HADMÉRNÖK

VIII. Évfolyam 4. szám - 2013. december

Som Zoltán
som.zoltan.kdi@office.uni-nke.hu

A KÖZIGAZGATÁSI INFORMATIKAI FELELŐSÖK OKTATÁSÁNAK KÉRDÉSEI

Absztrakt

Cikkem aktualitását a 2013. évi L. törvény adja [1]. A témakört hármas tagolásban kívánom megvizsgálni jelezve, hogy, hogy az informatikai biztonságnak és az informatikai felelősök oktatásának szervesen összefüggő témakörének csak egy meghatározott szeletét, az állami és önkormányzati szektorra vonatkozó aspektust tárgyalom alaposabban. Elsőként az informatikai biztonság és incidensek keletkezését, körülményeit és következményeit részletezem. Az informatikai biztonság fontosságát áttekintve, ezt követően az aktuális magyar helyzetet és törvényt vonatkozásait mutatom be. Áttekintem és javaslatot fogalmazok meg arra, hogy a megoldáskeresés során milyen lépéseket érdemes tenni, az egyes azonosított célcsoportokat hogyan érdemes megszólítani, illetve hogy ezen kihívásokra milyen lehetséges választ tudunk adni ma Magyarországon.

The actuality of my article is given by the L. law, 2013. I would like to examine the topic in a three-way split, indicating that I am showing the security of IT and the training of its leaders from the aspect of state and local government. First, the appearance of IT security and incidents, their circumstances and consequences. After reviewing the importance of IT security, I will present the actual Hungarian status from the respect of the law. By this review of mine I can show some paths of solutions, like 'best practice' solutions for raising IT security levels, and creating them. I will review and give suggestions about what kind of steps should be taken during the search for solutions and how to address target groups, then to what answers we can give to these challenges in Hungary today.

Kulcsszavak: *2013 évi L. törvény, informatikai, állami és önkormányzati szervezetek, kibervédelem, informatikai felelősök, informatikai biztonság ~ 2013, law L. information technology, state and local government organizations, cyber defense, IT leaders, IT security*

BEVEZETÉS

Napjaink szinte minden területét átszövi az informatika, és ez igaz a magán- és állami szektorra egyaránt. Könyvtárakat lehet megtölteni a témával foglalkozó tanulmányokkal hazai és nemzetközi szinten értelmezve egyaránt. Bár napjainkra természetessé vált az informatikai eszközök nyújtotta segítség használata, érdemes egy gondolatkísérletet végeznünk, egy nap vagy egy hét távlatában vizsgálva milyen szolgáltatásokat veszünk igénybe és milyen formában. Azért emelem ki a szolgáltatások formáját, mivel a már meglévő szolgáltatások is olyan folyamatos fejlődésen mennek át minden egyes szektorban, amely a költséghatékonyság jegyében jellemzően infokommunikációs eszközök igénybevételével történik. A teljesség igénye nélkül soroljunk fel néhány olyan példát, amelyet az emberek többsége igénybe szokott venni: közműszolgáltatások és távszámlák, banki ügyintézés, vagy az önkormányzati, állampolgári, adózási ügyeink intézése, egészségügyi adataink kezelése a háziorvosnál vagy a kórházban, vagy egy recept kiváltása. Elektronikusan tároljuk és kezeljük adatainkat. Ezen szolgáltatások kapcsán jellemző törekvés, hogy valamilyen elektronikus hozzáférést is biztosítva legyen az ügyfelek, állampolgárok számára. A költséghatékonyság pedig úgy jelenik meg, hogy csökken a papírfelhasználás, a call-centerekbe kevesebb hívás fut be (kevesebb hívást kell rögzíteni és tárolni), kevesebb ügyfél veszi igénybe a személyes ügyfélszolgálatot stb. Mindemellett egyes helyeken már kifejezett törekvés a személyes ügyfélszolgálat visszaszorítása. Ezen szervezeteknek és az adatgazdáknak elemi érdeke, hogy ezen adatokat biztonságban tudja, biztonságosan tudja kezelni, a szervezet reputációját megóvja [2]. Figyelembe véve azt a tényt, hogy a szoftver és hardver környezet folyamatosan változik, kiegészítve azzal, hogy a felhasználói elvárások is egyre magasabbak, kijelenthetjük, hogy valóban folyamatos kihívást jelent az informatikai biztonság megteremtése és fenntartása [3]. A 2013 évi L. törvény és végrehajtási rendeletei az állam és polgárai szempontjából fontos elektronikus információs rendszerek (informatikai rendszerek) védelemhez szükséges alapvető intézkedéseket határozza meg. Kérdés, hogy a törvényi szabályozásokat a jogalanyok milyen módon lesznek képesek átültetni a gyakorlatba, és hogy hogyan fogadja majd ezt a szakma. Hiszen minden ajánlásnak, eljárásnak, törvénynek vagy képzésnek stb. akkora jelentőse, mint amennyi a tényleges gyakorlatba beépül, haszna is ebben mutatkozik meg. „A hatékonyság és a gyorsaság, összességében pedig a gazdaságosság szempontjából a különböző rendeltetésű szervezetek egyike sem engedheti meg magának, hogy ne csatlakozzon az Internethez, élvezze annak előnyeit, azonban az előnyök mellett számos kockázat is felmerülhet.” [4]

AZ INFORMATIKAI BIZTONSÁGI RÉSEK KELETKEZÉSE

Hogyan, mikor és miért keletkezhetnek biztonsági rések? Teljesen biztonságos rendszer nem létezik, viszont a kockázat csökkentésére számos lehetőség van. Ezek közül az oktatásban és a folyamatos fejlesztésben rejlőket mutatom be saját tapasztalataim alapján. Bár mindenfajta elővigyázatosság mellett sem tudjuk megakadályozni a biztonsági rések keletkezését, az is igaz, hogy az informatikai rendszerrel kapcsolatos követelmények is növekednek, változnak. Ez igaz a szoftver és hardver összetevőkre a felhasználói elvárásokra is [5].

Az elektronikus közigazgatás teret hódít és ennek a térhódításnak következtében folyamatosan új elvárások fogalmazódnak meg az informatikai fejlesztés és üzemeltetés irányába. „A cél színvonalas, felhasználóbarát és biztonságos elektronikus szolgáltatások nyújtása a társadalom egésze számára. A követelmények megfogalmazása és teljesítése széles körű együttműködést igényel.” [5]

A szoftver életciklusok és fejlesztési ciklusok a határidős nyomás következtében rövidülnek. Kevesebb idő és kevesebb pénzügyi forrás áll rendelkezésre a fejlesztésre és a tesztelésre egyaránt. Másrészről pedig ezen fokozott tempó következtében a kiszolgáló személyzet is

kevésbé képzett, több lehetséges hiba marad(hat) az éles rendszerekben, amelyek adandó alkalommal támadási felületként szolgálnak. Ezen hibákat többféle motivációból hajtva lehet kihasználni. Ezek jellemzően a rombolás, tekintélyszerzés, további támadás előkészítése vagy az anyagi haszonszerzés, kémkedés. [6]

Az informatikai támadások kivédésére minden szervezet alkalmaz valamilyen védelmet. Erre a bank- és pénzügyi szektorban jellemzően nagyobb forrásokat tudnak fordítani, míg a privát szektorban egy kisvállalkozás nagyságrendekkel kevesebbet. Joggal vetődik fel a kérdés, hogy mi a helyzet az állami szektorban, ahol az állampolgárok szinten minden adata tárolva van digitális formátumban.

