ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel
ISBN 978-615-5491-56-6

Információbiztonság-tudatosság gyakorlat

Mádi-Nátor Anett, Kardos Zoltán

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalomjegyzék

1. Bevezető a tananyaghoz

Napjainkban információs társadalomban élünk. Gombamód növekszik a használatba vett elektronikai eszközök száma, egyre több és több a számítástechnikai eszköz, úgymint laptop, tablet, okostelefon, okostévé, okos hűtőszekrény, stb. (Internet of things – egymással az interneten keresztül kapcsolatban álló, beágyazott, de egyedileg azonosítható számítási kapacitással rendelkező eszközök; az IoT keretén belüli eszközök túllépnek a szimpla gép-a-géppel jellegű kommunikáción, és számtalan különböző protokolt, domain-t, applikációt használnak a kapcsolatteremtéshez.) Ráadásul a technikai fejlődés a legkülönfélébb okos eszközök, hordható elektronika felé halad (mely felöleli a hordható orvosi monitorozó eszközöket, de az állatokba ültethető nyomkövető eszközöket és a személyautók irányításához használt komputereket is), ami a már így is átláthatatlan méretekkel rendelkező internethez csatlakozva beláthatatlan mennyiségű információ halmazt és információáramlást eredményez. [1]

Napjainkban – 2014 nyarán – megközelítőleg 3 milliárd ember használ internetet nap, mint nap. A felhasználók száma bizonyos években kiugróan, más években kevéssé, de folyamatosan nő 1993 óta.[2] Jelenleg másodpercenként 38.000 keresés történik a Google-ben[3], 100 órányi új videó kerül feltöltésre a YouTube-ra[4], havonta kb. 250.000 ezer új alkalmazást töltenek le az Apple felhasználók[5], és ezalatt az időtartam alatt 30 milliárd tartalom megosztás történik a Facebook-on[6]. 2013-ban több mint 100 milliárd e-mail került elküldésre illetve fogadásra[7], és ebben az évben kb. 75 milliárd dollárt keresett az Amazon online eladásokon[8]. Ezek elképesztő számok.

A fenti statisztikák alapján látható, hogy a virtuális tér és annak használata hatalmas piacot és több milliárdnyi felhasználót teremt. Ebben a virtuális térben mind az eszközök, a rendszerek, mind azok felhasználói rengeteg támadásnak vannak kitéve. 2013-ban 1,8 millió

[1] http://en.wikipedia.org/wiki/Internet_of_Things
[2] http://www.internetlivestats.com/internet-users/
[3] http://www.internetlivestats.com/google-search-statistics/
[4] https://www.youtube.com/yt/press/statistics.html
[5] https://www.appannie.com/dashboard/64936/
[6] http://blog.kissmetrics.com/facebook-statistics/
[7] http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf
[8] http://expandedramblings.com/index.php/amazon-statistics/

kártékony és nem kívánt programot azonosítottak a kutatók.[9] Ezen kártékony programok célpontjai az informatikai rendszerek, eszközök, és nem utolsó sorban a felhasználók, az emberek „virtuális élete”.

Ráadásul ez a „virtuális élet” nem is feltétlenül marad meg a maga virtuális keretei között. A virtuális tér és az abban történő események az online bankolással, az e-közigazgatás bevezetésével, a webshopok használatával, az oktatásban szereplő diginapló elindulásával, online ételrendeléssel, e-mail-ek küldésével, fogadásával, fényképek megosztásaival, barátokkal való kapcsolattartással, események szervezésével, stb. a mindennapi fizikai életünkre vannak komoly hatással. A fizikai valóság észrevétlenül, mintegy 2 évtized alatt szinte teljesen ráépült az internet globális, gyors és bárhonnan elérhető szolgáltatásaira. Előrejelzéseink alapján a fizikai és a virtuális életterek összefonódása a jövőben tovább nő.

A fizikai életben rengeteg eszközzel védjük magunkat, zárakkal, ajtókkal, falakkal, rácsokkal, kerítéssel, önvédelmi eszközökkel, stb. Ugyanennek a mentalitásnak – a digitális információ védelmének – célszerű megjelennie a virtuális életben is.

Mindezek miatt létfontosságú, hogy egyénenként tudatosítsuk és rögzítsük magunkban – megtanuljuk – azokat az alapvető normatívákat, melyek miatt biztonságban tudunk létezni a virtuális világban is. Ennek az újfajta tudás megszerzésének a legalapvetőbb eszköze az internetet felhasználók információbiztonsági tudatosságának kialakítása, és annak folyamatos fejlesztése, avagy a technológiai fejlettség fokának megfelelő szinten tartása.

Az egyéni felhasználók mellett a szervezetek számára sem közömbös az, hogy sikeres válaszokat tudnak-e e megfogalmazni az információbiztonság új kihívásaira. Ezen lehetséges válaszok a gyakorlatban többrétegűek, optimális esetben átívelnek az információbiztonság-tudatosság növelését célzó képzésektől a törvényi megfelelésen és a megfelelő szervezeti struktúra elemek kialakításán át a lehetséges sérülékenységek stratégiai szemléletű kommunikációját és azzal párhuzamosan a felsővezetői elkötelezettséget megalapozó gondolatokig. A biztonságtudatossági gyakorlat c. tárgy a fenti válaszokba ad bepillantást.

[9] http://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/

2. A többszintű információbiztonság-tudatosság kialakítása, képzési programok

Mottó: Tegyük a jövőt együtt biztonságosabbá.

2.1. Általános megközelítés

Az információbiztonság-tudatosság és a kapcsolódó informatikai biztonsági képzési programok egyik legfontosabb célja a szervezetek egészséges működéséhez szükséges információbiztonsági és informatikai biztonsági biztosítékok helyes kialakítása és használata. Minden szervezetnek az igényeknek és a létező, valamint a tervezett biztosítékoknak megfelelő módon ki kell alakítania a saját információbiztonság-tudatosság növelő és informatikai biztonsági képzési programjait. A képzéseknek tartalmi szempontból a szervezet belső szabályozói mellett az érvényes törvényi szabályozás rendelkezéseit is figyelembe kell venniük.

Ezen képzések kialakításában a szervezet információbiztonsági vezetőjének alapvető szerepe van, egyrészt a képzések anyagának tartalmi kialakítása, másrészt jellemzően a képzések megtartása tekintetében is. Az információbiztonsági vezető ilyen felelőssége abban az esetben is fennáll, ha a képzést egy külső biztonsági partner szolgáltatja.

2.1.1. Miért is fontos a képzés?

Egy szervezet élete során számos új feladattal szembesül az adott dolgozói, felhasználói kör, és sok esetben kevéssé érthető számukra, hogy miért is van szükség az addig bevált munkavégzési gyakorlat változtatására. Tekintettel arra, hogy a bevezetett védelmi intézkedések jellemzően kockázatelemzés hatására kerültek meghatározásra, az információbiztonság-tudatosság képzést végző tréner/oktató, illetve a felsővezetés képes a birtokában lévő tényekkel alátámasztani a védelmi intézkedések módosításainak szükségességét. Az információbiztonság-tudatosság képzés tartalmazza a felhasználók tájékoztatását a már meglévő és az új biztonsági intézkedésekről, és kiemelt hangsúlyt fektet annak tudatosítására, hogy pontosan miért is van szükség a működési folyamatok szabályozására, esetenként módosítására, továbbá bemutatja azokat az előnyöket, melyek támogatják a munkavállalót.

Az informatika – és ennek nyomán az információbiztonság is – rohamosan fejlődő ágazat. Számos új fejlesztés és technológiai változás jelenik meg nap, mint nap, emiatt – tekintettel arra, hogy a fejlődés és változás számos új fenyegető tényezőt hordoz magában, melyek ismeretének hiánya nem jelenti azt, hogy azok nem is érinthetik az adott szervezetet – a rendszert működtető és használó munkatársak számára célszerű az alábbi képzéseket rendszeresen vagy eseti igény felmerülésével biztosítani, illetve elérhetővé tenni:

- szakmai képzések, mely tartalmazzák az újonnan bevezetett rendszerek hatékony és biztonságos üzemeltetését és használatát célzó intézkedéseket és munkafolyamatokat, valamint
- információbiztonság-tudatosságképzések, melyek képesek a szervezet munkatársainak figyelmét felhívni a releváns fenyegető tényezőkre, továbbá oktatni és tudatosítani bennük a megfelelő viselkedési formát a megelőzés és észlelés tekintetében.

2.1.2. A képzések hatásosságának mérése

Ahhoz, hogy a szervezet megbizonyosodjon a képzések/oktatások hatékonyságáról és hatásosságáról, célszerű egy komplex, előzetes és utólagos ellenőrzési rendszert, folyamatot is kialakítani. E folyamat kialakítása során a képzésen elhangzottak gyakorlati ellenőrzését kell megvalósítania a szervezetnek, mely történhet a tényleges munkafolyamatok helyszíni, személyes vizsgálatával, vagy komplex, előzetes és utólagos tesztek és ellenőrző kérdések formájában.

A képzések során elhangzottak betartását biztosítandó, célszerű megalkotni az ellenőrző, és a szükség esetén alkalmazható szankcionáló rendszert. Az ellenőrzések és a szankcionálás lehetőségének alkalmazásával a szervezet dolgozói hajlamosabbak felismerni és átérezni a képzéseken elhangzottak szükségességét, így nagyobb valószínűséggel fogják helyesen, és a szabályozóknak valamint a biztonsági szükségleteknek megfelelően végrehajtani napi munkafolyamataikat. A szabályok betartatásával biztosítható a bevezetett biztonsági, védelmi intézkedések által várt magasabb szintű információ- és informatikai biztonság megteremtése.

2.2. Információbiztonság-tudatosság program – komplex képzési koncepció, nagyobb szervezetek számára

A koncepció egy olyan átfogó, 5+1 szintű információbiztonsági-tudatosság növelési programot vázol fel, mely teljes körűen, valamint hosszú távon képes fejleszteni egy szervezet információbiztonsági szintjét, illetve annak felhasználóinak információbiztonság-tudatosságát.

Az információbiztonság-tudatosságnövelési program magában foglalja az adott szervezet általános felhasználóinak, kiemelt felhasználói jogokkal rendelkező vezetőinek, IT üzemeltetőinek, IT fejlesztőinek információbiztonsági tudatosítását, valamint egy olyan szervezeten belüli szakértői csoport kialakítását, mely a későbbiekben ún. „train the trainer" alapon önállóan képes tovább fejleszteni a szervezet más felhasználóinak, üzemeltetőinek, fejlesztőinek információbiztonsági-tudatosság szintjét – illetve a programokat támogató e-learning lehetőségeket.

2.2.1. Általános felhasználói szint - „Ön érték vagy kockázat a szervezet számára?"

A képzés elsődleges célja az általános felhasználók információbiztonság-tudatossági szintjének emelése, tudatosságának erősítése. Az előadások anyaga a szervezet információbiztonsági igényeinek és elvárásainak megfelelően kerül felépítésre és összeállításra.

Az információbiztonsági tudatosítás minden felhasználói szintű munkavállaló számára ajánlott – egyenként 60 perces élő előadások keretein belül, melyet a későbbiekben e-learning eszközök támogatásával célszerű szinten tartani, frissíteni, valamint továbbfejleszteni.

A felhasználói szintű biztonsági tudatosság alapja a gyakorlatban a szervezet információbiztonsági politikája/szabályzata és az abban megfogalmazott célok. A képzés előadásainak feladata a felhasználók gondolkodásmódját oly módon formálni, hogy az előadás meghallgatása után minden felhasználó komolyabban és tudatosabban kezelje a szervezet üzleti és egyéb természetű adatait, illetve törekedjen azok védelmére, a saját informatikai tudásszintjének megfelelően.

