A MÉDIA MÉRŐSZÁMAI ÉS A DIGITÁLIS KOMMUNIKÁCIÓ BIZTONSÁGÁNAK MUTATÓSZÁMAI

INDICATORS OF MEDIA MEASUREMENTS AND KPI'S OF THE DIGITAL COMMUNICATION SECURITY

KOLLÁR CSABA[1]

ABSZTRAKT

Tanulmányomban a bevezetést követően a médiatervezés módszertani alapjait tekintem át, majd a média mutatószámainak kategóriáit ismertetem. Az online/digitális média vonatkozásában több olyan utalást is teszek a mutatószámok ismérveire, amelyek az információbiztonság mutatószámainál is megjelennek. A digitális kommunikációról szóló részt követően az információ biztonságával és sebezhetőségével foglalkozom, megnevezve az információgyűjtés, az információtovábbítás, az információ feldolgozása, az információ tárolása, valamint a humán erőforrás ellen indított támadásokat. A digitális kommunikáció biztonságának mérésénél kisebb részben az intuitív, nagyobb részben az egzakt mérésről értekezem. Kitérek a teljesítménymutatók és teljesítménymutató indexek meghatározásainak a lépéseire. Írásművemet a kommunikáció és az információbiztonság egymással párhuzamosan futó folyamatainak közös területe fejlesztési lehetőségeire tett javaslataimmal zárom.

Kulcsszavak: információbiztonság, teljesítménymutató, mutatószám, KPI, KPX

ABSTRACT

In my study, following the introduction, I will review the methodological basis of media planning, afterwards I will present the categories of the media index numbers. Regarding the online/digital media, I will give several references to the indexes' criteria, which also appear in the index numbers of information security. After the part which deals with digital communication, I will continue

[1] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

with the security and vulnerability of information, indicating the gathering, the transmission, the processing and the conservation of information, as well as the attacks launched against the human resources. Regarding the measurement of the security of digital communication, on a lesser extent I will confer about intuitive measurement, while on a larger extent I will confer about exact measurement. I will also deal with the steps of determining performance indicators and the indexes of performance indication. I will conclude my study with recommendations concerning the possibilities for development of the joint areas of the parallel processes, which are present within communication and information security.

Keywords: information security, performance indicators, performance index, KPI, KPX

BEVEZETÉS

Az adatok korában a szervezeti működést a szervezet által „termelt" megannyi adattal és információval lehet jellemezni, s a belőlük képzett szervezeti tudás, tapasztalat és bölcsesség a garancia a hosszú távú, átlátható és tervezhető üzletvitelre. A szervezeti biztonság komplex értelmezésében helyet kap a munka- és termelésbiztonság mellett többek között a gazdasági, az informatikai és információ, valamint a kommunikáció biztonsága is. A szervezeteknek érdeke, hogy a róluk szóló, általuk létrehozott és gerjesztett kommunikációs folyamatokat kézben tartsák, mivel a hibás működés közvetlen és komoly hatással lehet a gazdasági és pénzügyi teljesítményre is. Olyan megoldásokat kell kínálni a szervezeteknek, munkavállalóiknak és partnereiknek, amelyek révén minden üzenet (vagy legalábbis azok közel 100%-a) célba ér, nem veszik el, s miközben a címzett felé száguld, nem módosítja harmadik fél, illetve a tartalmát sem ismerik meg idegenek. Az online médiafelületeken biztosítani kell a hírfogyasztó biztonságát is azzal, hogy csak a számára releváns tartalmakhoz fér hozzá, illetve, hogy a releváns tartalmak valós tények, nem pedig álhírek alapján születnek. A szervezetek számára nem ismeretlenek az olyan fogalmak, melyek az adatvagyonnal, az adatok védelmével kapcsolatosak. Ez azt jelenti, hogy az adatokat csak az arra illetékes személyek ismerhetik meg, azokat csak a megfelelő jogosultsággal rendelkező emberek módosíthatják, illetve törölhetik. A (digitális) kommunikáció és az adatok és információk biztonságával kapcsolatos folyamatok és aktivitások futnak párhuzamosan a szervezetek életében, tanulmányomban arra keresem a választ, hogy lehet-e a két terület mérésének módszertanában olyan közös pontokat találni, amelyek a szervezet számára előnyöket jelentenek.

A MÉDIATERVEZÉS MÓDSZERTANI ALAPJAI

A médiatervezéssel kapcsolatban Fazekas és Harsányi (2004:315) úgy fogalmaz, hogy „a kampánytervezés azon része, melyben meghatározásra kerülnek a (média)célok, a (média)stratégia, s ez alapján a felhasználandó médiumok köre, valamint a konkrét ütemezés egy adott kampányban". Incze és Pénzes (2002:166) egy praktikusabb definíciót ismertet,

miszerint „a médiatervezés nem más, mint válaszadás néhány kérdésre: kinek, hol, mikor, milyen médiumban, milyen erősen, mennyi ideig és mennyiért hirdessünk".
Szabó D. Tamás (1999:29) a médiatervezési munka kiindulópontjának az ügynökség és a megbízó közötti szerződés mellett a briefet tartja, amelyik „rövid tömör megfogalmazásában rögzíti a főbb pontokat", s segítségével „tisztázódnak és találnak egymásra a két fél elképzelései". Nevezett a MaRS[2] ajánlására hivatkozva ismerteti a médiatervezési briefet[3], melynek tanulmányom szempontjából lényeges elemei a következők (zárójelben saját és nevezett szerző megjegyzései):

- ügyfél (akitől az üzenet származik, aki, vagy akinek a megbízásából valaki az üzenetet elkészítette)
- kampány időzítése (mikor indul, meddig tart a kampány, szezonalitás fontossága)
- háttér (piaci helyzet)
- főbb versenytársak (konkurencia tevékenységének és aktivitásainak értékelése)
- célok (mi lehet a cél? ismertség, eladás, stb…)
- célcsoport(ok) (üzenet címzettjei)
- preferált média (az üzenet mely médiában jelenik meg)
- a kommunikáció tartalma, stílusa, hangvitele
- költségek
- előírt/elvárt mutatószámok

A következőkben a média mutatószámaival foglalkozom.

