkozóan megfelelő ismerettel, akkor kell valakit találni, aki igen. Csakis a topológia ismeretében lehetséges megérteni a tüneteket. Ez elvezet oda, hogy meghatározzuk az incidenst eredendően mi okozta, tisztában legyünk a hatáskörével, és megbecsülhessük az incidens üzleti hatásait.

- A cégen belül milyen pozícióban dolgozik, aki a bejelentést tette? Mennyire fontos az ő munkája a szervezet egészére nézve?

Egy incidens egész szervezetre vonatkozó hatását nem könnyű felmérni. Azonban egyes vezető pozícióban lévő személyek által bejelentett incidenseknek lehetnek akár nagyon komoly következményei is. Például, hogyha egy vezető nem tud e-mailben kommunikálni, akkor lehet, hogy pontosan ez a probléma fog adott megrendeléseket megghiúsítani, így hatása akár meglehetősen drámai is lehet.

Az előzőekben felsorolt kérdések jellemzően általános jellegűek. Ezek mellett az adott incidens jellegéből fakadóan egyéb kérdések is szükségesek. Ezekre azonban általános minták nincsenek, jellemzően szituációfüggők.

A kérdések jellege függ attól is, hogy az IRT a szervezetnek részét képezi-e vagy „külső” IRT végzi az incidens kezelési feladatot. Amennyiben belső IRT-ről beszélünk, akkor nagyobb valószínűséggel rendelkeznek a szükséges dokumentációkkal és ezért kevesebb kérdés feltevése szükséges. Amennyiben külső IRT-ről beszélünk, akkor nekik valószínűleg több kérdést kell feltenniük ahhoz, hogy a topológiát és a teljes rendszerfüggőségeket meg tudják állapítani.

Információgyűjtés közben nagyon fontos gyorsan és hatékonyan megérteni a problémát és az ezzel kapcsolatos feladatot. Fontos, hogy precízen jegyzeteljünk, hogy fontos részletek ne vesszenek el információgyűjtés közben. A korábbi jegyzetek átnézése segít abban, hogy újabb kérdéseket tudjunk feltenni, amelyek közelebb vezetnek a probléma megoldásához.

4.1.4. Az incidens hatókörének meghatározása

Az incidensek komolyságának nagysága meghatározza, hogy az adott incidens mennyire sürgős. Ez azonban nem szükségszerűen adja meg az incidens teljes hatókörét, ezáltal azt, hogy minek kell történnie az incidens kezelés következő lépéseként. Az incidens hatóköre tartalmazza a szervezet azon részlegeit, amelyekre az incidens vagy közvetlenül, vagy közvetetten hatással van. Mihelyt ezzel az információval is tisztában leszünk, ez megváltoztathatja az incidens komolyságát.

Ez a változás akár még komolyabbá, akár kevésbé komollyá tehet adott incidenst.

Egy incidens bejelentését követően meg kell nézni, hogy a bejelentett tüneteknek adott jelei látszódnak-e a hálózatban. Ez jelenthet például nagyobb hálózati forgalmat, a szokásostól eltérő CPU felhasználást, esetleg áram kimaradást, vagy eszköz újraindulást. A bekövetkezett események segítik megérteni az incidens legfőbb okát, és ezt követően tovább lehet lépni a megoldás irányába.

Ebben a fázisban különösen fontosak az analitikus képességek és a képzelő erő. A tüneteket le kell fordítani potenciális okokká, de nyitottnak kell maradni különböző eshetőségek megvizsgálására is. Nem szabad közvetlenül, elhamarkodottan következtetéseket levonni.

A nyitottság szintén fontos, hiszen akár napi szinten újabb és újabb támadási módszerek és technikák jönnek létre és lehetséges, hogy ezek közül tapasztalunk meg egy újat, amivel még korábban nem találkoztunk.

Amennyiben az incidenst bejelentő személy pontosnak tűnő leírást ad az adott incidenssel kapcsolatban, akkor is fontos a megfelelő eljárás lefolytatása. Egyáltalán nem biztos, hogy az észlelt tünetek mögött a vélt események találhatók.