Az egyes előadásokon felmerülő témák koncepcionálisan az alábbi hármasság köré szerveződnek: people, process, technology – emberi tényezők, folyamatok, technológia, továbbá hogy ezek az egymástól igen különböző tényezők milyen módon integrálhatóak egymásba annak érdekében, hogy a szervezet információ technológiai potenciálját szervezeti

szinten biztonsági szempontból növelni lehessen. Az emberi tényező a szervezet munkavállalóit, illetve a szervezet informatikai rendszerének felhasználóit jelenti, akik feladata egy biztonsági szempontból tudatos munkakörnyezet kialakítása és fenntartása. A folyamatok és az azokhoz tartozó policy-k/szabályzatok a szervezetet, mint szervezeti egységet jelenítik meg, és modellezik azt, hogy a szervezet hogyan viszonyul a saját információ- és informatikai biztonságához, illetve milyen intézkedéseket hoz a biztonság növelése érdekében, és azok az intézkedések a mindennapokban hogyan jelennek meg. A technológia azon eszközök összessége, amelyeken a szervezeti biztonsági intézkedések a mindennapokban megvalósulnak.

A fentiek mellett további, de sok esetben nem kisebb jelentőségű témák is említésre kerülnek a képzés során.

Social engineering – az emberi tényezőre hívja fel a figyelmet, arra világítva rá, hogy a szervezet munkavállalói és informatikai rendszerének felhasználói milyen módokon manipulálhatóak annak érdekében, hogy esetlegesen bizalmas szervezeti adatokat, információt adjanak ki. A social engineering tudatosítás része egy olyan gyakorlati útmutató, mely megvilágítja annak módját, hogy a szervezet felhasználói milyen módon ne váljanak áldozataivá egy lehetséges social engineering támadásnak.

Networking – főként a személyes és szervezeti, üzleti jellegű vagy egyéb érzékeny információ megosztásával foglalkozik, jellemzően valamely internetes közösségi felhasználás vonatkozásában, különös tekintettel arra, hogy a szervezet felhasználói gyakran nem szándékosan és nem tudatosan osztanak meg bizalmas adatokat másokkal interneten, illetve teszik azokat publikussá, ahelyett hogy azokat bizalmasan kezelnék. A networking tudatosítás az előbbiek elkerülésére ad gyakoralti útmutatót.

Phishing – információszivárgás, ebben a témában azon jelek tudatosítása kap kiemelt hangsúlyt, melyek arra utalnak, hogy személyes vagy üzleti/érzékeny adatok szivárognak ki és kerülnek rosszindulatú felhasználók birtokába, akik ezekkel az adatokkal esetlegesen képessé válnak bármilyen károkozás elkövetésére a szervezettel vagy annak felhasználóival szemben. A phishing tudatosítás az előbbiek elkerülésére ad gyakorlati útmutatót.

A képzés során ezen a ponton a szervezeti szintű információbiztonság egy elengedhetetlen eleme tudatosításra kerül, miszerint a felhasználóknak bármely kétség, gyanú, vagy kérdés felmerülése esetén a szervezet felelős informatikai szakembereihez kell és szükséges fordulniuk, az adott probléma elkerülése, illetve rosszabb esetben megszüntetése

érdekében. Ehhez a szervezetnek előzetesen ki kell jelölnie az ilyen esetekben felelős és segítséget nyújtani képes szakembereit, akik szakértői útmutatást nyújtanak, illetve a gyakorlatban segítik a szervezeti információbiztonsági intézkedések, policy-k, szabályzatok alkalmazását. Ez a felelős jellemzően az információbiztonsági vezető.

2.2.2. Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők tudatosítása

Hosszú távú tapasztalatok mutatják, hogy egy szervezet dolgozóinak információbiztonság-tudatossága akkor és úgy növelhető a leghatékonyabban, ha a biztonsági tudatosság javítására szolgáló intézkedések a szervezet felsővezetésének teljes támogatásával valósulnak meg, illetve ha a felsővezetők maguk is szem előtt tartják az információ biztonságát.

A javasolt képzési program második szintje a felsővezetői szint, melynek keretein belül a legkomplexebb, legátfogóbb, szervezeti szintű információbiztonsági koncepciót ismerhetik meg a szervezet felsővezetői, az ún. „HumanFirewall" koncepció[10] keretein belül. Erre azért van szükség, hogy a szervezet döntéshozó pozícióban lévő vezetői megismerjék, hogyan tudják az információbiztonságot döntéseik során szemponttá tenni, és hogy azt egyre inkább szemponttá is tegyék, valamint azért, hogy beosztottaik információbiztonsági képzéseit átlássák, és támogassák, illetve hosszú távú, rendszeres elvárássá tegyék azt. A felsővezetői támogatás fontossága különösképpen igaz a különféle biztonsági „policy-k", szabályzatok elkészítésével, elfogadtatásával, és azok napi szintű alkalmazásával kapcsolatban.

2.2.3. Szakértői képzés – „system hardening", sérülékenységmenedzsment üzemeltetők számára

A szakértői képzés koncepciójában különbözik az általános felhasználóknak illetve a kiemelt felhasználói jogokkal rendelkező vezetőknek szánt ismertető jellegű képzésektől. Az eltérés lényege abban fogalmazható meg leginkább, hogy a szakértői szintű információbiztonság-tudatosság képzés koncepcionálisan közelíti meg az informatikai rendszer lehetséges sérülékenységeit, kialakítja a komplex, sérülékenységmenedzsment megközelítést az eseti sérülékenységek elhárítására törekvő szakmai viselkedés helyett, így a

[10] https://blogs.rsa.com/configuring-the-human-firewall/

szervezet informatikai rendszer adminisztrátorai, működtetői, belső fejlesztői számára javasolt.

A szakértői képzés optimálisan 4 hetes, tematikájában a komplex szervezeti szintű információ technológiai és informatikai rendszerek, kockázati tényezők, valamint olyan lehetséges támadási, behatolási technikák bemutatására koncentrál, melyek a szervezet számára információbiztonsági szempontból veszélyt jelentenek.

A szakértői képzés akkor a leghatékonyabb, ha összekapcsolódik egy szervezeti szintű sérülékenységvizsgálat projekttel, és annak eredményeit beépítve a tematikába, a szervezet informatikai rendszereinek valós sérülékenységeit bemutatva, azokra szorosan épülve mutatja be azok lehetséges és szükséges megerősítési módszereit. Egy valós projekt eredményeire támaszkodva a rendszert működtető szakértők képessé válnak arra, hogy a projekt kimenetét képező jelentést szakmailag feldolgozzák, emellett konkrét esettanulmányokon keresztül sajátíthatják el azokat a módszereket, taktikákat és stratégiákat, amelyekkel hatékonyan és eredményesen ismerhetik fel, előzhetik meg, és védhetik ki a rosszindulatú támadásokat.

A képzés alatt javasolt a következő területek áttekintése: historikus megközelítés, a szervezet sérülékenységvizsgálat projekt eredményeinek ismertetése, incidensek kezelése, támadási technikák, védelmi technikák (webes alkalmazások védelme, belső hálózat védelme, wi-fi hálózat védelme), összefoglalás. Amennyiben a szervezet informatikai rendszerét vidéki telephelyeken is üzemeltetik, az ezeket üzemeltető szakértők számára és speciálisan az ő feladataikra külön tematika állítható össze, a képzés részeként. (Megjegyzés: a szakértői tréning legrövidebb javasolt időtartama 1 hét. 1 hetes tréning esetén a fenti tematika egyes elemei 1-1 nap alatt áttekintésre kerülnek.)

Tudásgarancia

A szakértői képzések vizsgával zárulnak, sikeres teljesítés esetén a szakértők számára a képzést megvalósító oktató központ oklevelet állít ki, valamint a képzés során megszerzett tudás megtartását a későbbiekben meghatározott periódusonként – jellemzően évente – e-learning módszerekkel ellenőrzi, az egyes szakértők tudásszintjének változásáról visszajelzést ad a szervezet számára. Amennyiben szükséges, szakmai továbbképzések megtartására, illetve a korábbiakban megszerzett tudás célzott fejlesztésére is célszerű lehetőséget biztosítani.

2.2.4. Szakértői képzés – a biztonságos fejlesztés szemszögéből

A fejlesztői képzés céljában és felépítésében nagyon hasonló az előbbiekben bemutatott szakértői-üzemeltetői információbiztonság-tudatosság növelését célzó képzéshez. A fejlesztői szintű információbiztonsági képzés koncepcionálisan közelíti meg az informatikai rendszer lehetséges sérülékenységeit, kialakítja a biztonságos fejlesztés megközelítést az eseti sérülékenységek elhárítására utólagosan törekvő szakmai viselkedés helyett, így alapjaiban képes átformálni egy szervezet által használt informatikai rendszerek felépítésének módjait, különös tekintettel a webes alkalmazásokra.

Napjaink egyik legnagyobb információ biztonsági fejlesztést igénylő területe a webes alkalmazások, ezek a napjainkban jellemzőnél biztonságosabbá tétele, eleve biztonságos kialakítása elengedhetetlen, mivel elmondható, hogy egy átlagos szervezet átlagos felhasználója informatikai érintettségű tevékenységének meghatározó részét webes felületeken keresztül végzi. Ehhez alkalmazkodva a szervezetek saját webes alkalmazásainak fejlesztését végző szakemberek kiemelten magas szakmai szempontok alapján történő információbiztonsági tudatosítása és tudatosságának növelése a szervezet elemi érdeke.

A szakértői képzés optimálisan 4-6 hetes, tematikájában a komplex szervezeti szintű webes alkalmazások, azok kockázati tényezői, valamint olyan lehetséges támadási, behatolási technikák bemutatására koncentrál, melyek a szervezet számára veszélyt jelentenek információbiztonsági szempontból.

Tudásgarancia

A szakértői képzések vizsgával zárulnak, sikeres teljesítés esetén a szakértők számára a képzést megvalósító oktató központ oklevelet állít ki, valamint a képzés során megszerzett tudás megtartását a későbbiekben meghatározott periódusonként – jellemzően évente – e-learning módszerekkel ellenőrzi, az egyes szakértők tudásszintjének változásáról visszajelzést ad a szervezet számára. Amennyiben szükséges, szakmai továbbképzések megtartására, illetve a korábbiakban megszerzett tudás célzott fejlesztésére is célszerű lehetőséget biztosítani.

2.2.5. Az informatikai biztonság kialakításáért felelős személyzet információbiztonság-tudatosság képzése

Az általános (és szakértői) információbiztonság-tudatosítás képzés mellett, melynek mindenkire vonatkoznia kell a szervezetben, különleges információbiztonsági képzés is

szükséges az informatikai biztonsággal foglalkozó személyzet számára. Az információbiztonsági képzés mélységének az informatikának a szervezeten belüli általános fontosságához valamint a tendelkezésre álló technikai lehetőségekhez kell igazodnia, és az adott szerep információbiztonsági követelményeinek megfelelően kell változnia. Amennyiben szükséges, sokkal kiterjedtebb oktatást, például egyetemi kurzusokon való részvételt is biztosítani kell az érintett dolgozók számára.

A különleges biztonsági képzésre küldendő személyzet kiválasztásakor a következőket célszerű figyelembe venni:

- az informatikai rendszerek tervezésében és fejlesztésében kulcsszerepet játszó személyzet (ld. 2.2.4 Szakértői képzés – a biztonságos fejlesztés szemszögéből c. fejezet),
- az informatikai rendszerek üzemeltetésében kulcsszerepet játszó személyzet (ld. 2.2.3 Szakértői képzés – „system hardening", sérülékenységmenedzsment üzemeltetők számára c. fejezet), és az
- szervezeti, projekt és rendszerszintű informatikai biztonsági vezetők.