A (média)mutatószámok kategóriái

Balassa és Klausz (2015), Fazekas és Harsányi(2004), Hamburger (1995), Incze és Pénzes (2002), Kollár (2004), Szabó (1999), Virányi (s.a.) többféle elv szerint foglalja csoportokba az egyes mutatószámokat, s rendszerint az adott médiumra jellemző mutatószámok/mérőszámok kerülnek egy kategóriába.
A ***nyomtatott médiánál*** többek között az elérésenkénti megjelenést (reach per issue), illetve a legnagyobb olvasottságot célszerű meghatározni. Az előbbi azt jelenti, hogy kik azok, akik rendszeresen olvassák az adott sajtóterméket. Ehhez képest magasabb értéket mutat a legnagyobb olvasottság (broadest readership), mivel itt a rendszeres olvasók és az alkalmankénti (lapszámonkénti) olvasók számának összege szerepel.
A ***klasszikus televíziónál és rádiónál*** beszélhetünk elérésről (reach), azt mutatja, hogy „egy adott műsor/csatorna a teljes nézettség milyen arányát érte el a vizsgált időszakban" (Hamburger, 1995:11). Egy másik gyakori mérőszám a nézettség (rating), amelyik azt jelentette, hogy a célcsoportba tartozó összes emberből hány százalék nézte/hallgatta az adott műsort meghatározott időben. Az affinitás (affinity) az mutatja számszerűen, hogy a célcsoport hogyan viszonyul egy adott műsorhoz, csatornához, napszakhoz (Incze – Pénzes, 2002), vagy másképp fogalmazva a médiának az a tulajdonsága, hogy „a teljes fogyasztói közül hány

[2] MaRS: „A MAKSZ Magyarországi Reklámügynökségek Szövetségeként 1995 májusában jött létre. A kommunikációs ügynökségek szövetségévé (MAKSZ) történő átalakulást elsősorban a kommunikációs szakmában dolgozó ügynökségek közös gondjai és problémái, és az ezek megoldását szolgáló együttgondolkodás és együttes cselekvés indokolta". http://maksz.com (letöltés ideje: 2018.02.10.).
[3] Mivel a MaRS átalakult MAKSZ-ra, így a brief ismertetésénél nevezett szerző, valamint a Szövetség érvényben levő Briefing Útmutatóját összevontan mutatom be. Tartalmuk gyakorlatilag azonos, a különbség nevezett szerző munkájának tartalmi tagolásában van.

százalék tartozik a célcsoportba" (Szabó, 1999). Az átlagos nézettségi idő (average time spent) azt határozza meg, hogy az adott programot, műsort átlagosan meddig nézték/hallgatták a megadott időben.
A digitális átállást követően már lehetőség van a közel 100%-os mintavételre is, mivel a digitális műsorszolgáltatást igénybe vevők csatornaválasztása, illetve az ott töltött idő adatai rendelkezésre állnak, így adatbányászat segítségével a rejtett összefüggések is felfedhetők.
Az ***online/digitális média*** vonatkozásában (internetes mérőszámok) részint az általános (weblap, klasszikus online hirdetés), részint a közösségi médiát tudjuk megkülönböztetni. Az általánosnál érdemes megnevezni a webszerverre történő kapcsolatok számát adott időben (hit), az oldalletöltések számát (page impression, vagy page view), ami a Magyar Reklámszövetség Internetes Tagozatának ajánlása alapján (idézi Incze és Pénzes, 2002:155) azt fejezi ki, hogy „hány teljes oldalt töltöttek le. Egy teljesen letöltött oldal tehát egy page impression-t eredményez, függetlenül az oldalon szereplő adatfájlok számától". Látható, hogy ez a mutató ugyan hasonlít a nézettséghez, mivel a médiahasználat mértékét méri, de az oldalletöltés nem foglalkozik a célcsoporttal. A látogatás (visit) Balassa és Klausz (2015:52) szerint az oldalra látogatások számát jelenti egy nap. Ha valaki „kétszer kattint az oldalra, az (már) két látogatásnak számít". A nevezett mérőszámok mellett az online hirdetéseknél a reklámmegjelenést (ad view), az átkattintást (click through), illetve az átkattintási rátát (click through rate) célszerű megkülönböztetni. Az első a weboldalon megjelenő adott hirdető reklámbannereit számolja, a kattintás pedig azt, hogy hányszor kattintottak a hirdetésre, illetve, hogy az oldalra látogatók, s a hirdetést látók hány százaléka kattintott a hirdetésre.
Balassa és Klausz (2015) a közösségi média típusainál a blogot, a wikit, a videomegosztást, a social networking-et, az aukciós oldalakat, a geolokációs alkalmazásokat, valamint a kiterjesztett valóság platformokat különbözteti meg.
A ***blogoknál*** a megtekintés száma (page view) alapján meghatározható, hogy adott időszak alatt hányan látogatták meg az oldalt. A blogbejegyzések többségénél vannak linkek, amelyek különböző weboldalakra mutatnak. A honlaplátogatások (website visit) azt méri, hogy a blog olvasói közül hányan kattintanak a linkre. Az oldallátogatások (pages per visit) mutató azt méri, hogy a felhasználó egy-egy látogatás alkalmával hány oldalt nyit meg, de mérni lehet vele az adott oldalon való tartózkodás idejét is. A blognál érdemes még mérni a blogra mutató linkek számát (backlinks), a feliratkozók számát (subscribers), a bejegyzések számát adott időszak alatt (number of posts published), a bejegyzések megosztását (social shares per post) is.
A ***Facebook*** vonatkozásában az elkötelezettségnek négy típusa jelenik meg Balassa és Klausz (2015) értelmezésében. A (1) hozzászólások (comments) azt méri, hogy egy adott bejegyzéshez hányan fűztek megjegyzést, a (2) like és egyéb érzelmek ikonikus jelzése azt mutatja, hogy az adott bejegyzésre hányan reagáltak érzelmi ikonokkal, a (3) megosztások (shares) száma azt méri, hogy egy bejegyzést hányan osztottak meg, (4) kattintások, mely mutató az elkötelezettség mérésénél nagyon fontos. Az elköteleződési rátát (engagement rate) a lájkok, a hozzászólások és a megosztások összege adja.
A ***Youtube***-nál mérhető többek között a megtekintések száma (views), a megtekintési idő (watched time), a feliratkozók száma (subscribers), az elköteleződés (engagement), a ***Twitternél*** az elköteleződési ráta. A ***Linkedin*** mérőszámai között fontos a kapcsolatok/ismerősök száma (total connections), a megtekintések száma (profile views), az ajánlások száma (recommendation), mely azt méri, hogy más felhasználók hányszor írtak ajánlást az adott