Például egy bejelentő az alábbi incidenst jelenti be:

„A webserververemet TCP SYN típusú támadással támadják.”

Ebben az esetben is próbáljuk meg megérteni, hogy milyen adatok alapján jutott a bejelentő erre a következtetésre. Hasonlóan, mint bármely incidens kivizsgálásakor tegyünk fel kérdéseket, amelyekből tudunk következtetni az állítás valóságára. Óvatosak legyünk, mert nem biztos, hogy a bejelentő helyes következtetést vont le, éppen ezért ennek automatikus átvitele mindenképp hibás incidenskezeléshez vezethet.

Ilyen esetben is tegyünk fel kérdéseket, amelyekből információkat nyerhetünk.

Például:

- Miből gondolja, hogy ez egy TCP SYN típusú támadás?
- Helyileg hol található a szerver?
- Honnét érkezik a befelé irányuló forgalom?
- Milyen web oldalak vannak tárolva a webserververen?

Ezen kérdések segíthetnek abban, hogy megértsük, hogy mik lehetnek a támadók esetleges motivációi. Bár közvetlenül ez nem segíti az incidens megoldását, de segíthet azt megválaszolni, hogy mi történhet a hálózatunkban. Esetleg ötleteket adhat arra nézve, hogy milyen technikai aspektusból lenne jó megvizsgálni az incidenst. Általában a DoS támadások használnak TCP SYN csomagokat, de az is lehetséges, hogy a teljes hálózatot próbálják

ugyanilyen módon támadni. Ilyenkor érdemes lehet a bejövő TCP SYN csomagokat analizálni, hátha segít a probléma megoldásában.

4.1.5. Távoli diagnózis és telefonos beszélgetés

Gyakran kerülhetünk olyan helyzetbe, hogy telefonon kérnek tőlünk segítséget. Ebben az esetben is fontos, hogy az alapvető elveket betartsuk, hogy az egész incidens-kezelő folyamatot sikeresen tudjuk kezelni.

- Ne essünk pánikba. Nyugodtan és racionálisan beszéljük át a történetet. Biztosítsuk a másik felet arról, hogy meg akarjuk érteni a problémáját.
- Jegyzeteljük le a mondottakat. Ez mindenképpen fontos lehet a későbbi analízishez.
- Figyeljünk oda a hívóra. Engedjük neki, hogy elmondja a problémáját, lehetőség szerint ne szakítsuk meg.
- Egyszerű kérdéseket tegyünk fel.

Például:

- Milyen operációs rendszert használ?
- Milyen szoftvert használ?
- Mi a szerver IP címe?
- Honnét érkeznek a támadások?

- Néha segíti a kérdésünk megértését, hogyha azt újrafogalmazzuk, és más formában tesszük fel.
- Próbáljuk meg a szakzsargont lehetőség szerint mellőzni.
- Az általunk nem ismert dolgokkal kapcsolatban legyünk befogadóak.
- Irányítsuk a beszélgetést, Amennyiben szükséges szakértőket vonjunk be a beszélgetésbe, de az egész társalgás irányítását tartsuk meg.

4.1.6. A probléma megoldása

Az incidens megoldása magában foglalja a probléma megértését és megoldását.

A probléma megértését követően lehetséges annak a megoldása, a lehetséges megoldások számba vétele. Ezt követően az egyes megoldásokat analizálni kell, és prioritási sorrendet kell felállítani köztük. Mindegyik esetében:

- Meg kell vizsgálni az erőforrás szükségleteket.
- Meg kell vizsgálni a hatékonyságát.
- Mik az esetleges hatásai? (Mit befolyásol?)

A reakció meghatározása:

Amint egy problémát megismertünk, előbb-utóbb eljutunk egy olyan pontra, hogy döntéseket kell hoznunk vele kapcsolatban. A döntésünk meghatározza, hogy milyen további cselekvések szükségesek.

Például szükséges-e adott szerver azonnali leválasztása a hálózatról, azért mert érzékeny adatokat tulajdonítottak el róla? A leválasztással meg tudjuk előzni a további adatlopást, viszont az ügyfeleink nem tudnak rendeléseket feladni, és ezáltal lehetséges, hogy bevételtől esünk el, és ügyfeleket veszünk el.