2.2.6. Szervezeten belüli információbiztonsági tudatosítást végző szakértői oktató csoport kialakítása – „train the trainer" koncepció

Napjainkban nagyobb szervezeteken belül joggal merül fel az igény egy olyan szervezeten belüli szakértői csoport kialakítására, mely a későbbiekben önállóan képes közvetíteni az elsődleges képzés során megismert információbiztonság-tudatosság alapelveit, így képes továbbfejleszteni a szervezet más felhasználóinak, üzemeltetőinek, fejlesztőinek információbiztonsági tudatossági szintjét, belső képzéseken keresztül.

Ezen szervezeten belüli oktató csoport kialakítása ún. „train the trainer" alapon történik, melynek során célszerűen komoly szakmai és oktatási tapasztalattal rendelkező, adott esetben hazai és nemzetközi elismertségnek örvendő szakértők készítik fel a szervezet által kijelölt oktatókat az információbiztonság-tudatosság alapelveinek közvetítésére, általános felhasználói, kiemelt felhasználói jogokkal rendelkező vezetői, üzemeltetői, valamint felhasználó szinteken egyaránt.

2.2.7. E-learning eszközök alkalmazása az információbiztonság-tudatosság képzési program különböző elemeiben, különös tekintettel az új belépőkre, a biztonsági tudatosság szintjének mérésére, valamint a biztonsági szabályzatok tudatosítására

Szakmai tapasztalatok alapján elmondható, hogy a leghatékonyabb képzési módszer az élő előadás. Mégis, az e-learning módszerek megjelenése óta egyre nagyobb az érdeklődés ezek alkalmazhatósága és hatékonysága iránt. A fent említett képzési szintek közül e-learning módszerek sikeresen alkalmazhatóak a szervezet felhasználói szintű dolgozóinak, valamint a szakértőinek a korábban, élő előadás sorozatokon megszerzett információbiztonság-tudatosságának mérésére, meghatározott időszakonkénti frissítésére, és kisebb részleteiben annak emelésére, kiegészítésére, akár egyénenként is, tetszőleges időpontban.

A gyakorlatban a legátfogóbban az általános és a szervezet speciális információbiztonsági igényeire szabott élő előadás és az arra szorosan ráépülő, tematikus e-learning anyagok kombinációja emeli leghatékonyabban a biztonsági tudatosság szintjét. Jellemzően az élő előadás után meghatározott időközönként összefoglaló jellegű e-learning módszerekkel (video és írásos (elektronikus) anyagok segítségével) az általános felhasználók és a szakértők alapvető biztonsági ismeretei és tudatossága először frissítésre, majd újraellenőrzésre, adott esetben a szervezet újabb információbiztonsági igényeinek megfelelően kiegészítésre kerülnek. Ezek a képi illetve elektronikus anyagok hatékonyan használhatóak új belépők biztonsági alapképzése során is, egyénenként és kisebb csoportokban egyaránt.

Lehetőség van külön, az információ biztonsági szabályzatok megismertetését, azok fontosságának tudatosítását, és mindennapi alkalmazásukat célzó video oktató anyagok elkészítésére is, gyakorlati útmutató jelleggel. Ezekhez is készíthetőek ellenőrző, és újabb ismereteket tartalmazó kiegészítő modulok is.

2.2.8. Információbiztonság-tudatosság mátrix

A „HumanFirewall” koncepció (ld. 2.2.2. Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők tudatosítása c. fejezet) szervezeti szinten a moduláris jelleggel, mátrix-szerűen összeállított e-learning anyagok alkalmazásával válik teljessé, mert így teljes mértékben személyre szabhatóvá és oktathatóvá válik az egyes munkakörök betöltőitől elvárt tematikájú és szintű információbiztonság-tudatosság, és ennek a tudatosságnak a

meghatározott időközönkénti ellenőrzése, valamint frissítése és kiegészítése is, általános és szakértői szinten egyaránt.

2.2.9. Az információbiztonság-tudatosság képzés értékelésének alapja és módszere

A képzés hatékonysága és a szervezet dolgozói információbiztonság-tudatosságának növekedése hasonló módon mérhető. Minden egyes élő előadáshoz és video illetve elektronikus kiegészítő oktatási anyaghoz (e-learning) tematikájában illeszkedő, statisztikai alapokon nyugvó kiértékelő modul társítható. Az értékelő modul szöveges és grafikonos formában egyaránt képes leképezni a dolgozók biztonsági tudatosságának minőségét és mértékét, kvantitatív és kvalitatív elemzési módszerek alapján.

A gyakorlatban általános felhasználói és szakértői szinten egyaránt, egy sorozaton belül az első képzési alkalom elején és az utolsó képzési alkalom végén kontroll mérésekre kerül sor (egy alkalmas képzések esetén a képzési alkalom kezdetén és végén kerül sor a kontroll mérésekre). A kontroll mérések alapját a tudatosság kezdeti szintjét, majd a képzés végét követően a tudatosság megváltozott szintjét mérő kérdések feltételét, majd azokra a résztvevők által adott válaszok kiértékelését jelentik.

A (kezdeti és végső) értékelő kérdésekre adott válaszok szemantikus kiértékelése, illetve maga az eredmény jelenti az alapot a szervezet általános biztonsági tudatossági szintjének megállapításához. Minden további, csoportos képzés illetve képzés sorozat alkalmával újabb mérésekre kerül sor, és ezek eredményei összevetésre kerülnek a korábbi mérési eredményekkel, a fent említett módszerek alapján. Így rendszeres időközönként, vagy igény szerint egyes képzéseket követően a szervezet vezetése objektív áttekintést kaphat egyrészt a képzések hatékonyságáról, másrészt a dolgozók/felhasználók biztonsági tudatossági szintjéről is, szervezeti szinten.

Kiegészítő modulként lekérdezhető az is, hogy a szervezet informatikai szakértői milyennek látják a szervezet informatikai biztonságát, hogyan változtatnák azt, és milyen új, szervezeti szintű intézkedések bevezetését tartanák/tartják szükségesnek. Ez a mérési modul is ismételhető, akár rendszeresen, akár esetileg, a szervezet igényeinek megfelelően.

2.3. Képzési programok – gyakorlati megközelítés

A szervezet valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is célszerű oktatásban részesíteni a saját feladatukkal kapcsolatban lévő információbiztonsági szabályzatokról, eljárásokról, feladatokról és az őket érintő információbiztonsági

felelősségekről. A szervezetnek olyan információbiztonság-tudatosító programokat célszerű megvalósítani, melyek magukba foglalják az információbiztonság napi szintű kezelési alapelveit, illetve a legalapvetőbb gyakorlati megközelítéseket, lépéseket.

E képzések magukban foglalják a biztonsági követelményeket, a jogi felelősséget – és az érvényes törvényi előírásokat –, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. Témák tekintetében kezdetben alapszinten szükséges megértetni az információbiztonsághoz kapcsolódó feladatokat, például: jelszavak kezelése, alapvető fizikai biztonsági intézkedések, e-mail használati kérdések, vírusvédelem, illetve magasabb szinten: a tűzfalak konfigurálása, valamint az információbiztonságot érintő események kezelése.

Ennek részeként kiemelten fontos a felhasználók megfelelő felvilágosítása a biztonsági eljárások és az adatfeldolgozó eszközök helyes használata tekintetében, a lehetséges információbiztonsági kockázatok minimalizálása érdekében. A felhasználóknak ismerniük kell az információbiztonsághoz kötődő felelősségüket is. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani.

Az információbiztonság-tudatosság növelését célzó gyakorlati képzések első szakaszát azelőtt célszerű lefolytatni, mielőtt a felhasználók megkapnák a hozzáférési jogot (jogosultság) azon informatikai rendszerekhez, vagy azon adatokhoz, mellyel később napi munkavégzésük során találkozhatnak.

Szükséges bevezetni a „szabályozók a gyakorlatban” („policy in practice”) tematikájú képzéseket is, annak érdekében, hogy a felhasználók – beleértve a felsővezetőket és a rendszerek üzemeltetőit is – képessé váljanak felismerni a szervezeti információ- és informatikai biztonsági szabályozóinak motivációit. Így válik esély arra, hogy a szabályozókat a felhasználók napi munkájuk során sikeresen, gondolkodva tartsák be.

Célszerű továbbá a szervezeten belül a képzést megelőzően kiosztani azokat a beosztásokhoz kötődő jogokat, szabályzókat és felelősségeket melyek az információbiztonsági feladatokkal kapcsolatosak.

2.3.1. Képzési terv

A felhasználók információbiztonság-tudatosság képzése Képzési Terven alapul. A szervezeten belül a Képzési Terv elkészítésére kijelölt személynek/szakértői csoportnak a szervezet információbiztonsági és informatikai vezetőivel – az informatikai biztonságpolitika

elveinek, valamint a saját hatáskörben meghatározott képzési elveknek megfelelően – a humánerőforrás-gazdálkodással, illetve a biztonsági vezetővel egyeztetve célszerű kidolgoznia a Képzési Tervet.

A Képzési Terv és (amennyiben rendelkezésre áll) a további képzési dokumentáció megfelelő fejezetei részletesen tartalmazzák az információbiztonság-tudatosság képzésre vonatkozó információkat.

2.3.2. Az informatikai rendszerek életciklusaihoz kapcsolódó információbiztonság-tudatosság képzések

Információbiztonsági és informatikai feljesztések, projektek során minden esetben célszerű ellenőrizni, hogy azokhoz szükséges-e különleges biztonsági képzést társítani. Valahányszor egy szervezetnél olyan tevékenységek vagy projektek kezdődnek, melyek speciális biztonsági követelményeket támasztanak, biztosítani kell a megfelelő biztonsági képzési program kialakítását és lebonyolítását még a projekt indulása előtt, lehetőség szerint még a tervezési szakasz folyamán.

3. Az információbiztonság irányítási szerepkörei és felelősségek – az Ibtv. által hozott változások[11]

Magyarország a világon élenjáróként, az elsők között alkotta meg a hazai állami és önkormányzati szervek elektronikus információbiztonságáról szóló, 2013. évi L. törvényt (közismertebb nevén Ibtv.), mely a következő bevezetőt tartalmazza: „A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."

Az Ibtv. – valamint a Nemzeti Kiberbiztonsági Stratégiáról szóló kormányhatározat – nyomán hazánkban 2013-tól kezdődően törvényi előírás és társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.

Ennek érdekében a törvény kötelezettséget állapít meg a szervezetek számára, kiemelten a szervezet vezetője, az elektronikus információs rendszer biztonságáért felelős személy számára.

3.1. A szervezet vezetőjének a feladata és felelőssége

A 2013. évi L. törvény (Ibtv.) 7. § 3. és 5. bekezdése alapján a szervezet vezetője jóváhagyja az adott szervezett biztonsági osztályba sorolását és felel a jogszabályoknak való megfelelőségéért, az adatok teljességéért és időszerűségéért. A szervezet vezetője továbbá indokolt esetben magasabb vagy alacsonyabb biztonsági osztályt is megállapíthat.

Az Ibtv. 11. § szerint a szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről. A védelem biztosítása magában foglalja:

- a jogszabályokban megfogalmazott követelmények teljesülésének a biztosítását,
- az elektronikus információs rendszer biztonságáért felelős személy kinevezését vagy megbízását, aki azonos lehet a Mavtv. szerinti biztonsági vezetővel,

[11] http://www.complex.hu/kzldat/t1300050.htm/t1300050.htm

- az információs rendszerekre vonatkozó informatikai biztonságpolitika és informatikai biztonsági szabályzat kiadását; az informatikai biztonsági stratégiának a meghatározását,
- annak a meghatározását, hogy a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra milyen szabályok vonatkoznak,
- gondoskodást az információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról, továbbá a biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatásáról,
- annak biztosítását, hogy a rendszer eseményei nyomon követhetőek legyenek,
- biztonsági esemény bekövetkezésekor a rendelkezésre álló erőforrások tükrében, a gyors és hatékony reagálást,
- hogy amennyiben a szervezet az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- hogy amennyiben a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
- a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatást,
- a rendszer védelme érdekében egyéb szükséges intézkedések elvégzését.

