HADMÉRNÖK

VI. Évfolyam 4. szám - 2011. december

Papp Zoltán
pappz.szeged@gmail.hu

AZ INFORMÁCIÓ TÁMADÁSA ANNAK TULAJDONSÁGAIN KERESZTÜL

Absztrakt

Fejlett korunkban a társadalmi, a gazdasági, illetve a rendvédelmi szektor működésében az információ központi szerepet tölt be, így annak megfelelő minősége elengedhetetlenül fontos ahhoz, hogy a döntés-előkészítő, a döntéshozó, illetve a végrehajtó folyamatok hatékonysága az igényeknek megfelelő legyen. Az adat, az információ a keletkezéstől a felhasználásig számos munkafolyamaton keresztül alakul át, ahol az eltérő indíttatású támadóknak – fázisonként különböző módszerrel, akár technikai, akár kognitív dimenzióban – lehetőségük van arra, hogy az adat, az információ különböző jellemzőit módosítsák, ezáltal gyakorolva hatást az adatgyűjtő, elemző, döntéshozó és végrehajtó folyamatokra.

Information has a central role in the functioning of the social, economic and law enforcement sectors in our modern age, therefore its appropriate quality is of utmost importance for operating efficient decision support, decision making and executive processes. From its creation until its actual usage, data and information undergo several work processes during which attackers of various motives – applying different methods in each phase either in the technical or the cognitive dimensions – are able to modify certain parameters of the data and information, thus impacting the data collecting, analyzing, decision making and executive processes.

Kulcsszavak: *információ, támadás ~ information, attack*

BEVEZETÉS

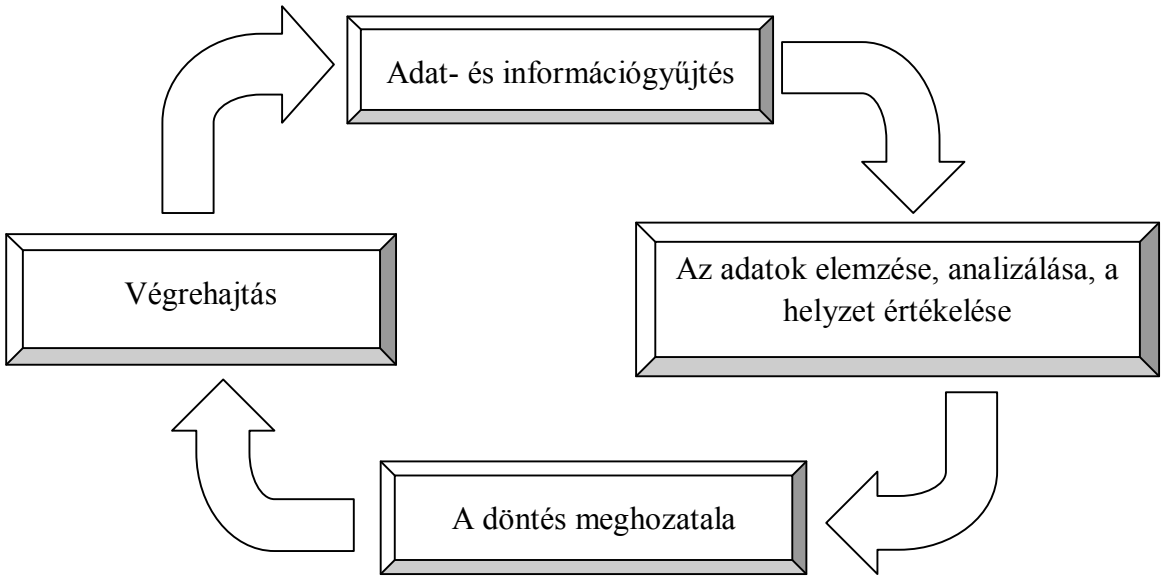
Az információ latin eredetű szó, amely értesülést, hírt, üzenetet, tájékoztatást jelent. Egyben az informatika alapfogalma. Számos jelentése, kifejtése köztudott, különböző tudományágak különböző módon közelítik meg, írják le. Egyértelműen elfogadott definíciója nem ismert. Általánosságban információnak azt az adatot, hírt tekintjük, amely számunkra releváns és ismerethiányt csökkent. Az egyik legleegyszerűsítettebb megfogalmazás szerint az információ nem más, mint valóság (vagy egy részének) visszatükröződése. [1] Tudományos értelmezését az információelmélet fogalmazza meg.

