Az informatikai sérülékenységek gazdasági összefüggései – A kiberbiztonság megjelenése a makro- és mikroelemzésekben

Dr. Horváth Attila

Vezető kutató
Információs Társadalomért Alapítvány
e-mail: horvath.attila@infota.org

Erdősi Péter Máté

PhD hallgató
Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola
e-mail: erdosi.peter.kdi@office.uni-nke.hu

Dr. Kiss Ferenc

Kutató
Információs Társadalomért Alapítvány
e-mail: kiss.ferenc@infota.org

Absztrakt

A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal – NKFIH által támogatott PD-109740 számú kutatási projekt keretében immár 3 éve vizsgáljuk az informatikai sérülékenységeket és azok lehetséges társadalmi, gazdasági hatásait. A kutatás három éve alatt főként arra kerestük a válaszokat, hogy a sérülékenységekből fakadó biztonsági problémáknak milyen áttételes hatásai jelennek meg a gazdaságban.

A következő tanulmányban az informatikai biztonság nemzetgazdasági, makrogazdasági stratégiai kérdéseit és gazdasági számszerűsítési lehetőségeit vizsgáljuk első sorban. Felvezetésként az infokommunikációs technológiák és ezen belül az IT-biztonság nemzetgazdaságban, gazdasági növekedésben elfoglalt helyével és szerepével foglalkozom, majd felvázolok egy hételemű modellt, amely jól reprezentálja egy nemzetgazdaság felkészültségét a digitális korszak előretöréséből eredő kihívásokra. Ezután megvizsgálok több alap és később kifejlesztett, alternatív makro mutatót, keresve bennük a fenti hatásokat, a kiberbiztonsági szempontok közvetett vagy közvetlen megjelenését. Végül pedig bemutatásra kerül egy mikro szintű modell, amelynek segítségével vállalati környezetben számszerűsíthetők a biztonsági erőfeszítések gazdasági hatásai.

Kulcsszavak: *makromutatók, gazdasági növekedés, GDP, GNP, infláció, FDI, GPI, HPI, kiberbiztonsági stratégia, kiberbűnözés, sérülékenység, biztonság, incidens kezelés, nemzetbiztonság*

1. Bevezetés: Az IKT és az IT-biztonság helye a nemzetgazdaságban

A legtöbb modern országban a gazdasági stratégia erőteljesen épít az infokommunikációs terület fejlődésére, fejlesztésére. Ehhez az egyik legfontosabb intézkedéscsomag, hogy gyors, megbízható és elérhető árú kommunikációs lehetőségeket biztosítsanak minden háztartás és vállalkozás számára, és ezzel elősegítsék az információs társadalomhoz és az új gazdasághoz való csatlakozást. A különböző szektor szintű modernizációs törekvések: e-kormányzat, e-bankolás, e-egészségügy, e-tanulás, új generációs energiaellátás és vezérlés, a közlekedés és közszolgáltatások automatizálása, intelligens városok és okos infrastruktúra kialakítása – szerepelnek első helyen a legtöbb állam hosszú távú innovációs stratégiájában. Például Kína „Internet Plus" stratégiája kifejezetten az elektronikus kereskedelem egészséges terjedését és fejlődését tűzte ki célul a világ egyik legnagyobb gazdaságában, a stratégia a kereskedelem mellett nagyban épít az ipari hálózatok és a bankrendszer szerves integrálására az e-korszakba, illetve kifejezetten támogatja az olyan új iparágak megjelenését és az olyan vállalatok terjeszkedését és innovációs törekvéseit, amelyek ezzel az országos szintű stratégiának megfelelő irányban alakítják ki és folytatják saját fejlesztéseiket, innovációs terveiket. (State Council of China, 2015) Kína, India, Európa, Észak-Amerika mind-mind a „digitális alapokon nyugvó tudásközpontú gazdaság" irányába szeretnének haladni, támogatva az IT-szektor számára munkaerőt biztosító képzési és átképzési tevékenységeket és minél több, a szektorhoz köthető munkahelyteremtő beruházást vonzani az adott országba a pénzügyi, egészségügyi, tudásmenedzsment és más határterületeken is. (Government of India, 2015)

Az Európai Bizottság a digitális szolgáltatások teljesen egységes, szabad és közös piacának megalkotásán munkálkodik a közösségen belül, hiszen a digitális szolgáltatásuk természetüknél fogva még könnyebben mozognak a nemzetállami határokon keresztül, így hozzájárulva az Európai Unió alapértékeit képező szabadságjogok, a tőke, a munka, az áruk és szolgáltatások valóban szabad áramlásának elősegítéséhez. Az előrejelzések szerint ez a „Digitális Közös Piac" (Digital Single Market Strategy) évi 415 milliárd euróval magasabb GDP megtermeléséhez vezet majd a közösség számára. (European Commission, 2015)

Természetesen a digitális technológiák kiterjedt alkalmazása felveti mindazokat a biztonsági kérdéseket és kockázatokat, amelyekkel a kutatás korábbi szakaszaiban kiterjedten foglalkoztunk. Az állami szintű alkalmazás egyenesen nemzetbiztonsági szintű kérdésként kezeli és jeleníti meg az informatikai biztonsági problémákat. A gazdaságfejlesztési stratégiáknak tehát egyre inkább figyelembe kell venni a biztonsági aspektusokat is, a nemzetbiztonsági, kiberbiztonsági megfontolásoknak pedig együtt kell haladniuk a digitális gazdaságfejlesztéssel.

A fejlődő országok kormányai még erőteljesebben, gyorsított ütemben igyekeznek felzárkózni a világhoz és ezek az agresszív kommunikációfejlesztési stratégiák a következő évek során további embermilliók számára teszik majd lehetővé a kapcsolódást a világhálóhoz és az arra épülő társadalmi- gazdasági-kommunikációs ökoszisztémához. (Hathaway-Spidalieri, 2015) A Világbank számításai szerint, a megfelelő szintű infokommunikációs hozzáférés egy ország lakosai számára jelentős GDP növekedést eredményez, kb. 1-2%-os GDP fejlődést lehet várni a lakosság minden 10%-ának bekapcsolásával a digitális kommunikációba. (World Bank, 2014)

A legfrissebb kutatások azt is alátámasztják, hogy az internet és az IKT kiterjedt alkalmazása, mind vállalati, mind állami szinten hozzájárul a hosszú távú versenyképesség és a szociális jóllét megteremtéséhez és fenntartásához, közvetve akár a teljes GDP 8%-áért is felelős lehet. (Dean, 2012) Néhány kutatás még messzebbre megy: ha az ipar (feldolgozóipar és termék előállítás) és energiaszektor (energia termelés, infrastruktúra, hálózatmenedzsment, stb.) súlyát és az abban rejlő, okos technológiák általi modernizációs és automatizálási lehetőségeket vizsgáljuk, ez a terület a világgazdaság 46%-át teszi ki, amely néhány éven belül akár 50% fölé is emelkedhet. (Evans-Annunziata, 2012)

Ez az erőltetett, gyors felzárkóztatás, különösen a fejlődő országok esetében komoly biztonsági kérdéseket vet fel, ahogy a dolgok internetével kapcsolatos kutatások során is megfigyelhettük a technológiai lehetőségek fejlődése gyakran magasan a biztonsági megfontolások evolúciója előtt jár. Az okos technológiák alkalmazása csábító, hogy rögtön a legmodernebb, 21. századnak megfelelő színvonalra emeljék ezek az országok a digitális infrastruktúrájuk színvonalát, a fejlődési lépcsőfokok kimaradása viszont sok esetben azzal fenyeget, hogy a biztonság területén nem történik meg az az ugrásszerű fejlesztés, ami az új infrastruktúrák 21. századi színvonalú védelméhez szükséges. (Horváth et. al., 2015) Így összességében az erőltetett digitalizáció olyan kockázatoknak teszi ki a nemzetgazdaságot, amelyre a résztvevők egyáltalán nincsenek felkészülve, nincsenek meg a magfelelő válaszok az esetleges incidensek esetén, és külső harmadik felek számára kihasználható sebezhetőségeket kínálnak, akár bűnözői csoportokról, akár terrorizmusról, akár a modern, digitális hadviselésről van szó.

Mindazonáltal, a nemzetgazdaságok nem engedhetik meg maguknak, hogy kimaradjanak ebből a gazdaságfejlesztési lehetőségből. De kevesen gondolják át az ezzel együtt járó jelenségeket: az új technológiák bevezetésével együtt járó mellékhatásokat és járulékos költségeket: a kívülről is jobban elérhető és befolyásolható kritikus infrastruktúrák, az állampolgárok sokkal magasabb adatvédelmi kitettsége, állami és üzleti titkok illetéktelen kezekbe kerülése, a kiberbűnözés és elektronikus csalások hatásai – ezek mind veszélyeztetik a gazdasági, társadalmi és politikai stabilitást. (Hathaway, 2014a)

Leegyszerűsítve: a kiberbiztonsági kockázatok és a költségek egyfajta adóként rakódnak a digitális növekedés hozadékaira.