A szervezet vezetőjének a felelősségét befolyásolja az, ha jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót kell a szervezetnek igénybe venni.

Amennyiben az adott szervezet szakmai irányítását ellátó miniszter elektronikus információs rendszerekre vonatkozó ágazati informatikai biztonságpolitikát és az ágazati informatikai biztonsági stratégiát fogad el, a szervezet vezetője köteles ezeket figyelembe venni a fenti kötelezettségeinek a teljesítése során.

3.2. Az elektronikus információs rendszer biztonságáért felelős személy feladata és felelőssége

Az elektronikus információs rendszer biztonságáért felelős személy az Ibtv. 13. § alapján az alábbi feladatokkal és felelősséggel rendelkezik:

- feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést,
- felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért és ennek körében:
    - gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról, valamint a követelmények teljesüléséről a közreműködők irányában is,
    - elvégzi vagy irányítja a fentebbi tevékenységek tervezését, szervezését, koordinálását és ellenőrzését,
    - előkészíti az informatikai biztonsági szabályzatot,
    - előkészíti az információs rendszereknek a biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását,
    - véleményezi a rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
    - kapcsolatot tart a hatósággal és a kormányzati eseménykezelő központtal;
- bármely a törvény hatálya alá tartozó elektronikus információs rendszert érintő biztonsági eseményről a jogszabályban meghatározottak szerint tájékoztatni köteles a jogszabályban meghatározott szervet.

Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül elektronikus információbiztonsági szervezeti egység hozható létre, amelyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

Az elektronikus információs rendszer biztonságáért felelős személy a közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban jogosult tájékoztatást kérni, megfelelőség alátámasztásához szükséges adatokat, illetve a rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot bekérni.

A büntetlen előélet követelményének való megfelelést az elektronikus információs rendszer biztonságáért felelős személy a szervezettel fennálló jogviszonya keletkezését megelőzően köteles igazolni.

Az elektronikus információs rendszer biztonságáért felelős személy köteles részt venni a meghatározott rendszeres szakmai képzésen, továbbképzésen.

3.3. Nemzeti Elektronikus Információbiztonsági Hatóság feladata és felelőssége

A Nemzeti Elektronikus Információbiztonsági Hatóság az Ibtv. 14.§ alapján ellátja a törvény hatálya alá eső elektronikus információs rendszerek biztonságának a felügyeletét. Az informatikáért felelős miniszter által vezetett minisztériumi szervezeti keretbe került beágyazásra a Hatóság, amely önálló feladat- és hatáskörrel rendelkezik.

A Hatóság az alábbi feladatokkal és felelősségi körökkel rendelkezik az Ibtv. 14. § alapján:

- az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése, a jogszabályban meghatározott követelmények teljesülésének az ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala,
- az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése,
- kockázatelemzés elvégzése,
- a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása,
- javaslattétel ágazati kijelölő hatóság részére a nemzeti létfontosságú rendszerelem kijelölésére,
- az információs társadalom biztonságtudatosságának elősegítése és támogatása,
- együttműködés elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,
- kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,
- kapcsolattartás a Nemzeti Média- és Hírközlési Hatósággal, továbbá a kormányzati eseménykezelő központtal és az ágazati eseménykezelő központokkal,
- kormányzati incidens-kezelő munkacsoport irányítása,

- véleményezési jog gyakorlása a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,
- együttműködés a kormányzati eseménykezelő központtal, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal,
- együttműködés a Nemzeti Média- és Hírközlési Hatósággal és a Nemzeti Biztonsági Felügyelettel ha a biztonsági esemény vagy fenyegetés helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hálózatot, szolgáltatást vagy ilyen szolgáltatást nyújtó szervet érint,
- éves és egyedi jelentések készítése a Kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, és a kibervédelem helyzetével kapcsolatban.

A Hatóság feladatainak ellátásához szükségesen az Ibtv. 15.§ szerint nyilvántartja és kezeli az alábbi adatokat, amelyek kezelésének a célja a szervezetek kötelezettség-teljesítésének és a hatósági ellenőrzésnek biztosítása:

- a szervezet azonosításához szükséges adatokat, a szervezet elektronikus információs rendszereinek megnevezését, az elektronikus információs rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatait,
- a szervezetnek az elektronikus információs rendszer biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, meghatározott végzettségét,
- a szervezet informatikai biztonsági szabályzatát,
- a biztonsági eseményekkel kapcsolatos bejelentéseket.

Adattovábbítás a fentebbi nyilvántartásból csak a törvény eltérő rendelkezése alapján végezhető.

A nyilvántartás működtetésének megkönnyítése céljából a szervezetek kötelesek bejelenteni a fent felsorolt adatok változásait. Ha a szervezet a törvény hatálya alá tartozó tevékenységet már nem végez, ennek bejelentését követő 5 év elteltével a Hatóság köteles törölni a fentebb említett adatokat. A Hatóság 5 év elteltével köteles törölni a nyilvántartásból az eredetileg bejelentett adatokat, ha azokra a szervezet változást jelentett be.

Az Ibtv. 16. § szerint a Hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek. Ennek érdekében jogosult:

- az érintett szervezeteknél biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni, valamint a követelményeknek való megfelelőség megállapításához szükséges dokumentumokat bekérni,
- a biztonsági osztályba sorolást, a biztonsági szint megállapítását, vagy a védelmi intézkedéseket ellenőrizni, az ott feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,
- a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában ellenőrizni az információbiztonsági követelmények megtartását,
- hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervezni, valamint a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviselni Magyarországot.

Ha a szervezet nem költségvetési szerv és a jogszabályokban foglalt biztonsági követelményeket illetve az ehhez kapcsolódó eljárási szabályokat nem teljesíti, vagy nem tartja be, a Hatóság:

- köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ahhoz kapcsolódó eljárási szabályok teljesítésére;
- ha a felszólítás ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nem teljesülés esetén megismételhető.

Ha a szervezet költségvetési szerv, és a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, vagy nem tartja be, a Hatóság:

- köteles felszólítani a szervezetet a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok teljesítésére,

- ha a felszólítás ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti, a szervezetet felügyelő szervhez – amennyiben a szervezet azzal rendelkezik – fordulhat és kérheti a közreműködését,
- ha a felszólítás és a felügyelő szerv közreműködése ellenére a szervezet a jogszabályokban foglalt biztonsági követelményeket és az ahhoz kapcsolódó eljárási szabályokat nem teljesíti, információbiztonsági felügyelő kirendelését kezdeményezheti.

3.4. Az információbiztonsági felügyelő feladata és felelőssége

Információbiztonsági felügyelő kirendelésére akkor van lehetőség, ha adott költségvetési szerv felszólítás és a felügyelő szerv közreműködése ellenére a jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályokat nem teljesíti. Ezt az Ibtv. 16.§tartalmazza.

Az Ibtv. 17.§ alapján a felügyelő kirendelését a Hatóság kezdeményezi az informatikáért felelős miniszternél. A miniszter dönt a kirendelésről, a kirendelés visszavonásáról és látja el a felügyelő szakmai irányítását.

A NEIH kirendelésre vonatkozó javaslatának, a 301/2013. (VII. 29.) Korm. rendelet alapján, tartalmaznia kell a kirendelés indokait, a korábbi, az érintett szervezettel kapcsolatos intézkedéseit, a felügyelő személyét, a kirendelés időtartamát.

Az információbiztonsági felügyelő a fenyegetés elhárításához szükséges védelmi intézkedések eredményes megtétele érdekében a 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló rendeletben meghatározott intézkedéseket, eljárásokat javasolhat, a szervezet intézkedései tekintetében kifogással élhet. Az információbiztonsági felügyelő pénzügyi kötelezettségvállalásra nem jogosult.

Az információbiztonsági felügyelő az informatikáért felelős miniszter által vezetett minisztérium kormánytisztviselője, akinek a kormányzati szolgálati jogviszonyára a minisztériumban főosztályvezető-helyettesi munkakörben alkalmazott kormánytisztviselőre vonatkozó szabályokat kell alkalmazni. Információbiztonsági felügyelőnek az a személy nevezhető ki, aki rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és

szakképzettséggel, valamint legalább 3 év vezetői gyakorlattal, továbbá aki vállalja a kinevezést, illetve vele szemben nem merül fel kizárásra okot adó körülmény. A fentebb említett körülményeket a 301/2013. (VII. 29.) Korm. rendelet tartalmazza.

A miniszter a megbízólevél kiállításával a felügyelőt határozott időtartamra rendeli ki az adott szerv elektronikus információbiztonsági tevékenységének felügyeletére. A kirendelés meghosszabbítását a hatóság vezetője kezdeményezheti a kirendelés idejének lejárta előtt, legfeljebb egy alkalommal, a folyamatban lévő intézkedések lezárásáig. Egy felügyelő egyszerre több szervezethez is kirendelhető.

3.5. Nemzeti Biztonsági Felügyelet feladata és kötelessége

Az Ibtv. 18.§ alapján nemzeti Szakhatóságként a Nemzeti Biztonsági Felügyelet került kijelölésre. A Felügyelet két fő tevékenységi köre a sérülékenységvizsgálatok és a biztonsági események műszaki vizsgálatának elvégzése.

Az alábbi tevékenységeket a Felügyelet végezheti:

- éves ellenőrzési terv alapján, és az Ibtv. szerinti biztonsági szintbe és osztályba sorolás ellenőrzéseként Szakhatóságként a Hatóság megkeresésére, továbbá egyedi esetekben a Hatóság felkérésére az érintett szervezet vezetőjét előzetesen tájékoztatva sérülékenységvizsgálatot, valamint biztonsági események adatainak műszaki vizsgálatát végzi, valamint
- a szervezet felkérésére sérülékenységvizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi.

A Szakhatóság a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálat lezárását követően haladéktalanul tájékoztatja a vizsgált szervezet vezetőjét és a Hatóságot.

A Felügyelet további feladatai:

- hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervez, illetve a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviseli Magyarországot,
- véleményezési jogot gyakorol a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,

- együttműködik a kormányzati eseménykezelő központtal.

3.6. A Kormányzati Eseménykezelő Központ feladata és kötelessége

A Kormányzati Eseménykezelő Központ feladatait az Ibtv. 19-20. § szabályozza. A Központot a törvényben foglalt biztonsági események kezelésére lett létrehozva és a katasztrófák elleni védekezésért felelős miniszter irányítása alá helyezve.

Az eseménykezeléssel kapcsolatos feladatkörök megoszlanak a Központ és az Ágazati Eseménykezelő Központok között az Ibtv. 19.§ szerint. A Kormányzati Eseménykezelő Központ lesz illetékes az Ibtv. 2. § (1) bekezdésben meghatározott szervek esetében. Ágazati Eseménykezelő Központok létrehozása szükséges az Ibtv. 2. § (4) bekezdésében meghatározott szervezetek és az önálló szabályozó szervek eseménykezelési feladatainak ellátására.

Az Ágazati Eseménykezelő Központ a biztonsági eseményekhez kapcsolódó és a nemzetközi együttműködés során tudomására jutott biztonsági események adatait köteles haladéktalanul a Kormányzati Eseménykezelő Központ részére továbbítani.

A Kormányzati Eseménykezelő Központ az Európai Kormányzati Eseménykezelő Csoport által akkreditált nemzeti eseménykezelő központként részt vesz a kormányzati eseménykezelő központok nemzetközi együttműködésében. Az Ágazati Eseménykezelő Központok a fenntartó döntése alapján részt vehetnek az eseménykezelő központok nemzetközi együttműködésében, és e célból akkreditálhatóak.