A döntés meghozatala nem egyszerű. Ebben az esetben az incidensért felelős személynek prezentálni kell az egyes intézkedések közvetlen következményeit és az illetékes személyek kezébe adni a döntést egyeztetve a bejelentővel.

Amennyiben a döntés megszületett az incidenssel kapcsolatban, az incidenskezelőnek el kell kezdeni az intézkedést az incidenssel kapcsolatos cselekvésekről és javaslatot tenni a szükséges reakciókkal kapcsolatban. A racionális döntések véghezvitele érdekében ilyenkor általában további adatgyűjtés szükséges.

A probléma „feltartóztatása”

Amikor a reakció terv kialakításra kerül, ez rendszerint két lépésből áll. Az első lépés a „probléma feltartóztatását”, a második pedig az ok megszüntetését jelenti. Ezen két lépést lehet, hogy egymás után többször is meg kell ismételni, amíg a problémát teljes mértékben irányítani tudjuk. A probléma feltartóztatása lehetővé teszi, hogy az adott szervezet folytatni tudja üzleti tevékenységét és lehetőséget a probléma megkerülésére.

A probléma feltartóztatása jelenti például:

- a támadó számítógép leválasztását a hálózatról
- a fertőzött számítógép kikapcsolását
- tűzfal beiktatását a forgalom korlátozására
- hozzáférési listákkal a kártékony forgalmak kiszűrését

Az utóbbi kettő intézkedéssel például megelőzhetjük, hogy a kártékony forgalom elérje a sebezhető számítógépeket. Itt bármely olyan intézkedés szóba jöhet, amellyel a támadást lelassíthatjuk, és ezzel időt nyerhetünk a továbbiak véghezviteléhez.

Hálózati szegmentáció

A végső módszer egy támadás elkülönítésére a hálózati szegmentáció. Ebben az esetben VLAN-ok segítségével adott számítógép elkülönítése elvégezhető az OSI modell 2. rétegében. Bár ez nem biztosít tökéletes izolációt, de mégis a segítségével gépek egy csoportja elszigetelhető, ezáltal egy számítógépes fertőzés terjedése lelassítható.

A szegmentálás hozzáférés vezérlési listák (access control list) segítségével is elvégezhető az OSI modell 3. rétegében. Magasabb rétegekben is léteznek lehetőségek a szegmentálásra. Például HTTP proxy segítségével lehet konfigurálni, hogy milyen weboldalt lehessen elérni.

A legszigorúbb megoldás a teljes internet kapcsolat leállítása a probléma megoldás idejére.

Probléma megoldás és szolgáltatások helyreállítása

Miután a probléma értékelése és feltartóztatása megtörtént elkezdődhet a döntés az incidenssel kapcsolatban. A döntés az incidenstől függ. A döntés lehet technikai megoldások

alkalmazása, architektúrális változtatások, folyamatok megváltoztatása azon cél elérése érdekében, hogy az adott funkcionalitás helyreálljon és a rendszer normálállapotba kerüljön.

A technikai megoldásokat kell legelőször megvalósítani, mivel ezek lehet elvégezni a leggyorsabban. Ezek tipikusan szoftver frissítések és foltozások, eszköz konfigurálások, új eszközök vagy szolgáltatások beszerzése vagy az előzőek kombinációja.

Az architektúrális és folyamatbeli változtatások hosszabb időt vesznek igénybe. Általában elmondható, hogy nem jó megoldás egy hálózatot újratervezni egy incidens miatt, mert lehet, hogy a kapkodásban még súlyosabb hibákat követünk el, mint amelyek korábban léteztek.

Az ismétlődés monitorozása

Miután egy incidens megoldásra került és a szolgáltatás helyre lett állítva, a következő lépés az incidens ismételt előfordulásának monitorozása. Hogyha a támadás kissé módosulni fog, akkor nem lehetünk abban biztosak, hogy az korábbi döntések az új esetben is működni fognak. Amennyiben nem történne az előfordulás monitorozása, akkor hasonló incidens ismét előfordulhatna rövid időn belül.

