HADMÉRNÖK

XIII. Évfolyam 4. szám – 2018. december

KIBERBIZTONSÁGI SZERVEZETEK KÖZÖTTI INFORMÁCIÓCSERE

INFORMATION EXCHANGE BETWEEN CYBERSECURITY ORGANISATIONS

MUNK Sándor

(ORCID: 0000-0001-8576-308X)

munk.sandor@uni-nke.hu

Absztrakt

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól.
A kiberbiztonság megteremtése és fenntartása a kiberbiztonsági szervezetek, az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű közös feladata, amely több szereplőre kiterjedő és széleskörű együttműködést igényel.
Jelen publikáció – egy háromrészes sorozat második részeként – leírja és értékeli a kiberbiztonsági szervezetek által kezelt, illetve a köztük áramló információkat, az információcsere alapvető jellemzőit.
„A publikáció a KÖFOP-2.1.2-VEKOP-15-2016-00001 'A jó kormányzást megalapozó közszolgálat-fejlesztés' projekt támogatásával, a Kiberbiztonsági Ludovika Kiemelt Kutatóműhely keretében készült”

Kulcsszavak: *kiberbiztonság, kiberbiztonsági szervezetek, kiberbiztonsági információcsere, interoperabilitás*

Abstract

Today's social, economic, and every-day activities are increasingly dependent on the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace.
Ensuring cyber security is a common task of cybersecurity organisations, IT system-network operators, citizens, and media, which requires wide range, extensive cooperation of these actors.
Recent paper – as a second part of a three-part series – describes and evaluates the information handled by, and flowing between cyber security organisations, and the basic features of information exchange.

Keywords: *cybersecurity, cybersecurity organisations, cybersecurity information exchange, interoperability*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.11.23.

BEVEZETÉS

Napjaink társadalmi, gazdasági, és mindennapi tevékenysége egyre növekvő mértékben függ a kiberteret alkotó, globálisan összekapcsolt, decentralizált informatikai rendszerek és hálózatok által nyújtott szolgáltatásoktól. Az informatikai szolgáltatások egyre jelentősebb mértékben járulnak hozzá az állami működés hatékonyságának, a vállalkozások eredményességének és versenyképességének, valamint az állampolgárok életminőségének javításához. A növekvő függőség egyben növekvő kiszolgáltatottságot, kockázatot is jelent, mivel az informatikai rendszerek, hálózatok, és az általuk kezelt adatok, információk biztonságának (bizalmasságának, sértetlenségének, és rendelkezésre állásának) megsértése maga után vonja az informatikai szolgáltatásokra épülő rendszerek, folyamatok, szolgáltatások biztonságának sérülését is, ami jelentős kihatással lehet az átfogó biztonság politikai, katonai, gazdasági, pénzügyi, és társadalmi dimenzióira is.

A kibertérben világszerte növekvő mértékben jelentkező kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a nemzeti kritikus infrastruktúra működtetésének biztosítására minden államnak, így – Magyarország Nemzeti Biztonsági Stratégiájában megfogalmazottak szerint – hazánknak is készen kell állnia. A kiberbiztonság megteremtése és fenntartása nem csak a kiberbiztonsági (információbiztonsági, informatikai biztonsági) szervezetek, hanem az informatikai rendszereket, hálózatokat működtető szervezetek, az állampolgárok, és a média kiemelt jelentőségű feladata.

A kibertér informatikai rendszereinek, hálózatainak globális, szövevényes összekapcsolódása következtében az egyik rendszer biztonságának sérülése elvezethet egy másik (más országban, más ágazatban működő) rendszer biztonságának sérüléséhez. Egy magán vállalkozás által üzemeltetett informatikai infrastruktúra támadásával támadhatóvá válnak az infrastruktúra szolgáltatásait igénybevevő kormányzati, gazdasági, és más informatikai rendszerek is. Az Internet lényegében bárhonnan könnyű útvonalat biztosít kibertámadások, kiberbűncselekmények végrehajtásához. Mindebből következik, hogy a kiberbiztonság fenntartása több szereplőre kiterjedő és széleskörű együttműködést igényel.

Jelen publikáció egy szélesebb körű, a kiberbiztonsági szervezetek információcsere igényeit, és az ehhez kapcsolódó interoperabilitási követelményeket vizsgáló kutatás második részét képezi. Az előzőben rendszerezésre kerültek a kiberbiztonsági szervezetek főbb típusai, és ezek funkciói, feladatai. A következő tárgya pedig a kiberbiztonsági szervezetek közötti információcseréhez kapcsolódó interoperabilitási problémák és követelmények vizsgálata lesz.

A kiberbiztonsági szervezetek által kezelt információk körét – más szervezetekhez hasonlóan – funkcióik, feladataik határozzák meg, amelyeket az előző publikációban mutattunk be. Jelen publikáció célja a kiberbiztonsági szervezetek által kezelt, illetve a köztük áramló információk, és az információcsere alapvető jellemzőinek feltárása, leírása és értékelése. Ennek érdekében a következőkben:

- rendszerezzük a kiberbiztonsági eseménykezelő és műveleti központok által kezelt, és a köztük áramló információk körét, amelyek között – különösebb indoklás nélkül is elfogadhatóan – kiemelt szerepet a kiberbiztonsági eseményekre, illetve a kiberbiztonsági sérülékenységekre vonatkozó információk játszanak;
- meghatározzuk a két említett csoportba tartozó legfontosabb információkat, és a szervezetek közötti cseréjük alapvető formáit;
- végül röviden rendszerezzük a két csoportba nem tartozó, további információkat.

KIBERBIZTONSÁGI SZERVEZETEK ÁLTAL KEZELT INFORMÁCIÓK

A kiberbiztonsági eseménykezelő és műveleti központok által kezelt információk körének általános érvényű meghatározása elsődlegesen a szervezetek funkciói, feladatai, és az ezekre vonatkozó előírások, ajánlások alapján, valamint a ténylegesen kezelt, közreadott információk

elemzésével lehetséges. Mivel az információk a világ dolgaira, azok tulajdonságaira és viszonyaira vonatkozó ismeretelemek, a kiberbiztonsági információk körének meghatározásához jó kiinduló alapot képezhetnek a kiberbiztonság alapvető fogalmait és azok kapcsolatrendszerét leírni szándékozó kiberbiztonsági ontológiák, amelyek felhasználhatóak az információkkal jellemzett legfontosabb objektumok azonosítására. A következőkben először áttekintjük, rendszerezzük a kiberbiztonsági szervezetek által kezelt információkat, majd összegezzük, hogy ezek közül mely információkat cserélnek más szervezetekkel és milyen formában.