Az Ágazati Eseménykezelő Központok a Kormányzati Eseménykezelő Központtal, mint nemzeti eseménykezelési koordinátorral, valamint a Nemzeti Kiberbiztonsági Koordinációs Tanáccsal együttműködnek.

A Kormányzati Eseménykezelő Központ az alábbi további feladatokat köteles ellátni az Ibtv. 20. § alapján:

- az Ágazati Eseménykezelő Központok szakmai támogatása,
- a nemzetközi eseménykezelési együttműködésekben Magyarország képviselete és az Ágazati Eseménykezelő Központok tájékoztatása a nemzetközi szervezetektől tudomására jutott információbiztonságot érintő eseményekről, fenyegetésekről,
- a szervezetekkel való kapcsolattartás a bejelentett biztonsági események fogadására, valamint az azok kezeléséhez szükséges operatív intézkedések megtétele és koordinálása,

- napi rendszerességű hálózatbiztonsági helyzetértékelések elvégzése,
- folyamatosan elérhető 24 órás ügyelet működtetése,
- a biztonsági események kivizsgálása során a biztonsági események adatai műszaki vizsgálatának elvégzése,
- a szervezeteknél előforduló biztonsági események adatainak gyűjtése, ezekről negyedévente jelentés készítése a Nemzeti Kiberbiztonsági Koordinációs Tanács részére,
- elemzések, jelentések készítése a Nemzeti Kiberbiztonsági Koordinációs Tanács részére a hazai és nemzetközi információbiztonsági irányokról,
- azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági eseményekről, ezek magyar nyelvű megjelenítése, illetve a nemzetközileg publikált sérülékenységek közzététele a Központ honlapján,
- hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatok szervezése, illetve felkérésre részvétel a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon, valamint
- együttműködés a Hatósággal és a Nemzeti Biztonsági Felügyelettel.

Az Ágazati Eseménykezelő Központok az általuk támogatott ágazatok tekintetében ellátják a Kormányzati Eseménykezelő Központ feladatait, kivéve ez alól a fentebb említett szakmai támogatást, amelyet a Központ lát el, valamint a nemzetközi CERT együttműködésben Magyarország képviseletét.

3.7. Nemzeti Kiberbiztonsági Koordinációs Tanács

A kormányzati koordináció biztosítására került létrehozásra a Nemzeti Kiberbiztonsági Koordinációs Tanács, amely a Miniszterelnökséget vezető államtitkár vezetése alatt áll, akinek a munkáját a Miniszterelnökség által delegált kiberkoordinátor támogatja.

A Tanács az Ibtv. 21. § feladatszabása alapján:

- összehangolja a törvény hatálya alá tartozó szervezetek együttműködését a kiberbiztonsággal összefüggő feladatok ellátásában,
- elősegíti a kiberbiztonság szabályozását, valamint a kiberbiztonság ágazati munkacsoportjainak munkáját,

- támogatja a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) munkáját,
- támogatja a források hatékony felhasználását,
- figyelemmel kíséri Magyarország Nemzeti Kiberbiztonsági Stratégiájának végrehajtását és erről jelentést tesz a Nemzetbiztonsági Kabinetnek,
- elősegíti a kiberbiztonságot érintő egységes magyar kormányzati álláspont kialakítását és hozzájárul Magyarország nemzetközi politikai képviseletéhez.

A Tanács munkáját az általa felkért szakmai, illetve nem kormányzati gazdasági vezetőkből álló Fórum és az ágazati kormányzati és nem kormányzati együttműködést biztosító kiberbiztonsági munkacsoportok segítik javaslattételi joggal és véleményezési lehetőséggel.

A külpolitikáért felelős miniszter figyelemmel kíséri és a kormány feladat- és hatáskörrel rendelkező szervei, valamint a Tanács felé jelzi az európai uniós kibertér-politikával kapcsolatos eseményeket és döntéseket, és a külpolitikáért való felelőssége körében képviseli a magyar álláspontot a nemzetközi fórumokon és a kétoldalú kapcsolatokban.

4. Az információbiztonsági szerepkörök és felelősségek változása – változás-menedzsment[12]

Egy szervezet információbiztonságát a hatályban lévő törvényi előírások és a tényleges munkafolyamatok során megvalósított információkezelési gyakorlat mellett az alkalmazott változás-menedzsment folyamatok és megoldások is meghatározzák, melyek szerencsés esetben a folyamatok megfelelő szintű betartását eredményezik. Az irányítási/szervezeti struktúrára, szabályozókra, és magukra a folyamatokra fordított figyelem előmozdítja a megfelelő, avagy megkívánt információbiztonsági szint fenntartását.

A szervezetnél kialakított és alkalmazott változás-menedzsment folyamatok elősegítésére adoptált formalizált irányítási struktúra egy fegyelmezettebb, hatékonyabb – és személyi változások esetén kevésbé sérülékeny – infrastruktúrát eredményez. A gyakorlatban a formalizálás folyamata szervezeten belüli kommunikációt igényel, megfelelően dokumentált folyamatleírásokat és egyéni munka- és felelősségi körök meghatározását vonva maga után (mely az automatizált eszközök és folyamatok esetén is érvényes, amennyiben ilyenekkel a szervezet rendelkezik).

Az egyéni felelősségi körök meghatározása ebben az esetben úgy kell, hogy megtörténjen, hogy az figyelembe veszi, jobb esetben elkerülhetővé teszi a lehetséges személyi változások nyomán fellépő esetleges információhiányt, illetve előre tisztázza a változások esetén átadandó és esetlegesen felülvizsgálandó felelősségi és tevékenységi köröket, munkafolyamatokat. A változás-menedzsment az egyének/munkavállalók/felhasználók esetén nem csak a fontosabb munkafolyamatok, projektek szempontjából hangsúlyos, hanem a felhasználók által kezelt adatok, információ, adatbázis hozzáférések, stb. biztonságos kezelése szempontjából is jelentős.

Azon szervezetek esetén, ahol változás-menedzsment folyamatok és megoldások nem kerültek bevezetésre, a megfelelő hatáskörrel rendelkező, azaz az információbiztonságért felelős vezetők feladata e folyamatok szervezeten belüli kialakítása és bevezetése. A megfelelő szabályozók és folyamatok meghatározásával ezen szervezetek is felelősséggel és

[12] ISO 27001

tervezhető módon, illetve gyorsabban és egyértelműbb módon képesek új üzletmeneti kihívásoknak megfelelni.

A fenti jellegű szabályozók célja a változás-menedzsment számára a magaszszintű irányelvek megfogalmazása és a követendő irány kijelölése. A változás-menedzsment szabályzat célszerűen előírja a változás-menedzsment és kapcsolódó ellenőrzési stratégiák alkalmazását információbiztonsági kockázatok felmerülése esetén:

- amennyiben az információ sérül és/vagy megsemmisül,
- az informatikai rendszer teljesítőképessége sérül és/vagy működésképtelenné válik,
- visszaesés következik be a szervezet termelékenységét érintően,
- jó hírnév elvesztése következhet be.

A változás-menedzsment további szükséges lépéseiről a vonatkozó ISO 27001 dokumentáció csomag adhat felvilágosítást.

5. Kockázati tolerancia – üzletmenet-folytonossági szempontból

A megfelelő szintű információ- és informatikai védelem meghatározása nem a piacon elérhető legjobb technológia beszerzését és alkalmazását jelenti. Nem minden esetben szükséges a legújabb és legdrágább fejlesztésű eszközöket beszerezni és beépíteni az adott rendszerbe – a beszerzett és felépített védelmi technológiának valójában sokkal inkább az aktuális szükségletekhez kell igazodnia. A biztonsági intézkedések ár-érték aránya egy adott szint fölött aránytalanul eltolódhat, így a gyakorlatban a szervezetek inkább felvállalnak egy bizonyos kockázatot a „fölösleges", vagy nem finanszírozható kiadások elkerülése érdekében.

5.1. Definíciók[13]

Kockázat[14],[15]: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Kockázatelemzés[16],[17]: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

Kockázatkezelés[18]: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása.

Kockázatokkal arányos védelem[19]: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

[13] http://en.wikipedia.org/wiki/IT_risk
[14] http://en.wikipedia.org/wiki/Risk
[15] http://en.wikipedia.org/wiki/IT_risk_management
[16] http://en.wikipedia.org/wiki/Risk_assessment_and_management
[17] http://en.wikipedia.org/wiki/IT_risk_management
[18] http://en.wikipedia.org/wiki/IT_risk_management
[19] http://en.wikipedia.org/wiki/IT_risk

5.2. Kockázatfelmérés, avagy megfelelőség-vizsgálatok (audit, compliance)[20]

Egy szervezeten belül a vagyonelemeket érintő kockázatok felmérését – itt elsősorban üzleti kockázatok felméréséről van szó – a szervezet vagyonleltárának elkészítését követően célszerű elvégezni. Ehhez olyan módszertant kell kialakítania illetve alkalmaznia a szervezetnek, mely illeszkedik a működés meghatározott információbiztonsági, jogi és szabályozási követelményeihez. A választott kockázat felmérési módszertant továbbá úgy kell kialakítani, hogy az biztosítsa a kockázatfelmérések során született eredmények összehasonlíthatóságát és megismételhetőségét.

A kockázatok felmérése érdekében a szervezetnek fenyegetettség- és sebezhetőség-elemzést kell végrehajtania – ezek megfelelőség vizsgálatok, jellemzően üzleti szempontú auditok végrehajtása során. A fenyegetettség és sebezhetőség-elemzés során végre kell hajtani a vagyonelemeket feldolgozó informatikai erőforrások feltérképezését és összerendelését az egyes vagyonelemekkel, továbbá végrehajtani az erőforrások sebezhetőség-vizsgálatát.

Az információvédelmet és a napi üzletmenetet kiszolgáló informatikai infrastruktúra megfelelőség-vizsgálatát szükséges mind a fizikai, logikai, mind a szervezeti biztonság részterületek vonatkozásában elvégezni. A vizsgálat során össze kell gyűjteni a szervezet informatikai erőforrásait, majd a kritikus információkat az erőforrásokhoz kell rendelni. A megfelelőség- illetve sebezhetőség-vizsgálatot a kritikus vagyonelemek feldolgozásában részt vevő minden informatikai erőforrásra el kell végezni.

Az egyes részterületek sebezhetőségét különböző módszerekkel lehet meghatározni: Szervezet, személyek esetén át kell vizsgálni a meglévő dokumentumokat, továbbá személyes interjúkkal meg kell győződni arról, hogy a munkavállalók mennyire ismerik az előírásokat, értékelni kell az alkalmazottak biztonságtudatosságának jelenlegi szintjét.

Sebezhetőségnek kell tekinteni: a hiányzó dokumentumokat, a létező, de a gyakorlatba be nem vezetett szabályzókat; a nem megfelelő minőségű szabályzókat; mindazon szabályokat, melyek végrehajtására nincsenek meg a személyi feltételek, valamint minden olyan esetet, amikor összeférhetetlenség áll fenn a végrehajtandó utasítás és

[20] http://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance

hozzárendelt felelős személy között (pl.: az adminisztrátor ellenőrzését az adminisztrátor önmaga végzi).

5.3. Kockázatelemzés

Az információ- és informatikai védelem szempontjából történő kockázatelemzés célja a lehetséges kapcsolat kiépítése a feltárt sérülékenységek és fenyegető tényezők között, a biztonsági hiányosságok, kihágások előfordulási valószínűségének meghatározása, az információvagyon biztonsági „kitettségének" a szervezet által vállalható és nem vállalható kockázatainak a meghatározása.