Monitorozást kell végezni a hálózat bejövő és a kimenő pontjai esetében, a hálózat kulcs fontosságú pontjaiban, és a cél eszközön is. Erre különféle technológiák léteznek:

- tűzfalak és hozzáférés vezérlési listák
- behatolás jelző és érzékelő rendszerek (IDS, IPS)
- hálózati folyammonиторozó rendszerek
- hálózati forgalom begyűjtésére használható eszközök (sniffer)
- hálózati menedzsment eszközök
- alkalmazás naplófájlok

Amennyiben nem történik megfelelő monitorozás, abban az esetben a hálózatban történő egyes tevékenységek rejtve maradnak. Utólagos felderítésre, elemzésre nincsen lehetőség.

4.1.7. POST-MORTEM analízis

Amikor valakivel történik valami, utólag érdemes végiggondolni, hogy pontosan mi is történt, és mennyire voltak helyesek az ott alkalmazott megoldások. Ez elsősorban azt a célt szolgálja, hogyha a későbbiekben ismét hasonló szituációba kerülünk, akkor ott milyen megoldást válasszunk. Megfelelők voltak a korábbi szituációban alkalmazott lépések, vagy jobb lett volna inkább más megoldást választani? Összefoglalóan erről szól a post-mortem analízis.

A post-mortem analízis során interjúkat kell készíteni, kérdőíveket kell kitölteni az érintettekkel, megkérdezni tőlük, hogy mi a véleményük az incidens kezelés folyamatával, hatékonyságával és az IRT működésével kapcsolatban. Ezen felmérések eredményét összegezve születik meg egy jelentés a tapasztalatokról.

A végső célja a post-mortem jelentéseknek, hogy meg lehessen találni azokat a pontokat és területeket, amelyek fejlesztésre szorulnak. Mi szükséges ahhoz, hogy hasonló incidensek hatását minimalizáljuk és ugyanolyan incidens bekövetkezését megelőzzük? A fejlesztendő területek lehetnek technikai természetűek, de lehetnek folyamatokhoz kapcsolódóak is.

Miután a szükséges cselekvések meghatározásra kerülnek, arról is kell gondoskodni, hogy valaki a jövőben ezeket végezze el, valósítsa meg.

Bár első hallásra a post-mortem analízis egyszerűnek hangzik, több mint egy egyszerű beszélgetés az incidensben érintettekkel.

Az incidensek analízálása

Az incidensek post-mortem analízise arra fókuszál, hogy melyek voltak azok a tényezők, amelyek lehetővé tették azt, hogy az incidens bekövetkezett és a szervezet milyen módon volt képes kezelni a szituációt.

Erre különféle kérdések megválaszolásával találhatjuk meg a választ.

A kérdéseket csoportokra oszthatjuk:

- Az incidens technikai aspektusai: *Miért történt meg az incidens?*
 - Volt egy operációs rendszer vagy alkalmazás sebezhetőség? Volt elérhető folt a sebezhetőségre? Alkalmazva lett a folt? Hatásos volt a folt alkalmazása? Milyen szolgáltatásokat befolyásolt?
- Az incidens azonosítása: *A szituáció rosszindulatúként került felismerésre?*
 - Meddig tartott felismerni, hogy egy incidens történt? Volt-e bármiféle jele ennek a korábbiakban? Mi akadályozta a gyors és pontos azonosítását az incidensnek?
- A jelzési folyamat és interakció: *A megfelelő embereknek jelezték a problémát? Ez még időben történt?*
 - Ki lett értesítve az incidenst követően? A megfelelő emberek értesítve lettek? Mindenki megfelelő időben lett értesítve? Az IRT válasza megfelelő és jól időzített volt?
- Hálózati képességek: *Mi volt a hatása a hálózati és számítógépes eszközökre?*
 - A hálózati és számítógépes eszközökre hatással volt az incidens? Mi volt az incidens hatása a rendszeren belül? Volt lehetőség az incidens szegmentálására a hálózaton belül?
- Üzleti hatás: *Milyen volt az incidens üzleti hatása?*
 - Milyen szolgáltatásokat befolyásolt? Milyen gyorsan lett helyreállítva? Mit jelentett ez a teljes szervezetre vonatkozóan? Volt-e bármilyen érezhető hatása az incidensnek az ügyfelek elégedettségére vonatkozóan?