A bankszektor esetében létezik olyan nemzetközi sztenderdnek tekinthető ajánlás, amely segítséget ad az informatikai folyamatok kialakítására (COBIT, ITIL, ISO27001), ilyen és hasonló ajánlások más iparági szektorokban is megtalálhatóak. Ellenben jelenleg az állami és önkormányzati szervek esetében idáig nem volt egy olyan naprakész, egységes előírás, amely sorvezetőként vagy alapként szolgálhatna az egyes szervezetek életében. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának 12. sz. ajánlása [7] 1996-ból nagyon komoly alapokat fektetett le, de a gyors technikai változások ezen ajánlások frissítését tették szükségessé, így született meg a Közigazgatási Informatikai Bizottság 25. ajánlása a Magyar Informatikai Biztonsági Ajánlások (MIBIK, [8] IBIR, [9] IBIK, [10] IBIV, [11] MIBÉTS, [12] IBIX[1] [13]). Ennek a folyamatnak a folytatása a 2013 évi L. törvény, definiálja az új informatikai fogalmakat is.

Ahogyan az állami szolgáltatások egyre inkább digitalizálódnak, úgy ezen helyeken egyre fokozottabban kell figyelni az informatikai biztonságra. Azonban az informatikai biztonság nem egy állapot, amelyet ha elérünk, akkor befejeztük a munkát és nyugodtan hátradőlhetünk. Ez a megfontolás határozza meg bármilyen ajánlásnak a gyökerét. Hiszen ezen ajánlásokat, vizsgákat, biztonsági rendszereket és szoftvereket, beszállítókat, egyszóval mindent, ami az informatikának összetevője és komponense lehet, bizonyos időnként felül kell vizsgálni, frissíteni kell. És vajon mi az informatikai biztonság legsebezhetőbb pontja? Ez a pont az ember, a felhasználó, de még a szakértő, az informatikai vezető, sőt az informatikai biztonságért felelős szakember is ide tartozik. Hiszen bármely rendszer csak annyira erős, mint amennyire a leggyengébb eleme. Ha ez az elem egy képzetlen felhasználó vagy óvatlan informatikus, akkor a legdrágább és legfrissebb védelmi megoldások komplex rendszerének biztonsági szintje is konvergál ezen leggyengébb összetevő biztonsági szintjéhez. Az Egységes Kormányzati Gerinchálózat (EKG) számos előnyös és kiaknázható tulajdonsággal bír. Nagyobb biztonság érhető el ezen a viszonylag zárt hálózaton, valamint az EKG előnye az is, hogy a felhalmozódó adat és tapasztalat birtokában forgalmi statisztikák és anomáliák alapján könnyebben kimutatható a normálistól való eltérés [14].

És hogy miért is történnek informatikai, biztonsági incidensek? A romboláson kívül, a gazdasági és anyagi haszonszerzés, erődemonstrálás és számos egyéb motivációja lehet. Sokkal költséghatékonyabb, nehezebben lenyomozható és még nehezebben bizonyítható, hogy pontosan mi is történt, hiszen maga a bizonyíték is digitális és hamisítható, eltüntethető. Számos nemzetközi példa azt mutatja, hogy a nagyhatalmak is előszeretettel használják ezeket az eszközöket. Például az USA héber nyelvű weblapot tart fenn az Iráni atomprogram szoftveres tönkretételére, de legalábbis hátráltatására. Ezen megoldások olcsóbbak, mégis látványosak és kevésbé bizonyítható, hogy az esetleges támadást ki hajtotta végre [15], [16].

[1] MIBIK: Magyar Informatikai Biztonsági Keretrendszer. IBIR: Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma. IBIK: Informatikai Biztonsági Iránymutató Kis Szervezetek Számára. IBIV: Az Informatikai Biztonság Irányításának Vizsgálata. MIBÉTS: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma. Az IBIX elsődleges célja, hogy segítséget nyújtson az informatikai biztonság megfelelő szintjének kialakításához önkormányzati és más informatikai szempontból kis méretű környezetben.

Összességében a motiváció többféle lehet. A keletkezés okaiban pedig a folyamatosan változó szoftver és hardver környezet, valamint az emberi tényező is közre játszhat. A direkt katonai konfliktus kifejlődésének valószínűsége csekély a feszült politikai helyzet és ellentétes gazdasági érdekek ellenére. Az eddigi történések alapján az a tendencia látható, hogy fokozatosan a nem hagyományos hadviselés irányában elmozdulva, a közvetlen katonai lépések elkerülésével történik a konfliktuskezelés [17].

EGYSÉGBEN AZ ERŐ!

Egy ilyen komplex problémára milyen megoldást várunk? Először is fontos tisztázni, hogy a felmerülő kérdésekre nincsenek kész válaszok. A legtöbb szervezet ajánlások alapján dolgozik, ezen ajánlásokat implementálják az adott munkaszervezetre, törvényi és egyéb körülményekre. Kész megoldások abban a speciális helyzetben lennének csak lehetségesek, ha két teljesen egyforma szervezet folyamatosan azonos fejlődési állomásokon tartózkodna. Azonban ebbe az iterációba belegondolva, könnyen belátható, hogy a felmerülő tapasztalatok és visszacsatolások miatt már nagyon rövid időn belül különbségek adódnának.

Ahogy bevezetőben is megfogalmaztam, az informatika áthatja mindennapjainkat. És ezért is nagyon sok vetülete van az informatikának, hiszen minden szakterületnek megvan az eljárásrendje. Azonban bármely területen is használunk informatikai megoldást, nem működhet tökéletesen, ha nem vagyunk tisztában az adott területen és a határterületeken alkalmazott protokollokkal. A tökéletes működés egyrészt természetesen egy ideologizált állapotot jelent, másrészt pedig az érintettek megelégedettségét, a biztonságot és a fejlődési spirált is magában kell, hogy foglalja.

Mindemellett az emberi tényezőt sem hagyhatjuk figyelmen kívül. Ezt két pólusán csak említés szintjén vizsgálva, az egyik részről felhasználóként, másik részről pedig a rendszerben kiemelt jogokkal jelen lévő valamilyen power user vagy adminisztrátor szerepében kell figyelemmel kísérnünk a jelenlétét.

A fent említett összetevők sokaságát egyeztetve arra a következtetésre jutunk, hogy ötvözni kell a nemzetközi és hazai tapasztalatokat, figyelembe kell venni a szakterületre vonatkozó ajánlásokat. Az adott területért felelős személynek ezek tekintetében naprakésznek kell lennie. A naprakészség a szakma gyors változásainak következtében havi – negyedéves, de mindenképpen fél évesnél gyakoribb, rendszeres továbbképzést feltételez.

Mindezekkel arra kívánok rámutatni, hogy egy adott szervezet ideális informatikai szolgáltató infrastruktúrája csak akkor valósulhat meg – mint ezt a későbbiekben majd részletesebben is kifejtem –, ha minden kapcsolódó terület összhangban működik, organikus egészet képezve. Ennek következtében jönnek létre, jöhetnek létre olyan szinergiák, amelyek további fejlődést indukálnak, nem feltétlenül a tervezhető növekedéshez, hanem esetleg meg nem tervezett új megoldásokként bukkanhatnak fel. Ez természetesen egy ideologizált állapot, ahol minden munkavállaló (biztonság)tudatos felhasználó és motivált is abban, hogy többet tegyen, mint amennyi feltétlenül szükséges a munkaköri kötelességében. Vessük össze ezt az állapotot a hétköznapok széles spektrumú tapasztalataival és a gondolatkísérlet, illetve gyakorlati tapasztalatok mentén már kipróbált működő, valamint kipróbálásra javasolt megoldásokkal, amelyeket az alábbiakban ismertetek.