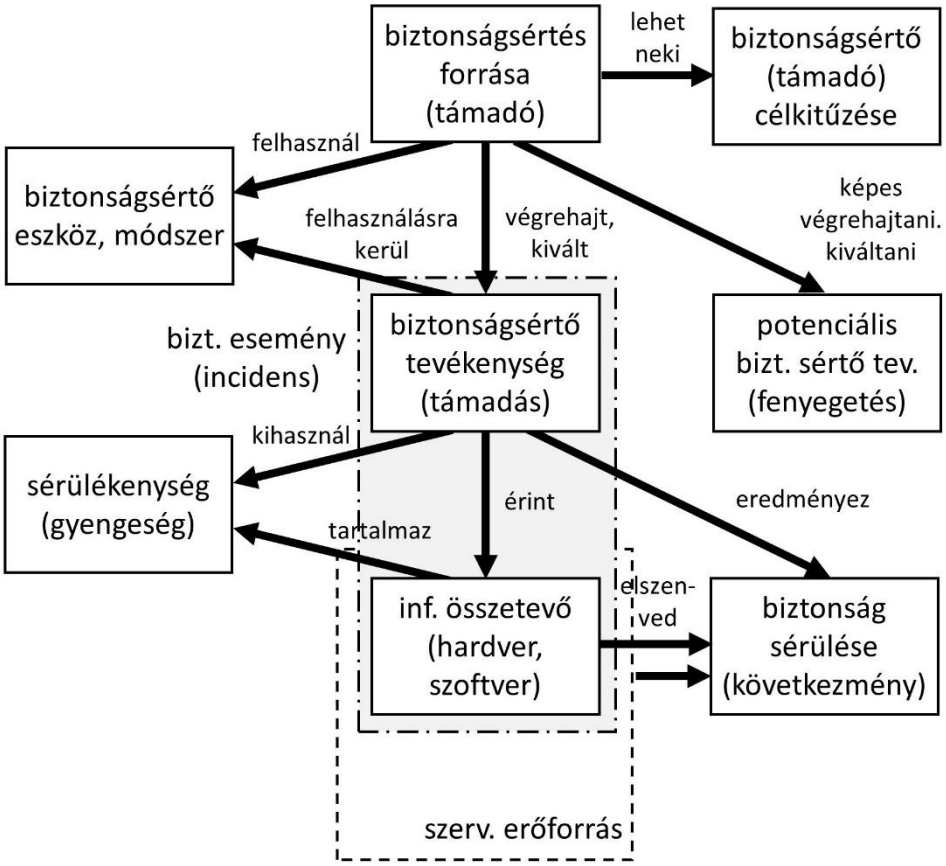
A ***kiberbiztonsági szervezetek által kezelt információk*** elméleti alapjait a kiberbiztonsági[1] taxonómiákban, ontológiákban, információcsere szabványokban szereplő alapvető objektumok képezik. Az információk ugyanis mindig dolgok (objektumok) jellemzőit, kapcsolatait írják le, így az információk körének meghatározásához először az információkkal jellemzett objektumok körét kell meghatározni. Az ontológiák, taxonómiák alapvető fogalmai között pedig értelemszerűen megtalálhatóak azok a dolgok (objektumok), amelyekre vonatkozóan a kiberbiztonsági szervezetek információkat kezelnek, cserélnek. Bár az elért eredmények ellenére egységesen elfogadott kiberbiztonsági ontológia mindmáig nincs, de a különböző változatok[2], illetve a következő fejezetben részletesebben ismertetett adatformátumok tartalma témánk szempontjából elegendő mértékben egybevág.

A kiberbiztonsági információk által jellemzett legfontosabb objektumok elsőként egy ma is sokszor hivatkozott 1998-as jelentésben [1] jelentek meg. A jelentés a kiberbiztonsági események bekövetkezésének útját és az egyes összetevők (támadó, eszköz, sérülékenység, [támadó] tevékenység, [támadás] célpontja, nem megengedett eredmény, [támadó] célkitűzése) típusait írta le. Ezek az objektumok mindmáig a kiberbiztonsági szervezetek tevékenysége során használt fogalmak, amelyekre vonatkozó információk a szervezetek által kezelt információk között kiemelt helyet foglalnak el.

A napjainkig megjelent kiberbiztonsági (informatikai biztonsági) ontológiákban további alapvető objektumok kerültek meghatározásra, amelyek közül a kiberbiztonsági szervezetek közötti információcsere szempontjából legfontosabbnak ítélteket a következő ábra tartalmazza.

[1] Vagy részben eltérő tárgyú információbiztonsági, informatikai biztonsági, számítógép biztonsági ontológiák, taxonómiák.

[2] A körre vonatkozóan lásd például a kiberbiztonsághoz kapcsolódó 10 taxonómiát, 4 információcsere/megosztás szabványt és 13 ontológiát áttekintő 2017-es publikációt. [2]



1. ábra: A kiberbiztonság kiválasztott alapvető fogalmai és kapcsolatrendszerük

A fenti ábrából hiányzik számos további fogalom (objektum) is, amelyek a különböző ontológiákban megjelennek, pld. a biztonságsértő (támadó) összetett műveletei, a biztonság megőrzését szolgáló biztonsági intézkedések (kontrollok), sérülékenység javítások, vagy a biztonságsértő tevékenységet jelző megfigyelhető "nyomok". Ezekkel jelen publikációban terjedelmi okokból nem, vagy csak korlátozott mértékben foglalkozunk.