Amennyiben a korábbiakban felsorolt kérdéseket megválaszoljuk, akkor az adott incidens legfontosabb jellemzői felismerhetők. Ezen incidensek jellemzőiből, kialakulási feltételeikből tudunk következtetéseket levonni arra vonatkozóan, hogy melyek adott infrastruktúra vagy folyamat gyenge pontjai.

Az IRT analizálása

Ez a rész azt vizsgálja, hogy az IRT milyen teljesítményt nyújtott. Ez több részre bontható fel:

- A bejelentés folyamata hogyan történt: Hogyan és mikor kapcsolódott be az IRT?
 - Milyen módon történt az IRT értesítése? Megfelelően hatékonyan történt-e az első bejelentés? Az IRT megkapta az összes fontos információt a bejelentőtől?
- Az IRT eskalációs és kommunikációs eljárása: Ki végezte el az IRT részéről az eskalációt és hogyan lettek más csoportok bevonva?
 - Sikerült elérni a megfelelő embereket? Megfelelő volt a támogatást kapott az IRT a „menedzsmenttől”? Sikerült felvenni a kapcsolatos az összes külső szervezettel? Megfelelő volt a kommunikáció az incidenssel kapcsolatban?
- Incidens kezelése: Hogyan lett az incidens kezelve?
 - Megfelelően lett az incidens diagnosztizálva? Megfelelő volt az incidenssel kapcsolatos reakció? Elég gyorsan történt az incidensre adott válasz megszületése? Az IRT részéről meg volt a megfelelő tudás az incidens kezeléséhez? Rendelkezésre álltak a megfelelő erőforrások a probléma hatékony megoldására?

Amennyiben a felsorolt, vagy hasonló kérdéseket megválaszoljuk, akkor megismerhetjük az IRT működését és képességeit. Mindez egy fontos visszacsatolás abban a tekintetben, hogy megfelelően képzett és felvértezett csapat áll-e rendelkezésre, hogy felvegye a harcot az incidensekkel.

5. Az incidens-menedzsmenthez kapcsolódó alkalmazások

Az incidens-menedzsmenthez különféle számítógépes alkalmazások kapcsolódnak. Ezek egy része kötődik a naplózási szolgáltatáshoz, másik része segít az incidensek felderítésében, de ezen túl léteznek olyan web-es rendszerek, amelyeket kifejezetten IRT-k számára fejlesztettek ki. Ezek segítségével az incidens kezelés teljes folyamata végig követhető, a rendszerben az incidensek tárolásra kerülne, és az adott incidens aktuális állapota megtekinthető.

5.1. A naplózási szolgáltatás

Ahhoz, hogy egy informatikai rendszer történéseivel tisztában legyünk fontos a naplózási szolgáltatás beállítása. A naplózási szolgáltatás kimenetei lesznek a napló fájlok, amelyekbe különféle formátumok szerint naplóbejegyzések kerülnek. Ezek a naplóbejegyzések alkalmasak az utólagos elemzésre, vagy egy bizonyos esemény bekövetkezésekor az azonnali riasztásra. A naplózás tehát abban játszik szerepet, hogy definiálja, hogy mi fog automatikusan eseménynek minősülni.

A naplózással kapcsolatos legfontosabb kérdések:

- Mit akarunk pontosan naplózni?

Például: Minden rendben van-e? Valaki belépett a rendszerbe adott IP címről, adott protokollal. Milyen a diszk foglaltság?

- Mi a célja a naplózásnak?

Például: Teljesítményfigyelés; utólagos diagnosztika; a rendszer és adott alkalmazások működésének figyelése

- Mihez fogunk kezdeni az elkészült naplókkal?