Megállapítható, hogy nem lehet szigorúan és szegregáltan kezelni az informatikát a munkahelyi szabályoktól, és az adott munkaszervezetben tapasztalható munkamoráltól. Sőt az informatikát eszközként lehet és kell is felhasználni a munkaszervezetek nagyobb hatékonyságú működéséhez. Tekintettel arra, hogy informatikai eszközzel támogatott folyamatokból épül fel az állami szektorban dolgozó munkaidejének jelentős része, természetes, hogy az informatika kiemelt jelentőséget kell, hogy élvezzen más sztenderdizált folyamatok mellett, vagy akár előtt.

ÁLLAMI ÉS ÖNKORMÁNYZATI SZERVEK KAPCSÁN FELMERÜLŐ JELLEMZŐ KIHÍVÁSOK

A Magyarországi tapasztalatok alapján kijelenthetünk néhány, talán közhelynek számító megállapítást. Gyakori probléma a forráshiány, amely hardver-, anyagi- és humánerőforrás kapcsán is megjelenhet az adott munkaszervezetben. Ennek következménye lehet, hogy nehezen implementálódnak a napi gyakorlatba az ajánlások, törvények, belső szabályozások. Ez elválaszthatatlan a túlterheltségből, és alulmotiváltságból fakadó tényezőktől. Eddig is léteztek ajánlások, azonban lényeges változás a tárgyalt törvény tekintetében, hogy a jelenlegi szabályozás már nem „csupán" ajánlás, hanem törvény, másrészt illeszkedik a kor kihívásaihoz a gyors változásokhoz, például az időnkénti felülvizsgálat megszabásával és a korszerű szakszavak definíciójával. Sok esetben a szabályozás és a napi rutin eltér egymástól, gyakran a legfontosabb, a felelősség, illetve a személyi felelősség kérdésköre hiányzott. [18]

Először a felelősség szempontjából érdemes vizsgálni a kérdést, azaz megfogalmazni, hogy incidens esetén ki lesz számon kérhető. Három klasszikus és jól elkülönülő válasz létezik erre, pontosabban három fő csoportra lehet bontani a szervezetek körét. Az első, ideális állapotban a felelősségi körök jól körülhatároltak és egyértelműen beazonosítható minden feladat. A második esetben vannak vakfoltok, ezek származhatnak abból, hogy több felelőse van egy területnek, vagy hogy egyáltalán nincs felelőse. Jegyezzük meg, hogy mindkettő egyformán rossz alternatíva. A harmadik eset pedig, amikor komoly hiányosságok vannak a szabályozásban, vagy egyáltalán nem szabályozottak a folyamatok. Rendszerint ilyenkor szokásjogon alapulva működik a szervezet vagy az IT egység. Nincs dokumentáció, a munkahelyi hagyományok alapján alakulnak ki az eljárások, a szervezethez érkező új kolléga is ez alapján szerzi be tapasztalatait. Nem kérdőjelezi meg az esetleges rossz gyakorlatokat sem, mivel annak kialakítását, miértjét már nem ismeri meg.

Felmerül, hogy mennyire függnek össze az informatika-biztonsági, munkaszervezési és financiális kérdések. A válasz az, hogy organikus kapcsolatban vannak. Hiszen ha van egy olyan modell, aminek része az időnkénti tényleges felülvizsgálat, akkor meghatározottak a munka- és felelősségi körök. Ebből következik az is, hogy a folyamatok és munkakörök optimalizáltak, nem végez el duplán senki egy munkafolyamatot, nincs feleslegesnek tekinthető időfelhasználás. Természetesen a jó szakembereket, akik vállalják, hogy a szakterületükön folyamatosan képzik magukat, az elvándorlás megakadályozása, illetve minimalizálása érdekében részben financiális kérdésként kezelve a kérdést meg is kell tudni tartani.

Egy modell átültetése a hétköznapokban hosszú folyamat is lehet. Viszont az jól látható, hogy az állami és önkormányzati szerveknél nincs egységes ajánlás az informatikával összefüggő folyamatok kezelésére. Ettől természetesen még vannak különböző helyi szabályozások amelyek foglalkoznak részben vagy egészben ezen kérdésekkel, azonban inkább részben, és szervezetenként eltérő megfogalmazásban. Itt merül fel az igény, hogy ha van erre megoldás, annak a megoldásnak vagy tervnek része kell, hogy legyen a tapasztalatok megosztására alkalmas színtér is.

Tapasztalatom szerint a két legjellemzőbb nehézség a financiális és a motivációs hiányosságok kérdése, amely felmerül bármelyik folyamat megreformálásakor. Így ezeket kívánom a továbbiakban részletesebben elemezni, fókuszban természetesen az informatikai felelősöket és az informatikai biztonságot tartva.

Az eddigiekben megállapítottam, hogy a munkaszervezet egészét vizsgálva, nem bontható élesen külön az egyes munkafolyamatok szabályozása. Tehát az informatikai és az informatikai biztonság megteremtéséhez szükséges folyamatok eredményességéhez a többi, nem tisztán informatikai területen is szabályozott, transzparens eljárásoknak kell lennie, működnie.

INFORMATIKÁVAL ÖSSZEFÜGGŐ FOLYAMATOK KEZELÉSE AZ ÁLLAMI ÉS ÖNKORMÁNYZATI SZERVEKNÉL

A törvény végrehajtása során számos kérdés merül fel. Vizsgálhatjuk elsőként az érintettek körét. A törvény jól meghatározza egyrészt azon munkavállalók körét, másrészt a beszállítókat, egyéb partnereket, akiket a biztonsági intézkedések során számba kell vennünk. A példa kedvéért tekintsünk egy olyan céget, ahol ISO minősítésű beszállítókat alkalmaznak, és a cégnél nem ellenőrzik a szállító által hozott árut tételesen. A munkaszervezési kérdések, a munkához való hozzáállás és a munkaszervezetben uralkodó általános eljárások és folyamatok nem különülnek el élesen. Szembesülünk tehát azzal a kérdéssel, hogy hogyan érhetjük el részben informatikai eszközök segítségével, hogy a szervezetben a munkafolyamatok – ezen belül a vizsgálatom fókuszterülete, az informatikai biztonság – kialakuljon és megfelelően fejlődjön? Milyen más megoldások, hatások jöhetnek szóba arra vonatkozólag, hogy ne (csak) külső kényszerítő körülmény legyen a motiváló (törvényi) erő?

Ha elfogadjuk azt, hogy az egyes munkafolyamatok összefüggnek és hatással vannak egymásra, akkor az érintettek körét jól láthatóan a tisztán informatikai biztonsági munkavállalókról ki kell terjeszteni a teljes munkaszervezetre. A továbbiakban ismertetem a különválasztható csoportokat, majd részletesebben a tisztán informatikai biztonságért felelős szakemberek csoportjára vonatkoztatott tapasztalatokat, ajánlásokat és teendőket ismertetem.

Az első a vezetői támogatottság (a nem szakmai vezetőről van szó). Amennyiben a vezető érzékeli a nemzetközi szinten is sokasodó IT biztonsági incidensek számosságát és végső soron felismeri, hogy a szervezet vezetőjeként felelős lesz egy esetleges jövőbeli ilyen típusú biztonsági incidensért, akkor elemi érdeke, hogy rendszerezett folyamatok és jól körülhatárolt felelősségi körök legyenek definiálva.

A második szint a security officer (SO, biztonsági szakember) és az IT üzemeltetés (rendszergazdák) szintje, valamint ezek határterületei. Tegyük hozzá gyorsan, hogy direkt bontom külön ezeket a funkciókat, bár sok helyen csak egyszerűen informatikus a megnevezése mindenkinek aki az IT osztályon dolgozik. Ezen a szintéren is a személyes érintettség megvizsgálása fontos. Ezt két részre bontható. Az egyik, hogy a szabályok megfogalmazása, írásbeli elfogadtatása transzparenciát eredményez munkaszervezeten belül és kívül egyaránt fontos tényező. Hosszú távon a jól szabályozott folyamatoknak köszönhetően több az automatizálható emberi és egyedi beavatkozást igénylő, kevesebb hibalehetőséget rejtő feladatok száma.