Becslések szerint a 20 legfejlettebb országot tömörítő G20-as tömb mintegy 2,5 millió munkahelyet veszített csak a hamisítás és a kalózkodás hatásaként, és a kormányok, ezzel együtt pedig az állampolgárok is évente átlagosan mintegy 125 milliárd dolláros veszteséget szenvednek el kiber-bűncselekmények miatt, az elmaradt adókat is beleértve. (Frontier Economics, 2011) Az Egyesült Államok becslése szerint csak a szellemi tulajdon elleni bűncselekmények következtében évi 300 milliárd dollárt vesztett az amerikai gazdaság, ami a GDP kb. 1%-ának felel meg. (The National Bureau of Asian Research, 2013)

Ahogy az IKT egyre szélesebb körben kerül alkalmazásra, növekszik az internet penetráció, ezzel együtt exponenciálisan növekszik a kitettség, a kapcsolódó kockázatok, a gazdasági költségek is, hacsak a biztonsági kérdések nem fogják a modernizációs stratégiák szerves részét képezni, lekövetve a technológiai fejlődést. Egy digitalizált társadalom csak akkor maradhat ellenálló a fejlődés negatív aspektusaival szemben, ha az innovációs stratégiák gerincének a biztonsági aspektusok is szerves részét képezik.

A járulékos veszteségek számszerűsítése arra kényszerítik a politikai döntéshozókat is, hogy a biztonságot erőteljesebben beépítsék a gazdaságfejlesztési programokba, létrehozva egy nemzeti biztonsági stratégiát, megfelelő forrásokat biztosítva annak fejlesztéséhez. (Hathaway, 2014b) A biztonsági kockázatok átláthatósága és számszerűsítése közös érdekké teszi a biztonsági fejlesztéseket és annak költségeit mind az állami szervek, mind a vállalkozások és az állampolgárok számára. Többféle módszertan is létezik arra nézve, hogy ez a számszerűsítés a döntéshozók számára megvalósulhasson. Nemzetgazdaságok szintjén ilyen például a CRI (Cyber Readyness Index) (Hathaway et.al., 2015), szervezetek szintjén pedig a ROSI (Return on Security Investments)-modell (Sonnenreich, 2006), amely mikro szinten igyekszik mérni a biztonságba való befektetések hatásait.

2. A kiberbiztonság helye a nemzetgazdaságban

Nemzetgazdasági szinten 7 pillére van annak az ökoszisztémának, amelybe a biztonsági aspektusoknak szervesen be kell épülni ahhoz, hogy az adott országot megfelelően felkészültnek tekinthessük informatikai biztonsági kérdésekben, ahogy Melissa Hathaway és kutatótársai ezt megfogalmazták (Hathaway et.al., 2015):

1. Létezik-e az adott országban nemzeti kiberbiztonsági startégia?
2. Megoldott-e e szervezett incides-kezelés?
3. Megfelelően kezeli-e a törvényhozás és a bűnüldözés a kiber-bűncselekményeket?
4. Része-e az adott ország azoknak az információ-megosztó hálózatoknak, amelyek segítenek megfelelően és gyorsan reagálni a fenyegetésekre?
5. Megfelelő-e az informatikai biztonsági kutatás-fejlesztésbe való befektetések aránya?
6. Része-e az IT-biztonsági problémák kezelése a diplomáciai, külpolitikai, illetve kereskedelempolitikai tevékenységnek?
7. Megfelelő szintű-e a kibervédelem és az incidenskezelés a honvédelmi, külső elhárítási területen?

2.1. A nemzeti kiberbiztonsági stratégia

Az első és legfontosabb kérdés, hogy létezik-e egy olyan átgondolt és összeszedett kiberbiztonsági intézkedés csomag, ami képes összehangolni az adott ország gazdaságfejlesztési törekvéseit a biztonsági kérdésekkel. A stratégiának tartalmaznia kell a legfontosabb fenyegetéseket gazdasági mérőszámokkal megfogalmazva, bemutatni a szükséges lépéseket, programokat és intézkedéseket, amelyek szükségesek a fenyegetések elhárításához és az ország digitális infrastruktúrájának megfelelő színvonalú védelméhez. A stratégiának le kell fedni az állampolgárok, a vállalkozások és a közigazgatási szervezetek igényeit, az általuk alkalmazott megoldásokat és erőforrásokat. Egy ilyen átfogó terv segít a kiberbiztonsági incidensekből származó GDP-csökkenés lefaragásában, valamint növeli az ország biztonságát és ellenálló képességét. A jó stratégia nem csak megfogalmazásában kell, hogy mindenre kiterjedjen, de gyakorlatiasnak, végrehajthatónak is kell lennie, olyan operatív akciókra kell tudni lebontani, amelyeket a törvényhozás, az oktatás, a bűnüldözés, a kutatás-fejlesztés, a közigazgatás, stb. a maga szintjén és területén képes értelmezni és akciókká transzformálni. Nevén kell nevezni a problémákat és meg kell nevezni azokat a hatóságokat, akik felhatalmazást kapnak az adott problémakör kezelésére, a stratégia adott részeinek végrehajtására, és ezért felelősséggel, elszámoltathatósággal tartozik.

A legfőbb cél tehát a megfelelő kiberbiztonsági stratégia kinyilvánítása, amely figyelembe veszi a gazdasági aspektusokat és kockázatokat-

Szervezeti háttér:

- Szükséges ennek végrehajtásához a felelősségi körök megfelelő definiálása, amelyet a stratégia meghatározott pozíciókhoz rendel.
- Azonosítani kell azokat a kormányzati szervezeteket, amelyekre a stratégia közvetlen vagy közvetett hatással van, vagy pedig a végrehajtásban van meghatározó szerepük.
- Be kell azonosítani a kereskedelmi szektor azon szervezeteit, vállalkozásait is, amelyeknek szerepe lehet a stratégia sikeres megvalósításában.

Erőforrások:

- Természetesen szükséges a megfelelő emberi és pénzügyi erőforrások biztosítása a stratégia végrehajtásához.
- Meg kell határozni, hogy a GDP mekkora része takarítható meg, illetve szükséges ráfordításként a stratégia sikeres megvalósítása során.

Eredmény indikátorok:

- A megvalósításhoz szükséges a kritikus digitális infrastruktúra azonosítása, amelyet meg kell védeni. Ezen belül azonosítani kell a kritikus szolgáltatásokat, amelyek működésének fenntartása stratégiai jelentőségű a nemzetgazdaság számára.
- Nemzeti szabványokat kell létrehozni a kritikus infrastruktúrák és szolgáltatások üzletmenet folytonossági követelményeinek meghatározására, valamint megfelelő jelentési rendszert, amely a kieséseket és zavarokat a kulcs területeken mérni és értékelni képes.

2.2. Reagálási képesség a biztonsági incidensekre

A nemzetgazdasági szintű IT-biztonsági felkészültség második eleme, hogy kialakításra kerüljön egy hatékony reagálási képesség a különböző biztonsági incidensekre. Ez gyakran különböző nemzeti hálózatbiztonsági csoportok formájában valósul meg. A felállított szervezetek csoportok feladatai többek között a fenyegetések megértése, értelmezése és prezentálása a döntéshozók számára olyan formában, hogy az ő számukra is értelmezhetővé váljon, a fenyegetések és sérülékenységek és a megoldási javaslatok publikációja, az IT-bizotnság oktatás és a legjobb gyakorlatok terjesztése, az IT-biztonsági veszélyforrások érzékelés, beazonosítása, elhatárolása és kezelése, az incidensek elemzése, a reaktív intézkedések megszervezése és levezénylése valamint a ellenálló képességet növelő intézkedések és gyakorlatok promóciója a gazdasági szereplők széles köre számára.

A legfontosabb feladatok ebben az esetben tehát:

- egy incidens kezelési terv létrehozása vészhelyzetek és katasztrófák esetére
- A szektorközi összefüggések azonosítása és feltérképezése, amelyek szükségesek a katasztrófák tovagyűrűző hatásainak előre jelzéséhez és kezeléséhez
- A tervezetet folyamatosan frissíteni kell a mindenkori igényeknek megfelelően
- A nemzetgazdasági szintű kockázatok felmérése és publikálása a kormányzati szervek, kritikus infrastruktúrák és szolgáltatási hálózatok szintjén

Szervezeti háttér:

- Létre kell hozni a nemzeti hálózatbiztonsági és incidenskezelő szervezeteket
- Ki kell jelölni azokat a hatósági kontaktokat, amelyek ellátják információval a szervezetet a kormányzati szervek oldaláról, és akik az incidens kezelésben felelősen részt tudnak venni az az adott intézmény oldaláról
- Ki kell jelölni azokat a kontaktokat, akik a kritikus infrastruktúrák üzemeltetésében képesek megtenni ugyanezen lépéseket
- Egy korai riasztási hálózat létrehozása, amelyen keresztül megfelelően tudnak terjedni a kritikus információk

Erőforrások:

- Létre kell hozni és fenn kell tartani a hálózatbiztonsági szervezeteket, megfelelő forrásokat biztosítva kijelölt feladataik ellátásához
- Fenn kell tartani a korai riasztási rendszert, rendszeres gyakorlatokkal tesztelve annak működését, hogy egy valódi katasztrófahelyzetben minden a terveknek megfelelően tudjon üzemelni, a rendszeres gyakorlatok a nemzetgazdaság általános ellenálló képességét is növelik a kritikus pontokon való felkészültség javításával.