Például: tároljuk, mert muszáj; gyanús mintákat keresünk benne, adatokat bányászunk belőle, célzottan keresünk benne

A naplózó szolgáltatások operációs rendszer specifikusak. Más alkalmazások érhetőek el Linux és Windows rendszerekben erre a feladatra. Bár kétség kívül léteznek manapság szabványos megoldások a naplózási feladatra.

Manapság az egyik legnépszerűbb naplózó program a syslog-ng, amely a magyar BalaBit IT Biztonságtechnikai Kft terméke. A syslog-ng rendelkezik egy Open Source

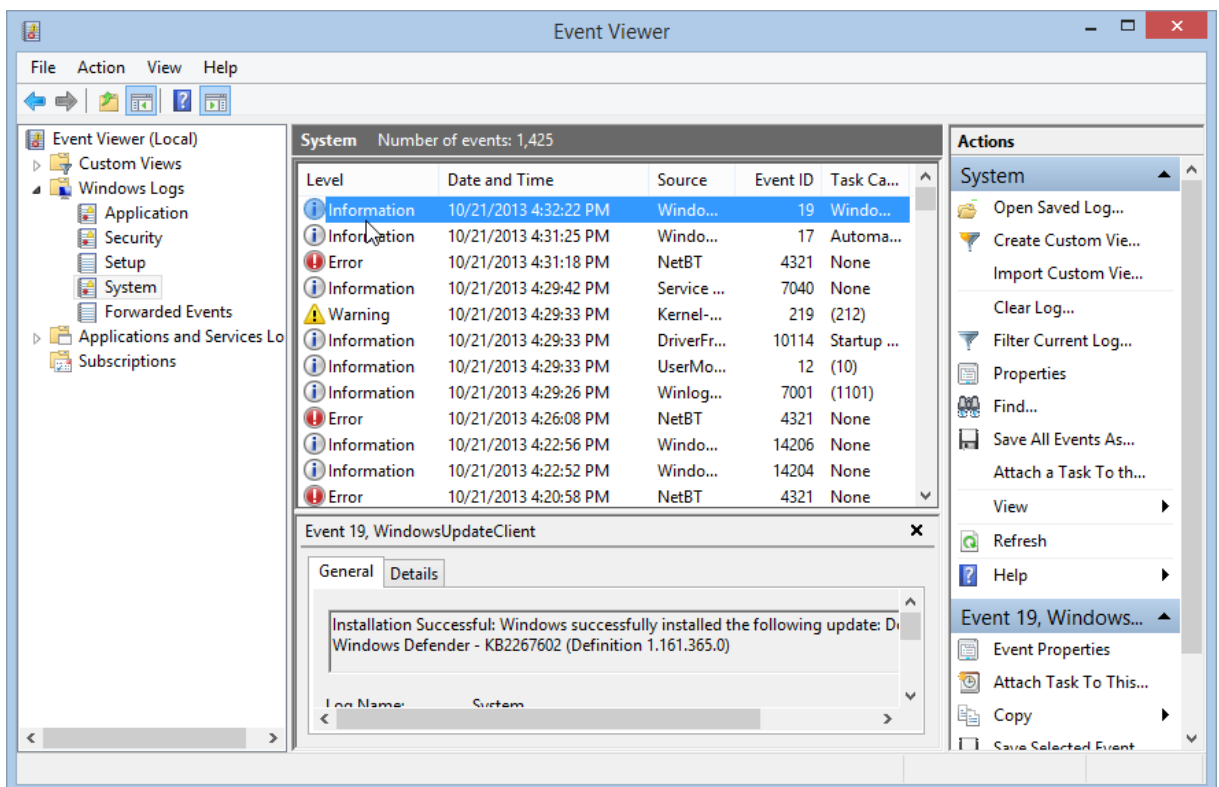
Edition verzióval. Ez az ingyenes, nyílt forrású verzió egy kiforrott, nagy teljesítményű naplózó szolgáltatást biztosít, a Linux/Unix világ egyik leggyakrabban alkalmazott központi naplózó szervere. Becslések szerint több millió szerveren működik világ szerte, így valószínűleg az egyik legsikeresebb magyar terméknek számít. A szoftver szerver és kliens módban egyaránt működik. A hagyományos UDP alapú protokoll mellett TCP alapon is működik, és támogatja a TLS alapú titkosított átvitelt is. Heterogén környezetben is rugalmas, biztonságos naplózási infrastruktúra építésére használható.