A harmadik és jellemzően legnagyobb csoport a felhasználók, akiknél szintén megvizsgálhatjuk érdekeltté tétel kérdését. Természetesen, egyrészről ha az előző két szinten megvan a támogatottság, akkor az már fél siker és technológiailag is szinten minden szabály betartatható. A legjobb mégis, ha a munkaszervezet egésze érdekelt is az IT biztonság betartásában. Erre a mélységi ismertetés nélkül az EU Safer Internet [19] ismeretterjesztő programja nyújt lehetséges megoldás. A program oktatási moduljai jól felhívják a figyelmet a munkahelyen kívüli a való életben ránk leselkedő veszélyekre [20]. Internetes zaklatás, csalás, bankkártya adatok védelme, kéretlen reklámlevelek kezelése, stb. Melyeket elsősorban a fiatalok vonatkozásában tárgyal, de mára már kortól és más szűkítő tényezőtől mentesen mindenkire érvényes és aktuális [21].

Az eddigiek összegzéseként az kristályosodik ki, hogy egy ilyen, informatikai biztonsági szempontból ideális és felkészült szervezetben meg kell teremteni a naprakészséget szakmailag [22]. És hogyan lehet ezt megteremteni? Erre kívánok bevált módszereket, ajánlásokat ismertetni az alábbiakban.

A JELENLEGI HELYZET FELMÉRÉSE, CSELEKVÉSI TERV, FELZÁRKÓZTATÁS, EGY SZÓBAN: OKTATÁS

Az alaposan áttekintett helyzet és a kihívások boncolgatása után kérdés, hogy milyen megoldás működik, milyen ajánlások megoldások vannak a törvény által megfogalmazott elvárásoknak történő megfeleléshez? Milyen főbb lépések mentén érdemes megkezdeni, vagy folytatni a megfeleléshez szükséges munkát? Gyorsan szögezzük is le, hogy a törvény nagy mozgásteret hagy arra, hogy minden munkaszervezet saját maga alakítsa ki a belső informatikai rendjét, vagy ha már van, akkor csak hozza összhangba a törvénnyel. És erre is elég rugalmasan legalább fél éves intervallumot biztosít.

Abból a feltételezett állapotból kiindulva, hogy egy fiktív állami munkaszervezetnél nincs, vagy nem teljesen van összhangban az informatikai folyamatok és informatikai biztonság kérdése, az alábbi ajánlást fogalmazom meg.

Fontos áttekinteni az aktuális állapotot, onnan lehet jól visszamérni majd a változásokat. Azt állítom, hogy bármilyen jellegű változtatásnak, kezdeményeznék szükséges, de nem elegendő feltétele, hogy viszonylag jól mérhetően számszerűsíteni tudjunk olyan mérőszámokat, amelynek későbbi javítását fejlesztését tűztük ki célul. Ez hatalmas motivációs lehetőség a folyamatok mozgásban tartásához is, hiszen, már kismértékű javulás is kimutatható. Tehát mérőszámokat kell találni és a skála alappontját, mint az aktuális helyzetet ki kell jelölni.

A cselekvési terv első pontjai között kell, hogy szerepeljen a kommunikáció. Egyrészt azért, hogy világos legyen a szervezet célja és minden egyes munkavállaló tisztában legyenek azzal, hogy mi és miért történik. Azaz meg kell tudni mutatni, hogy mi ebből az egyes egyének haszna és mi a munkaszervezet érdeke. Praktikus ezen ’küldetésnyilatkozat’ vagy informatikai cselekvési terv készítésébe minél több munkavállalót bevonni. Ennek több oka is van, a teljesség igénye nélkül minél több véleményt ismerünk, annál jobban felkészülhetünk a várható fogadtatásra. Másrészt a munkában részt vevő munkavállalók mivel részt vettek a folyamatban, magukénak érzik azt és támogatni fogják a későbbiekben.

Egy példa: a felhasználók számára biztonságos internet oktatás hozadéka lehet, hogy nem csak a munkahelyen, de a hétköznapi életben is jobban fog tudni vigyázni a személyes adataira. A munkaszervezet szempontjából pedig kisebb várható költsége lesz egy biztonsági incidensnek, de az is lehet, hogy be sem következik, ha már a felhasználók is idejekorán gyanút fognak és nem nyitják meg a fertőzött vagy spam leveleket.

Fontos összetevő, ha nem a legfontosabb azonban a vezetői támogatáson túl az informatikai vezetők és a power userek (vagy épp a security officer képzése) rendszeres képzése. Cikkem elsődleges prioritása is az, hogy ennek fontosságára rávilágítsak. Hiszen a nemzetközi tapasztalatok és a naprakész oktatások tudják megteremteni az alapot és az adott munkaszervezetbe beinjektálni a naprakész információkat, amelyek szükségesek a védekezéshez. Olyan információk és képzések, amelyek jellemzően csak fizetős módon érhetőek el, vagy szükséges gyakorlatot a képzésen lehet megszerezni [23], [24]. Itt is természetesen meg kell mutatni a már a felhasználóknál hivatkozott előnyöket, például: ha automatizálhatóak a folyamatok, akkor ezzel időt lehet megtakarítani. Ha szabványosíthatóak a hardverek és a szoftverek, akkor csökkenthető a hibabejelentések sokfélesége. Ha pedig a felhasználók nem rendszergazdák a gépeiken, akkor valószínűsíthető, hogy ritkábban van szükség a számítógépek újratelepítésére. Az ajánlások, formalizált eljárások számos előnnyel járhatnak.

Informatikai szempontból véve tehát indokolt a munkaszervezet minden dolgozójának az oktatás. Ez az oktatási spirál a fejlődés egyik mozgatórugója [25].

A kérdés másik fele főleg financiális természetű. Egyrészt értékes munkaidőt vesz el a dolgozóktól, amíg oktatáson ülnek, másrészt pedig az oktatás megtartását vagy külsős és fizetett oktatóra kell bízni, vagy pedig belsős oktatóra, akit viszont először el kell küldeni tanfolyamra,

hogy ő maga felkészüljön. Azonban egy ilyen program beindítása akár költségmentesen megoldható. Hosszú távon vizsgálva, olcsóbb a képzés, mint a helyreállítási költségek finanszírozása.

AJÁNLÁSOK ÉS OKTATÁS KAPCSOLATA, AZ OKTATÁS ELVI KIVITELEZÉSE

Amire még szükség van, hogy elindulhasson a törvényi megfeleléshez szükséges munka, az egy cselekvési terv. A tényleges tennivalókat főbb lépésekben az alábbiakban összegzem.

A közösen a munkavállalók bevonásával megfogalmazott és a vezetőség által támogatott küldetésnyilatkozat jó támpont a folyamat elindításához. Erre rakódhatnak a napi folyamatok szabványosításának és formalizálásának folyamatos bevezetései, pl.: hogy jelentsük be hibát, mit tegyünk, ha spam üzenetünk érkezett stb. A mérhető mutatókat vizsgáljuk meg bizonyos időközönként, kérjünk visszajelzéseket, hogy érzékelni tudjuk, megfelelő irányban haladnak-e a folyamatok. Ha lemaradó, vagy elkülönülő csoportot érzékelünk, aki ellenáll a változásnak, akkor igyekezzünk a többség véleményformáló erejére építeni. Például egy képzés során nyilvánosságra hozhat, hogy csak 5 fő nem vett részt eddig a képzéseken. Általában az emberek nem szeretnek a kisebbséghez, a kívülállókhoz tartozni. Ezen információk legyenek nyilvánosak, de ne kirekesztőek. Akár az is megmutatható, hogy melyik egység, osztály milyen létszámban delegálta a kollégákat az oktatásokra.