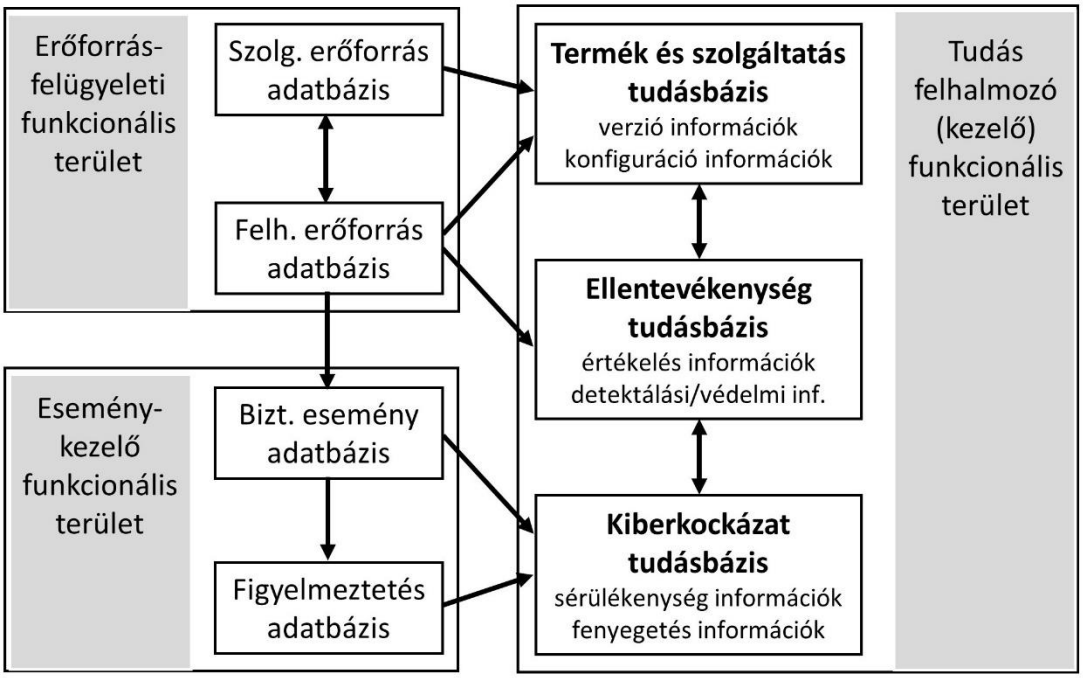
A *kiberbiztonsági szervezetek által a gyakorlatban kezelt információk* más megközelítésben, a kiberbiztonsághoz kapcsolódó funkciók szerint csoportosítva is modellezhetőek. Jelen publikációban ennek alapját a Nemzetközi Távközlési Egyesület X.1500 sorozatba tartozó, a kiberbiztonsági információk cseréjére vonatkozó szabványai[3] (ajánlásai) képezik.

A szabványsorozat célja, hogy meghatározza azokat a technikákat, amelyek segítségével a kiberbiztonsági szereplők (elsősorban üzemeltető, fejlesztő, gyártó, illetve eseménykezelő szervezetek) megbízható módon cserélhetnek kiberbiztonsági információkat. Ez az információcsere jelentős szerepet játszik a megfelelő szintű kiberbiztonság fenntartásában, az infrastruktúra védelemben, és a kiberbiztonsági eseménykezelő, vagy műveleti központok eredményes működésében.

Az X.1500 alapszabvány [3] 1. melléklete tartalmaz egy kiberbiztonsági információcsere ontológiát, amely az kiberbiztonsági információkat három funkcionális területre[4] csoportosítva

[3] International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Series X.1500 Cybersecurity information exchange (CYBEX).
[4] Operation domain.

tartalmazza. A három funkcionális terület az eseménykezelés, az erőforrás felügyelet, és a kiberbiztonsági tudás felhalmozás (kezelés). A funkcionális területek által kezelt adatbázisokat és tudásbázisokat, valamint a köztük fennálló kapcsolatokat a következő ábra szemlélteti.



2. ábra: A kiberbiztonsági információcsere ontológia modellje[5]

Az erőforrás felügyeleti funkcionális terület rendeltetése az informatikai erőforrásokhoz kapcsolódó biztonsági eseményeket megelőző és kárelhárítási (telepítési, konfigurálási, és felügyeleti) feladatok megvalósítása. A funkcionális terület két információcsoportot (adatbázist) kezel. A felhasználói erőforrás adatbázis a szervezet informatikai erőforrásainak biztonsági szempontból lényeges adatait (listáját, konfigurációit, felhasználási szintjét, biztonsági eljárásokat, értékeléseket, stb.) tartalmazza. A szolgáltatói erőforrás a szervezeten kívüli, a szervezet által használt (pld. felhő alapú) erőforrások szükséges adatait tartalmazza.

Az eseménykezelő funkcionális terület rendeltetése a kiberbiztonsági biztonsági események kezelése (detektálása, értékelése és megválaszolása), valamint figyelmeztetések kiadása. A funkcionális terület két információcsoportot (adatbázist) kezel. A biztonsági esemény adatbázis a felhasználói erőforrás adatbázis adatainak felhasználásával, azok elemzésével kerül bővítésre, és esemény, biztonsági esemény, valamint támadás adatokat tartalmaz. A figyelmeztetés adatbázis a szervezeten belüli, vagy kívüli tájékoztatásra szánt statisztikai adatokat, figyelmeztetéseket (riasztások és segítséget nyújtó javaslatok) tartalmaz. Alapját a biztonsági esemény adatbázis, és a kiberbiztonsági kockázat tudásbázis adatai képezik.

A kiberbiztonsági tudás felhalmozó (kezelő) funkcionális terület rendeltetése a különböző, köztük külső forrásokból származó, kiberbiztonsághoz kapcsolódó információk gyűjtése, előállítása, rendszerezése. A funkcionális terület által kezelt információk három tudásbázisba csoportosíthatóak. Az információk szervezeten kívüli forrásai közé az informatikai termékek fejlesztői, gyártói, valamint a kiberbiztonsági szakterület szervezetei, kutatói tartoznak. A kiberbiztonsági kockázat tudásbázis ismert, és az adott szervezet számára releváns sérülékenységekre és fenyegetésekre vonatkozó információkat tartalmaz. Az ellentevékenység tudásbázisba az informatikai erőforrások biztonsági értékeléséhez felhasználható információk (szabályok,

[5] ITU-T X.1500 Figure II-1 – CYBEX Ontology Model alapján [3, 17. o.]

feltételek, konfiguráció ellenőrző listák, stb.), valamint a fenyegetések bekövetkezését detektáló, vagy azokat megakadályozó szabályok és feltételek tartoznak. Végül a termék és szolgáltatás tudásbázis a termékek, szolgáltatások megnevezéseire, verzióira, javítócsomagjaira, valamint a termékek, szolgáltatások ismert, ellenőrzött konfigurációira vonatkozó információkat foglalja magában.