Eredmény indikátorok:

- Bizonyított incidenskezelési képesség, ellenállóképesség a biztonsági kihívásokkal szemben, a kritikus szolgáltatások és infrastruktúra növekvő üzletmenet folytonossága és rendelkezésre állása
- A nemzeti hálózatbiztonsági központok bizonyított kríziskezelési képessége, időben kiadott és megfelelő hatékonysággal kommunikált riasztások.
- Folyamatos kutatások a biztonsági területen, a már lezajlott incidensek mintázatainak és eredményeinek folyamatos vizsgálata, amely folyamatosan javítja a védekezési képességeket.
- Rendszeres gyakorlatok kidolgozása és megvalósítása, amelyek segítenek minden érintett szereplőnek felkészülni az éles vészhelyzetekre. Megfelelő forgatókönyvek, cselekvési tervek kidolgozása, és alkalmazási képességük gyakorlati megkövetelése.

2.3. Kiberbűnözés és --bűnüldözés

Az államnak el kell köteleznie magát, hogy megvédi a polgárait és az intézményeit, vállalatait a kiberbűnözéstől. Ehhez ki kell alakítani a megfelelő jogrendszert, illetve a bűnüldöző hatóságot fel kell vértezni a megfelelő szakértelemmel, technológiai infrastruktúrával és felhatalmazással, hogy hatékonyan vehesse fel a küzdelmet az új típusú bűnelkövetőkkel szemben. A technológiai modernizáció igénye nem csak a bűnüldözésre, hanem az ügyészségi és bírósági gyakorlatra is ki kell hogy terjedjen, hogy a vád és bizonyítási eljárásokban képesek legyenek felhasználni a cselekmények technológiai színvonalának megfelelő eljárásokat alkalmazni. Természetesen ezen a területen semmire nem mennek a hatóságok megfelelő nemzetközi együttműködés nélkül, hiszen a kiber-bűncselekmények esetében hatványozottan könnyebb határon átnyúló módon megvalósítani a cselekményeket, akár a valós fizikai elmozdulás teljes nélkülözése mellett.

A jog és bűnüldözés eszközei mellett az általános digitális infrastruktúra fejlesztés is kiemelt terület a kiberbűnözés elleni harcban, hiszen a fertőzött hálózati eszközök és infrastruktúra segítségével a támadók sokkal könnyebben mozoghatnak észrevétlenül, és hatékonyabban tűntethetik el a nyomaikat. Így a felderítés esélyeinek növeléséhez egyértelműen fontos az országos hálózati infrastruktúrát a lehető legtisztábban, menedzselt és megfigyelhető módon kézben tartani a hatóságok számára.

A fő cél ebben az esetben a kiberbűnözés elleni küzdelem iránti elkötelezettség, ennek hivatalos deklarációja egyrészt a nemzeti stratégiában való megjelenítés által, másrészt a különböző kiberbűnözés ellenes nemzetközi szervezetekben való részvétel útján.

Ki kell alakítani a megfelelő jogszabályi környezetet, ami megteremti a kiberbűnözés üldözésének és visszaszorításának alapjait.

Szervezeti háttér:

- Ki kell alakítani a kiberbűnözés elleni osztályokat csoportokat minden hatósági szinten, megfelelő szakképzettségű specialisták alkalmazásával: bűnüldözés, ügyészség, bíróság, ügyvédek, törvényszéki szakértői-elemzői kör, terrorelhárítás, hírszerzés, stb.
- Szükséges egy magas szintű koordinációs szervezet felállítása, amely összefogja a fenti szereplők munkáját, illetve összekapcsolja a lokális szervezeteket a nemzetközi egyezményekben foglalt kötelezettségekkel, illetve a nemzetközi együttműködés alapján működő szervezetekkel.

Erőforrások:

- Megfelelő szakértelemmel bíró humán erőforrás alkalmazása a kritikus területen. Mivel ez a szakértelem legtöbbször az IT-iparban, a versenyszférában van meg, a globális munkaerőhiány miatt ennek komoly költségei lehetnek HR-oldalon.
- Meg kell határozni a kiberbűnözésből eredő éves veszteségeket (összegszerűen, GDP %-ában, stb.), ez alapján lehet a védekezésre fordított keretösszeget meghatározni, ebből a forrásból pedig a szakembereket, a technológiát és az infrastruktúrát finanszírozni.

Eredmény indikátorok:

- A nemzet joganyag modernizálása illetve kiegészítése azon esetekkel, tényállásokkal, amelyeket a korábbi jogszabályok egyáltalán nem kezelnek. Telekommunikációs jog, szerzői jogok, adatvédelem, elektronikus kereskedelem és szolgáltatások ezek a legfontosabb területek ezen a téren.
- A büntető törvénykönyv felkészítése a szerzői jog, digitális infrastruktúra, számítógépes rendszerek, támadása, megváltoztatása, elérhetetlenné tétele, stb. típusú jól definiált tényállásokkal és ezek hatékony szankcionálása.
- Demonstrálni a hatékony fellépést az állami infrastruktúra védelmén keresztül: csökkenteni a fertőzöttségi arányokat, gyorsan és hatékonyan reagálni az incidensekre, botnetek és kártékony kódok elleni programokat hirdetni és végrehajtani, mérhető csökkenést elérve ezeken a területeken.

2.4. Információ-megosztás

Mivel nemzetközi és szektor-, intézményközi problémáról van szó, egyértelmű, hogy az ismeret, a fenyegetések időben való felismerése az egyik kulcs momentum a védekezés területén. Az információ megosztó megoldások, amelyek lehetővé teszik a kormányközi, illetve az iparágon belüli és iparágak között kommunikációt a problémákról, kiemelten fontosak ahhoz, hogy a védekezés hatékony legyen. A fenyegetések beazonosítása, kockázati szintjük meghatározása, a célzott támadások mechanizmusainak feltárása és a védekezési lehetőségek bemutatása – a hatékony ellenlépések szempontjából elsődleges, hogy ezt ne kellejen minden megtámadott vagy potenciálisan veszélyeztetett szereplőnek újra és újra saját erőből elvégezni, hanem a felfedezés után ezek az információk közkinccsé váljanak, segítve a szakemberek munkáját a többi területen is, hozzájárulva ezzel a megelőzéshez.

A hagyományos információ megoldások a nemzeti CSIRT (Computer Security Incident Response Team) (ITU, 2015) és CERT (Computer Emergency Readiness Team) szervezetekhez (Kruidhof, 2014) kötődnek.

Összességében négy féle információ megosztó megoldás képzelhető el és van használatban a világ különböző nemzetgazdaságaiban:

- kormányzati működtetésű
- iparági működtetésű
- non-profit szervezet
- hibrid akadémiai-kormányzati-iparági együttműködés

Mindegyik megoldásnak megvannak a maga előnyei és hátrányai, mindazonáltal egyik sem lehet sikeres, ha az adott szervezet nem képes maga iránt megfelelő bizalmat kiépíteni, tiszta célokat és feladatokat kitűzni, ezeket átlátható módon megvalósítani és megfelelő módon kommunikálni. Definiálni kell a megosztandó információk minőségét, összetételét, formátumát, illetve a hozzáférésekre jogosultak körét. A lehető legszélesebb körű védelemhez ez utóbbinak célszerű minél kiterjedtebbnek lennie, sok ország követi el azt a hibát, főként az első, tisztán kormányzati működtetésű megoldások esetében, hogy túlzottan csak az államigazgatás, az intézmények belső igényeire fókuszál és figyelmen kívül hagyja, vagy második vonalba szorítja az üzleti szféra és a lakosság igényeit.

A minőségi, gyakorlati tanácsokkal, akciótervekkel kiegészített biztonsági, sérülékenységi információkhoz való valós idejű hozzáférés kulcsfontosságú a digitális fenyegetettségi szint csökkentésében.

A fő cél tehát egy állam és szektorközi információcsere hálózat felállítása, amely minőségi, strukturált és s gyakorlati információk továbbítására alkalmas.