Tekintettel arra, hogy a biztonság a tudatosan felvállalt kockázatokon keresztül realizálódik, a szervezet felsővezetőinek a kockázatok vállalására vonatkozó döntései alapján szükséges kialakítani a szervezet információ- és informatikai védelmi infrastruktúráját, mechanizmusait.

A kockázatelemzés során a szervezet feladata, hogy megvizsgálja, hogy az egyes feltárt fenyegetések milyen sebezhetőségen keresztül, milyen támadási forgatókönyv szerint képesek kifejteni hatásukat, azaz milyen összefüggés állítható fel.

A fenyegetések valószínűsége és a sikeres fenyegetés által elszenvedhető kár mértéke alapján alapfenyegetettségemként el kell döntenie a szervezetnek, hogy az a szervezet számára elfogadható-e vagy sem, azaz eléri-e a vezetés által elfogadott és meghatározott kockázatkezelési szintet.

Az alkalmazott kockázatelemzési módszertant, továbbá a kockázatelemzés során feltárt kockázatok kezelési módjának szabályait dokumentumban kell rögzíteni.

A kockázatelemzés végrehajtását követően a szervezet rendelkezni fog az informatikai erőforrások sérülékenységeit kihasználó fenyegető tényezők listájával, valamint azok sebezhetőségekkel történő összerendelésével. Megismeri és meghatározza a feltárt fenyegető tényezők bekövetkezési valószínűségét, továbbá meghatározza az elfogadható és nem elfogadható, tehát a későbbiekben kezelendő kockázatok listáját.

5.4. Kockázatkezelés

A kockázatkezelési intézkedések célja azoknak a biztonsági kockázatoknak az elfogadható/méltányos költségen történő azonosítása, kézbentartása, minimalizálása vagy megszüntetése, amelyek hatással lehetnek az információs és informatikai rendszerekre.

A szervezetnek meg kell határoznia, és ki kell alakítania kockázatkezelési folyamatát, melyhez meg kell teremtenie a szabályozási környezetet olyan formában, mely tartalmazza a kockázatkezelés során kötelezően elvégzendő lépéseket, a kapcsolódó feladatokat és felelősségeket.

A szervezet által nem elviselhető kockázatok kezelésére ellenintézkedéseket vagy védelmi intézkedéseket kell foganatosítani. A védelmi intézkedések kidolgozása során javasolt, megvizsgálni a bevezetéshez szükséges idő és erőforrás ráfordítást, továbbá a költséghatékonyságot. Célszerű csoportosítani a védelmi intézkedés javaslatokat funkciójuk és hatásuk alapján, mely csoportok lehetnek hibamegelőző (preventív), hibaérzékelő (detektív) és hibajavító (korrektív) kontrollok.

A kockázatkezelés során bevezetett kontrollok, védelmi intézkedések, amennyiben teljes egészében nem szűntetik meg a kezelendő sebezhetőségeket, felvethetnek új fenyegetési lehetőségeket, esetleg az információbiztonsági rendszerben új sebezhetőségi pontok jelenhetnek meg, amelyek ún. Maradványkockázatot hordozhatnak magukban. Emiatt a kockázatkezelés során figyelemmel kell kísérni a bevezetett kontrollok hatásosságát, és amennyiben maradványkockázatok realizálódnak, akkor szükséges azokat szabályozott formában kezelni, újra a döntéshozó személy vagy fórum elé terjeszteni, és dönteni a maradványkockázatok kezelési módjáról.

A kockázatkezelés eredményeképpen a szervezet számára rendelkezésre állnak a kockázatok kezelésére kidolgozott védelmi intézkedések, melyek tartalmazzák a bevezetéshez szükséges erőforrásokat, a védelmi intézkedés bevezetésének ütemezését, továbbá a várható költségeket. A meghatározott védelmi intézkedések bevezetésének priorizálását végre kell hajtani, és a meghatározott prioritások alapján ki kell alakítani a védelmi intézkedések sorrendjét.

6. A szervezeti struktúra hatása az információbiztonság menedzsmentre (és annak hatása a szervezeti struktúrára)[21]

Az alábbi fejezet célja annak bemutatása, milyen kölcsönhatás áll fenn a szervezeti struktúra és az információbiztonság között.

Napjaink üzleti, üzletmeneti (működési) módszerei és a kapcsolódó trendek kihangsúlyozzák annak szükségességét, hogy az információbiztonsággal foglalkozni kell, mert az új trendek új kockázatokat hordoznak magukban.

6.1. A szervezeti struktúra hatása az információbiztonság menedzsmentre

A szervezetek – jellemzően költségcsökkentési okokból, vagy a szükséges szakértelem könnyebb „beszerzése" okán – egyre nagyobb mértékben szervezik ki bizonyos, sok esetben kulcsfontosságú folyamataik megvalósítását ún. harmadik félhez, avagy külső szolgáltatóhoz. Ez a folyamat egy kvázi kiterjesztett szervezetet hoz létre, melynek alkotó szervezeti egységei nagyon különböző technológiákkal, üzleti kultúrákkal, munkafolyamatokkal, és információbiztonsági nézetekkel, érzékenységgel rendelkeznek. Emellett jellemzően jelen vannak külső tanácsadók, távolról munkavégzők, és irodán kívüli, külső helyszínen dolgozó munkavállalók is, akik mindegyike – már csak a fizikai távollét okán is – újabb információbiztonsági kockázatokat jelenít meg (ld. 2.2.1. Általános felhasználói szint - „Ön érték vagy kockázat a szervezet számára?" c. fejezet).

Ebben a helyzetben elsődleges fontosságúvá válik a hatékony információbiztonsági kockázatkezelés képessége, így az információbiztonsági vezető szerepe is stratégiai fontosságúvá válik, de minimum jelentősen felértékelődik. Az információbiztonsági vezetés azonban többé már nem oldható meg egy munkavállaló kijelölésével és felelőssé tételével, elengedhetetlen az információbiztonsághoz kapcsolódó feladatok ellátására egy olyan, szakemberekből álló csapatot létrehozni, akik megfelelő információbiztonság-tudatossággal is

[21] http://digitalstrategies.tuck.dartmouth.edu/cds-uploads/publications/pdf/SecurityOrg.pdf

rendelkeznek egyéb informatikai szaktudásuk mellett (ld. 2.2.5. Az informatikai biztonság kialakításáért felelős személyzet információbiztonság-tudatosság képzése c. fejezet).

A felsővezetők, információbiztonsági vezetők, és a kijelölt, információbiztonsági szempontból tudatos „team" alapvetően három területen képes komoly hatást gyakorolni a szervezetre, ezek:

- Az információbiztonsági szint és az információbiztonsági fejlesztések hatékonyságának mérése, és hosszabb távon a kapott eredmények összehasonlíthatósága (benchmarking),
- a biztonság szempontú gondolkodásmód bevezetése a szervezeti kultúrába, valamint
- azon modell kialakítása, mely stratégiai beruházásnak tekinti az információbiztonságot.

Mindezek akkor is érvényesek, ha szükség van az információbiztonság kialakítására vagy gyökeres átalakítására – a szükséges feltételek hiánya miatt.

Az információbiztonsági vezetők számára jellemzően az alábbi területek jelentik a legnagyobb kihívást:

- A szervezet információbiztonság-tudatosságának növelése – illetve az információbiztonság értelmezése, mely nem feltétlenül az egyéni felhasználók tudatosságának kialakítását jelenti, hanem sok esetben a szervezet különböző egységeinek valódi információbiztonsági szükségleteinek felmérését, kialakítását, azok tudatosítását, az adott szervezeti egység szintjén. Az ilyen jellegű szervezeti szintű tudatosítás felsővezetői szinten kell, hogy kezdődjön, de leginkább azt a középvezetői réteget kell, hogy érintse, mely a napi üzletmenetért felelős, és az annak fenntartásához szükséges döntéseket hozza.
- A szervezet munkavállalói magatartásának változtatása a szükséges irányba – szorosan kapcsolódóan a felhasználók információbiztonság-tudatosság növelő programjához. Ennek egyik módja olyan vezetők bevonása az általános tudatosság-növelő programokba, emellett felelőssé tétele az információbiztonságért (is), akik egy-egy működési területért egy személyben már felelősek.
- Személyes adatok és a szellemi tulajdon védelme – ez elsősorban a szervezet által kezelt személyes és kiemelt munkafolyamatokhoz kapcsolódó adatok védelmét jelenti, és magában foglalja pl. a felhasználók azonosítását.

6.2. Elmozdulás a technológia felől az információbiztonság menedzsment felé

A biztonság felépítésének tradicionális megközelítése a naprakész technológiák megvásárlása és rendszerbe állítása, illetve kész megoldások beszerzése volt. Ezzel szemben napjainkban elmozdulás figyelhető meg a tekintetben, hogy a felsővezetők egyre nagyobb arányban – a szükséges minimális technológia beruházás mellett – inkább tanácsadást, a megfelelő szabályozók kialakítását, és a szabályozóknak, szabványoknak történő megfelelést várják el a külső szolgáltatóktól (consulting, policies, compliance).

6.2.1. Vezetés elköteleződésének elérése

Fontos, hogy a vezetés bizonyíthatóan felelősséget vállaljon az információbiztonság tudatossággal kapcsolatos tevékenységekért, ideértve azok létrehozását, bevezetését, működtetését, ellenőrzését és felülvizsgálatát, továbbfejlesztését és karbantartását.

Az idesorolható konkrét felelősségek a következők:

- az Informatikai Biztonsági Szabályzat elkészítése,
- a célok, a hatás- és felelősségi körök meghatározása,
- folyamatos kapcsolattartás a biztonsági vezetés és az üzleti vezetők között,
- gondoskodás a működéshez szükséges erőforrásokról,
- az üzleti szempontból elviselhető kockázatok szintjének meghatározása.

Az informatikai biztonság olyan felelősség, amelyen a vezetés valamennyi tagja osztozik. Ezért kellő elkötelezettséggel és a szükséges erőforrások rendelkezésre bocsátásával képes a vezetés támogatni az információ- és informatikai biztonságot, akár egy stratégiai tanácsadó testület létrehozásával. Ennek a testületnek olyan embereket kell magába foglalnia, akiknek megvan a követelmények azonosításához, politikák kialakításához, biztonsági programok írásba foglalásához, a munka értékeléséhez és az információbiztonsági és/vagy az informatikai biztonsági vezető irányításához szükséges képessége. A hatékony működéshez szükséges, hogy a stratégiai tanácsadó testületnek legyenek olyan tagjai is, akik komolyabb háttérrel rendelkeznek a biztonság és az informatikai rendszerek műszaki területén, de olyan tagjai is, akik az informatikai rendszerek, mint szolgáltatások nyújtásában, valamint felhasználásában vesznek részt. Mindezen területek tudására és tapasztalatára szükség van.

A felsővezetés hatáskörébe tartozik**:**

- javaslattétel az stratégiai tanácsadó testület számára a stratégiai tervezéshez,
- az információ- és informatikai biztonsági irányelvek és feladatok vizsgálata és jóváhagyása, a megvalósításhoz szükséges humán és anyagi erőforrások biztosítása,
- az információs erőforrások súlyos veszélyhelyzeteknek való kitettségében bekövetkező jelentős változások nyomon követése,
- az információ- és informatikai biztonsági események nyomon követése,
- az információ- és informatikai biztonság fokozását szolgáló jelentős kezdeményezések jóváhagyása,
- az információ- (és amennyiben releváns, az informatikai) biztonsági vezető személyének kijelölése, feladat- és hatáskörének meghatározása.

Ezen a ponton fontos megjegyezni azonban, hogy pusztán a szabályozóknak történő/törvényi megfelelés még nem teszi biztonságossá egy szervezet működését, a biztonság tényleges kialakításához képzésre, gondolkodásmód váltásra, szervezeti átalakításra és elkötelezett, az információbiztonságot stratégiai szempontból átlátó felsővezetésre is szükség van.