KIBERBIZTONSÁGI SZERVEZETEK KÖZÖTTI INFORMÁCIÓCSERE ALAPJAI

A ***kiberbiztonsági szervezetek közötti információcsere*** áttekintéséhez először fel kell vázolnunk a *kiberbiztonsági szervezetek közötti együttműködési kapcsolatok* főbb típusait. Ezek közé a következők tartoznak:

- kiberbiztonsági eseménykezelő központ, illetve a felügyelete alá, szolgáltatási körébe tartozó kiberbiztonsági műveleti központok (üzemeltető szervezetek) közötti kapcsolatok;
- "fölé-alárendelt", átfogóbb-szűkebb felelősségi körű (pld. nemzeti és ágazati; vagy egy ágazaton belül nemzetközi, regionális, szövetségi és nemzeti) eseménykezelő központok közötti kapcsolatok;
- "mellérendelt", egymást nem átfedő felelősségi körű (pld. különböző nemzeti, vagy különböző ágazati) eseménykezelő központok közötti kapcsolatok;
- kiberbiztonsági eseménykezelő és műveleti központok, illetve informatikai termékek fejlesztői, gyártói közötti kapcsolatok;
- kiberbiztonsági eseménykezelő és műveleti központok, illetve katonai, rendőri, és nemzetbiztonsági szervezetek közötti kapcsolatok (jelen publikációban a továbbiakban ezen kapcsolatokkal nem foglalkozunk).

A kiberbiztonsági információk megosztásának feltételeit – a jogszabályi előírások keretei között – az egyes szervezetek információ-megosztási politikái és a szervezetek közötti bizalmi viszonyok határozzák meg. Emellett *az információcsere, megosztás megvalósításának módja* is többféle lehet[6]:

- két szereplő közötti egy- vagy kétirányú információcsere (peer-to-peer);
- centralizált elosztásra épülő információmegosztás (hub-and-spoke);
- több szereplő közötti közvetlen információmegosztás (post-to-all);
- valamint ezek ötvözetére épülő hibrid megoldások.

Az információcsere, megosztás technikája lehet lekérdezés-válasz, vagy előjegyzés-automatikus értesítés alapú.

Az egyes megoldások összefüggésben állnak a résztvevők közötti bizalmi szinttel. A több szereplő közötti közvetlen információmegosztás magas bizalmi szintet feltételez. A centralizált elosztásra épülő megoldás működőképes lehet magas és közepes bizalmi szint esetében (utóbbi esetben a központi elosztó szűrési lehetőségeire építve). Végül a két szereplős információmegosztás, az egyedi korlátozások érvényesítésének lehetősége miatt nem követel magas, vagy közepes bizalmi szintet sem.

A *kiberbiztonsági szervezetek közötti információcsere alapvető rendeltetése*, hogy ennek révén minden szervezet hozzájusson a tevékenységéhez, és ezt a tevékenységet megalapozó döntéseihez szükséges információkhoz. Ehhez azokat az információkat kell megosztani, rendelke-

[6] Részletesebben lásd pld. a kapcsolódó MITRE tanulmányt [4], és az ITU-T X.1550 szabványt [5].

zésre bocsátani, amelyek az információt felhasználó szervezet számára szükségesek és elégségesek. Ezt az ENISA dokumentumai közvetlenül hasznosítható információnak[7] nevezik, és szükséges tulajdonságai közé a relevanciát, időszerűséget, pontosságot, a meghatározott célok szempontjából teljes körűséget, valamint az "emészthetőséget" sorolják. Ez utóbbi olyan formát jelent, amely lehetővé teszi az adatok egyszerű importálását, a lényeges alapadatok és mutatók[8] kinyerését.

Az ***információcsere alapvető jellemzőit*** a következőkben a kiberbiztonsági eseménykezelő és műveleti központok nézőpontjából, az általuk kezelt információk típusai szerint, négy csoportra (eseményekre, sérülékenységekre, fenyegetésekre vonatkozó, és további információkra) tagolva fogjuk tárgyalni.

A *kiberbiztonsági eseményekre (incidensekre) vonatkozó információk cseréje* az incidenst 'elszenvedő' szervezettől (műveleti központtól) az eseménykezelő központokhoz, majd esetleg további szervezetekhez irányul. A biztonsági események jelentési kötelezettségét előírhatja jogszabály, az önkéntes bejelentésre sor kerülhet segítséghez jutás céljából, vagy az átfogó kiberbiztonság érdekében, de el is maradhat.

A biztonsági eseményekre vonatkozó információkat az eseménykezelő szervezetek tárolják, értékelik, kiegészítik, és szükség esetén fenyegetések jelzéseként továbbítják más kiberbiztonsági szervezeteknek. Az értékelés eredménye lehet új sérülékenység felismerése, vagy feltételezése. A biztonsági eseményekre vonatkozó információk időszakonként rendszerezésre, összegzésre kerülnek.

A *kiberbiztonsági sérülékenységekre vonatkozó információk cseréje* a sérülékenységeket leíró bejelentéssel indul, amit bárki megtehet. A bejelentés történhet közvetlenül a gyártóhoz, vagy – amennyiben van ilyen – a felügyelő, szolgáltatást nyújtó kiberbiztonsági eseménykezelő központhoz, illetve közvetlenül a médiában. A sérülékenységek életciklusának négy alapvető szereplője: a felfedező/bejelentő; a koordinációs szerepet játszó kiberbiztonsági eseménykezelő központ; az érintett termék fejlesztője, gyártója; illetve a sérülékenységgel rendelkező informatikai összetevőt felhasználó alkalmazói kör. [8, 20. o.]

Az új sérülékenységekről a kiberbiztonsági szervezetek tájékoztatják az érintett gyártót, esetleg nyilvánosságra hozzák, illetve a megszerzett információkat egymással megosztják, és ennek alapján naprakész nyilvántartást vezetnek (ami lehet a felügyeletük alá tartozó szervezetek által üzemeltetett informatikai összetevők alapján szűrt). Egyes kiberbiztonsági szervezetek globális sérülékenység nyilvántartásokat vezetnek, illetve tesznek közzé. A sérülékenységek nyilvánosságra hozatalát különböző szempontok határozhatják meg, aminek eredménye lehet: nincs közzététel, teljes közzététel, gyártón keresztüli (a megoldás kidolgozását követő) közzététel, vagy korlátozott közzététel. [8, 23-25.]

A sérülékenységekkel érintett informatikai összetevők gyártói a bejelentett sérülékenységeket kivizsgálják, azok megszüntetésére, vagy hatásaik csökkentésére megoldásokat, javítócsomagokat dolgoznak ki, és adnak közre. Ezek a kiberbiztonsági szervezetekhez is eljutnak, amit nyilvántartásaikban, működésük során felhasználnak.