Az ajánlások és oktatás elválaszthatatlan egységet alkot. Az ajánlás megfogalmazza azokat a sarkalatos pontokat, amely mentén az adott szervezetre le lehet képezni az szabályozást, a helyi adottságoknak megfelelően, beleértve a tényleges időszakos felülvizsgálatot is. Az oktatás pedig azért szükséges, hogy a teljes munkaszervezet nagyjából egy nyelvet beszéljen egységes IT biztonsági tudatossági szinten legyen, vagy legalább közösen tartson abba az idealizált irányba. Itt kell megemlítenem, hogy a szervezet IT biztonsági szintje konvergál a legkritikusabb pont irányába, azaz csak annyira erős, mint a leggyengébb pont.

Kit kell oktatni, vagy kivel kell kezdeni az oktatást? A három jól elkülönülő szintér: nem szakmai vezető, szakmai vezető valamint az informatikai felelős, aki lehet security officer vagy éppen a rendszergazda is. A felhasználók csoportja közül az elsőt (a vezetőt) rögtön kizárhatjuk, hiszen onnan a támogatás szükséges „csak”. (Természetesen az oktatási programon való látványos részvétel elvárt.) A másik két szintéren pedig elkerülhetetlen és szükségszerű az oktatás, viszont fontos a sorrend és a bevezetés. A 2013. évi L. törvény 1 §. 6. és 26. pontjai egyértelműen megfogalmazzák, hogy a kiberbiztonság fejlesztéséhez elengedhetetlen a védelemre és a tudatossági szint növelésére irányuló oktatási koncepció kidolgozás, kivitelezése.

Tapasztalataim szerint egy ideális és lehetséges bevezetési folyamat az lehet, hogy a rendszergazdai szinten biztosítjuk a negyed éves – fél éves továbbképzési lehetőséget. Ezt követően pedig a technikai segítséggel támogatva általános belső oktatást indítanak a rendszergazdai szintről a felhasználói szint felé. Ahhoz hogy ez megvalósuljon természetesen szembe kell nézni a hétköznapi realitásokkal, pár kihívással.

Miután a folyamatokat és az elméleti munkaszervezési háttér át lett tekintve, ideje olyan technikai megoldást keresni, amely képes az elvárásokat idő és költséghatékonyan kezelni. Azaz megvalósulhat az informatikai biztonságért felelős személyek rendszeres oktatása továbbképzése, teret biztosít a hasonló munkaszervezetek közötti tapasztalatcserére és a szervezet további munkavállalói számára is kerülhetnek bele általános informatikai oktatási anyagok. A technikai megvalósítás kérdéseit az ennek kapcsán felmerülő kérdésekre adott válaszokat a későbbiekben részletesen ismertetem.

Összegezve, a törvény mellé egy olyan egységes keretrendszer és oktatási anyag létrehozására lenne szükség, amely segíti a törvénynek való megfelelést a helyi színtereken. Az egységes oktatás további hozadéka lenne, hogy formalizálódnának a folyamatok a

munkaszervezetekben, növekedne a helyi tudásszint, előre nem tervezhető szinergikus folyamatok indulhatnak el. Ez a gondolat elvárás szintjén meg is jelenik a törvényben: amelynek itt az 1 §. 6. és 26. pontját emelném ki. Ez egyértelműen megfogalmazza, hogy az adminisztratív védelemnek része kell, hogy legyen a védelemre vonatkozó oktatás. Tekintve, ezen törvény által érintett többezres létszámot, azaz mekkora létszámú személynek lenne szüksége a megfelelő naprakész informatikai, biztonsági ismeretek elsajátítására és annak naprakészen tartására, az egy főre jutó költség elenyészőnek tekinthető még abban az esetben is, ha fajlagosan egy központi távoktatásos tudásbázis, keretrendszer létrehozása számottevő financiális forrásokat igényel. Egy ilyen tudásbázis központi létrehozása mellett a fenti szempontokon kívül az szól még, hogy az egyes kisebb-nagyobb szervezeteknél jellemzően nincs meg a szükséges kapacitás, tudás ahhoz, hogy ilyen rendszert hozzanak létre, töltsenek fel tartalommal és üzemeltessenek [26].

AJÁNLÁS A TECHNIKAI MEGVALÓSÍTÁSRA, AZ INFORMATIKAI TECHNOLÓGIÁVAL SEGÍTETT OKTATÁS

Milyen szoftver megoldást válasszunk? Ha a fentebb definiált elvárásokban és elvárt eredményekben egyetértés van, akkor is a technikai kérdés még jelenleg nyitott. Mivel és hogyan legyen megvalósítva? Számos olyan oktatási módszer és oktatási keretrendszer van, melyeket adott szervezetre vagy adott általános elvárásokra fejlesztettek ki. Ezek közül vannak ingyenes és nyílt forráskódú programok valamint fizetős, licensz díjas megoldások is. Leszögezhetjük, hogy a nagy létszámú érintett, a földrajzi távolságok miatt és a különböző időbeli ráérések összehangolásának problematikájából egyedüli nyertesként valamilyen távoktatásos megoldás kínálkozik kizárólagosan. (Az előbbiekben részletesebben megfogalmazott elvárások, például a költséghatékonyság alatt az utazás, rezsi költség, terem és eszköz bérlet, szállás, munkaidő kiesés, stb. összesített költségek minimalizálására való törekvést értem.) Fontos szempont viszont, hogy az alkalmazott keretrendszer a tanulási eredményességnek és a tartalomnak legyen alárendelve. Azaz olyan beépített eszközökkel rendelkezzen, amely alkalmas arra, hogy az adott információ legjobb elsajátítása, beépülése valósulhasson meg.

Az ilyen keretrendszerekre gyakran használják az e-learning kifejezést, távoktatás vagy a blended learning módszereket. Ez utóbbi vegyes típusú, komplex tanulást jelent, melynek lényege, hogy a tanítandó anyaghoz rendeli hozzá az optimális módszert [27], [28].

Néhány mondatban érdemes definiálni, hogy itt mit értünk alatta, vagy milyen további előnyöket várunk ettől a megoldástól. A főbb elvárások a 2013. évi L. törvénynek megfelelés, azaz a munkaszervezet informatikai biztonságának biztosítása. Az elvárt eredmények bármely munkaszervezetnél a specializált elvárások minél költséghatékonyabb elérése, továbbá a bevezetéshez mérőszámok definiálása és ezek objektív mérésének megteremtése. Jelen esetben olyan a célnak és a feldolgozott téma megfelelő tudásátadásához szükséges oktatási anyagokat, kidolgozott gyakorló és ellenőrző feladatokkal kombinálva, amely csak az EKG-hálózatból érhető el, azonosítást követően. Az oktatási anyagok a jogosultság alapján bármikor és tetszés szerinti alkalommal elérhetőek, hiszen a cél az átvinni kíván információ minél hatékonyabb rögzítése. Ezek az alapvető elvárások, melyeket valószínűleg tovább érdemes specifikálni pontosítani.

Egyrészt a fentebb megfogalmazott elvárásokon kívül egy hagyományos klasszikus előadáshoz képest számos egyéb mérőszám válik kiértékelhetővé. A teljesség igénye nélkül néhány példa: adott feladatok megoldási mutatói, a videók és oktatási anyagok legtöbbet és legkevesebbet látogatott, nézett részei, az anyagok jellemző megtekintési ideje és rendszeressége szervezetenként és egyéb olyan felhasználói szokások válhatnak

kiértékelhetővé, amelyek segítik a további képzési anyagok létrehozását, a meglévők fejlesztését.