Az adat magában sem jelentéstartalommal, sem információval nem bír. A jelentéstartalom az adatra vonatkozó valamilyen értelmezési szabályokat feltételez, és az adat ilyen szabályok szerinti értelmezése vezet a jelentéstartalomhoz. A jelentéstartalom pedig csak akkor szolgál információval az értelmező számára, ha azzal ő új ismeret birtokába kerül. [2]

Az információs társadalomban ahhoz, hogy az egyének, illetve szervezeteik, szerveződéseik az életüket, tevékenységüket hatékonyan, gazdaságosan és célszerűen tudják irányítani információkra van szükségük, mégpedig pontosan azokra információkra, amelyek ezekhez a feltételekhez szükségesek. Az információnak – hogy szerepét, fontosságát betöltse – mindig a megfelelő helyen, a kellő időben, a kívánt tartalommal és célszerű formátumban kell rendelkezésre állnia. Mint látszik, a felhasználó szempontjából több feltétel egyidejű megléte esetén hasznosítható csak az információ. Ha az információ, illetve annak valamely tulajdonsága nem felel meg a felhasználó – akár egy személy, akár egy szervezet – igényeinek, akkor az hatással lesz a döntés kimenetelére, vagy akár a végrehajtás minőségére is.

A VEZETÉSI CIKLUS

A különböző entitások az adatokkal, az információkkal kapcsolatos tevékenységüket az információs környezet különböző dimenzióiban végzik. A számukra szükséges információkat különböző tulajdonságú, pontosságú és megbízhatóságú forrásokból szerzik be, amelyeket aztán saját szempontrendszerük alapján feldolgozzák, elemzik, értékelik. Az értékelési szakaszt követően az egyének, illetve a szervezetek céljaik elérése, küldetésük betöltése érdekében döntési alternatívákat állítanak fel, majd a rendelkezésre álló erőforrásaik, lehetőségeik függvényében meghozzák a számukra legoptimálisabbnak tűnő döntést. A döntési folyamat lezárultával kezdődnek el a célok elérése érdekében kezdeményezett műveletek, melyeket akár a fizikai, akár az információs térben egyaránt végrehajthatnak. A végrehajtás minőségét, hatékonyságát a pontos és hiteles információk nagyban képesek növelni. A végrehajtott műveletek értelemszerűen hatást gyakorolnak a környezet különböző dimenzióira, melyből lehet következtetni a műveletek eredményére. A hatás felmérése, illetve a további intézkedések megtétele érdekében a fentebb vázolt információgyűjtés - értékelés - döntés - végrehajtás – úgynevezett vezetési ciklus – újrakezdődik [3:167]:

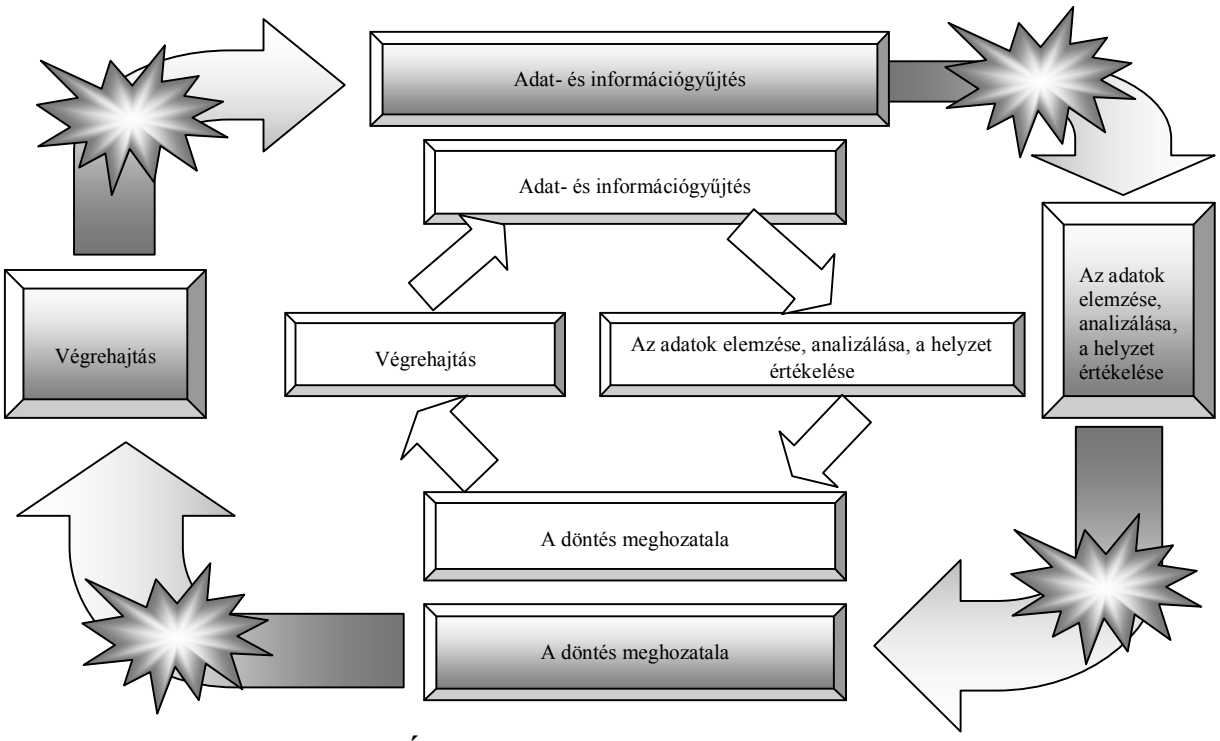


1. Ábra. A vezetési ciklus [3:167]

A ciklusban feltüntetett pontok által végzett munka eredményességére kihatással van az előző folyamatok tevékenységének, információinak minősége. A ciklusba bekerülő adatok, információk pontossága, hitelessége a feldolgozás során torzulhat

A ciklus meghatározott idő alatt zajlik le, mely nagyban összefügg az entitás információgyűjtő lehetőségeivel, a helyzetet elemző, értékelő szakemberek képzettségével, a vezetők tapasztalatával és a végrehajtók rutinjával, képességeivel, valamint a minden munkafázis mögött meghúzódó technikai, informatikai, kommunikációs eszközök fejlettségével. Amennyiben a környezet a vezetési ciklus időintervallumánál gyorsabban változik, akkor a döntéshozatal során meghozott döntések már nem a valós helyzetre reagálnak, és ez a körülmény a végrehajtás hatékonyságát is jelentősen ronthatja, sőt akár hatástalanná is teheti, így ahhoz, hogy egy szervezet saját helyzetét, pozícióját a saját környezetében pontosan ismerje a fenti ciklust a lehetőségeinek függvényében minél többször szükséges végrehajtania.

Ha ugyanabban a környezetben két ellenérdekelt fél tevékenykedik, melyek lehetnek akár szembenálló hadseregek, vagy akár gazdasági társaságok, illetve egyéb felek (például rendészeti szervek és terrorcsoportok), akkor elemi érdekük, hogy a pontos helyzetismeret érdekében vezetési ciklusuk idejét csökkentsék. Az időért folytatott harcban a feleknek több lehetőség is rendelkezésükre áll. Egyrészt saját szervezetük és technikai eszközeik hatékonyságának növelésével vívhatnak ki maguk számára előnyt, azonban az ebben rejlő lehetőségek korlátozottak, másrészt irányként megfogalmazódhat, hogy az ellenérdekelt fél információs folyamataiba beavatkozva növeljék annak ciklusidejét, rontsák az ottani rendszerben kezelt információk minőségi jellemzőit, mellyel a vezetés hatékonyságát csökkenthetik [3:167].