Szervezeti háttér:

- A kormányközi információcseréhez megfelelő hatósági jogkörökkel ellátott szervezet felállítása szükséges, amely rendelkezik a szükséges felhatalmazással és szakértelemmel az érzékeny információk kezeléséhez és megosztásához.
- Egy olyan szervezeti struktúra kialakítása, amely hatékonyan képes több szektorral kommunikálni, rendelkezik azokkal a mechanizmusokkal (technológiák, szabványok, jelentési sztenderdek), amely az általa továbbított információkat könnyen felhasználhatóvá teszi a különböző piaci szereplők számára. Az információ áramlásnak kétirányúnak, valós idejűnek és megfelelően szakmainak kell lennie.
- Akadémiai és non-profit szervezetek és kezdeményezések támogatása, amely képes a hibrid modellben, a fenti szervezetek által ki nem töltött résekben is működni, az előzőek által le nem fedett ügyfélkört is elérni, egy magasabb tudományos és szakmai szintet képviselni és ezáltal a gyakorlati információk mellett a K+F szektornak is megfelelő inputokat szolgáltatni.

Erőforrások:

- A szervezet felállításához és működtetéséhez szakértő humán erőforrás, technológiai infrastruktúra szükséges. Az adatbázisok és riportok folyamatos elérhetőségét és bővítését frissítését kell megfelelő forrásokkal támogatni.

Eredmény indikátorok:

- Először is egy valóban gyakorlatban is hasznosítható szektorközi incidens monitoring és menedzsment funkció létrejötte, amely bizonyítottan, a részt vevő szervezetek tapasztalatai alapján is hasznos és használható információkat szolgáltat, amelyek segítségéve valóban, mérhető módon hatékonyabb a megelőzés, illetve az esetleges incidensek elhárítása.
- A kritikus információk államigazgatáson belüli eljuttatási képessége a megfelelő helyekre, ahol valóban hasznosítani fogják azokat, olyan struktúrában és formátumban, amely az adott érintettek számára kezelhető és könnyen feldolgozható.

2.5. K+F befektetések

A megfelelő IT-biztonsági felkészültség alapfeltétele, hogy az ország áldozzon az alap- és alkalmazott kutatásra a biztonsági területen. A digitális fejlődés mára minden szektort átalakított, ez az átalakulás pedig magával hozta a biztonsági kérdések előtérbe helyezését a növekedés és a fejlődés fenntartása érdekében.

Ezen a területen mind az államnak, mind az üzleti szférának megvan a szerepe, egymást kiegészítve tudnak valóban hatékony K+F támogatási rendszert létrehozni. Mobil internet, felhő szolgáltatások, big data, dolgok internete ezek mind olyan kulcs területek, ahol a széles körű elterjedéshez a bizalomépítésbe is fektetni kell, ehhez pedig a biztonságon keresztül vezet az út. Az Európai Unió H2020 programja például mintegy 80 milliárd EUR-t allokált technológiai K+F célokra. Ennek kiemelt területei a szektorral foglalkozó PhD-kutatások támogatása, az ipari technológiai fejlesztések és ezek menedzsmentjének megvalósítása, valamint a különböző szociális-gazdasági problémák technológiai fejlesztések útján történő megoldási lehetőségei, mindez nemzetközi, pán-európai együttműködésben megvalósítva. (European Commission, 2014) Az Egyesült Államok szintén sokat költ a terület kutatási programjaira, a Nemzeti IT K+F program mintegy évi 4 milliárd USD-ból gazdálkodik a 2016-2020 időszakban. (NITRD, 2015)

A kutatás-fejlesztés azonban nem elégséges, fontos, hogy az ötletek működő megoldások formájában öltsenek testet, ezt a különböző Innovációs alapok, inkubátor szervezetek segítik elő, mind piaci, mind állami környezetben.

A fő célok ezen a területen:

- Az állam és a vállalatok deklarált elköteleződése egy hatékony IT-biztonsági K+F rendszer létrehozására és fenntartására
- Nyilvános ösztönző mechanizmusok bevezetése (pl. adókedvezmények, fejlesztési támogatások) az IT-biztonság új vívmányinak (kutatások, technológiák, folyamatok, eszközök, stb.) támogatása érdekében
- Ösztönző mechanizmusok bevezetése az akadémiai szférában, az IT-biztonsági képzések, tudás létrehozás és megosztás és készségfejlesztés támogatása érdekében

Szervezeti háttér:

- Legalább egy szervezet létrehozása vagy kinevezése arra a feladatra, hogy koordinálja, összefogja, szervezze és menedzselje a nemzeti és nemzetközi K+F programokat és együttműködéseket
- Diplomás programok létrehozása felsőoktatási partnerekkel a terület oktatásának, tudásmegosztásának, szakember utánpótlásának megvalósítására.
- Az eredményeket gyűjtő, kutatásokat és visszaméréseket elvégző szervezet létrehozása, amely képes mérni és ezáltal visszajelzést adni az egyes programok hatékonyságáról, valamint a programok eredményeinek valódi gyakorlati alkalmazhatóságáról.

Erőforrások:

- Megfelelő anyagi és emberi erőforrás szükséges az új tudás létrehozásához, valamint a szakember utánpótlás oktatásához, kineveléséhez.
- Megfelelő anyagi és pénzügyi erőforrásokra van szükség a kutatási eredmények, alap technológiák valódi, gyakorlatban is használható termékekké, szolgáltatásokká való átalakításához.

Eredmény indikátorok:

- Kiírt és sikeresen végrehajtott programok, amelyek megfelelnek az elvárt tudományos, technikai és mérnöki standardoknak.
- Az állam bizonyított elkötelezettsége az alap és alkalmazott kutatási programok megvalósítása során finanszírozóként, illetve támogatóként.
- Az átjárás megteremtése az üzleti és az állami programok között. A gyakorlatias üzleti finanszírozású eredmények átültetése az állam működésébe, illetve az állami, akadémiai szféra eredményeinek hatékony transzfere az üzleti felhasználók irányába.

2.6. Diplomácia és külkereskedelem

Mivel határon átnyúló problémakörről van szó, teljesen természetes, hogy az IT-biztonsági kérdéseknek egy állam külpolitikájában is jelentős szerepet kell kapniuk. Nemzetközi szinten kell mindenki által elfogadható válaszokat keresni a közös problémákra. A kiberbiztonsági kérdések mára számos nemzetközi szinten is jelentős problémakörrel vannak szoros kölcsönhatásban, mint az emberi jogok, a gazdasági fejlődés, kereskedelmi egyezmények, többcélú katonai és polgári technológiák, biztonság, stabilitás, béke és konfliktuskezelés. Sok esetben nemzetközi konfliktusok, villongások, terrorizmus, háborús cselekmények is megjelenhetnek tisztán a digitális térben, amelyre a nemzetbiztonsági területeken kell megfelelő válaszokat adni. bár minden országnak vannak a fenti területeken szakdiplomatái, ők sokszor nem látják át ezeknek a területeknek, a digitális, informatikai vetületeit, ezért szükség van olyan szakértőkre, akik ebben segíteni tudnak.

Különböző szabadkereskedelmi egyezmények támogatják a digitális javak és szolgáltatások szabad áramlását. Az EU-USA között megkötött Biztonságos Kikötő (Safe Harbour) egyezmény (ITA, 2016) pedig az amerikai cégek adatkezelési, adatvédelmi gyakorlatát ismerte el európai szintűnek, noha alapvető különbségek vannak a két régióban az adatvédelmi elvek és szabályozások között. Az új Európai uniós Adatvédelmi direktíva létrehozásával pont ezt az egyezményt számolja fel az Európai Unió (Court of Justice of the European Union, 2015), ami szakértők szerint akár az európai GDP 1,3%-os csökkenését is eredményezheti, meggátolva, illetve megnehezítve a szabad és hatékony ügyfélkiszolgálást a nagy amerikai technológiai vállalatok (Google, Apple, Amazon, Facebook, stb.) számára. (AmCham, 2015) Ezzel együtt viszont az Európai Unió még erőteljesebben ragaszkodik a szigorúbb szabályozáshoz, a saját értékrendszeréhez és az állampolgárai európai normáknak megfelelő védelméhez, amely nem feltétlenül hátrányos a társadalom biztonságérzetére nézve.

A fő célok tehát ezen a területen:

- A kiberbiztonság deklarált szerepeltetése a külpolitika és a nemzetbiztonság alapvető összetevői között, megjelenítése magas szintű államközi, szakpolitikai tárgyalásokon.
- Az IKT és a biztonság deklarált megjelenítése a nemzetközi kereskedelem politikában, tárgyalásokban, és kereskedelemben.

Szervezeti háttér:

- Szakértő tanácsadói és diplomáciai személyzet alkalmazása a külügyben vagy ennek megfelelő szervezetekben, akik megbízása a kiberbiztonsági diplomácia folyatására is kiterjed

- A fenti kérdések súlyuknak megfelelő, legfelsőbb diplomáciai szinten való kezelése, és a kiberbiztonság kiemelése az elsődleges nemzeti diplomáciai célok között.