Az ún. blended képzések elkészítése nagyon komoly erőforrásokat emészt fel a tapasztalatok szerint. Ezen oktatási forma a célhoz rendeli hozzá az eszközt. Tehát ha adott ismeretanyag megfelelő elsajátítása gyakorlatorientált képzést tesz szükségessé, akkor az adott modul feldolgozása a megfelelő beépülés érdekében ennek az elvárásnak a jegyében kerül feldolgozásra. És ez teljesen elkülönülhet, illetve különböző lehet egy olyan modul feldolgozásától, amelyik pusztán elméleti és a definíciók ismertetésére szorítkozik.

További előnye egy ilyen rendszernek, hogy az adott és a mért válaszokból jól kirajzolódik az esetlegesen fejleszthető vagy fejlesztésre szoruló terület. pl.: ugyanazt a részt sokkal többször nézték meg, ugyanaz az ellenőrző vagy gyakorló feladat nagy százalékban tolódott el valamilyen irányban, adott kérdés megválaszolása sokkal több időt igényelt. Azaz ilyen rendszer esetében lényegesen több információ mérhető és szerezhető a képzésről, mintha csak a végén kérdőívet töltenének ki a hallgatók, vagy ha csak a gyakorló, vizsga feladatok eredménye állna rendelkezésre. Egyes kérdések megválaszolása között eltelt idő is sokat árulhat el a tananyagfejlesztők számára. Természetesen komoly biztonsági intézkedéseket kell tenni, hogy csak a jogosultak férjenek hozzá az oktatási anyagokhoz.

A blended oktatási módszer lényeges szempontja, hogy a hatékony információ átvitel érdekében választjuk meg az eszközt. Tehát bizonyos anyagoknál jól használható bármely ingyenes e-learning rendszer, más részeknél lehet, hogy videó anyagok praktikusak a cél érdekében [29], [30]. Szükség van olyan platformra amelyet számos egyetemen alkalmaznak a távoktatásos rendszerű képzésben tanuló, vagy levelező tagozatos hallgatók képzésére, hogy kérdést tegyenek fel, konzultációs felületet biztosítson a rendszer. Legyen ajánlott irodalom, és definiálni kell a minimálisan szükséges technikai szintet, ami a rendszer használatához szükséges. Ezen általános irányelvek mentén kérőíves technikákkal gyűjtött információk kiértékelését követően biztos, hogy többféle szoftveres megoldás közül lehet választani.

A blended oktatási koncepcióval nyitott marad a lehetőség, hogy új technológiák, technikák, szoftverek, megoldások esetén azok beépüljenek egy komplex rendszerbe, annak érdekében hogy adott modul és ezáltal az egész ismeretanyag, információátviteli eredményessége növekedjen.

EGYES SZÍNTEREKEN A RENDSZERES OKTATÁS BEVEZETÉSÉNEK HATÁSVIZSGÁLATA

A legelső kérdés, amit meg kell válaszolni és tisztázni, hogy milyen rövid és hosszú távú eredményekre számíthatunk és hogyan érdemes hozzákezdeni. Egyrészt az online reputáció biztonsága megfizethetetlen, ez olyan alapfelvetés, amely mérhetetlen, de vélhetőleg alapvető cél. A felhasználók és a informatikai felelősök oktatása jól különválasztható. Először a felhasználók oktatásának tapasztalatáról a várható eredményekről kihívásokról, majd részletesebben a IT felelősök kapcsán vizsgálom meg a kérdést.

A felhasználók rendszeres képzésének első komolyabb kihívása lehet a kritikus tömeg elérése. Azaz olyan pont elérése, amikor már kevesebben vannak azok, akik nem vettek részt ilyen oktatáson. Fontos, hogy ezen első oktatási alkalmak kellőképpen élvezetesek és informatívak legyenek, semmiképpen ne legyenek túl hosszúak. Érthető és hasznos ismereteket fogalmazunk meg, sikerélményt kell, hogy megéljen a képzésen részt vett személy.

Javasolt nem frontális, hanem interaktív, prezentációval, videó bejátszásokkal tarkított és 30 percnél nem sokkal hosszabb előadásokkal kezdeni, a végén időt hagyni az esetleges kérdések megválaszolására, valamint az előadást követően az elhangzott előadás kivonatát e-mailben vagy más formában is eljuttatni a résztvevőknek. A legfontosabb cél az első előadásokon az aktivitás. Próbáljuk meg bevonni a dolgozókat és interaktívvá tenni az előadást. Találjunk

olyan, a hétköznapi életből vett példát, helyzetet, amely kihívást okozott, és tudunk rá jó megoldást kínálni. Igazi értékként tekintsünk az előadás végén feltett kérdésekre. Egyrészt mert visszajelzést szolgáltatnak számunkra (vagy az előadó számára), másrészt egy jó kérdés vagy a kérdésre adott válasz lehet, hogy másokat is érdekel a közönség soraiból. Fontos megköszönni a részvételt és a visszajelzéseket, kérjünk javaslatokat a következő oktatás témájára.

A konkrét, már a folyamat elején jelentkező eredmények egyike, hogy informatikai oktatás szóbeszéd tárgya lesz. Az ott elhangzott információkat megvitatják a kollégák, esetleges saját tapasztalatokról is tájékoztatják egymást. Gyakoriak az olyan visszajelzések, hogy az ott elhangzott információkat miként sikerült felhasználni és beépíteni a napi tevékenységbe. Ezeket (esetenként név nélkül) érdemes összegyűjteni és a széles közönség elé tárni, nem csak az oktatási reklám, hanem azért is, mert hátha van, akiben ott volt a kérdés, de nem tette fel. Vagy a fentebb már említett jó kommunikációs szokások, transzparencia jegyében tegyük ezeket közzé. Összességében a kívánt folyamat során számos olyan visszajelzés van, amelyet talán úgy lehet összefoglalni, hogy egy közös nyelv kerül kialakításra. Pontosabban definiálni tudja a felhasználó az igényeit, jobban el tudja különíteni a információkat, legyen az egy social enginering vagy egy spam levél, vagy akár csak annyi, hogy bizonytalanság esetén mer kérdezni és bejelenteni az eseményt az üzemeltetés felé. Tapasztalataim alapján 3-6 hónapon belül érezhető és mérhető változások tapasztalhatóak. Ezen kívül a cikkemben már egyszer említett EU Safer Internet program önkéntes oktatóját meghívva jó és érdekes előadással kezdődhet egy ilyen program. Az ilyen oktatás korosztályra szabható, hiszen korosztályonként változik a kiemelt fenyegetettség típusa. Számos egyéb tényező is mérhetővé válhat, életkor, lakhely szerinti összefüggésben [31], [34].

Az informatikai felelősök oktatása ennél több nyitott kérdést vet fel. Viszont ebben az a jó, hogy a megoldási lehetőségek számossága is több. Míg a felhasználók esetében viszonylag könnyen megoldható a helyszíni képzés akár a helyi informatikus által, addig a magas szintű informatikai képzéshez szakember szükséges és jóval forrás. Amennyiben az adott munkaszervezet erre képes pénzügyi forrásokat biztosítani akkor a munkavállalót el tudja küldeni képzésekre, ezek jellemzően viszont csak Budapesten érhetőek el, ill. megfelelő létszám esetén természetesen helyi képzést is lehet kérni. Ezért is tartottam végig fókuszban azt a lehetőséget, hogy valamilyen központi megoldásra lenne szükség, hiszen a kis munkaszervezetek, vagy ahol nem megoldott a kollégák helyettesítése, nincs feltöltve minden státusz, vagy ahol egyszerűen ez nem volt beletervezve az éves költségvetésbe, stb. ott ezek kivitelezésének sikeressége kérdéses.