fiókhoz, az elérés (reach), a bejegyzések száma (posts), a kedvelések (likes) száma, illetve a hozzászólások (comments) száma.

Az utóbbi időben egyre nagyobb hangsúlyt kap az egyén mobileszközökön (elsősorban okostelefon) történő médiafogyasztása, így a média mutatószámainál egy új kategóriát lehet megkülönböztetni: a ***mobil eszközöket***. A tartalmak egy része egyaránt megjelenthet számítógépen és mobiltelefonon, a megtekintések, látogatások, letöltések, kattintások arányából következtetni lehet a felhasználók szokásaira, attitűdjeire, s lehetőség van összehasonlító elemzések elvégzésére is.
A mutatószámok médiatípus szerinti felosztása mellett léteznek a költségekhez, valamint a tartalomhoz kapcsolódó mutatószámok is.

A ***költség típusú, költséghatékonyságot kifejező mutatószámok*** azt vizsgálják, hogy bizonyos számú ember elérése mennyibe kerül, valamint, hogy mennyi egy kampány médiumonkénti költsége, illetve összköltsége. Az ezer kontaktusra eső költséget (cost per thousand) a hirdetések elhelyezési költségének és a hirdetéssel várhatóan elért személyek számának hányadosa alapján képzik. A CPP-vel (cost per point) a célcsoport 1%-ának elérési költségét mérik. Ha az online médium bevételt is termel, akkor esetében számolni lehet a felületén elhelyezett valamennyi reklámból (banner, PR-cikk, stb.) származó bevétellel (revenue), a látogatásokra jutó bevétellel (revenue per visits), illetve az oldalra jutó bevétellel (revenue per page) is, ez utóbbi a hirdetés teljes bevétele és az oldalletöltések számának a hányadosa alapján kerül kiszámításra.

A ***tartalomhoz kapcsolódó mutatószámoknál*** alapvetően nem önmagában a megtekintés, hanem annak értékelése, véleményezése kerül a fókuszba. A Facebooknál a like (tetszik) mellett az imádom, a vicces, a hűha, a szomorú és a dühítő lehetőségek közül is választani lehet, s a választott lehetőségek egymáshoz viszonyított aránya révén a tartalom fogadására, a vele való azonosulásra is következtetni lehet. Ugyancsak következtetni lehet az azonosulásra, illetve az érzelmi érintettségre a tartalmak megosztásának számai, illetve a megtekintés és a megosztás hányadosa alapján, valamint az adott tartalomhoz fűzött megjegyzések száma alapján is. Önmagában az adott oldalt követők, illetve az adott személyt ismerők száma, illetve e szám időbeli változása (progresszív, degresszív), s e változás dinamikája is enged következtetni az üzenetek tartalmának fogadtatására.

GONDOLATOK A DIGITÁLIS KOMMUNIKÁCIÓRÓL

A digitális kommunikáció meghatározásakor a definíciók két aspektusból közelítik a témát. Egyfelől digitális kommunikáció révén valósul meg minden olyan üzenet, amely digitális eszközökön keresztül történik, másfelől digitális kommunikációnak tekintjük a digitális formában küldött bármilyen típusú információt. Jelen tanulmánynak nem célja, hogy állást foglaljon a kétféle megközelítés egyike mellett, vagy, hogy megadja a két fogalom szinergikus summázatát.
Az üzenet gyűjtőkategória, melynek részét képezi a weboldalon olvasható írott tartalom, az e-mail, az SMS, az MMS, a(z okos)telefonon keresztül megvalósított beszélgetés, a számí-