Források:

- A megfelelő anyagi és emberi erőforrások biztosítása a nemzetközi tárgyalásokkal, külügyi kérdésekkel foglalkozó szervezetek, valamint a diplomáciai testületek számára.

Eredmény indikátorok:

- Részvétel mindazon nemzetközi megállapodásokban, egyezményekben és együttműködésekben, amelyek a nemzetközi kiberbiztonság fenntartását, javítását és bővítését tűzték ki célul.
- A nemzetközi kereskedelmi tárgyalásokban az IT-biztonság, mint szerves szempontrendszer szerepeltetése. A biztonsági aspektusok nevesített megjelenítése az ország által kötött nemzetközi kereskedelemi, gazdaságfejlesztési egyezményekben.

2.7. Honvédelem és külső elhárítás

Az utolsó kérdés a nemzeti kibervédelemmel kapcsolatban, hogy a honvédelem, illetve az elhárítás intézményei képesek –e megvédeni az országot egy külső kibertámadástól, illetve megfelelően reagálni, kezelni az ilyen eseteket. Az országok közötti konfliktusok egyre hangsúlyosabban megjelennek a virtuális terekben is, a kibertámadások kiváló eszközt jelentenek az ellenség háttér országának gyengítésére, gazdasági és politikai destabilizálására, félelem keltésére, dezinformációk terjesztésére akár a lakosság, akár a gazdasági szereplők körében. A valódi támadást egyre többször előzi meg az ellenség előzetes „megpuhítása" a virtuális terekben.

Ahogy az államigazgatás, illetve az ipar, ezen belül a hadiipar, a biztonság kritikus iparágak és a kritikus infrastruktúrák, iparágak üzemeltetése is egyre jobban függővé válik a világhálótól a digitalizáció, és a távoli menedzsment, összekapcsolt rendszerek, felhő alapú megoldások jegyében, úgy válik egyre inkább felvonulási és támadási területté a kibertér.

A leg eklatánsabb példa erre a Stuxnet vírus, amelyet kifejezetten célzottan az iráni atomprogram ellen vetettek be 2010 során. Ipari létesítmények megfertőzésével komoly fizikai károkat okozott az urán dúsítására használt berendezésekben, a programot évekkel vetette vissza a támadás. (Horváth et. al., 2016)

Mára minden jelentősebb katonai hatalom, illetve szövetség kidolgozta a maga kiber hadviselési és elhárítási stratégiáját, háttéranyagait: USA, NATO, Kína, Oroszország, Dél-

Korea, Izrael – csak néhány fontosabb ország, amely komoly deklarált katonai és védelmi célú kiberstratégiával rendelkezik. (Hathaway et.al., 2015)

A fő célok ezen a területen:

- A katonai, honvédelmi szintű kibervédelemmel foglalkozó szervezet létrehozása és ennek nyilvános deklarációja
- A fenti szervezet számára magas szintű direktívák megalkotása arra nézve, hogy támadás esetén mik a jog- és felelősségi körei, milyen módon reagálhat a kiber-fenyegetésekre.
- Megfelelő jogköröket adni a fenti szervezetnek, hogy reagálási kapacitásokat hozzon létre az esetleges támadások ellen az ország területén belül és kívül egyaránt.

A szervezeti háttér:

- Egy országos szintű szervezet létrehozása a hadseregen belül, amely feladata a nemztet kibervédelme.
- Egy másik, országos szintű szervezet létrehozása a hadsereg kötelékén kívül, amely feladata a nemztet kibervédelme.

Erőforrások:

- Mind a hadsereg kötelékén belül, mind kívül, jellemzően a polgári titkosszolgálatok kötelékében működő szervezetek számára biztosítani kell a megfelelő szakértő humán erőforrást, illetve a működéshez szükséges anyagi és technológiai erőforrásokat.

Eredmény indikátorok:

- Kormányzati-szintű gyakorlatok tartása, amelyek mérik, és demonstrálják a nemzet kibervédelmi felkészültségét
- Országos-szintű gyakorlatok tartása, amelyek mérik, és demonstrálják a nemzet kibervédelmi felkészültségét
- Közös gyakorlatok tartása a szövetségesekkel, katonai védelmi szervezetekkel (pl. NATO), amelyek demonstrálják az együttműködési képességet és az információáramlást a hatékony kibervédelem kialakítása érdekében.
- A felelősségteljes kibertérben való tevékenységekre vonatkozó magatartási kódex kidolgozása, és azon beavatkozási küszöbök megállapítása, ahol a fenti kibervédelmi szervezetek már akcióba léphetnek.
- Gyors reagálású vészmegoldások és elhárítási mechanizmusok kidolgozása, amelyek a nemzeti CERT-hálózattól függetlenül működnek, és kritikus kibertámadások, incidensek esetén mozgósíthatók.

Összefoglalóan megállapítható, hogy nemzeti, nemzetgazdasági szinten egyetlen ország sem felel meg teljes körűen a fenti kritériumoknak. Ám a fenti szempontrendszer mentén jelentősen javítható egy ország IT-biztonsági felkészültsége, illetve a legjobb gyakorlatok, a maximális szint megismerése lehetőséget ad a forrás allokációnál, illetve a fejlesztési irányok meghatározásánál egy valóban átgondolt, tudatosan építkező biztonságfejlesztési stratégia, intézkedéssorozat megvalósítására.

3. Az informatikai biztonság helye a makro mutatókban

A fenti elemzésben főként az IKT, illetve az IT-biztonság GDP-re és gazdasági növekedésre gyakorolt hatásairól esett szó. Meg kell azonban vizsgálni, hogy a makrogazdasági számításokban figyelembe veszik-e egyáltalán a biztonságot és ezen belül az IT-biztonságot, mint összetevőt, ha ennyire szerves részét képezi a modern gazdaságoknak, illetve hogy összességében milyen hatást gyakorol a kiberbiztonság és az ide köthető incidensek az egyes makro mutatók alakulására.

A biztonság természetes emberi igény Maslow híres ötszintű piramisában (Maslow, 1943) a második szintet teljes egészében a biztonság különböző aspektusai foglalják el, mivel ma az emberek egyre több időt töltenek online, különböző virtuális terekben, az itt megtapasztalt biztonság, a kapcsolódó biztonságérzet szintén nagyon fontos szerepet játszik.

Elöljáróban kijelenthető, hogy nevesítve, közvetlenül egyetlen ma alkalmazott makrogazdasági mutató sem veszi figyelembe az informatikai biztonság gazdasági hatásait számításaiban, változóiban, ami a digitalizáció és az azzal járó kockázatok szerepét vizsgálva a gazdaságban, előre vetíti azt a problémát, hogy a gazdasági fejlődés az innováció jelenlegi húzóágazata jelenleg egyáltalán nem képviselteti magát ezekben a klasszikus mutató alapú nemzetközi összehasonlításokban. Természetesen ezzel megnehezíti, a biztonság, mint koncepció és hatásmechanizmus értő bemutatását és kezelését az alapvetően a fenti mutató mozgására alapuló gazdasági döntési mechanizmusokban, a gazdaság minden szintjén. A fentiekben a GDP-re ,illetve a gazdasági növekedésre gyakorolt közvetett hatásokkal már foglalkoztunk, ebben a fejezetben áttekintjük a fontosabb egyéb makro mutatókat és kapcsolatukat az IT-biztonság területével.

Az informatikai biztonságot, minta fentiekben is látható volt, lehet költség oldalról közelíteni, ez esetben általában a kiberbűnözés létezésén lapuló, az általa előidézet közvetlen és közvetett költségeket próbálják mérni. A nagy, biztonsággal foglalkozó szervezet kutató intézetek, minden évben megkísérlik megbecsülni a kiberbűnözés teljes költségét a világban.

Kutatások 2-3 billió dollár közé tették az internetes gazdaság teljes méretét 2015 folyamán, és a becslések azt mutatják, hogy ennek az összegnek a 15-20%-a (PWC, 2016), más becslések szerint kb. 450 mrd dollár vész el a kiberbűnözők tevékenységének következtében. (McAffee-CSIS, 2014)

Ezeket az összegeket már lehet a GDP-hez viszonyítani, illetve ezek a veszteségek a gazdasági növekedési mutatókra is kihathatnak összegszerűen. Sok mutató a GDP-ből indul ki, vagy a számításoknak részét képezi a GDP, ezek esetében természetesen a biztonsági incidensek, költések hatásainak GDP-re gyakorolt hatásai áttételesen hatást gyakorolnak a származtatott mutatókra is.