A *kiberbiztonsági fenyegetésekre vonatkozó információk cseréje* a potenciális biztonságsértő eseményekre vonatkozó – a kiberbiztonsági kockázatkezelésben felhasználásra kerülő – információk cseréjét jelenti, amelyben jelentős szerepet játszanak a potenciális biztonságsértőkre,

[7] Actionable information [6, 2-4. o.]

[8] Az [kiberhírszerzési] alapadat (observable) a kiberfenyegetés elleni hírszerzés (cyber threat intelligence) szakkifejezése, amely mérhető/megfigyelhető esemény, vagy állapotot leíró tulajdonság a kibertartományban/kibertérben. A mutató pedig meghatározott alapadatok háttér információkkal kiegészített mintázata, amely adott dolgot, vagy viselkedést reprezentál. [7, 14. o.]

támadókra, valamint az általuk alkalmazott módszerekre, eljárásokra vonatkozó elemzett, értékelt, szintetizált információk. Míg a sérülékenységekhez kapcsolódó információk a károkozó biztonsági események "saját oldali/belső" részét, addig a fenyegetésekhez kapcsolódó információk a "támadó oldali/külső" részét képezik.

A fenyegetésekre vonatkozó információk egy része a kiberbiztonsági eseménykezelő és műveleti központokban is előállítható, azonban ez speciális képességeket, megoldásokat igényel. Az új funkció, szakterület megnevezésére született a kiberfenyegetés elleni hírszerzés (Cyber Threat Intelligence[9], CTI) mindmáig bizonytalannak tartott, de rohamléptekben terjedő fogalma [9], és születtek meg az ezzel foglalkozó – az eseménykezelő szervezetek hagyományos funkcióit meghaladó – szervezetek, szervezeti elemek.

KIBERBIZTONSÁGI ESEMÉNYEKRE VONATKOZÓ INFORMÁCIÓK

A kiberbiztonsági eseménykezelő és műveleti központok folyamatosan fogadják, elemzik, és szükség esetén továbbítják a hatókörükbe tartozó szervezeteket, informatikai rendszereket, hálózatokat érintő kiberbiztonsági eseményekre (incidensekre) vonatkozó információkat. Ezek alapvetően belső információk, elsősorban az érintett szervezetek, és az őket támogató eseménykezelő központok között áramolnak.

A biztonsági eseményekre vonatkozó információk két nagy csoportba sorolhatóak: az elsődleges nyers esemény információkra, valamint az értékelt esemény információkra. Az információk köre – amely az incidenskezelés során folyamatosan bővülhet, pontosodhat – minimálisan a bejelentőre, a bekövetkezett eseményre, az érintett összetevőre, az esemény következményeire, valamint (külső) forrására, módszerére vonatkozó információkat tartalmazza.

Konkrét kiberbiztonsági eseményekre vonatkozó információk más szervezetek számára, az információk szenzitív jellege miatt csak korlátozottan kerülnek továbbításra.[10] Az eseménykezelő központok eseményekre vonatkozó információkat oszthatnak meg [10, 9-13. o.]:

- más eseménykezelő központokkal (megelőző jelleggel, fenyegetések, vagy az esetleges továbbgyűrűző hatások jelzésére);
- hálózat- (internet) szolgáltatókkal (támadások korlátozása, támadók azonosítása céljából);
- informatikai gyártókkal, szolgáltatókkal (eseménykezelés segítése céljából);
- bűnüldöző szervekkel (a kapcsolódó bűnügyi lépések megtétele érdekében);
- eseményinformáció megosztást támogató szervezetekkel (az általános kiberbiztonság növelése céljából);
- a támogatott ügyfélkörrel, felhasználókkal, közvéleménnyel.

A ***kiberbiztonsági eseményre vonatkozó alapvető információk*** közé a bejelentőre vonatkozó információk, az eseményhez kapcsolódó időpont információk, valamint az esemény rövid leírása tartozik.

A *bejelentőre vonatkozó információk* közé a szokásos általános információk (név, elérhetőségek, képviselt szervezet [ha van]) tartoznak. Szerepük egyrészt a további kapcsolattartás feltételeinek biztosítása, másrészt – és ez talán még jelentősebb is – felhasználásra kerülnek a

[9] A hírszerzés/hírszerzési információ (intelligence) általános értelmezés szerint a szervezeti döntéshez a szervezeten kívülről szükséges információk megszerzése, elemzése, értékelése, illetve maga az elemzett, értékelt információ.

[10] Az incidensekre vonatkozó információk ezen kívül összesített, szintetizált formában, kiberbiztonsági helyzetértékelések, fenyegetés értékelések formájában közreadásra kerülhetnek.

bejelentés hitelességének, megbízhatóságának megítélése során. Amennyiben az eseményt kiberbiztonsági szervezet jelenti be, nyújt róla tájékoztatást, az együttműködést segítheti az eseményhez a bejelentő szervezetben hozzárendelt azonosító (tracking number).

Az *eseményhez kapcsolódó időpont információk* közé az észlelés időpontja, a bekövetkezés időpontja, valamint a befejeződés időpontja tartozik. Az észlelés és a befejeződés időpontja egyértelműen meghatározható. A bekövetkezés időpontja lehet feltételezett, megközelítő, vagy bizonyítható, és az észlelést követően lefolytatott vizsgálatok alapján kerülhet meghatározásra, majd a későbbi vizsgálatok alapján pontosításra.

A ***kiberbiztonsági esemény besorolása*** a megfelelő bejelentési, eseménykezelési eljárásrendeknek megfelelő kategória rendszerre épül. Mint a szakterületen más esetben is, egységesen elfogadott kategória rendszerrel nem találkozhatunk, több kategória rendszer, taxonómia is létezik. Ez utóbbiak megnevezése általában esemény, vagy fenyegetés taxonómia.[11]

Az *Egyesült Államok szövetségi incidens jelentési irányelvei* hét kategóriából álló besorolást írnak elő.[12] A kategória rendszer elemei:

CAT 0 - gyakorlat, biztonsági tesztelés
CAT 1 - jogosulatlan hozzáférés
CAT 2 - szolgáltatás akadályozás
CAT 3 - rosszindulatú kód
CAT 4 - helytelen használat
CAT 5 - felderítés, információgyűjtés
CAT 6 - kivizsgálás alatt álló esemény

Az *Európai Unióban alkalmazott megoldásokról* és egy referencia taxonómia kialakításának irányairól az ENISA 2018 januárjában adott ki egy tanulmányt. [12] A tanulmány alapját az Európai CSIRT Hálózat (eCSIRT.net) taxonómiája, valamint az EUROPOL Közös taxonómia a bűnüldöző szervek és a kiberbiztonsági eseménykezelő központok számára képezi. Mindkét taxonómia két szintű, felső szintjei – két a bűnüldözési terület szempontjából nem releváns kategóriától eltekintve – azonosak, de a második szintek már eltéréseket mutatnak.