tógép közvetítésével létrejött szöveges-, hang- és videochat, a blog, a wikitartalom, a közösségi média felületein folytatott diskurzusok, az online multimédiás tartalmak, s ide sorolom a tartalmakra adott válaszreakciókat is (pl.: kedvelés).
A digitális kommunikációra írásművemben úgy tekintek, mint a hagyományos világ digitális leképezése során keletkezett digitális világban, illetve a virtuális valóságra és egyéb kevert valóságokra épülő platformokon megvalósuló kommunikáció/eszmecsere, ahol az előbbi esetben a tartalmakat előbb digitális formába kell átalakítani (analóg-digitális átalakító, pl.: scanner, digitális fényképezőgép), míg utóbbinál a programozók fantáziájára van bízva, hogy milyen elvek mentén alakítsák ki a képzeletbeli világokat. Értelmezésemben a digitális kommunikáció másik sajátossága az, hogy az analóg-digitális átalakítást követően, vagy amikor az egyén belép az online világba, akkor az egy labirintushoz hasonlít, melynek komolyabb és részletesebb technikai, informatikai működését rendszerint nem kell megértenie ahhoz, az üzenetét eljuttassa a címzetthez. A shannon-waeveri modellben (1949) értelmezett küldő üzenetét kódolja (értve ezalatt, hogy leírja, elmondja, felveszi, rögzíti, stb.), majd ez a küldő által kódolt üzenet a rendszer sajátosságai szerint műszaki-informatikai értelemben is kódolódik (pl.: csomagokra bontják, címkézik, stb.) annak érdekében, hogy a vezetékes és/vagy vezeték nélküli hálózatokon keresztül eljusson a címzetthez, akinél az aktuális informatikai eszköz (pl.: számítógép, laptop, okostelefon, okostévé) előbb műszaki-informatikai értelemben dekódolja azt (pl.: összekapcsolja a csomagokat), majd a címzett dekódolja a tartalmat. A csatorna zaj, a környezeti zaj, a szemantikai és szintaktikai zaj, a fiziológiai zaj, a pszichológiai zaj és a kulturális zaj mellett a digitális környezetben számolni lehet az információ (és így az üzenet) biztonságos célba juttatását, vagy az üzenet (tartalom) elérhetőségét veszélyeztető tényezőkkel is, melyeket részint informatikai-technikai, részint humán/támadó zajnak definiálok írásomban. A következő részben az információ biztonságával foglalkozok részletesebben.

Az információ biztonsága és sebezhetősége

Az információbiztonság az MSZ ISO/IEC 27001:2006 szabvány szerint „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá egyéb tulajdonságok, mint a hitelesség, a számonkérhetőség, a letagadhatatlanság és a megbízhatóság szintén ide tartoznak”. A bizalmasság, titkosság olyan tulajdonság, amely „biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé, és nem hozzák azok tudomására”. Sértetlenség alatt a „vagyontárgyak pontosságának és teljességének védelmét biztosító”, rendelkezésre álláson pedig olyan tulajdonságot értünk, amely lehetővé teszi, hogy „az adott objektum – feljogosított entitás által támasztott igény alapján – hozzáférhető és igénybe vehető legyen”. A szabvány által leírt definíciók és azok tartalmi elemzése felveti annak szükségességét, hogy az adatokat és az információkat a szükséges mértékben védjük annak érdekében, hogy azok felhasználásával az egyén és a szervezet számára tudást, tapasztalatot és bölcsességet tudjunk képezni, vagy saját maguk tudjanak képezni. Ezt a folyamatot veszélyezteti egyfelől az adatok és információk manipulálása, módosítása, törlése, illetéktelen személyekhez kerülése, másfelől az adatokat és információkat tároló, illetve azokat közvetítő rendszerek sebezhetősége – összességében a kritikus infrastruktúrák gyenge pontjai és az ellenük indított támadások.

Munk (2008) a kritikus infrastruktúra általános fogalmát úgy értelmezi, hogy „mindazon infrastruktúrák (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége), amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létére, lét- és működési feltételeire jelentős negatív hatással jár". Haig (2015) a kritikus infrastruktúra elleni fenyegetések forrásánál az egyes személyeket, a jogosulatlan felhasználókat, a terroristákat, a különböző nemzeti szervezeteket, a külföldi hírszerző szolgálatokat, illetve a katonai szervezeteket azonosítja, akik a komplex információs támadást a fizikai, az információs (ezeket összefoglaló névvel technikai jellegűnek is hívjuk) és a kognitív (vagy más névvel humán) dimenziók mentén követik el. A fizikai dimenzióhoz sorolható az elektromos berendezések megrongálása, az elektromos hálózat kiiktatása például robbantással, kábelek elvágásával, fizikai rombolóerő alkalmazásával. Az informatikai dimenzió részét képezik az informatikai folyamatok elleni támadások, az adatszerzés és –manipulálás, valamint végleges törlés többek között vírusok, kémprogramok, adathalász e-mail-ek, DoS és DDoS[4] támadások révén. A kognitív dimenzióban megvalósuló támadásoknál a támadóknak nem kell komoly informatikai tudással rendelkezniük, hiszen elsősorban kommunikációs és pszichológiai ismereteik és tapasztalataik alapján gyakorolnak hatást áldozataikra, például humán típusú social engineering módszerekkel, hamis, csúsztatott, manipulált üzenetekkel, valós, a címzettek viselkedését szándékosan befolyásolni akaró hírekkel. Ezek a technikák részint a fizikai világban beszéd formájában, részint a nyomtatott és az elektronikus média segítségével jutnak célba. A támadók Haig (2015:102-103) szerint öt, egymástól jól elkülöníthető felületen támadnak:

1. Az ***információgyűjtés*** humán, vagy szenzor alapon történik, az előbbinél gyakran a nyilvánosan, legális eszközökkel megszerezhető adatok és információk (OSINT) gyűjtése zajlik. A támadás során a cél az adatok és információk gyűjtésének megakadályozása, vagy késleltetése, hamis adatok közlése, az adatok manipulálása.
2. ***Információtovábbítás*** alatt a különféle, információ továbbítására alkalmas vezetékes és vezeték nélküli hírközlési hálózatok funkcióját, részint a szóbeli közlést értjük. A támadók az adatokat és az információkat eltéríthetik, a továbbítását akadályozhatják, vagy késleltethetik, illetve jogosulatlanul férhetnek hozzá.
3. Az ***információ feldolgozása*** történhet manuális és számítógépes módon is, az utóbbinál különböző hardverek és szoftverek (programok, alkalmazások) szolgáltatják azt a környezetet, amiben a feldolgozás megtörténik. Támadás során részint a rendszerek fizikai működését szabotálhatják (pl.: áramkimaradás, rongálás), vagy rosszindulatú programokkal (pl.: vírus) férnek hozzá, vagy késleltetik az adat- és információfeldolgozást.
4. Az ***információtárolás és az adattárolás*** a feldolgozott adatok és információk tárolását jelenti részint papír alapon, részint elektronikus úton. Ez utóbbinál a támadók hamis adatokat tudnak bevinni, a meglevő adatokat törölhetik (megsemmisítés) és módosíthatják, illetve azzal, hogy az adatokhoz hozzáférhetnek, ellophatják azokat.
5. A ***humán erőforrás*** a fenti négy terület működtetésében, fejlesztésében, üzemeltetésében, az adatok és információk gyűjtésében, továbbításában, elemzésében, tárolásában vesz részt. A támadás célja, hogy a social engineering (pszichológiai és

[4] DoS és DDoS támadás: (elosztott) szolgáltatásmegtagadással járó támadás, vagy más néven túlterheléses támadás, amelynek során a támadók célja, hogy a rendszert nagyon lelassítsák, illetve megbénítsák, így a rendszer szolgáltatásai (pl.: weblap) nem érhetők el a felhasználók számára.

kommunikációs manipuláció) módszereivel kihasználják hiszékenységüket, segítőkészségüket, naivitásukat, s hozzáférést szerezzenek az adatokhoz, információkhoz, s így megszerezzék, módosítsák, töröljék azokat.

A DIGITÁLIS KOMMUNIKÁCIÓ (BIZTONSÁGÁNAK) MÉRÉSE

A fentiek alapján látható, hogy az adatok és az információk, valamint a velük kapcsolatban levő műszaki-informatikai és humán tényezők mennyire sebezhetők. Bár az ideális az lenne, ha valamennyi támadást meg lehetne akadályozni, a gyakorlatban inkább a támadások számának minimalizálására, illetve arra törekednek, hogy támadások esetén minél kisebb legyen az okozott kár, végleges adat- és információvesztés ne következzen be, s minél hamarabb vissza lehessen állítani a támadás előtti állapotot. Az info-kommunikációs rendszerek működésének leírására, illetve monitorozására kidolgozott mutató- és mérőszámok, valamint ezek feldolgozása, elemzése, a köztük levő kapcsolatok megismerése és vizuális bemutatása (adatvizualizáció) hatékonyan képes támogatni (1) a vezetőket a biztonságosabb környezet kialakításához szükséges döntések meghozatalában, illetve (2) a szakembereket abban, hogy az informatikai támadásokat minél nagyobb arányban tudják megakadályozni, illetve az incidenseket minél hatékonyabban legyenek képesek kezelni.

A média és a biztonság mérőszámai – intuitív megközelítés

A jelenlegi probléma véleményem szerint az, hogy ugyan a mutatószámok használatának kialakult gyakorlata van, s a médiatervezés során – ahogy azzal tanulmányomban már foglalkoztam – a mutatószámok meghatározása és értelmezése révén a kommunikációs kampány viszonylag egzakt módon, számszerűsítve értékelhető, s bizonyos információbiztonsági folyamatok ugyancsak egzakt mérésére is számos példa van, a két terület metszéspontjában megjelenő mérés- és kiértékelés a módszertan vonatkozásában meglehetősségen hiányos.

A digitális kommunikáció mérésénél tanulmányom média mutatószámainál leírt gondolatok jó alapot jelenthetnek. Ezek a weboldal leterheltségére, a látogatók számára, az adott oldalon eltöltött időre, az ismerősök számára, az oldalon tanúsított látogatói aktivitásokra utalnak. Miközben a kampányok sikerességeinek egyik ismérve lehet az, ha az adott kampányidőszakban jelentősen megnövekszik az oldalra látogatók száma, a kampányidőszakon kívüli kiugró látogatás információbiztonsági szempontból gyanús lehet. Ugyancsak gyanús lehet, ha ugyan sokan látogatnak az oldalra, de ott csak nagyon rövid időt töltenek el. Pozitívan értékelendő, ha valakinek/valaminek egy tudatos kampány részeként rövid idő alatt sok ismerőse/követője lesz a Facebookon, Linkedinen, de nem a megszokott kommunikációs aktivitásra utal az, ha a kampányidőszakon kívül közel egy időben 10-15 olyan személy jelöl ismerősnek, akinek nincs semmilyen közös pontja velünk.

Az intuitív megközelítés mellett a különböző mutatószámok használatával egy objektívebb képet tudunk alkotni arról, hogy az online kommunikációs felülettel kapcsolatban tanúsított aktivitás egy normális folyamat része, vagy érdemes biztonsági ellenőrzést végezni.