2. Ábra. A vezetési ciklus [3:167]

Az információs folyamatokba történő beavatkozás eredményét három tényező befolyásolja jelentősen:

- A támadó mekkora támadási potenciál birtokában van. Ez azt mutatja meg, hogy a fenyegető tényezők összessége mennyire képes kompromittálni az információs rendszer biztonságát. A potenciál mértékét befolyásolja a támadó szakértelme, a rendelkezésére álló erőforrások és technikai eszközök, valamint motivációja.

A támadási potenciál annál nagyobb:

- minél nagyobb szakértelem birtokában van a támadó identitás,
- minél több erőforrás és technikai eszköz áll rendelkezésére,
- valamint minél motiváltabb (elszántabb) a támadás végrehajtására.

A támadási potenciál mértékére kihatással van, hogy mekkora a támadás végrehajtásához szükséges, illetve a valójában rendelkezésre álló idő aránya, tovább az is, hogy a támadó a rendszerről előzetesen mekkora ismeretanyaggal rendelkezik.

- A kérdéses információs rendszer milyen sérülékenységi pontokkal rendelkezik. Olyan véletlenül, vagy szándékosan létrejövő adminisztratív és technikai hibák és gyengeségek összessége, melyet a támadók kihasználhatnak. A sérülékenységi pontok feltérképezésére három lehetőség van:
- a sérülékenységi pontokat a támadó az információs rendszer előzetes ismerete nélkül kísérli meg azonosítani,
- részleges adatok állnak rendelkezésére,
- illetve a rendszer teljes felépítésére, működési elvére vonatkozó információk, folyamatábrák a birtokában vannak.

Az utóbbi két esetben feltételezhető, hogy a támadó a műveletek előkészítése során akár különböző technikai eszközök, akár humán információszerző források alkalmazásával feltérképezte a sérülékenységi pontokat.

- Milyen adminisztratív és technikai védelmi intézkedéseket milyen minőségben foganatosítottak.

Egy szervezet információs rendszerének biztonságára nagymértékben kihatnak az üzemeltetésükkel kapcsolatos belső utasítások, melyek pontosan megfogalmazzák az információkhoz való hozzáférés, kezelés rendjét, az azokon – szervezeti egységenként – végezhető lehetséges műveleteket, illetve módját és természetesen a jogosult beosztási szinteket. Az adminisztratív szabályzóknak mindig illeszkednie kell a szervezet tevékenységi köréhez és belső struktúrájához, mivel ellenkező esetben a munkafolyamatokban bizonytalanságok, hiányosságok és biztonsági rések jelentkezhetnek, melyek segíthetik a támadót.

A technikai eszközökkel megvalósított védelem során szintén fontos az adminisztratív intézkedések meghozatala, azonban ezek mellett elengedhetetlen a megfelelő, a várható támadási módozatoknak hatékonyan ellenálló technológia és modern eszközök alkalmazása.

INFORMÁCIÓS FOLYAMATOK ÉS A TECHNIKA KAPCSOLATA

Napjainkban az információs folyamatok egyre nagyobb hatékonyságát, a vezetési ciklus gyors körforgását már fejlett infokommunikációs eszközrendszerek, valamint az ezekből összeálló, akár globális kiterjedésű információs infrastruktúrák, érzékelő-észlelő rendszerek biztosítják. Tekintettel, az infokommunikációs hálózatokkal való összefonódásra az információs folyamatokban kezelt információk bizonyos minőségi paraméterei nagyban összefüggnek a kérdéses hálózat adat- és üzembiztonságával, illetve az általa nyújtott szolgáltatások minőségi jellemzőivel. Erre való tekintettel a vezetési ciklus manipulálása – például a ciklusidő növelése – elérhető az információs rendszer alapját jelentő technikai berendezések, illetve az alkalmazott technológia támadása révén is.