Egy naplóbejegyzés lehet az alábbi:

```
May 5 23:53:05 server04 sshd[19286]: Accepted password for kami from 192.168.62.5 port 34317 ssh2
```

A bejegyzés formailag különböző lehet, de biztosan tartalmazza a legfontosabb információkat: mikor történt az esemény, milyen gépen, milyen program generálta, mi az eseményhez tartozó üzenet.

Windows 8.1 rendszerben az eseménynapló az alábbi lehet, ahol az előzőekben felsorolt eseményhez tartozó mezők szintén elérhetők.



6. ábra A Windows 8.1 esemény naplója

5.2. Számítógépes „nyomelemzés” (forensics)

Amikor informatikai eszközökön dolgozunk, akkor a használt operációs rendszerek és programok a tevékenységeinkről naplót vezetnek. Ezek a naplófájlok szolgálhatnak alapjául adott bizonyítási eljárásoknak. Mivel a naplófájlok időbélyeggel vannak ellátva, ezért az események láncolata ezekből a fájlokból sok esetben visszafejthető.

Tegyük fel, hogy az alábbi incidens történt egy ügyfél elmondása alapján:

- Az ügyfél ellátogat a netbankjába, de többszöri belépés után sem tudott belépni.
- Egyszer felugrott egy ablak, hogy írja be a biztonsági kódot, időközben kapott egy SMS-t.
- Beírta az SMS-ben kapott kódot, ezután már be tudott lépni.
- Viszont gyanút fogott és megnézte az utalásait. Észrevette, hogy történt egy olyan, amit nem ő kezdeményezett.
- A gépet gyorsan kikapcsolta és értesítette a bankot.
- Amit még tudunk, hogy adott felhasználónévvel dolgozott a számítógépén és Firefox-ot használt.
- A netbanki rendszer csak az utalás megerősítéséhez küld SMS-t, a bejelentkezéshez nem.

Ilyen vagy hasonló incidens bejelentését követően az alábbi a kivizsgálás folyamata:

- Image fájl készítése a teljes diszkról, vagy adott partíciónról (például egy Linux live CD-vel), az Image fájl mentésekor fontos, hogy ellenőrző összegek is készüljenek (például: MD5, SHA1). A partíció méretétől függően ez 2-3 óra is lehet. Fontos, hogy az eredeti diszk tartalmát sohasem változtatjuk meg, a másolaton végzünk minden műveletet, keresést.
- Támasszuk alá vagy cáfoljuk meg az ügyfél meséjét!
Ellenőrizzük, hogy az általa elmondottak megállják-e a helyüket! Ezek ellenőrzését a napló fájlok felhasználásával tehetjük meg.
- Adatgyűjtés: fájlrendszer és registry vizsgálata, böngésző history és rendszeresemények vizsgálata. Különbőféle, erre a célra kifejlesztett

alkalmazások segítségével vizsgáljuk meg a fájlrendszert, és keressünk nyomokat!

Például: Ki jelentkezett be korábban az incidens előtt? Milyen programok indulnak el automatikusan a bejelentkezést követően? Milyen új fájlok lettek a fájlrendszerben, illetve mik módosultak az adott időtartományban?

Ezen lépéseket követve előbb utóbb felgöngyölíthetjük az eseményeket. Amennyiben megtaláljuk azt a kártékony kódot, amely a gépünkre került, abban az esetben szakértőkkel analizáltathatjuk annak a működését, megtudhatjuk, hogy mik voltak azok a körülmények, amelyek lehetővé tették az adott incidens bekövetkeztét.

5.3. Incidens-menedzsmenthez fejlesztett szoftver

Az IRT-k munkájának a támogatása egy fontos informatikai feladat. Manapság erre a célfeladatra is léteznek olyan alkalmazások, amelyek megkönnyítik a gyakorlati munkát, és hatékonyan segítik az incidenskezelést.