A GNI, vagyis a bruttó nemzeti jövedelem a második leggyakoribb mérőszám, szintén a GDP-ből eredeztethető. Mivel nem marad meg az országhatárokon belül, hanem foglalkozik a külföldre ki, illetve a külföldről beáramló jövedelmekkel is, itt a biztonság hatásait is szélesebb nemzetközi kontextusba lehet helyezni. A fenti költségek összevezetési módszere természetesen itt is működik, figyelembe kell venni azonban, hogy mivel maga a kiberbűnözés is egy erősen nemzetközi jelenség, egy-egy fontosabb, számos külföldi ügyféllel rendelkező célpont sikeres megtámadása jelentős nemzetközi pénzmozgást képes generálni és így közvetetten, főként negatív irányban módosítani a nemzeti jövedelmet.

A munkanélküliségre főként a fejlett országokban van negatív hatással az informatikai sérülékenységek kihasználásával foglalkozó szektor. A szellemi tulajdon lopása, ipari kémkedés ennek folyományaként pedig a másolás, a hamisítás, a védett technológiák, márkanevek és kereskedelemi utak felhasználása a fejlett országokban megszűnő munkahelyeket von maga után, hiszen az ellopott információk segítségével a jellemzően alacsonyabb általános munkaerő-költségekkel bíró, kelet-európai, ázsiai és afrikai helyszínekre áramlik a tudás és ezáltal a gyártási képesség is. Fent már látható volt, hogy számítások szerint a G20 országokban, mintegy 2,5 millió munkahely szűnt meg, vagy nem képesek feltölteni a fenti okok miatt. (Frontier Economics, 2011)

Az inflációra, vagyis az általános árszínvonal emelkedésre az IT-biztonság hatása meglehetősen direkt: minél erőteljesebb a fenyegetés, a cégeknek annál többet kell biztonsági kérdésekre költeniük, illetve az esetlegesen bekövetkező incidensekből eredő károk szintén a vállaltok, illetve az állami működés költségszintjét növelik, amelyet előbb-utóbb az árakban is érvényesíteni kell. Minél kritikusabb kérdés a kiberbiztonság, annál nagyobb hiány lesz a szükséges képességekkel rendelkező szakemberek piacán, ami szintén felfelé hajtja az árakat. Bizonyos szegmensekben tehát egyértelmű direkt hatása van a kiberbiztonsági incidenseknek az inflációra, de összességében is megjelenik ez az áttételes, felhajtó hatás.

A biztonság a direkt külföldi tőkebefektetés (FDI) esetében sem része a számításoknak közvetlen módon, viszont jelentős hatással van rá, hiszen a vállalatok a nemzetközi terjeszkedés megtervezésekor gondosan mérlegelik és optimalizálják a kockázatokat, mielőtt kiválasztják a megfelelő célpontot. Az FDI nagyon fontos tényező egy ország egyensúlyának fenntartásában, különösen a kisebb, nyitott gazdaságokban. Természetesen a külföldi vállalatok is nagy hangsúlyt helyeznek arra, hogy védve legyenek egyrészt a hamisítástól, ipari kémkedéstől, másrészt pedig biztonságban tudhassák a saját és ügyfeleik adatait. Egy olyan gazdaság tőkevonzó képessége tehát, ahol a biztonságos körülmények nem csak a társadalmi-politikai, de az informatikai szinten is fennállnak, ahol erős a szerzői és az iparjogvédelem, ceteris paribus biztosan jobb az ezeket a feltételeket nem, vagy csak hiányosan teljesítő versenytársainál. (Bath, 2012)

A standard makromutatók mellett következzen néhány alternatív megoldás:

A Happy Planet Index (HPI) az egyik új felkapott mutatószám, ami teljesen más oldalról próbálja megközelíteni egy ország teljesítményét, még pedig azon keresztül, hogy mekkora boldogsági szintet képes biztosítani a lakosainak, már ha elfogadjuk, hogy a boldogság egzakt módon mérhető. A mutató összetevői között megtaláljuk a várható élettartamot, a tapasztalt jóllétet, az egyenlőtlenségek nagyságát, illetve az ezzel járó ökológiai lábnyom nagyságát. A fentiek közül a kiberbiztonság a tapasztalt jóllét kategóriáját képes befolyásolni, a biztonságérzet, adataink, magánszféránk, vagyonunk biztonsága és sérthetetlensége nagyban befolyásolja, hogy jó érzéssel vagyunk –e képesek létezni ebben a környezetben, nyugodtan használni a technológiát és a szolgáltatásokat.

1995-ben az Egyesült Államokban a Redifining Progress kutatócsoport (C. Cobb–T. Halstead–J. Rowe) GPI (Genuine Progress Indicator GPI), vagyis valódi fejlődés mutató néven publikálta legújabb kutatási eredményeit. 2004-ben pedig a Sustainability Indicators Program keretében ismertették legújabb jelentésüket. (Szlávik, 2007) A mutató a GDP-ből indul ki, amit számos tényezővel korrigál, többek között a bűnözés közvetlen negatív, költségnövelő hatásával is. Bár a mutató nem beszél kifejezetten az informatikai bűnözésről, de mivel ez is egy alcsoport, itt majdnem közvetlenül és nevesítve szerepelnek a kiber bűncselekmények társadalmi költségei, együttesen persze a bázisként szolgáló GDP-re történt módosító hatásaival.

Látható tehát, hogy a biztonság, mint természetes emberi igény, és az üzletmenet, illetve a nemzetbiztonság szempontjából fontos tényező, valamilyen áttételes módon szinte mindenhol kap szerepet. Direkt módon viszont, bármennyire is a digitális fejlődés jelenleg a gazdasági növekedés és az innováció motorja, nem jelenik meg a makrogazdaság elemzésekor. Ennek viszont szükséges lesz megváltoznia, hiszen a felvázolt fejlődési pálya természetes módon hozza magával ezeket a kockázatokat, az egyre kiterjedtebb felhasználás, egyre többet. Az iparról és a szolgáltatási szektorról már más helyen is

kijelentettük, hogy előre menekül a technológiai fejlődésbe, és a járulékos, kiegészítő területekről, mint a biztonság, gyakran megfeledkezik. Az elemzők és a közgazdászok viszont jó lenne, ha nem követnék el ezt a hibát és felismernék, hogy a jövő növekedési és jövedelemtermelési lehetőségei szempontjából egy új, kritikus területtel nézünk szembe.

4. Mikroszintű GDP elemek

A vállaltokat méret szerint csoportosítva vizsgáltuk, ugyanis a nagyobb anyagi erőforrásokkal rendelkező társas vállalkozások alapvető eltéréseket mutatnak az egyéni, vagy néhány főt foglalkoztató szektortól, ahol sok esetben inkább a lakossági szektorral való hasonlatosság tűnik ki, mind az informatikai eszközök felhasználási szokásaiban, mind pedig a szakértő karbantartás hiányában és a védelmi megoldások alkalmazásában.

A vállalati szférában, bár a biztonságtudatosság és a biztonsági eszközök használata jóval elterjedtebb, szintén komoly kockázatok rejlenek, hiszen itt is széles körben alkalmazzák a legkritikusabb sérülékenységeket hordozó szoftvereket, operációs rendszerként, a napi irodai munkához és a vállalat legfontosabb vagyonát jelentő adatbázisok kezelésére is.

A vállalati biztonsági politikák nem egyenszilárdságú alkalmazása, a védelmi eszközök alkalmazásának túlsúlya az integrált, és sokszor egyszerűbb, szervezési intézkedéssel szemben, nemzetgazdasági szintű kitettséget jelent, veszélyezteti a vállalati szektor működését és adatainak bizalmasságát, integritását.

Az utóbbi évek során, ahogy a vállalatok mind több kritikus üzleti folyamat támogatására alkalmaznak különböző informatikai megoldásokat, mind nagyobb adatvagyonnal gazdálkodnak, a rendszerekkel szembeni kitettségük is fokozódott. Így még abban az esetben is nagyobb kockázattal néznének szembe, ha mindeközben az IT-biztonsági fenyegetések nem nőttek volna.

A mobilitás iránti igény erősödése és a hordozható eszközök terjedése szintén növeli a kockázatokat. A notebookok, amelyek a tolvajok kedvelt célpontjának számítanak, a vállalati pc-állomány mind nagyobb hányadát adják. Megfelelő óvintézkedések nélkül egy ingzsebben elférő pendrive-on vagy egy mobiltelefon memóriájában ma több adatot lehet szinte észrevétlenül kicsempészni a vállalattól, mint amennyit egy évtizeddel ezelőtt egy közepes méretű cég fájlszerverein összesen tároltak. (Horváth, 2011b)

Az informatikai biztonság kérdése messze túlmutat a sebezhetőséget csökkentő szoftver- és hardverkomponenseken. Több azoknál. Stratégiai szemléletben előkészített terven alapuló döntések sorozata, rendszeresen felülvizsgált és következetesen betartatott szabályok összessége, amelyek megvalósítási eszközei között találunk hardver- és szoftvereszközöket is.