A folyamatok mérőszámai

A szakirodalom (Parmenter, 2010, Hubbard és Seiersen, 2016, Baroudi, 2010, Tipton és Krause, 2008, Frey, Lüthje és Reich, 2013, Zimmerman, 2017, valamint ETSI és Deloitte ajánlásai) számos mutatószám-csoportot nevez meg, úgymint: KPI (teljesítménymutató), KRI (kockázatmutató), KRA (területek eredményei), KPA (teljesítményterület), KCI (ellenőrző indikátor), KPX (teljesítménymutató index), ISI (információbiztonsági indikátor), KPSI (biztonsági indikátor) melyek közül tanulmányomban hangsúlyosan a KPI-val, illetve érintőlegesen a KPX-vel foglalkozom.
A KPI (key performance indicator – legfontosabb teljesítménymutatók) célja, hogy magas szintű áttekintést nyújtson a szervezet és főbb operatív egységeinek múltbéli teljesítményéről, amelyek szinte kizárólag a történelmi adatokra (megtörtént, rögzített események) irányulnak. A KPX (key performance index – legfontosabb teljesítménymutató index) egy vagy több KPI összefoglalója vagy korrelációja, amely jelzi a folyamat egy meghatározott területének általános teljesítményét.
A KPI-ok és a KPX meghatározásának a lépései a következők:

1. A célok meghatározása
2. Kritikus sikertényezők meghatározása
3. KPI-ok meghatározása
4. Adatgyűjtés
5. KPI-ok kiszámítása
6. KPI-okból KPX-ek meghatározása/kiszámítása
7. Szofisztikált elemzés
8. Következtetések megfogalmazása

A (1) ***célok meghatározásánál*** érdemes konkrétan megfogalmazni az elvárásokat. A szervezeti (digitális) kommunikáció biztonságosabbá tétele célkitűzés ugyan filozófiai szinten kiváló gondolat, de a gyakorlatban a célt úgy kell megalkotni, hogy abból a (2) ***kritikus sikertényezők*** meghatározhatóak legyenek. Ilyen sikertényező lehet az, hogy egy éven belül 20%-kal csökken a végpontokra (felhasználók számítógépére) érkező fertőzött e-mail-ek száma. Természetesen a sikertényezők eléréséhez szükség lehet erőforrások hozzárendelésére is, pl.: új hardver- és szoftverkomponensek beszerzése és üzembe helyezése, munkatársak (tovább)képzése, stb. A (3) ***KPI-ok meghatározásánál*** a Deloitte ajánlást ismertetem az alábbiakban (1. táblázat):

1. táblázat *A Deloitte ajánlása a KPI-lap elkészítésére (saját szerkesztés)*

KPI neve	A KPI rövid neve, verziószáma, készítés dátuma, sorszáma
KPI státusza	Kidolgozás alatt, tesztelés alatt, bevezetve, kivezetve
Leírás	A KPI leírása, mit takar/jelent az adott mutató
Feladat	Mi a feladata, mit kér a KPI, miért fontos ez a mutató
Érdekelt felek	Kire vonatkozik a KPI
Típus	Mennyiségi, minőségi, mérföldkő, küszöb, tartomány

Fontosság	Alacsony, közepes, magas
Egység/osztály	Milyen szervezeti egységet érint
Módszer	Annak a módszere, hogy hogyan kell mérni a KPI-t
Mérés tárgya	SOC[5] hatékonyság, vállalati fenyegetettség, IBIR[6], érettség…
Eszközök	Azok az eszközök, amelyek a mérést és jelentést támogatják
Gyakoriság	Nap, hét, hónap, negyedév, év, több, mint egy év
Megjegyzés	Kiegészítő információk. A szabály megalkotásához, vagy a szabályozáshoz szükséges?

A KPI-lap összefoglalja az adott KPI-val kapcsolatos fontosabb tudnivalókat. Ezek közül a típus ötféle KPI-t különböztet meg, úgymint:

1. Kvantitatív: objektíven merhető, mennyiségi adatok: bejelentett biztonsági események száma
2. Kvalitatív: minőségi adatok: különböző tesztek eredményei
3. Mérföldkő: bizonyos időpont, vagy tevékenység elvégzésének dátuma: tanúsítvány felülvizsgálati ideje
4. Küszöbérték: elér valamilyen szintet, vagy beleesik valamilyen tartományba: informatikai incidensek gyakorisága tartósan átlag feletti szinten van
5. Tartomány: minimum és maximum értékek, melyek között a mért érték elfogadható

A fontosság és a gyakoriság között a gyakorlatban kapcsolat van. Azok a teljesítménymutatók, melyekről úgy döntöttek az információbiztonsági szakemberek, hogy fontosak (magas), azok méréséhez erőforrásokat is rendeltek annak érdekében, hogy a mérés gyakorisága biztosítható legyen.

Az (4) ***adatgyűjtés*** előtt meg kell határozni azokat a mérőpontokat és eszközöket, ahonnan az adatokat gyűjteni lehet. Mivel a digitális kommunikáció biztonságának mérésénél nem csak a gazdasági, hanem a biztonság-fókuszú mutatószámok megalkotása is cél, ezért rendszerint a szervezetbe érkező adatforgalmat fogadó/küldő hálózati eszközök, routerek, tűzfalak, stb. valamint az ezeken futó szoftverek és alkalmazások jelentik azokat a mérőpontokat, amelyek adatokat tudnak szolgáltatni. A gyakorlatban az alábbi dolgok mérése szükséges:

- Idő
    - Válaszidő
    - Reakció idő
- Mennyiség
    - Db.
    - Érintettek száma
    - Adatok, információk mennyisége

[5] SOC: Security Operations Center, Biztonsági Központ, a szervezetnek az a része (osztálya, részlege), amelyiknek az a feladata, hogy megelőzze és elhárítsa a szervezet ellen irányuló kibertámadásokat, valamint naprakészen tartsa a szervezet információ- és informatikai biztonsági rendszereit.

[6] IBIR: információbiztonsági irányítási rendszer

- Költség
- Stb.