Ilyen nyílt forráskódú megoldás a Request Tracker (RT). Amely elérhető a <https://www.bestpractical.com/rt> oldalról. Az újabb Linux disztribúciókban, például Debian 7.x alatt csomagként elérhető. A feltelepíthető csomag neve request-tracker4. Az alkalmazás működéséhez szükség van Apache webserverre, és a mod_perl beépülő Apache modulra. Az egész rendszer Perl programozási nyelven megírt szkriptek felhasználásával működik.

Home Search Articles Tools Admin Logged in as jesse RT for example.com BEST PRACTICAL™

RT at a glance New ticket in General Search... Edit

^ 10 highest priority tickets I own Edit

#	Subject	Priority	Queue	Status
1	Office has run out of coffee!	0	Office	(pending 1 other ticket)
2	Order more coffee	0	Office	(pending 2 other tickets)

^ 10 newest unowned tickets Edit

#	Subject	Queue	Status	Created	
3	Obtain Series-C funding	General	new	47 minutes ago	Take

^ Bookmarked Tickets Edit

#	Subject	Priority	Queue	Status
4	Evaluate responses to RFP for coffee roasts	0	General	new

^ Quick ticket creation

Subject:

Queue: Owner:

Requestors:

Content:

Create

^ My reminders

^ Quick search Edit

Queue	new	open	stalled
General	2	-	-
Office	1	1	-

^ Dashboards Edit

RT System's dashboards Subscription

SLA Performance dally at 6:00 AM

^ Refresh

Don't refresh this page.

7. ábra A Request Tracker fő képernyője

A rendszer legfontosabb jellemzői, előnyei:

- Tetszőleges operációs rendszerből, az elterjedt böngészőprogramok segítségével használható.
- Működik mobil eszközökön is.
- „Dashboard” jelleggel működik, minden egy központi felületen keresztül érhető el.
- E-mail integráció.

- PGP támogatás használata a levelezésben akár aláírásra, ellenőrzésre, vagy pedig titkosításra és visszafejtésre.
- Idő figyelés.
- SLA funkciók figyelése.
- Diagramok, jelentések készítésének lehetősége.

Ilyen vagy hasonló rendszer megkönnyíti az incidensek kezelését, és segíti a teljes incidens-menedzsment folyamat által igényelt tevékenységeket.

6. Összefoglalás, összegzés

Az incidens-menedzsment gyakorlati szempontból fontos egy cég/intézmény életében. Mivel mindennapi életünk részévé vált az infokommunikációs technológiák használata, ezért a számunkra szükséges adatokat szinte bárhonnét elérhetjük megfelelő hitelesítést, és kapcsolat titkosítását követően. Bármely rendszerben történhetnek incidensek, amelyek lehetnek különféle hálózati, hardver és szoftver, emberi problémák következményei. De emellett fel kell készülnünk külső és belső támadásokra is. Az incidens kezelés gyakorlatának kialakítása azért fontos különösen, mert nem tudjuk előre, hogy mi fog történni a következő pillanatban az informatikai rendszerünkben. Egy jól elkészített BCP és DRP felhasználásával, és megfelelő tudással rendelkező IRT-vel azonban meg tud cégünk/intézményünk felelni ezen új kihívásnak is.

Irodalomjegyzék

- [1] CISM Review Manual 2013, ISACA, 2012.
- [2] CISM Review Questions, Answers & Explanations Manual 2012 Supplement 2012, ISACA, 2011.
- [3] CISM Review Questions, Answers & Explanations Manual 2013 Supplement 2013, ISACA, 2012.
- [4] Damir Rajnovic: Computer Incident Response and Product Security, Cisco Press, 2011, ISBN 978-1-58705-264-4
- [5] ITILv3: <http://www.itiil-officialsite.com>
- [6] ITILv3 magyarul: <http://users.nik.uni-obuda.hu/itiil/>
- [7] Ethical Hacking konferencia 2013: www.netacademia.hu/Konferencia

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



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