Az eCSIRT.net felső szintű kategóriái a következőek:

- visszaélésszerű tartalom
- felderítés, információgyűjtés
- rendelkezésre állás megsértése
- csalás
- egyéb
- rosszindulatú kód
- behatolások
- információ jogosulatlan elérése, módosítása
- sérülékenység
- tesztelés

A ***kiberbiztonsági esemény által érintett összetevőkre*** vonatkozó információk a reagáló eseménykezelési feladatok megvalósítását szolgálják. Ezek közé az érintett összetevők típus információi, és egyedi jellemzői tartoznak. Az összetevők lehetnek rendszerösszetevők, szolgáltatások, szoftver összetevők, szoftver folyamatok, fájlok. A *típus információk* közé tartozhatnak: az összetevő rendeltetése, funkciója; a szoftver összetevő típusa; az operációs rendszer platform típusa. Ezek az információk (amennyiben az információkat kezelő szervezetek rendelkeznek ilyenekkel) szinkronban kell legyenek a sérülékenység, illetve a szervezeti erőforrás nyilvántartásokban foglaltakkal.[13] Az *egyedi jellemzők* többek között lehetnek: az érintett összetevő azon hálózati azonosítói (IP cím, név), földrajzi helye, alkalmazott javító csomagok köre, stb.

A ***kiberbiztonsági esemény következménye, hatásai*** az eseménykezelés fontos információi közé tartoznak, alapvetően befolyásolják az esemény súlyosságának meghatározását, az ese-

[11] A két fogalom egymás kiegészítője: az esemény bekövetkezett fenyegetés, a fenyegetés potenciális esemény.
[12] Az Egyesült Államok hadereje egy ennél részletesebb, kilenc elemből álló besorolási rendszert alkalmaz. [11]
[13] Részletesebben lásd a következő pontban, a sérülékenységek tárgyalásánál.

ménykezelő tevékenységek prioritásait, a ráfordítandó erőforrások, és az együttműködési feladatok körét. A következményekre, hatásokra vonatkozó információk típusuk szerint lehetnek igen/nem, többszintű mérési skála szerinti besorolás, vagy mennyiségi jellegűek.

Az *Egyesült Államok központi eseménykezelő szervezete* (US-CERT) online esemény bejelentő felületén például a következőket kell/lehet megadni:

- az informatikai rendszer bizalmassága, sértetlensége, rendelkezésre állása sérülése;
- a hatás mértéke a szervezet működésére, kritikus, és nem kritikus szolgáltatásaira;
- az érintett rendszerek száma;
- az érintett felhasználók száma;
- az információs hatás jellege;
- az érintett rekordok száma;
- a helyreállítás várható időtartama.

Az *ENISA irányelvei szerint* a kiberbiztonsági események hatásaira vonatkozóan éves jelentésben, vagy egyedi jelentésekben elsősorban a következő adatok továbbítandóak/továbbíthatóak [13, 12-13. o.][14]:

- érintett szolgáltatások (jelenleg távközlési szolgáltatások);
- érintett felhasználók száma;
- esemény időtartama;
- valamint további, távközlési szolgáltatás specifikus jellemzők.

A *magyar Hun-CERT* online esemény bejelentő felületén az okozott kár milyensége, becsült összege, vagy egyéb jellemzői adhatók meg szöveges formában.

A ***kiberbiztonsági esemény forrására***, az esetleges támadó, károkozó félre, összetevőre vonatkozó azonosító információk az eseménykezelés során elsősorban a káros hatás, támadás elszigetelése, megszüntetése során használhatóak fel. A kiberbiztonsági szervezetek ezen információkat juttatják el partner szervezeteiknek, a hálózat-szolgáltatóknak, vagy a bűnüldöző szerveknek. Ide tartoznak mindenekelőtt az esemény vizsgálata során feltárt hálózati azonosítók (IP címek, IP tartományok, nevek), e-mail címek, honlap címek, és más, a támadó félhez köthető, megszerzett információk.

Az azonosító információk mellett az eseménykezelés során általában rögzítésre kerül az esemény forrásának, okának típusa, amelyre különböző besorolási rendszerek léteznek.

Az *ENISA irányelvek szerinti alapvető okok* a következők lehetnek [13, 13-14. o.]:

- emberi hiba;
- rendszerhiba;
- természeti jelenség;
- rosszindulatú tevékenység;
- külső fél hibája.

A ***kiberbiztonsági esemény lefolyására***, a támadás módszerére, eszközeire vonatkozó információk egyaránt hasznosíthatóak az esemény kezelése, elhárítása, illetve azt követően, a sérülékenységek és fenyegetések kezelése során. Ide tartoznak a biztonságsértés, támadás következő jellemzőire vonatkozó információk:

- a végrehajtott lépések, a támadás útvonala;
- a kihasznált sérülékenységek;
- az alkalmazott módszerek, felhasznált eszközök.

[14] Az európai szabályozás jelenleg a távközlési szolgáltatók; elektronikus azonosítási és bizalmi szolgáltatást nyújtó szolgáltatók; valamint a felhő-, elektronikus kereskedelmi és kereső szolgáltatásokat nyújtók számára írja elő meghatározott szintű események bejelentési kötelezettségét.

Az Egyesült Államok központi eseménykezelő szervezete a támadás útvonalára (módszerére) a következő besorolás alkalmazását írja elő [10, 25-26. o.]:

- külső/cserélhető adathordozó;
- kimerítés;
- web;
- email;
- megszemélyesítés;
- helytelen használat;
- eszköz elvesztése, ellopása;
- egyéb.

A fentiekben felsorolt információk mellett ***további információk*** is kapcsolódnak a kiberbiztonsági eseményekhez, amelyek felhasználásra kerülhetnek az eseménykezelési folyamatokban, és továbbításra kerülhetnek kiberbiztonsági szervezetek között is. Ezek közé tartozhatnak többek között a következők:

- az eseményekhez kapcsolódó tárgyi bizonyítékok (napló fájlok, kódrészletek, stb.);
- az eseménykezelési végrehajtott feladatai, történeti információi;
- kapcsolatok más kiberbiztonsági eseményekkel.