Napjainkban a külső szolgáltatók egyre nagyobb arányban az információbiztonság-tudatosság emelését célzó képzésekből (information security awareness) érik el bevételeik meghatározó részét, mely markáns hangsúlyeltolódást jelez. Ez azt jelzi, hogy az információbiztonság kritikus üzleti funkcióvá vált.

A megváltozott szervezeti gondolkodás ilyen módon ma már valósággá teszi azt, hogy a napi üzletmenetre jelentős hatással bíró döntések esetén az információbiztonsági szempontok és megfontolások felülírják az adott döntés megvalósítását, de legalábbis késleltetik/módosítják azt, amennyiben az eredetileg tervezett változtatás káros hatással lenne, vagy komoly kockázatot jelentene a szervezet információbiztonságára. Ez akkor előremutató, ha az információbiztonságért felelős szervezeti egység javaslatokat is nyújt alternatív, a biztonságot mégis garantáló megoldásokra – például úgy, hogy a napi üzletmenet során elfogadható kockázatok összevetésre kerülnek a szervezet célkitűzéseivel, és az összevetés nyomán kerülnek kidolgozásra azok az információbiztonsági megoldások, melyek kompromisszumos módon teszik lehetővé az üzletmenet és a biztonság elvárásainak párhuzamos megvalósítását (ld. kockázatarányos védelem).

6.3. Az információbiztonság hatása a szervezeti struktúrára

Gondosabban, átgondoltabban felépített szervezeti struktúrák esetén az információbiztonságért felelős csoport további kisebb, konkrétabb feladatokkal rendelkező egységekre bontódik, ezek pl. az információbiztonságért, stratégiai kockázat menedzsmentért, üzletmenet folytonosságért, hálózat üzemeltetésért, infrastruktúráért, rendszerek felépítéséért, szabályozók kialakításáért, stb. felelős egységek. Ezen egységektől az információbiztonsági vezető gyűjti össze a felsővezetői döntések támogatásához szükséges információbiztonsági vonatkozású információt, hogy azt továbbítva a szervezet stratégiai döntéshozói felé megvalósulhasson az információbiztonság szempontjainak beépítése az üzletmenetet, munkafolyamatokat, beruházásokat, stb. befolyásoló stratégiai döntésekbe.

Szervezetenként változó az a stratégiai vezető, akinek a szervezet információbiztonsági vezetője beszámol – emiatt nehéz egyetlen jól bevált struktúrát minden szervezetben azonosan bevezetni – az viszont célszerű, hogy az érintett stratégiai vezető döntési jogkörrel rendelkezzen beruházások és más kapcsolódó pénzügyi kérdések tekintetében, annak érdekében, hogy a szükséges és szakmailag indokolt információbiztonsági beruházások megvalósulhassanak. Ennél szerencsésebb esetben maga az információbiztonsági vezető is rendelkezik pénzügyi vonatkozású döntési jogkörrel.

Napjainkban elterjedőben van az a vélekedés is, hogy a szervezetek biztonsági struktúrájának felépítése kevésbé fontos, mert az meghatározóbb, hogy a biztonsági szempontok valójában figyelembe legyenek véve, és a szükséges biztonsági intézkedéseket valaki végre is hajtsa/betartassa a szervezeten belül. Ez pedig leginkább a döntési helyzetben lévő, szakmailag hozzáértő, hiteles információbiztonsági vezető.

Az elmúlt 10 év megfigyelései alapján kijelenthető, hogy a megfelelő jogkörrel rendelkező, hiteles (információbiztonsági) vezetők három jól körvonalazható téren képesek befolyást gyakorolni a szervezetre. Elsőként, a biztonsági szint növelésével képesek hozzájárulni a biztonsági szint és az elvégzett munka hatékony – és jó esetben összehasonlítható – méréséhez, másodsorban meg tudják alapozni azt a szervezeti kultúrát, mely a biztonságot állandóan jelenlévő dologként közelíti meg, ezáltal minden munkavállalóval megérteti, hogy ez a felmerülő kockázatok része (ld. 2.2.2. „Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők tudatosítása” c. fejezet), harmadrészt kialakíthatnak olyan biztonsági szempontú beruházási modelleket, melyek minden projekt részét kell, hogy képezzék.

6.4. A szervezeti kultúra hatása az információbiztonságra – a felsővezetés (és az információbiztonsági vezető) szerepe az információbiztonság megteremtésében

Az információbiztonság szempontjából különlegesen fontos a szervezeti kultúra, annak okán, hogy a szervezet általános információbiztonsága valójában annak tagjain, az egyéneken, továbbá azok aktuális viselkedésén múlik. A szervezet dolgozóinak tudatos információbiztonsági magatartását – a megfelelő képzés mellett – leginkább a felsővezetői elkötelezettség és tudatosság befolyásolja pozitív irányban, melyet a dolgozóknak meg is kell tapasztalniuk (a valóságban hallaniuk kell).

A tudatos felsővezetői magatartás kulcsa a felsővezetők információbiztonsági képzése (ld. 2.2.2. „Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők tudatosítása" c. fejezet). A felsővezetők tudatosságának növelése a szervezet szempontjából azért kiemelten fontos, mert növelni tudja annak esélyét, hogy az információbiztonsági szempontból tudatosabb felsővezető egy, a szervezet működését markánsan befolyásoló stratégiai döntés esetén figyelembe veszi az információbiztonság szempontjait is. Ennek a folyamatnak a döntéstámogatója az információbiztonsági vezető.

Az információbiztonsági vezető feladata láttatni a felsővezetéssel, hogy az információbiztonság szerencsés esetben nem cél, hanem a szervezet egészséges működésének előfeltétele, mely oly módon mozdítja elő a munkafolyamatok, projektek sikeres, költségkímélő megvalósulását, hogy megakadályozza az információ kompromittálódásából vagy elvesztéséből adódó jellemzően jelentős kárt.

Az információbiztonsági kérdések és döntések ily módon történő átláthatóbbá tétele jellemzően növeli a szervezeten belül a biztonságra szánt forrásokat is, ily módon a szervezeti kultúra változása hosszú távon pozitív hatással van az információbiztonsági fejlesztésekre szánt forrásokra.

Ezzel együtt a biztonság akkor válik különösen fontossá, ha javítja a teljesítményt és a megbízhatóságot. Ehhez pedig az szükséges, hogy az információbiztonsági vezető sikeresen működjön együtt a szervezet további egységeivel annak érdekében, hogy a biztonság beépüljön az üzleti, üzletmeneti stratégiákba és tervekbe. Ez utóbbi szervezetei szintű stratégiai együttműködéshez elengedhetetlen a felsővezetői támogatás.

6.5. Az információbiztonsági elvek érvényesítése külső beszállítók, partnerek tekintetében

Az információbiztonság sok esetben túlnyúlik a szervezet keretein. Bármely olyan esetben, amikor a szervezet külső beszállítóktól, partnerektől vesz igénybe olyan szolgáltatást vagy végeztet el olyan munkafolyamatokat, melyek során a szervezet szempontjából kritikus adatok, információ kerül a külső partner információs rendszereibe, pl. feldolgozás céljából, tekintetbe kell venni a vonatkozó információbiztonsági kritériumokat. Ilyen esetekre a hatályos hazai jogi környezet azonos biztonsági szint megvalósítását írja elő a szervezet és a külső partnerek számára. Természetszerűleg az előírt információbiztonsági kritériumok meglétét szükséges a külső partnernél ellenőrizni és betartatni is.

7. Kommunikációs eljárások az elkötelezettség és a támogatás megszerzésére

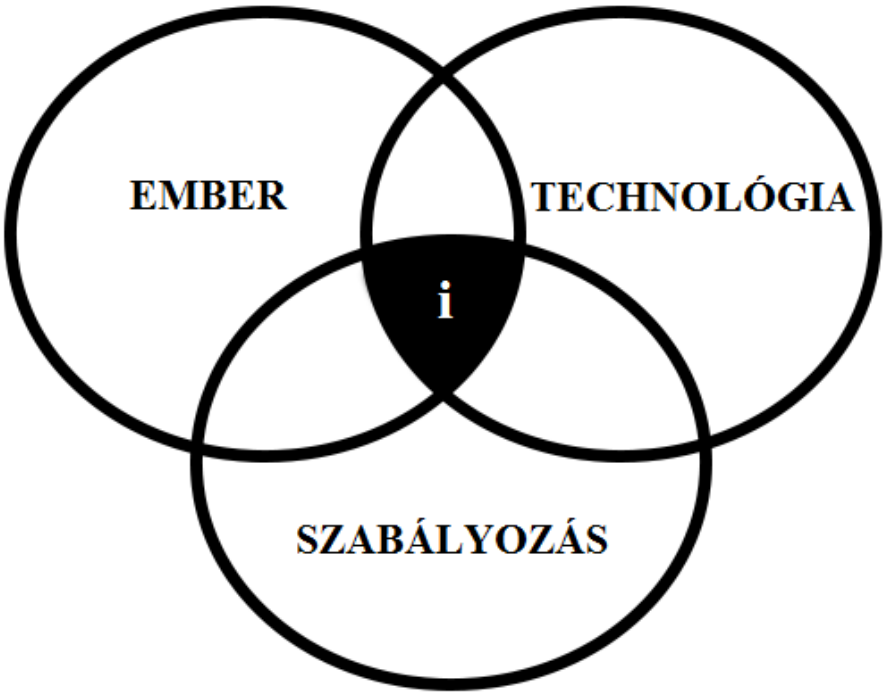
7.1. Hogyan kommunikáljuk az információbiztonság komplex problematikáját a felsővezetők felé?

Az információ biztonságos kezelésének feltétele és alapja az ún. „információbiztonsági PPT modell – The People, Policy, Technology PPT Model: Core Elements of the Security Process, (Steven Schlarman 2001)”[22] mindhárom elemének – ember/people, a szabályozás/policy/process és a technológia/technology megfelelő, együttes kezelése.

Az ember, szabályozás, és a technológia hármas felosztása a folyamatirányítási PPT modellre (People, Process, Technology) vezethető vissza. Az információbiztonság úgy értelmezi ezt a felosztást, hogy az információnak a három halmaz metszéspontjában szükséges elhelyezkedni a biztonságos állapot megteremtéséhez.

Ez azt jelenti, hogy az alkalmazott technológiának összhangban kell lennie a bevezetett biztonsági intézkedésekkel és a felhasználók, üzemeltetők képességeivel, képzettségeivel, motiváltságaival.