Az eszközök és a szoftverek/alkalmazások működésével kapcsolatban – jobb esetben – folyamatosan gyűjtenek és rögzítenek adatokat a logfájlokba, s a fejlettebb rendszereknél arra is lehetőség van, hogy amennyiben a meghatározott szint fölé/alá kerül egy érték, vagy elér egy bizonyos szintet, akkor a rendszer riasztást küldjön a szakembereknek.
A (5) ***KPI-ok számítása*** rendszerint egyszerű feladat, mivel vagy eleve a mért adat egyben KPI is lehet (pl.: a szervezetbe meghatározott idő alatt érkező e-mail-ek száma), vagy könnyen kiszámítható (pl.: a szervezetbe érkező fertőzött e-mail-ek aránya az összes e-mailhez képest). Néhány példa a KPI-okra:

- Adott idő alatt a felhasználók által küldött e-mail-ek
- Adott idő alatt a felhasználók által fogadott e-mail-ek
- A küldött e-mail-ekből hány % volt fertőzött
- A fogadott e-mail-ekből hány % volt fertőzött
- A biztonságos/folytonos üzletmenetet veszélyeztető kockázatok előfordulási gyakorisága
- Fenyegetésfajták száma/aránya
- Naponta/hetente/havonta mennyi időt áll az info-kommunikációs rendszer
- A jelzéstől az incidens kezelésének a megkezdéséig eltelt idő
- Átlagos ügykezelési idő
- Hibásan spamnak minősített üzenetek aránya

(6) ***KPI-okból KPX-ek meghatározása***. Az említett szakirodalmak nem egységesek a KPI-ok számát illetően. Azok a szerzők, akik nem foglalkoznak a KPX-ekkel, egy bizonyos terület mérésére maximum 8-10 KPI-t javasolnak, míg azok, akik számára a KPI csak jó alap a KPX-ek meghatározásához, inkább a KPX-ek számát maximalizálják 8-10-re, s a KPI-okkal kapcsolatban általánosságban úgy fogalmaznak, hogy annyi KPI-nak kell rendelkezésre állnia, hogy a KPX-ek az elvárt gyakoriság és pontosság mellett legyenek meghatározhatók. A KPX-ek a KPI-okhoz képest komplexebb jelentéssel bírnak, s lehetővé teszik kevesebb mutatószám mellett is a digitális info-kommunikációs folyamatok viszonylag egzakt nyomon követését, ellenőrzését. KPX írja le többek között a rendszer rendelkezésre állási idejét, a hálózati infrastruktúrát, a jogosultságkezelést, az info-kommunikációs eszközökön futó szoftverek és alkalmazások frissítéseinek a kezelését. A KPX-ek és az ezeket támogató KPI-ok megalkotása összességében megalapozott segítséget nyújt az olyan kérdések eldöntéséhez, hogy a szervezet változtasson-e stratégiai irányt az információbiztonság területén (ami közvetlen hatással van a szervezeti kommunikációra is), hogyan lehet támogatni a szervezet vízióját, misszióját és stratégiáját. Mivel a KPI-ok és a KPX-ek gyakran a vezetőknek szóló, jelentésekben is szerepelnek, ezért nagyon fontos, hogy a nem informatikai végzettséggel rendelkező menedzsment is értelmezni tudja ezek tartalmát. Pl.: a KPI-ok/KPX-ek alapján meghatározták, hogy a közösségi média munkahelyi használata veszélyt jelent a szervezet számára. A vezető ilyenkor olyan döntést hoz(hat), hogy tiltja ezeknek a használatát, holott ezzel a szervezet kommunikációs igazgatóságának/osztályának a munkáját is megnehezíti. A helyes döntés ilyenkor inkább az, hogy felülvizsgálják az adott munkakörhöz tartozó informatikai és kommunikációs jogosultságokat, majd ennek alapján

bizonyos munkaköröknél továbbra is engedik a közösségi média használatát, de ezzel párhuzamosan a használóknak egy biztonságtudatosságot erősítő rövid képzést is tartanak.
Bár már a KPX-ek is komplexebb képet adnak a KPI-okhoz képest, az info-kommunikációs rendszer és környezete (értve ezalatt a belső-külső humán kommunikációs ágenseket is) működésének a vizsgálata amellett, hogy új és izgalmas terület, sokkal hatékonyabbá tudja tenni a szervezeti biztonság védelmét jelen és jövő időben egyaránt. A (7) ***szofisztikált elemzés*** révén megalapozott válaszokat lehet találni a rendszer és környezetének megannyi eseményére többek között az alábbi elemzési módszerek segítségével:

- Okok értelmezése
- A rendelkezésre álló tények elemzése
- Idősoros elemzés: trendvonal, szezonalitás, prognózis
- Gyakoriság, átlag, módusz, medián, terjedelem, szórás
- Becslés
- Valószínűségszámítás
- Korrelációszámítás
- Hálózatkutatás, szociometria -> KPI-metria
- Adatvizualizáció
- A használt KPI-ok/KPX-ek újragondolása

Az elemzés után a folyamat zárásaként a (8) ***következtetések megfogalmazása*** következik. Miközben a kommunikációs kampányok mutatószámainak elemzésekor rá lehet mutatni, vagy következtetni lehet a kampány erős és gyenge oldalaira, a hiányosságokra, az alul- illetve felülteljesítés okaira, addig a KPI-ok és KPX-ek alkalmazásának első időszakában rendszerint nem a következtetések megfogalmazása a legfontosabb, hanem – ahogy a hetedik pontban utaltam rá – a használt KPI-ok/KPX-ek újragondolása annak érdekében, hogy a szervezet ki tudja alakítani azt a mérési rendszert, amelyiknél hosszabb távon már csak kisebb korrekciókra van szükség. Ezért is fontos a KPI-lapokon feltüntetni a teljesítménymutató verziószámát, a készítés és az aktualizálás/frissítés dátumát. A szervezetek infokommunikációs rendszere mérésének ebben az érettségi szakaszában az teljesen elfogadott, hogy a KPI-okat és a KPX-eket cserélgetik, esetleg a mérési pontok helyében, vagy az azok által szolgáltatott adatok mintavételezési gyakoriságában változtatnak.