A biztonsági incidensek gazdasági hatásinak kutatásában a Sagesecure kutatóintézet elemzéséből indultunk ki, amely elemezte a biztonsági incidensekből fakadó leállások nagyságát. Ezt vetettük össze a KSH adataiból (KSH 2015, KSH 2016) származó, számításokkal, amelyek segítségével a kiesett idő értékét próbáltuk meghatározni. Számításaink alapja a munkaidő értéke, vagyis, egységnyi időre jutó GDP-termelő képesség volt.

A Sagesecure (Sonnenreich, 2006) kutatásai szerint a különböző biztonsági incidensekből fakadó problémák naponta akár 240 percnyi hasznos munkaidő kihasználhatóságát korlátozzák, vagy teszik teljesen lehetetlenné a vállalati szférában.(1. táblázat.) Ez az idő látszólagosan rövid, 10-15 perces kiesésekből áll össze és a különböző kártékony programokkal (vírus spyware, keylogger, féreg, stb.), konkrét támadásokkal kapcsolatos események mellett leginkább az ezek ellen való szakszerűtlen és átgondolatlan védekezési megoldások okoznak kiesést.

1. táblázat. A biztonsági intézkedésekből fakadó problémák okozta időkiesés

Probléma	Átlagos időveszteség (perc)
Alkalmazáshoz és rendszerhez kötődő leállások	10
Email szűrés és SPAM	15
Sávszélesség hatékony kihasználása. Áteresztőképesség	10
Nem hatékony és hatástalan biztonsági politikák	10
Biztonsági politikák szigorúsága	10
Rendszerhez kötődő kiesések és frissítések az IT részéről	10
OS és alkalmazások biztonsági javításai	10
Nem biztonságos és nem hatékony hálózati topológia	15
Vírusok, vírus ellenőrzés	10
Férgek	10
Trójai, keylogger	10
Kémprogramok	10
Felugró hirdetések	10
Kompatibilitási problémák	15
Engedély alapú biztonsági problémák (felhasználónév/jelszó)	15
Fájlrendszer rendezetlensége	10
Sérült vagy elérhetetlen adatok	15
Rendszerinformációk és adatok illetéktelen elérése vagy eltulajdonítása	15
Biztonsági mentések visszaállítása	15
Alkalmazás használati problémák	15
Teljes idő	240

Forrás: Sagesecure (Sonnenreich, 2006)

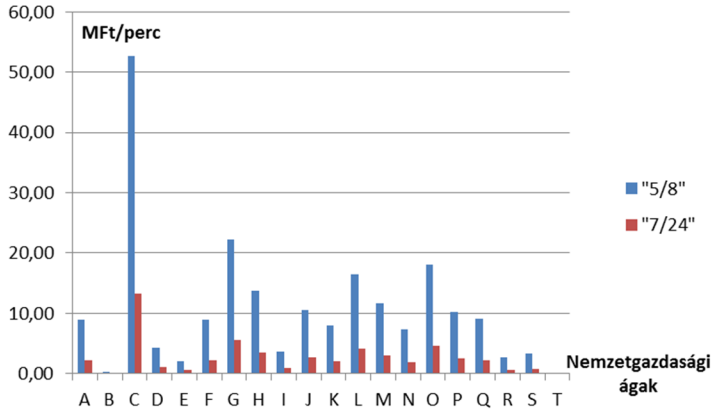
Gyakori az üzemidőben futtatott teljes biztonsági ellenőrzés, amely kapacitás kieséseket okoz, a rosszul menedzselt sávszélesség és hálózati topológiák, a frissítések és biztonsági patchek munkaidőben való telepítése, valamint az ezekből gyakran adódó kompatibilitási problémák megoldása. Látható, hogy a hatékony és jól végrehajtott biztonsági politika mennyire fontos, hiszen a nem kellően szervezett védekezés legalább akkora kieséseket tud okozni, mint a valódi támadások. A fenti 240-ből 100 percnyi kiesés teljes egészében az IT-biztonsági politika végrehajtásának tudható be. (Horváth, 2011a) Ide sorolhatók egyébként

a túlbonyolított, túl szigorú biztonsági ellenőrzési, jogosultsági és beléptetési rutinok is, amelyek rendszerhasználati nehézségekhez vezetnek az alkalmazottak körében.

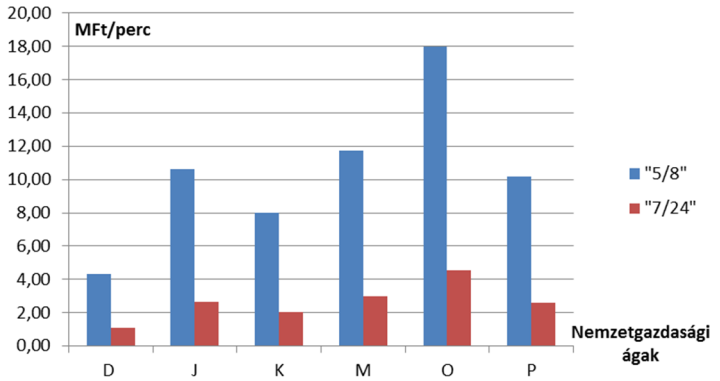
A KSH adatok alapján (KSH, 2016) az egy percre jutó kiesett GDP illetve bruttó hozzáadott érték nagysága jelentősen szór a leginformatika-intenzívebb iparágakban, mint amilyen a közigazgatás, a pénzügyi, biztosítási tevékenység, az informatika, kommunikáció, az oktatás vagy az energetikai ipar.

A pontos érték megállapítása nem egyszerű. Tekintettel arra, hogy a GDP és a bruttó hozzáadott érték közötti különbséget jelentő termékadók és támogatások egyenlege iparáganként megoszlása nem állt rendelkezésre, így az alább közölt adatok a bruttó hozzáadott értékre vonatkoznak. Az egy percre jutó kiesett érték számításánál két elméleti határesetet használtunk az éves 8760 óra arányosításánál. Az „5/8" heti 5 napos munkahéttel és munkanapi 8,5 órás munkaidővel számolva, illetve a „7/24" heti 7 napos munkahéttel és három műszakos folyamatos munkavégzéssel számolva. Ugyanakkor tény, hogy vannak 7/24-es rendelkezésre állású szolgáltatások, mint például az internetes rendszerek, a közigazgatás, a rendfenntartás és védelem alaprendszerei, ugyanakkor a napközbeni irodai, ügyfélszolgálati munkavégzés, az ügyfelek szokásai stb. napi, heti és éves ciklusokban változnak, azaz egyes időszakokban bizonyos szolgáltatások rendelkezésre nem állása eltérő hozzáadott érték kiesést eredményezhet. Emiatt megállapítható, hogy a vizsgált iparágakban a tényleges kiesés e kettő között van valahol, ennek pontosítása további kutatásokat igényel.

Fentiek figyelembevételével az informatikai szolgáltatások kieséséből származó, egy kiesés percre jutó veszteség – részben az adott iparág teljesítményétől, részben a számítási módszertől függően – 1,1–4,5 illetve 4,3–18 millió forint között szór, azaz átlagosan 2,8 és 11 millió Ft között van. (1. és 2. ábra.) Ezek az ágazatok az átlagnál valamivel magasabb munkaerő költségekkel is bírnak, így a kiesések hatásai még súlyosabbak. Pozitív irányba korrigálja az összefüggéseket a pótlás és az IT-biztonsági, különösen a backup megoldások megléte, bár a Sagesecure kutatói ezt többnyire már figyelembe vették.



1. ábra. Az egy percre jutó kiesett bruttó hozzáadott érték nagysága a nemzetgazdasági ágakban. A nemzetgazdasági ágak jelölése az ábrákon: A Mezőgazdaság, erdőgazdálkodás, halászat; B Bányászat, kőfejtés; C Feldolgozóipar; D Villamosenergia-, gáz-, gőzellátás, légkondicionálás; E Vízellátás; szennyvíz gyűjtése, kezelése, hulladékgazdálkodás, szennyeződésmentesítés; F Építőipar; G Kereskedelem, gépjárműjavítás; H Szállítás, raktározás; I Szálláshely-szolgáltatás, vendéglátás; J Információ, kommunikáció; K Pénzügyi, biztosítási tevékenység; L Ingatlanügyletek; M Szakmai, tudományos, műszaki tevékenység; N Adminisztratív és szolgáltatást támogató tevékenység; O Közigazgatás, védelem; kötelező társadalombiztosítás; P Oktatás; Q Humán-egészségügyi, szociális ellátás; R Művészet, szórakoztatás, szabad idő; S Egyéb szolgáltatás; T Háztartások tevékenysége. (KSH, 2016)



2. ábra. Az egy percre jutó kiesett bruttó hozzáadott érték nagysága néhány informatika intenzív nemzetgazdasági ágban

5. Következtetések

Megállapítható tehát, hogy a vállalati hatékonyság mindenképpen romlik, és az iparági adatokból, valamint az 1. táblázat statisztikáiból kiindulva kijelenthető, hogy naponta akár 100 millió Ft-os nagyságrendű bruttó hozzáadott érték, illetve GDP csökkenéssel lehet számolni egy informatikailag nem kellőképpen felkészült nagyobb szervezet esetén. Mindemellett nem feledkezhetünk meg az áttételes hatásokról sem. Főként a közhivatalok és az államigazgatási rendszerek esetében, az informatikai rendszerek kiesése nem pusztán a munkavégzés elmaradása vagy lassulása a probléma, hanem az ügyfélkiszolgálás lassulása/kimaradása miatt a nemzetgazdaság többi részéből is elvonja a munkára fordítható időt, illetve felesleges leállást, várakozásokat generál, ami többlet munkabér kifizetéssel, a felmerülő többlet folyó költségekkel, a szerződéses határidők nem teljesítéséből fakadó kötbér és egyéb terhek megjelenésével továbbgyűrűző veszteségeket okoz. Ez pedig visszahat a GDP további csökkenésére.