Az információs folyamatok hátterében álló infokommunikációs eszközrendszerek alapvetően öt fő tevékenységi területhez kapcsolódnak:

- *információszerzés:* A számítógépes hálózatok, a kommunikációs rendszerek ma már szerves részei az információszerzés folyamatának, mind technikai, mind pedig humán dimenzióban egyaránt. Adatok keletkeznek a különböző érzékelő-észlelő, tájékoztató, navigációs rendszerekben, stb., továbbá a humán forrásból származó információk – különböző technikai eszközök alkalmazása révén – is e szakaszban kerülnek be a vezetési ciklusba. Ebben a szakaszban felmerülhet a különböző információs rendszerek közötti interdependencia is, mivel előfordulhat, hogy egy információs rendszer információszerző képessége részben vagy nagyban összefügg egy másik rendszer információ szolgáltatási kapacitásával, lehetőségével.
- *továbbítás:* Szinte minden információs folyamatra, vezetési ciklusra jellemző, hogy az adatokat nem a megszerzés helyén fogják feldolgozni, illetve a származtatott információk birtokában megint csak máshol fognak dönteni az optimális intézkedésekről, valamint az intézkedések konkrét végrehajtásáról, így a különböző állomások között az információt továbbítani szükséges, mely háttérfunkcióval szemben a különböző szervezetek – alaprendeltetésük függvényében – más-más szintű elvárásokat támasztanak.
- *tárolás:* Ez a funkció az előző ponthoz hasonlóan, azonban attól eltérően, nem a földrajzi eltolódásokat hivatott kiküszöbölni, hanem az időbelieket. Alapvető követelmény, hogy a ciklusban lévő munkafolyamatok egymásutániságából adódó, illetve információtechnológiai és más okokból (például folyamatos gyűjtés vagy későbbi felhasználásból) létrejövő szünetekben az információk ne vesszenek el.
- *feldolgozás:* A modern döntéshozatali folyamatokban már olyan nagy mennyiségű és sokrétű információ van jelen, hogy a számítógépes rendszerek alkalmazása nélkül – melyek az adatokat rendszerezik, összefűzik, keresik – már nem is lehetne hatékony

információfeldolgozást megvalósítani. Egy olyan szervezet életében, mely a vezetési ciklus időperiódusának csökkentésére törekszik, nem engedheti meg, hogy a rendelkezésére álló információk feldolgozását végző rendszereire ne kiemelt figyelemmel tekintsen.

- *megosztás, szolgáltatás:* Az információs folyamat legutolsó fázisa, amikor is a feldolgozott információ különböző technológiai megoldások révén a jogosultsági szinteknek megfelelően eljut a megfelelő döntéshozói, illetve végrehajtói körhöz.

Napjainkban egyre jobban jellemzővé válik, hogy a különböző szervezetek működési költségeik racionalizálása érdekében nem építenek ki saját infokommunikációs infrastruktúrát, hanem azt a piaci szféra szereplőitől, gazdaságossági megfontolások alapján különböző szerződéses viszonyok alapján veszik igénybe. Ez főleg a továbbítás tevékenységköréhez tartozik, de az egyre jobban terjedő felhő-alapú technológiák miatt a szervezetek más tevékenységeket (például adattárolást, adatfeldolgozást) is külső szolgáltatókra bízzák.