Tehát a jól bevált és nemzetközileg is a hazai felsőoktatásban is már teret hódító elterjedt módszer az távoktatás alkalmazása lehet a megoldás. A törvényt alapul véve, valamilyen képzési tematikai kidolgozását követően implementálható moduláris rendszerben a képzési információ. Ehhez először egy pilot projekt keretében kijelölt létszám fér csak hozzá és a visszajelzések feldolgozását követően lehetne megnyitni a szélesebb kör számára. A mi szempontunkból mindössze annyi a távoktatási megoldás lényege, hogy nem szükségeses hosszú utazásokat megtenni, rendszeresen, nagy létszámú embernek. Valamint az adott oktatási anyag nem csak egyszer hangzik el, hanem lehetőség van gyakorlásra, próbafeladatok megoldására, teszt írásra és kérdésfeltevésre is. Ezen mérhető tapasztalati adatok pedig visszadolgozhatók a rendszerbe, azt fejlesztve. A modularitáson pedig azért van nagy hangsúly, hiszen munkaszervezet és egyéni szaktudás és egyéni munkaterület függvényében különböző információkra lehet szüksége egyes munkavállalóknak. Bár az alapok, azaz a sztenderdek és ajánlások mindenki számára kötelező elméleti modult jelent. Azt követően egyes modulokban, a tematika összeállításában lehetnek eltérések.

Tekintve viszont, hogy ez mind egy nagy egységes rendszerbe tagozódik be, így az adott munkavállaló papírt, igazoló dokumentumot szerezhet arról, hogy éppen melyik modult és milyen eredménnyel végezte el. Így állami szektoron belüli munkahely váltáskor ez

univerzálisan képes megmutatni, hogy pontosan milyen informatikai képzettséggel rendelkezik. Itt ismét képbe kerül a kritikus tömeg, azaz ha már a munkahelyi humánerőforrás vezetők tudnak erről, akkor elvárt papír lesz a felvételin. És a munkavállaló előképzettségét elhivatottságát fogja mutatni.

A fentebb vázolt komplex megoldás lényege, hogy minden érintett megtalálja benne a számítását és célját, sőt ezen túlmenően a rendszer sajátja, hogy fejlődési lehetőséget organikusan magában foglalja. Sikeres működés esetén pedig az informatikai felelősök körén kívülre a felhasználókra is kiterjeszthető a rendszer, természetesen más tematikával. Csoportdinamikai folyamatok részletesebb áttekintése nélkül is ki tudom jelenteni, hogy változásokat idéz elő. Ezen pozitív változások hatással lesznek további munkafolyamatokra, valamint a rendszeres oktatás best practice minta lehet egyéb területeken is ezen gyakorlat bevezetésére. Tekintettel arra, hogy az informatika a legtöbb folyamatban bele van foglalva (szoftver, hardver, elektronika) így praktikus ezen folyamatokkal kezdeni.

KITEKINTÉS ÉS TÁVLATI HATÁSVIZSGÁLAT

Felvetődik a kérés, hogy mi történik, mi feltételezhető, a rendszer működése milyen pozitív változásokat eredményezhet majd társadalmi és mikro, makro szinten?

Társadalmi szinten vizsgálva, minden olyan folyamat, amely az állampolgárok, jelen esetben az állami szektorban dolgozó munkavállalók oktatását tűzi ki célul csak pozitív hatásokat hozhat. Az alap tudásszint általános emelkedése várható tőle. Valamint a tanulásra való hajlandóság és az LLP programok általános megítélésének javulása [32].

Ezen kívül a távoktatásos rendszer bevezetése pozitív hatás gyakorolna a távmunka elfogadottabbá tételére [33]. Szinergiák léphetnek fel a családbarát munkahely szélesebb körben történő elterjedésével. Prognosztizálható, hogy pár év alatt minimum szintű elvárás lenne a közszférában a felhasználói és informatikai felelős vonatkozásában is bizonyos modulok teljesítésének megléte, igazolása. Amely a társadalom további rétegeibe gyűrűzve hozzájárulna a digitális írástudás, az internet használat és az általános informatikai biztonsági tudásszint emeléséhez.

Sok munkaszervezet feltételezi azt, hogy jól szabályozottak a folyamatai, azonban minden olyan szituáció, amikor egyéni döntést kell, hogy hozzon a munkavállaló és ez ezer esetben megvizsgálva egyszer is eltérő lehet, akkor ott létezik valami apró részletkérdés, ami nem teljesen szabályozott. Lehet ilyen a dolgozók ki és belépése a munkaszervezetbe, a hozzáférési jelszavak átadásának menete, vagy a régi azonosítók és hozzáférések visszavonásának kérdése. Nem vállalkozhatok arra, hogy minden ilyen folyamatot beazonosítsak cikkemben, hiszen pont arról van szó, hogy a törvényi szabályozást a helyi szintérre kell implementálni. És felvetődik a kérdés, hogy mikor érdemes ezt elkezdeni, van-e valamilyen ideális időpont? Meglátásom szerint minél hamarabb érdemes a folyamatot elindítani, mivel annál gyorsabban derülnek ki esetleges neuralgikus pontok, kevéssé szabályozott folyamatok. Valamint annál hamarabb lesznek meg az első visszacsatolások, amelyek a változtatáshoz, fejlődéshez szolgáltathatnak üzemanyagot. A várhatóak kihívások, azonban ezen információkat a munkaszervezet előnyére lehet fordítani. Hiszen hosszú távon minden munkavállalónak az az érdeke, hogy a munkahelye biztonságban legyen, költséghatékony legyen a működtetés, maga a munkavállaló szakterületén és a kapcsolódó területeken képzett legyen. Az a személy, akiben munkálkodik az erre való törekvés minden bizonnyal örülni fog a képzési lehetőségnek, ahol fejlődhet. Természetesen a program folyamán biztos merülnek fel majd kidolgozásra szoruló kérdések, pl.: szülési szabadságról, vagy tartós kiküldetésből visszatérő dolgozók hogyan pótolhatják az anyagot; Más telephelyen dolgozók, vagy a beszállítók, akikre szintén vonatkozik a törvény hogyan tudnak ha nem is az oktatási anyaghoz, de ajánlásokhoz hozzájutni, annak megfelelni, stb.

Egy olyan ország, egy olyan ország gazdasága, ahol fejlődésre, tanulásra nyitottak munkavállalók, és ezt meg is kapják, valamint az állami szférában naprakész informatikai és informatikai biztonsági képzésben részesülnek, sikerre van ítélve. Hiszen jellemzően a forprofit szektorból begyűrűző gyakorlatokat, ha meg nem is előzné ez a kezdeményezés, de mindenképp hasonló szintre emelné, ezáltal megjegyzem az átjárhatóság is könnyebb lenne, amely további lehetőségeket rejt magában.

A hosszú távú célokat és előnyöket biztonsági szempontból ez a mondat summázza legjobban: „A szabályozás jó alapot ad arra, hogy kiépüljön az a kultúra, az a szervezetrendszer és az a műszaki védelem, amire néhány éven belül nagy biztonsággal rá lehet ültetni azt a kibervédelmi szabályozást, mely a hiányzó elemeket, így az ország összehangolt támadása során szükséges lépéseket tartalmazza.” [34]

Eddig a pontig azonban még sok a teendő, számos aprónak tűnő tematikus kérdésre kell választ találni, vélhetőleg ezeket először is felmérés révén a szükséges az információt be kell gyűjteni. Hiszen el kell tudni különíteni a programban nem csak a két nagy csoportot az informatikai felelősöket és a felhasználókat, de a elsőn belül további tagozódást is érdemes létrehozni, a konkrét szakterület függvényében.