KIBERBIZTONSÁGI SÉRÜLÉKENYSÉGEKRE VONATKOZÓ INFORMÁCIÓK

A kiberbiztonsági sérülékenységekről a kiberbiztonsággal foglalkozó szervezetek globális, és szervezeti szintű nyilvántartásokat, adatbázisokat tartanak fent, és használnak tevékenységük során. A globális nyilvántartások között kiemelt szerepet játszik a MITRE cég által kezelt Sérülékenységek Listája (Common Vulnerabilities and Exposures, CVE)[15], valamint az Egyesült Államok arra épülő, azt kiegészítő Nemzeti Sérülékenység Adatbázisa (National Vulnerability Database, NVD), a web alkalmazásokra vonatkozóan pedig a Nyílt Web Alkalmazás Biztonsági Projekt (Open Web Application Security Project, OWASP) sérülékenység listája.

A kiberbiztonsági sérülékenységekre vonatkozó információk köre minimálisan a sérülékenység azonosítását és leírását, az érintett informatikai összetevőt (összetevőket), valamint a sérülékenység kihasználásának következményét tartalmazza. Ezen kívül szerepelhetnek kiegészítő információkra vonatkozó hivatkozások; a sérülékenység értékelése, súlyossági szintje; a kihasználás lehetőségei, már ismert eszközei; valamint a sérülékenységet megszüntető, vagy hatását korlátozó megoldások (ezekkel részletesebben nem foglalkozunk).

A ***sérülékenységek azonosítása, leírása*** alapvető szerepet játszik a kiberbiztonságban érintett szervezetek közötti információcserében. A legszélesebb körben alkalmazott *sérülékenység azonosító* a MITRE Sérülékenységek Listájának CVE azonosítója, amelynek egyediségét egy eljárás- és szervezetrendszer[16] biztosítja. A nemzetközileg alkalmazott azonosító mellett kiberbiztonsági szervezetek saját azonosítókat is alkalmaznak, a magyar nemzeti CERT (GovCERT-Hungary) azonosító formátuma CH-99999[17]. Saját azonosító alkalmazását teszi szükségessé az is, hogy egy kiberbiztonsági szervezet új, még nem igazolt, vagy nyilvánosságra nem hozott sérülékenységekre vonatkozó információkat is kezelni tudjon.

A *sérülékenységek leírásának* rendeltetése, hogy rövid szöveges formában elegendő információt nyújtson az egyes sérülékenységek megtalálásához, illetve a hasonló sérülékenységek megkülönböztetéséhez. A CVE lista útmutatója szerint a leírás jellemzően tartalmazza a sérülékenység típusát, az érintett terméket, gyártót, verziót, a kihasználás következményeit (hatását), valamint a kihasználáshoz szükséges elérési módot.

[15] Az 1999 januárjától vezetett lista 2018 elején mintegy 95000 sérülékenységet tartalmazott. Az évi bővülés 2016-ig 4000-8000 között volt, 2017-ben mintegy 14000 új sérülékenység került a listába.
[16] CVE sérülékenységi listáért felelős hatóságok (CVE Numbering Authority, CNA) többszintű rendszere.
[17] 2010 júliusáig CHK-AH-EEEE-999.

A ***sérülékenységek osztályozása*** számos különböző szempont szerint lehetséges, amelyeket elsősorban a kiberbiztonsági statisztikai elemzések, gyakorisági adatok összeállítása, trendek meghatározása során lehet felhasználni. Az osztályozás történhet az érintett informatikai összetevők, a sérülékenység kihasználásának következményei, és nem utolsósorban a sérülékenység típusa szerint.

Az egyedi sérülékenységek típusokba sorolásának széles körben használt változata a már említett *Gyengeségek Felsorolása* (CWE), amely a szoftver gyengeségek[18] típusainak szervezett, belső kapcsolatokat tartalmazó listája. A CVE egyedi sérülékenység lista elemeihez, mint kiegészítő információt, az NVD rendel CWE sérülékenység típust.

A CWE lista négyféle elemet tartalmaz:

- egyedi gyengeség típusokat, amelyek absztrakciós szintjüktől függően lehetnek gyengeség osztályok[19], alap gyengeség típusok, és gyengeség változatok;
- összetett gyengeségtípusokat, amelyek több gyengeség típus összekapcsolódó együttesei, vagy sorozatai;
- gyengeség típus kategóriákat, amelyek azonos tulajdonságokkal rendelkező gyengeség típusok összességei;
- végül gyengeség típus nézeteket, amelyek bizonyos nézőpontból összeválogatott gyengeség típusokat tartalmaznak.

A mintegy 90 CWE sérülékenység típussal szemben a web alkalmazások sérülékenységeit tartalmazó OWASP sérülékenység lista csak tíz átfogó sérülékenység kategóriát tartalmaz. Az OWASP Top Ten kiadvány 2013-as és 2017-es kiadása kategória listái között négy változás is bekövetkezett.

A magyar nemzeti CERT sérülékenység listájában a támadás típusának kötött listából választható megadása szerepel.

A ***sérülékenység által érintett szoftver összetevőkre (termékekre) vonatkozó információk*** a CVE sérülékenység listában csak szöveges formában, a leírásban szerepelnek. A sérülékenységekhez ezeket az információkat formalizált formában (az osztályozáshoz hasonlóan) az NVD rendeli.

Az adatbázisban szereplő információk az Egyesült Államok szabványosítási szervezete (NIST[20]) által kezelt *Platformok Felsorolása* (Common Platform Enumeration, CPE) szabványos formátumában, kötött listából választhatóan szerepelnek. A CPE az informatikai összetevők (termékek) következő információit tartalmazza: típus (alkalmazás, hardver, operációs rendszer), készítő (szállító), megnevezés, verzió, módosítás, kiadása (pld. server, pro, x86), végül nyelv.

A magyar nemzeti CERT által közreadott sérülékenység listában az érintett rendszerek kötött listából választható megnevezése, valamint az érintett verziók szöveges leírása szerepel.

A ***sérülékenység kihasználásának feltételeire és következményeire vonatkozó információk*** alapvető jelentőségűek a sérülékenységből fakadó biztonsági kockázatok értékeléséhez. A CVE sérülékenység listában a feltételek nem, a következmények pedig csak szöveges formában, a

[18] Szoftver megvalósításban, kódban, tervben, vagy architektúrában meglévő hiba, amely egy rendszert, vagy hálózatot - ha nem kerül kezelésre – sérülékennyé tehet támadásokkal szemben. […]

[19] CWE 2017-es 3.0 verziójában a több mint 700 egyedi gyengeség típus között mintegy 90 gyengeség osztály, több mint 300 alap gyengeség és mintegy 300 gyengeség változat található.