Tekintettel arra, hogy a nyers és a feldolgozott információk, adatok fizikailag gyakorlatilag az információs rendszerek alapját jelentő infokommunikációs infrastruktúrákban vannak jelen, így annak műszaki paraméterei, biztonságára vonatkozó tulajdonságai közvetlenül is összefüggésbe hozhatók a benne kezelt információk bizonyos jellemzőivel. Ennek az lehet a következménye, hogy ha egy szervezet minél jobban kiszervezi információs tevékenységét külső szolgáltatók számára, annál kevesebb lehetősége van befolyásolni az érintett tulajdonságokat, illetve annál jobban kiszolgáltatottá válik az infrastruktúra üzemeltetőjének, így nem fogja maradéktalanul ismerni a várható fenyegetettségeket, illetve azok szintjét, amiből adódóan a várható zavarokra sem fog tudni kellően felkészülni.

AZ INFORMÁCIÓ TULAJDONSÁGAI ÉS A LEHETSÉGES TÁMADÁSI MÓDOZATOK KÖZÖTTI ÖSSZEFÜGGÉSEK

A támadó, céljainak függvényében az információs rendszerben kezelt információk különböző tulajdonságainak manipulálásával jelentősen képes befolyásolni a vezetési ciklus különböző állomásainak eredményét, így – az egymásra-épülés jellegéből adódóan – egy generált hiba a ciklus következő állomásán már esetleg hatványozottan jelentkezhet.

A vezetési ciklust kiszolgáló infokommunikációs rendszer sebezhetőségi pontjainak ismeretében a támadó felmérheti, hogy mely tulajdonságok vonatkozásában lehet érdemi lehetősége arra, hogy beavatkozzon az ellenérdekelt fél információs tevékenységébe.

Az információ támadhatósága szempontjából elengedhetetlenül szükséges annak funkcionális jelentését, illetve minőségi követelményeit is megvizsgálni. Az információ analizálása során az alábbi jellemzőket lehet, illetve kell tanulmányozni, melyekből következtetni lehet, annak minőségére, használhatóságára, valamint az információs rendszerben betöltött fontosságára, illetve támadhatóságára [4:12]:

- Időszerűség: Az információt akkor kell szolgáltatni, amikor arra szükség van, azaz a kérdésre adott válasznak a kérdező által megkívánt időtartományon belül kell megérkeznie. E paraméter kapcsán a támadónak – amennyiben az információ rendelkezésre állási és felhasználási helye nem egyezik meg – a továbbítást végző infokommunikációs rendszer manipulációja révén érhet el eredményeket. A kommunikáció akadályozása mindkét irányba kiterjedhet, vagy a kérdés, vagy a válasz ne érjen célba, illetve csak olyan jelentős időveszteséggel, hogy az az információ e tulajdonságával szemben támasztott követelményt már ne elégítse ki, így a döntéshozó nem lesz birtokában minden szükséges információnak. Az infokommunikációs rendszer támadása során az ellenérdekelt fél széles palettáról

választhat, a fizikai pusztítás eszközeitől kezdve, az elektronikai ellentevékenységen át, akár a számítógép-hálózati hadviselés eszközrendszeréig.