ÖSSZEFOGLALÁS

A 2013. évi L. információbiztonsági törvény megfogalmazza a határidőket és teendőket ezzel párhuzamosan nagy mozgásteret hagy az a szükséges folyamatok elinduljanak és a megfelelő eljárásrend kialakuljon. A fentebb olvasható ajánlások és következtetések alapját a Szegedi Tudományegyetemen 2011 óta folyó pilot folyamat eredményeire alapoztam és azokból levont következtetésre. Mivel a nemzetközileg is zajló folyamatok azt mutatják, hogy nem megkerülhető a megfelelő informatikai biztonság létrejötte, így minden szervezet számára érdemes minél előbb bekapcsolódni ebbe a munkába, hiszen annál nagyobb tudás halmozódhat fel a szervezeten belül a tanulási folyamat következtében. „Az új törvény legfontosabb rövid távú hatása az, hogy jogalapot teremt a közigazgatás és a kritikus információs infrastruktúrák védelmére.” [34]

Sok szempontból hiánypótlás történt, hiszen végre megtörtént a jogalap kimondása egy esetleges közigazgatási felhő létrehozásához, bátor jelentkezőket vár ez a lehetőség. Általánosítva pedig az új technológiák bevezetésének lehetőségét is megteremteni a törvény. Úgy gondolom a következő években komoly változások történhetnek, komoly fejlődési potenciál van a közigazgatási informatika és informatikai biztonság területén. Amennyiben a változásra, a tanulásra nyitott emberek ezen kezdeményezésnek élére tudnak állni és azt a bizonyos kritikus tömeget sikerül ezen folyamatba bevonni, együtt dolgozni a sikerért /a biztonságos magyar kibertérért.

Felhasznált irodalom:

[1] A 2013. évi L. törvény, Az állami és önkormányzati szervek elektronikus információbiztonságáról

[2] Az Európai Parlament és a Tanács 2003/98/EK Irányelve a közszféra információinak további felhasználásáról, 2003. november 17.

[3] Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, Hadmérnök 7.évf 4.szám, 142-151 http://hadmernok.hu/2012_4_krasznay.php (2013.11.01)

[4] Papp Zoltán: a számítógép-hálózatok tűzfalainak támadása, Hadmérnök, VII. Évfolyam 2. szám - 2012. június

[5] Nagyné Takács Veronika: A közigazgatási informatikai rendszerek fejlesztésével kapcsolatos felhasználói elvárások, Hadmérnök, VII. Évfolyam 4. szám - 2012. december

[6] Krasznay Csaba: A modern kor gyermekkatonái – hogyan védjük az ifjú hackereket? Elhangzott: 2012.09.25, II. Nemzetközi Konferencia: Az internet hatása a gyermekekre és a fiatalokra Budapest, Magyar Tudományos Akadémia

[7] Bodlaki Ákos,Csernay Andor, Mátyás Péter, Muha Lajos, Papp György Dr.,Vadász Dezső , Informatikai rendszerek biztonsági követelményei, Informatikai Tárcaközi Bizottság ajánlásai, 1996.

[8] Muha Lajos: Magyar Informatikai Biztonsági Keretrendszer (MIBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[9] Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos: Informatikai Biztonsági Irányítási Rendszer (IBIR), Budapest: Miniszterelnöki Hivatal, 2008.

[10] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: Informatikai Biztonság Irányítási Követelmények (IBIK), Budapest: Miniszterelnöki Hivatal, 2008.

[11] Balázs István, Déri Zoltán, Lobogós Katalin, Muha Lajos, Nyíri Géza, Sneé Péter, Váncsa Julianna: Informatikai Biztonság Irányításának Vizsgálata (IBIV), Budapest: Miniszterelnöki Hivatal, 2008.

[12] Balázs István, Szabó István: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS), Budapest: Miniszterelnöki Hivatal, 2008.

[13] Krasznay Csaba, Muha Lajos, Rigó Ernő, Szigeti Szabolcs: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX), Budapest: Miniszterelnöki Hivatal, 2008.

[14] Egységes Kormányzati Gerinchálózat, http://www.ovit.hu/sikerrel-zarult-az----ekg----megvalositasanak-elso-fazisa.html (2013.11.01)

[15] PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ, 2012. II. negyedéves jelentés: http://www.cert-hungary.hu/sites/default/files/news/cert_2012_quart_2.pdf (2013.11.01)

[16] Cserháti András: A Stuxnet vírus és az iráni atomprogram, http://wwwold.kfki.hu/fszemle/fsz1105/CserhatiAndras.pdf

[17] Bukovics István, Fáy Gyula, Kun István: Struktúra és funkció a hálózatalapú hadviselésben Hadmérnök, VII. Évfolyam 4. szám - 2012. december

[18] ITIL v3 nemzetközi sztenderd, ajánlás az informatikai folyamatokra, http://www.itil-officialsite.com/ (2013.11.01)

[19] EU Safer Internet Program, http://ec.europa.eu/information_society/activities/sip/index_en.htm (2013.11.01)

[20] Jancsák Csaba: Az ifjúságkutatás nemzetközi tendenciái 315 In.: Arcátlan (?) nemzedék, Szerkesztette: Bauer Béla, Szabó Andrea Nemzeti Család- és Szociálpolitikai Intézet Budapest, 2011.

[21] Som Zoltán: Az internet veszélyei és ajánlás ennek kezelésére, elsősorban a tizenéves általános iskolások vonatkozásában, Módszertani Közlemények, 2013. 53. évfolyam, 2. szám.

[22] Muha Lajos: Infokommunikációs Biztonsági Stratégia, Hadmérnök 2009. március, p. 220.

[23] ISACA: 2012 IT Risk/Reward Barometer: Europe, p. 1-2; www.isaca.org/risk-reward-barometer

[24] Annual Incident Reports 2011, ENISA, 2012. 8, 12, 15. oldal. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annualreports/annual-incident-reports-2011

[25] Muha Lajos, Nemeslaki András: Információbiztonság az oktatásban In: Zala Mihály (szerk.) ISCD 12.

[26] Szabó Mária, Singer Péter, Varga Attila: Tanulás hálózatban. Elméleti összefoglaló és gyakorlati tanácsok az eredményes hálózati tanulás megvalósításához. Budapest: Oktatáskutató és Fejlesztő Intézet, 2011

[27] Forgó Sándor, Hauser Zoltán, Kis-Tóth Lajos: A blended learning elméleti és gyakorlati kérdései, http://nws.iif.hu/ncd2005/docs/ehu/029.pdf (2013.11.01)

[28] Forgó Sándor, Hauser Zoltán, Kis-Tóth Lajos: Tanulás tér- és időkorlátok nélkül, http://epa.oszk.hu/00000/00011/00088/pdf/iskolakultura_EPA00011_2004_12_123-139.pdf (2013.11.01)

[29] Allison Rossett, Felicia Douglis, and Rebecca V. Frazee: Strategies for Building Blended Learning https://files.pbworks.com/download/F13oAVrgw5/ablendedmaricopa/1240589/Strategies%20Building%20Blended%20Learning.pdf (2013.11.01)

[30] How to Create a Blended Learning Internal Proposal / Business Case http://www.solutionstraining.co.uk/pdf/how2create.pdf (2013.11.01)

[31] EU: The Lifelong Learning Programme: http://ec.europa.eu/education/lifelong-learning-programme/doc78_en.htm (2013.11.01)

[32] Az Európai távmunka megállapodás és a végrehajtásáról szóló elemzések, http://www.szmm.gov.hu/main.php?folderID=10007 (2013.11.01)

[33] Dr. Muha Lajos, Dr. Krasznay Csaba: Kibervédelem Magyarországon: áldás vagy átok? http://www.hwsw.hu/hirek/50206/kibervedelem-biztonsag-jog-torveny.html (2013.11.01)

[34] Jancsák Csaba 2008: Az Ifjúsági korosztályok. In. Nagy Ádám (szerk.): *Ifjúságügy*. Budapest: Új Mandátum. 19–59