Látható tehát, hogy bármelyik szintről is indulunk ki, a digitális korszakban az informatikai problémák, sérülékenységek, biztonsági incidensek a gazdaság minden szintjén kezelést igényelnek, hiszen jelentős lokális és ezeken a lokális hatásokon keresztül persze globális veszteségeket okozhatnak, amelyek befolyásolják a jövedelemtermelő képességet, a versenyképességet és az általános gazdasági fejlődést, ezáltal pedig jelentős szerepük van a nemzetgazdaságok működőképességének alakításban.

Köszönetnyilvánítás

Jelen tanulmány elkészítését a PD-109740 számú „IT és hálózati sérülékenységek tovagyűrűző társadalmi-gazdasági hatásai” című projekt támogatta a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal – NKFIH finanszírozásával.

Irodalomjegyzék

[1] American Chamber of Commerce (AmCham), 2015: "EU Courts of Justice's decision in the Schrems case could disrupt transatlantic business, hurt the EU economy and jeapordise a Digital Single Market," Press Release, 6 October 2015, http://www.amchameu.eu/sites/default/fles/press_releases/press_-_ecj_decision_on_schrems_will_disrupt_transatlantic_business.pdf

[2] Bath, Vivienne 2012: Foreign Investment, the National Interest and National Security - Foreign Direct Investment in Australia and China, Sydney Law School, Legal Studies Research Paper No. 12/31, 2012. április, http://poseidon01.ssrn.com/delivery.php?ID=412117110095126119126068065102012011022024001018005001005071087094009018071073082025052011123123001038027091097113108088112066041023045020021083069067082079012065008011009009069121011126116010028070030125025125070080110119097096074073012012010125090&EXT=pdf

[3] Court of Justice of the European Union, 2015: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, Press Release 117/15 (6 October 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[4] Dean, David et al., 2012: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy, Boston Consulting Group report (January 2012): 2.

[5] European Commission, 2014: ICT Research & Innovation," Horizon 2020: The EU Framework Programme for Research and Innovation, http://ec.europa.eu/programmes/horizon2020/en/area/ict-research-innovation

[6] European Commission, 2015b: Digital Single Market: Bringing down the barriers to unlock online opportunities, http://ec.europa.eu/priorities/digital-single-market/.

[7] Evans, Peter C. - Annunziata, Marco 2012: Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric (26 November 2012): 13.

[8] Frontier Economics London, 2011: Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy, (London, Frontier Economics Ltd, 2011): 47.

[9] Government of India, 2015: Programme Pillars, Digital India: Power to Empower, http://www.digitalindia.gov. in/content/programme-pillars.

[10] Hathaway, Melissa – Spidalieri Francesca, 2015: Sustainable and Secure Development: A Framework for Resilient Connected Societies, in Observatory of Cyber Security in Latin America and the Caribbean http://belfercenter.hks.harvard.edu/files/oas-resilient-connected-societies.pdf

[11] Hathaway, Melissa 2014a: Cyber Readiness Index 2.0 & Lessons Learned in the Design of national Cyber Security Strategies, (presentation at the OAS-IDB Regional Workshop on Cyber Security Policies, Washington D.C., 23 October 2014).

[12] Hathaway, Melissa 2014b: Connected Choices: How the Internet Is Challenging Sovereign Decisions, American Foreign Policy Interests 36, no. 5 (November 2014): 301.

[13] Hathaway, Melissa et al., 2015: CYBER READINESS INDEX 2.0, Potomac Institute for Policy Studies, http://www.potomacinstitute.org/images/CyberReadinessIndex2.0.pdf

[14] Horváth, Attila Dr. – Erdősi, Péter Máté – Kiss, Ferenc Dr., 2016: A szoftver sérülékenységek kihasználási módozatai – Informatikai támadások, támadók és biztonság 2013-2016. In: Horváth Attila – Kiss Ferenc (ed.): IT és hálózati sérülékenységek társadalmi-gazdasági hatásai, ISBN 978-615-80061-5-6, Információs Társadalomért Alapítvány, Komlóska.

[15] Horváth, Attila Dr. –Kiss, Ferenc Dr. –Szanyi, István –Török, Marianna, 2015: Modern ICT technologies – situation and trends, In: Ferenc Kiss (ed.): Tourism and ICT Aspects of Balkan Wellbeing - A Balkán Jóllét Turisztikai és IKT Vonatkozásai, 155-186. old., ISBN 978-615-80061-2-5, Információs Társadalomért Alapítvány, Komlóska.

[16] Horváth, Attila Dr., 2011a: IT és hálózati sérülékenységek tovagyűrűző hatásai a gazdaságban, NETWORKSHOP 2011. konferencia, Kaposvári Egyetem, 2011. április 27-29.

[17] Horváth, Attila Dr., 2011b: Informatikai sérülékenységek és kockázatok – a társadalmi-gazdasági hatások tükrében (A második év eredményei), 8. Országos Gazdaság-informatikai Konferencia OGIK'2011, Szent István Egyetem, Győr, 2011. november 11-12..

[18] International Trade Administration (ITA), 2016: Welcome to the U.S.-EU Safe Harbor, http://2016.export.gov/safeharbor/

[19] IT Governance Institute, 2008: Enterpride Value: Governanceof IT investments - The Val IT Framework 2.0, IT Governance Institute, Rolling Meadows. IL 60008 USA, http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT 1.aspx

[20] Kruidhof, Olaf, 2014: Evolution of National and Corporate CERTs – Trust, the Key Factor, in Best Practices in Computer Network Defense: Incident Detection and Response, ed. Melissa E. Hathaway, (Amsterdam: NATO Science for Peace and Security Series, IOS Press, February 2014).

[21] KSH, 2015: Adattáblák az egyes nemzetgazdasági ágak jövedelemtermelő képességéről, és az IT-eszközök használatáról regionális bontásban; www.ksh.hu 2015.

[22] KSH, 2016: 3.1.4. A bruttó hozzáadott érték értéke és megoszlása nemzetgazdasági áganként – ESA2010 (1995–) http://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_qpt002c.html

[23] Maslow, A.H.,1943:"A theory of human motivation".Psychological Review. 50 (4): 370–96. , http://psychclassics.yorku.ca/Maslow/motivation.htm

[24] McAffee-CSIS, 2014: Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies (CSIS) – McAffee Inc. – Intel Security http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[25] NITRD, 2015: The Networking and Information Technology and Research Development Program, Supplement to the President's Budget FY 2016 (February 2015), https://www.whitehouse.gov/sites/default/fles/microsites/ostp/fy2016nitrdsupplement-fnal.pdf

[26] PWC, 2016: The Global State of Information Security® Survey 2016, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

[27] Sonnenreich, Wes, 2006: *Return On Security Investment (ROSI): A Practical Quantitative Model,* Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006

[28] State Council of China, 2015: Internet Plus, Guo Fa 40 (2015). Translated by U.S. State Department.

[29] Szlávik J. (szerk.) 2007: Környezetgazdaságtan. BME GTK Közgazdaság-tudományok Intézet, Typotex Kiadó, Budapest.

[30] The International Telecommunications Union (ITU), 2015: CIRT Programme, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx.

[31] The National Bureau of Asian Research, 2013: The IP Commission Report: The report of the commission on the theft of American intellectual property, National Bureau of Asian Research 2013. május, http://www.ipcommission.org/report/ip_commission_report_052213.pdf

[32] Várhalmi A. Miklós, 2008: *Az infokommunikációs közművek biztonsági kockázatai és az információs hadviselés*, „Társadalom és gazdaság – új trendek és kihívások" c. tudományos konferencia, Baja, www.varhalmi.hu/cucc/361433.rtf; 2010.okt.

[33] World Bank, 2014: Overview, Information & Communication Technologies Program, last modifed 2 October 2014,http:// worldbank.org/en/topic/ict/overview.