- Aktualitás: Az adott identitásról érvényes, naprakész információt kell szolgáltatni, vagyis a válaszadó ne olyan információt szolgáltasson, mely már nem a valós állapotot tükrözi. Az aktualitás tulajdonságnál is hatékonyan használhatók az időszerűségnél vázolt támadási módok, melyek a kommunikációt akadályozzák, azonban ezek itt még kiegészíthetőek olyan módszerekkel, melyek arra irányulnak, hogy az információs rendszer első lépcsőjeként is értelmezhető adatgyűjtő, érzékelő mechanizmusok ne tudjanak rendeltetésszerűen működni, illetve félre legyenek vezetve.
- Időperiódus: Az információ érvényességére vonatkozó időtartam, ami vonatkozhat múltra, jelenre és jövőre. Az információs folyamatok szempontjából rendkívül fontos, hogy az adatok megszerzésének gyakorisága illeszkedjen a leírni kívánt környezeti jellemző változásának gyakoriságával, mivel csak ez garantálja azt, hogy aktuális információ legyen a birtokunkba. A múltra, illetve a jelenre vonatkozó pontos információk segítenek a jövőre vonatkozó tendenciák, becslések minél pontosabb meghatározásában. E jellemző a védekezés során lehet fontos, amennyiben valamelyik egyik félnek van lehetősége és erőforrása ahhoz, hogy környezeti jellemzőit az ellenérdekelt fél időperiódusánál gyorsabban változtassa.
- Elérhetőség: Az a paraméter, mely megmutatja, hogy az információra vonatkozó kérdésre milyen gyorsan és milyen könnyen vagy nehezen szerezhető meg a válasz. A támadó célja e paraméter esetében az, hogy a válasz megszerzésének idejét oly annyira elnyújtsa, hogy mire az a döntéshozóhoz ér, már ne a valóságot tükrözze. Ezt elérheti az információs folyamatok (információszerzés, továbbítás, feldolgozás) lassításával, vagy amennyiben erre lehetősége van, az információgyűjtés tárgyát képező entitás módosításával.
- Megbízhatóság: Az információnak, a benne előforduló hibákból származtatott minőségi jellemzője. A hibamentesség bár minden rendszerben alapkövetelmény, azonban ez nem minden esetben biztosítható, így az információ felhasználása során egyfajta tűréshatárt kell bevezetni, melynek keretein belül fel lehet készülni az esetleges eltérésekre, és azok hatásait kezelni lehet. Egy hatékony információs rendszerben elemezni kell a hibás adatok révén megvalósuló esetleges következményeket is. A megbízhatóság az információ egyik legsarkalatosabb jellemzője, így ez a támadások egyik legfontosabb célja. Az információs megbízhatósága – melyen sok esetben a pontosságot is érthetjük – több ponton is támadható. Az információszerzés folyamatában már a keletkezés szakaszában lehetőség van a megbízhatóságot befolyásolni, mely egyrészt elérhető, a környezeti jellemzők módosításával, hogy az adatgyűjtő-rendszerek ne a valóságot észleljék, másrészt pedig az adatgyűjtő-rendszerek műszaki paramétereinek befolyásolásával is. Megfelelő támadópotenciál birtokában az információs rendszerben kezelt adatok megbízhatósága manipulálható a továbbítás és a tárolás szakaszaiban is. Az adatok, információk módosítása esetén figyelembe kell venni, hogy a túlzott torzítás (dezinformálás) a támadás tényét azonnal leleplezheti.
- Jelentőség: A felhasználó valódi információigényéhez kapcsolódó fogalom, ami a felhasználó számára az információ fontosságát jelzi, melyet becsülni lehet abból, hogy az információ megszerzésére mekkora erőforrásokat szabadítanak fel egy szervezeten belül. Ezen paraméter támadása abszurd módon a megszerezni kívánt információ védelmével érhető, ha az ellenérdekelt felet lehetőségeinkhez mérten elzárjuk az őt érdeklő adatoktól. Ez az elzárás jelentheti azt, hogy védjük saját információinkat, de jelentheti azt is, hogy az ellenérdekelt felet olyan más

információs infrastruktúráktól szigeteljük el (akár a kérdéses struktúra támadásával), ahonnan információk kerülnek át saját rendszerébe. További közvetett támadási mód lehet, ha a szervezetet elvágjuk azoktól az erőforrásoktól, melyeket az információ megszerzésére tudna fordítani.

Teljesség: Fontos szempont, hogy minden információ rendelkezésre álljon a döntéshozatal során. A teljesség problematikájához tartozik az is, hogy ha egy információ egy másik információra hivatkozik, akkor a hivatkozott információnak is elérhetőnek kell lennie. A teljesség hiánya a döntéshozó bizonytalanságát erősíti. Hogy a teljesség a követelményeknek megfeleljen, fontos, hogy minden egyes részinformáció eljusson a döntéshozóhoz. E tulajdonság támadása gyakorlatilag magának az információnak a támadásával egyezik meg, mivel ha a részinformáció bármelyik tulajdonságát lehet támadni, akkor az kihat a teljes információra, ez által fejtve ki a hatást.