[20] National Institute of Standards and Technology.

leírásban szerepelnek. Ezt a NVD egészíti ki a sérülékenységek jellemzőit és értékelését szabályozó *Sérülékenység Pontozási Rendszer* (Common Vulnerability Scoring System, CVSS)[21] megfelelő elemei felhasználásával.

Az NVD a feltételekre vonatkozóan az egyes sérülékenységekhez (2-4 kategóriába sorolással) megadja a kihasználás hozzáférési feltételét, a támadás összetettségét, a szükséges jogosultsági szintet, és a felhasználói közreműködés mértékét. A következmények a bizalmasság, sértetlenség, és rendelkezésre állás megsértésének három kategóriára épülő értékelésével (nincs, alacsony = részleges, magas = teljes) kerülnek megadásra.

A magyar nemzeti CERT által közreadott sérülékenység listában a feltételre vonatkozóan a szükséges hozzáférés kötött listából (távoli, helyi, fizikai) választható megadása, a következményekre vonatkozóan pedig a három fokozatú besorolás helyett a bizalmasság, a sértetlenség, vagy a rendelkezésre állás elvesztésének hiánya, vagy bekövetkezése szerepel.

A ***sérülékenység súlyossága*** szintén a biztonsági kockázatok értékeléséhez használható. A sérülékenység adatbázisokban szereplő súlyosság természetesen nem helyettesíti az érintett szervezet biztonsági kockázat értékelését, de orientálja a szervezetet.

A súlyosság a CVE lista NVD kiegészítésében a Sérülékenység Pontozási Rendszerre alapozva szerepel. A pontozási rendszer a súlyosság 0-10 közötti pontértéket alapvetően a kihasználás feltételeinek és következményeinek besorolása alapján, néhány további (időleges és környezeti) tényező figyelembevételével határozza meg. A pontérték alapján a súlyosság egy ötfokozatú skálán (minimális, alacsony, közepes, magas, kritikus) is megadásra került.

A magyar nemzeti CERT által közreadott sérülékenység listában a súlyosság az fentiekkel megegyező ötfokozatú skálán kerül megadásra, ahol az egyes kategóriák az érintett szoftverek magyarországi elterjedtségét is figyelembe véve kerülnek meghatározásra.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegzésképpen megállapíthatjuk, hogy a kiberbiztonság, a kiberteret alkotó, hálózatba kapcsolódó informatikai rendszerek és szolgáltatásaik biztonsága napjaink egyik legfontosabb szervezeti, nemzeti, regionális, és globális biztonsági kihívása. A kibertér informatikai rendszereinek, hálózatainak szövevényes összekapcsolódása a kiberbiztonság fenntartását csak számos különböző szereplő együttműködésére épülve teszi lehetővé.

A kiberbiztonsági szervezetek közötti információcsere alapvető rendeltetése, hogy ennek révén minden szervezet hozzájusson a tevékenységéhez, és ezt a tevékenységet megalapozó döntéseihez szükséges információkhoz. Ennek az információcserének hagyományos, strukturálatlan (telefonos, szöveges, e-mail) információkra épülő megoldásai mindmáig léteznek, azonban egyre inkább előtérbe kerül az információk kiberbiztonsági tevékenységet támogató informatikai rendszerek, adatbázisok közötti, emberi közreműködést nem igénylő cseréje is.

A kiberbiztonsági szervezetek által kezelt információk négy nagyobb csoportra (eseményekre, sérülékenységekre, fenyegetésekre vonatkozó, és további információkra) tagolhatóak. A szervezetek az eseményekre vonatkozó információkat folyamatosan fogadják, elemzik, és szükség esetén továbbítják a hatókörükbe tartozó, valamint együttműködő szervezeteknek. A kiberbiztonsági sérülékenységekről globális, és szervezeti szintű nyilvántartásokat, adatbázisokat tartanak fent, és használnak tevékenységük során.

[21] A CVSS szabvány kezelője az Eseménykezelő és Biztonsági Csoportok Fóruma (Forum of Incident Response and Security Teams, FIRST).

FELHASZNÁLT IRODALOM

[1] HOWARD, J. D.-LONGSTAFF, T. A.: *A Common Language for Computer Security Incidents.* – Sandia National Laboratories, Albuquerque,1998 október.

[2] MAVROEIDIS, V.-BROMANDER, S.: Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. – In. *Proceedings of the European Intelligence and Security Informatics Conference*, Attica, Greece, 2017 szeptember 11-13. (91-98. o.)

[3] Recommendation ITU-T X.1500, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATION AND SECURITY. Cybersecurity information exchange – Overview of cybersecurity. Overview of cybersecurity information exchange. – Telecommunication Standardization Sector of International Telecommunication Union, 2011 április.

[4] Cyber Information-Sharing Models. An Overview. – MITRE Corporation, 2012 október.

[5] Recommendation ITU-T X.1550, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATION AND SECURITY. Cybersecurity information exchange – Exchange of policies. Access control models for incident exchange networks. – Telecommunication Standardization Sector of International Telecommunication Union, 2011 április.

[6] *Actionable Information for Security Incident Response.* – European Union Agency for Network and Information Security, Heraklion, 2014 november.

[7] BARNUM, S.: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX) v1.1 – MITRE Corporation, 2014 február.

[8] *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*. – European Union Agency for Network and Information Security, Heraklion, 2015 november.

[9] CHISMON, D.-RUKS, M.: *Threat Intelligence: Collecting, Analysing, Evaluating.* – MWR InfoSecurity - CERT-UK - Centre for the Protection of National Infrastructure, 2015 március.

[10] CHICONSKI, P.-MILLAR, T.-GRANCE, T.-SCARFONE, K.: *Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide.* – National Institute of Standards and Technology, 2012 augusztus.

[11] CJCSM 6510.01B, Cyber Incident Handling Program. – US DoD Joint Chiefs of Staff, 2014 december.

[12] *Reference Incident Classification Taxonomy. Task Force Status and Way Forward.* - European Union Agency for Network and Information Security, Heraklion, 2018 január.

[13] Technical Guideline on Incident Reporting. Technical guidance on the incident reporting in Article 13a Version 2.0. – European Union Agency for Network and Information Security, Heraklion, 2013 január.