ZÁRÓ GONDOLATOK

A szervezet céljaiért elkötelezett munkatársainak érdeke, egyfajta belső késztetése, s bizonyos esetekben munkaköri kötelessége is, hogy kommunikáljanak a szervezet külső és belső érintettjeivel, reagáljanak a szervezettel kapcsolatos hírekre, megjegyzésekre, munkálkodjanak a szervezet márkájának és különféle márkadimenzióinak a kommunikációján. Ugyancsak érdeke a szervezet céljaiért elkötelezett munkatársainak, hogy mindent megtegyenek annak érdekében, hogy a szervezet a biztonság komplex értelmezésében – s így az információbiztonság és a gazdasági biztonság területén is – minél alacsonyabb kockázat mellett működjön. Rendszerint belső szabályzatok foglalkoznak azzal, hogy a szervezet mely munkavállalói nyilatkozhatnak a szervezettel kapcsolatban, illetve, hogy milyen helyes és biztonságtudatos magatartást kell tanúsítania a munkavállalóknak. A párhuzamos gondolatmenet mentén az is megállapítható, hogy a szervezetek kommunikációs aktivitásai mellett már

a szervezetek információbiztonsági folyamatai is mérhetők. A feladat az, hogy ezek az egymással gyakorlatilag párhuzamosan futó területek minél hamarabb találkozzanak annak érdekében, hogy az információbiztonság ne menjen a kommunikációs aktivitás rovására és fordítva, a kommunikációs aktivitások ne veszélyeztessék az információbiztonságot. Tanulmányomban azt szerettem volna érzékeltetni, hogy a két területnek számos olyan közös pontja van, amelyik lehetővé tudja tenni az együtt gondolkodást, s a kellő intelligenciával bevezetett és elemzett, az információbiztonsághoz kapcsolódó mutatószámok nem csak az információbiztonság, hanem a (digitális) kommunikáció biztonságosabbá és ezáltal hatékonyabbá tételében is lehetőséget jelentenek. Jelenkorunkban, az adatok korában ugyanis a szervezetek valamennyi folyamata mérhetővé válik, de ezek a területenkénti mérések csak akkor vezetnek eredményre, ha az elemzések során a komplex szemléletmód, a valamennyi terület fejlődését szem előtt tartó vezetői döntések érvényesülnek.

FELHASZNÁLT IRODALOM

Balassa Lilla – Klausz Melinda (2015): *A közösségi média mérése. Hogyan elemezd a mutatókat és hozz ki minél többet az oldalaidból*. szerzői kiadás, Veszprém.
Baroudi, Rachad (2010): *KPI mega library*. author's edition, Scott Valey.
Deloitte (2006): *You Can't Manage It If You Can't Measure It*.
Európai Távközlési Szabványok Intézete (ETSI) ajánlása „Information Security Indicators (ISI); Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection" címmel.
http://www.etsi.org/deliver/etsi_gs/ISI/001_099/003/01.01.02_60/gs_isi003v010102p.pdf (letöltés ideje: 2019.01.10.)
Fazekas Ildikó – Harsányi Dávid (2004): *Marketingkommunikáció*. Szókratész Külgazdasági Akadémia, Budapest.
Frey, Stefan – Lüthje, Claudia – Reich, Christoph (2013): *Key Performance Indicators for Cloud Computing SLAs*. EMERGING 2013: The Fifth International Conference on Emerging Network Intelligence.
Haig Zsolt (2015): *Információ, társadalom, Biztonság*. NKE Szolgáltató Kft, Budapest.
Hamburger Béla (1995): *A médiatervezés módszertana*. Magyar Reklámszövetség, Budapest.
Hubbard, W. Douglas – Seiersen, Richard (2016): *How to measure anything in cybersecurity risk*. John Wiley & Sons, New Yersey.
Incze Kinga – Pénzes Anna (2002): *A reklám helye. A hatékony médiatervezés és –vásárlás kézikönyve*. Stardust Publishing Kft, Budapest.
Kollár Csaba (2004): *Reklám- és reklámszöveg kutatás*. PREMA Consulting, Budapest.
Magyarországi Kommunikációs Ügynökségek Szövetsége: Briefing útmutató médiatenderek esetén. http://maksz.com/downloads/mediaugynoksegi-briefing-utmutato.pdf (letöltés ideje: 2019.01.10.)
MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Következmények.
Munk Sándor (2008): *A kritikus infrastruktúrák védelme információs támadások ellen*. In.: Hadtudomány, XVIII. évf., 2008/1, 95-106 p.
Parmenter, David (2010): *Key performance indicators*. John Wiley & Sons, New Yersey.

Shannon, Claude E. – Weaver, Warren (1949): *THE MATHEMATICAL THEORY OF COMMUNICATION*. The University of Illinois Press, Urbana.
Szabó D. Tamás (1999): *Médiatervezés a reklámban*. Budapesti Közgazdaságtudományi Egyetem, Budapest.
Tipton, Harold F. – Krause, Micki (szerk., 2008): *Information Security Management Handbook*. Auerbach Publications, Boca Raton.
Virányi Péter (szerk., s.a.): *Fogalomtár a reklámról*. KOTK, Budapest.
Zimmerman, Timothy A. (2017): *Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis*. National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8177 (letöltés ideje: 2019.01.10.)