- Igazolhatóság: Ugyanarra a kérdéskörre különböző helyekről, válaszadóktól, információs csatornákból származó válaszok mennyiben egyeznek meg, illetve mennyire térnek el, ami az információk ellenőrzöttségére, felhasználhatóságára vonatkozhatnak. Az igazolhatóság nem megfelelő szintje szintén a döntéshozó bizonytalanságát növeli. Az igazolhatóság a teljességhez hasonlóan egy olyan paraméter, mely egy párhuzamosan futó, gyakorlatilag azzal megegyező információs folyamattól függ, így támadása magának az információnak a támadásával egyezik meg.
- Bizalmasság: Az információ e tulajdonsága azt hivatott biztosítani, hogy ha az ellenérdekelt fél már részben eredményesen támadta az információs rendszer valamely folyamatát (például továbbítást, tárolást) az információ akkor is csak az arra felhatalmazottak számára legyen elérhető, érthető. A támadó, megszerezve a titkosított információkat, megfelelő szakértelem és elegendő számítási kapacitás birtokában kriptográfiai módszerek segítségével juthat hozzá a kívánt információhoz.

KONKLÚZIÓ

Az információs társadalom kapcsán gyakorlatilag törvényszerűségként kijelenthető, hogy az információt felhasználó környezetében szinte mindig létezik egy olyan másik ellenérdekelt entitás (személy, hadsereg, terrorcsoport, szervezet, gazdasági társaság), mely arra törekszik, hogy a felhasználó információs folyamataiba beavatkozva a felhasználót az optimálistól eltérő döntésre kényszerítse, így szerezve előnyt magának az ellenérdekelt fél.

Elérni kívánt cél az lehet, hogy az ellenérdekelt fél a döntési ciklusához szükséges információkhoz ne jusson hozzá (elérhetőség), ne a szükséges időben kapja meg azokat (időszerűség és aktualitás), vagy a kapott információk pontatlanok legyenek (pontosság) , továbbá, hogy ne legyenek ellenőrizhetők (megbízhatóság, igazolhatóság), stb.. Amennyiben az információs rendszerben kezelt információk ellen alkalmazott eljárás, vagy eljárások összessége minél több minőségi jellemzőt érint, annál eredményesebbnek tekinthető az információs támadás.

Egy információs művelet előkészítése során a támadónak objektíven fel kell mérnie, hogy mekkora támadási potenciál birtokában van. Az elérni kívánt cél függvényében meg kell határoznia, hogy azt a rendszerben kezelt információk, mely tulajdonságainak manipulálásával érheti el leghatékonyabban. Az információs rendszer üzemeltetőjének szempontjából pedig azt kell meghatározni, hogy melyek azok a tulajdonságok, melyek a működés szempontjából kiemelten érzékenyek a támadásra, és melyek védelmét akár külön erőforrások bevonásával is erősítenie kell. Továbbá azt is célszerű felmérni egy szervezetnek,

hogy az információs folyamatokba kívülről bevont, vagy épp kiszervezett – más szervezetek által biztosított, és más elvek, módok alapján védett – folyamatok esetleges támadása mennyiben érintheti, milyen kihatással lehet a saját rendszerének működésére.

Felhasznált irodalom

[1] Wikipedia - http://hu.wikipedia.org/wiki/Inform%C3%A1ci%C3%B3, letöltve: 2011. május 20.

[2] Ujváriné dr. Melich Katalin - A gazdasági informatika alapjai, Perfekt Zrt. 2008., ISBN 978-963-394-734-0

[3] Haig Zsolt, Várhegyi István - Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest 2008., ISBN 9633273919

[4] Papp Zoltán - Kritikus információs infrastruktúrák elleni lehetséges támadások (Diplomamunka), ZMNE-BJKMK, Budapest 2009.,