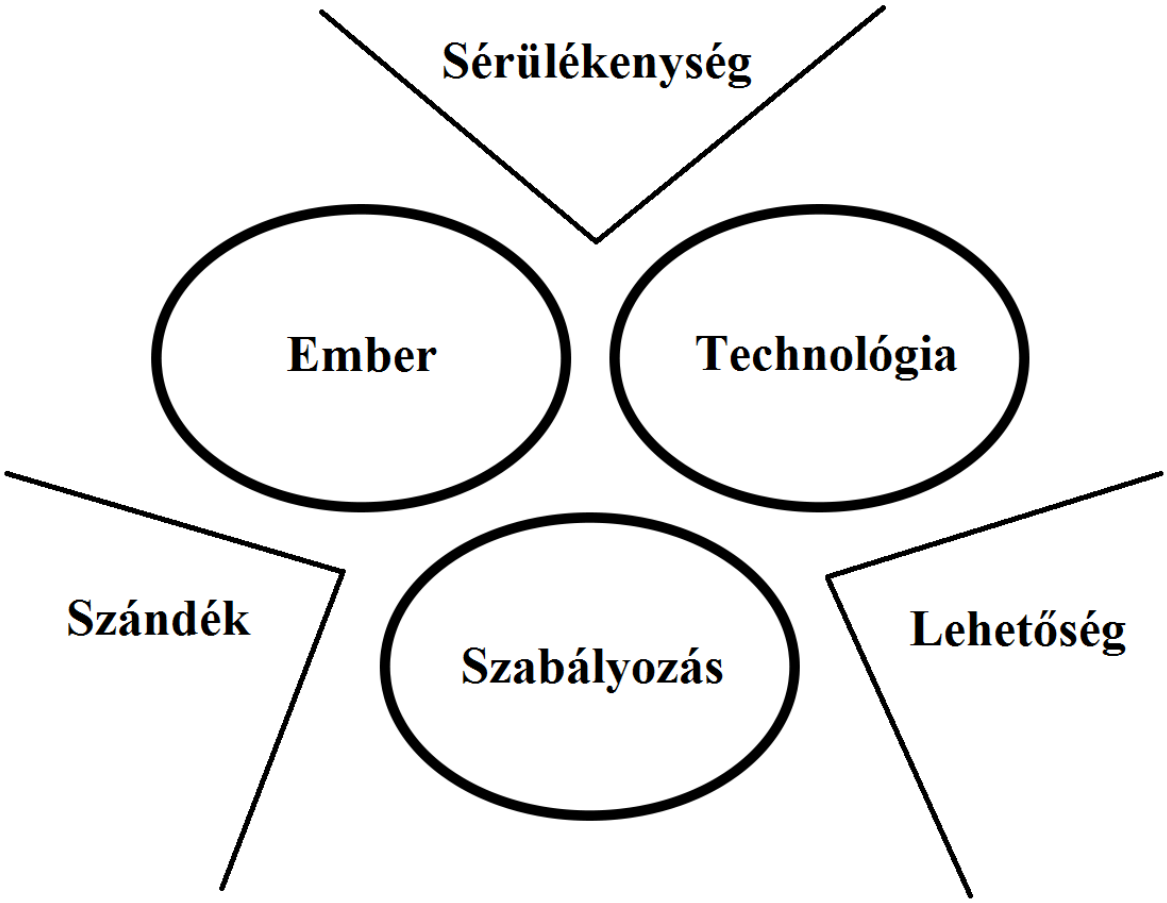
[22] http://www.tandfonline.com/doi/abs/10.1201/1086/43315.10.5.20011101/31719.6#preview



Abban az esetben, ha ezen elemek közül bármely kezelése nem megfelelő, avagy nem megfelelő a menedzsment támogatása a helyes kezelés kialakításában, akkor az információ veszélynek van kitéve, azaz az információ biztonságos kezelése nagy valószínűség szerint sérül.

7.1.1. Problémák, megoldási lehetőségek – kötelezettség profilok fejlesztési lehetőségei

Egy információs rendszer folyamatos változásban van. Adott környezetben folyamatosan jelennek meg például új fejlesztések, ezáltal avulttá válhatnak a régi eszközök. Új beszerzésekkel további eszközök kerülnek a rendszerbe, ezzel tovább növelve annak heterogenitását, továbbá az alkalmazottak fluktuációja is elkerülhetetlen, mely szintén komoly kockázatot hordoz magában – az újabb dolgozók információbiztonság-tudatosságának megfelelő szintre emelése időt vesz igénybe, és ez az „időDelta” sérülékenység-ablakot képez a rendszer védelmi képességeit csökkentve.



Az információ védelmére törekvő harmonikus „együttállást” folyamatosan gyengíti az összes halmaz egymástól történő eltávolodása. A két-két halmaz közti eltávolodások különböző kockázat növelő faktoroknak adhatnak teret. Ezen faktorok a szándék (ember a szabályozással szemben, illetve attól eltávolodva), sebezhetőség (ember a technológiával szemben, illetve attól eltávolodva), lehetőség (szabályozás a technológiával szemben, illetve attól eltávolodva). A halmazok egymástól való eltávolodásának kezelése elengedhetetlen egy biztonságos rendszer fenntartásához.

7.1.1.1. Szándék – kapcsolódó kötelezettség profilok

Az esetleges kártékony szándék az ember és a szabályozás halmazok távolodásakor kap teret. A probléma alapja, hogy a biztonsági szint gyengül, ha a felhasználók és üzemeltetők nem tartják be a biztonsági házirendet – vagy a vonatkozó, ilyen tartalmú dokumentumot – vagy nem is létezik ilyen házirend.

Megoldás: a felsővezetésnek úgy kell kialakítani a mindenkor aktuális házirendet, hogy azt a rendelkezésre álló körülmények között a felhasználók be kell, hogy tudják tartani

és ezzel párhuzamosan megfelelően motiváltak is legyenek e szabályozások irányában – ez megfelel a felhasználók kötelezettség profiljának kialakításával, fenntartásával, fejlesztésével.

A felhasználók szándékának befolyásolására képes egy szervezet a három lehetséges kockázati faktor közül a legegyszerűbben és a legkisebb anyagi ráfordítást igénylően, információbiztonság-tudatosítás képzéseken keresztül hatást gyakorolni. (Ld. még „szabályozók a gyakorlatban" képzés, „2.3. Képzési programok – gyakorlati megközelítés" fejezet.)

Közvetett hatásként is bezárulhat az ember – szabályozás olló, a kártékony szándék számára nem hagyva lehetőséget, ez azonban csak a többi két probléma helyes kezelése mellett lehetséges. A gyakorlatban a kártékony humán szándék azért nem nyerhet teret a másik két probléma (sérülékenység, lehetőség) kezelésével, mert a támadónak túl nagy energia-befektetésre lenne szüksége ahhoz, hogy megérje számára kompromittálni a rendszert, például egy, jelszavak és hozzáférések megszerzésére irányuló, de a szervezet felhasználóinak magas információbiztonság-tudatossága miatt sikertelen „social engineering" kampány esetén. (A sikertelen kampány ebben az esetben arra utal, hogy a szervezet dolgozói képesek felismerni a social engineering mögötti káros szándékot, és adott esetben nem adják ki a saját hozzáféréseiket jogosulatlan támadó számára, ezzel a jogosulatlan támadónak csak a technikai eszközökkel történő behatolás lehetőségét hagyva meg.).

7.1.1.2. Lehetőség – kapcsolódó kötelezettség profilok

A rendszerek információbiztonsági szintje gyengül akkor, ha az alkalmazott technológia nem képes támogatni az aktuális biztonsági házirendet, vagy más vonatkozó szabályozókat. Ha a technológia nem képes megvalósítani a házirendben támasztott követelményeket, hiába lesz megfelelő, erős szabályozás, az hamis biztonságtudatot eredményez a vezetésben. Problémát jelent ennek a fordítottja is, ha a házirend nem követi a technológiai lehetőségeket, melynek azonnali következményeként a jelentős, vagy megfelelő összegű biztonsági fejlesztések nem érik el a hatásukat (az alkalmazott információbiztonsági technológia drága, mégis hatástalan lesz).

Megoldás: a felsővezetők számára szükséges világossá tenni azt – azaz a felsővezetői kötelezettség profilt kialakítani –, hogy a technológiai háttér fejlesztése és/vagy a házirend technológiához történő felzárkóztatása, a technológia és a szabályozók harmóniában tartása elengedhetetlen, különösen abban a tekintetben, hogy a szabályozóknak az alkalmazott technológiához igazítása töredék költségráfordítást igényel a szükséges technológiai

fejlesztések jellemző költségigényével szemben (ld. 2.2.2. Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők tudatosítása c. fejezet).

7.1.1.3. Sérülékenység – kapcsolódó kötelezettség profilok

Az információ biztonsága szempontjából a legkritikusabb állapot az, ha a felhasználók, üzemeltetők képzettségi szintje nem alkalmas az aktuális, alkalmazott technológia kezelésére. Minél jobban távolodik a technológia fejlettségi szintje a kezelő személyzet felkészültségi szintjétől, a „tudásolló" annál nagyobbra nyílik, ezáltal egyre nagyobb lesz a megfelelő szakértelem hiányából adódó sérülékenységek mennyisége, melyek jogosulatlan, esetlegesen rosszindulatú felhasználók által kihasználhatóak.

Megoldás: a felhasználó, üzemeltető személyzet képzése, és megfelelően képzett szakemberek alkalmazása, valamint az üzemeltetők biztonsági szempontú kötelezettség profiljának kialakítása. Ezzel együtt, az alkalmazott információvédelmi technológia és azzal párhuzamosan a támadási technológiák, módszerek folyamatos fejlődése miatt elengedhetetlen a szakértők folyamatos vagy rendszeres továbbképzési lehetőségének megteremtése – ezen keresztül tartható fenn, illetve tölthető meg szakmai tartalommal az üzemeltetői kötelezettség profil. (ld. 2.2.3. „Szakértői képzés – „system hardening", sérülékenységmenedzsment üzemeltetők számára" c. fejezet, 2.2.5. „Az informatikai biztonság kialakításáért felelős személyzet információbiztonság-tudatosság képzése" c. fejezet).

Annak az alapvetésnek a tekintetében, hogy az ideálisnak mondható információbiztonsági állapot a szervezet rendszerein végrehajtott sérülékenységvizsgálatok adott időközönkénti megismétlésével és a felhasználói, technológiai auditok, ellenőrzések gyakoriságának növelésével érhető el, valamint hogy az alkalmazott technológiák sérülékenységeinek kiküszöbölése érdekében nagyon fontos a megelőzés, továbbá hogy a biztonsági intézkedéseket a támadás elkerülése érdekében kell bevezetni, nem a támadás után, a rendszereket üzemeltető szakértők információbiztonság-tudatosságának növelése a szervezet alapvető érdeke.

A szakértők biztonságtudatos szakmai magatartásával a rendszerek sérülékenységei mintegy 80%-kal csökkenthetőek – ez valójában a „bérből és fizetésből megoldható" állandó biztonsági szempontú bér jellegű ráfordításként is értelmezhető költséget jelenti – mivel a drasztikusan lecsökkentett sérülékenység lehetőségekkel – melyek egyben támadási

lehetőséget is jelentenek – a kihasználásukra irányuló szándék is csökken, mivel a feladat egyre nehezebb, időigényesebb és költségesebb lesz.

A szakértők tudásának naprakészen tartása feltétele az alkalmazott technológiák által nyújtott szolgáltatások legmagasabb fokú alkalmazásának, így az megteremti az alkalmazott technológiák – információbiztonsági szempontból történő – leginkább költséghatékony felhasználását.

8. Összegzés

Egy modern szervezet biztonságudatossági gyakorlatainak helyes megteremtése nem egyszerű feladat, de alapvető szükséglet.

Az utóbbi 2 évtized során – a szervezetek vonatkozásában – a biztonság által felölelt terület növekvő tendenciát mutat, és egyre inkább „lefed" olyan területeket is, mint üzletmenet folytonosság, bekövetkezett káresemények hatásainak elhárítása, információbiztonság (mely az informatikai biztonsággal szemben nem csak a technológiai kontrollokért felelős), megfelelőség, információbiztonság-tudatosság növelő képzési programok, stb. Ennek a folyamatnak a legfőbb letéteményese az információbiztonsági vezető, aki a modernebb szervezeti struktúrákban jellemzően felsővezetői döntéstámogató pozícióban, a felsővezetés tagjaként támogatja a szervezet biztonságtudatos stratégiai és napi működését.

Az információbiztonsági vezető feladata nem könnyű; meg kell tudnia érteni a szervezet működéséből fakadó információbiztonsági kockázatokat, azok csökkentési lehetőségeit a PPT modellnek megfeleltethető munkavállalók-szabályozók-rendelkezésre álló technológia háromszögében, képesnek kell lennie kipróbált, stabil módszerek és a legújabb technológiák együttes alkalmazására, rendelkeznie kell projektmenedzsment látásmóddal a kézzelfogható, mérhető eredmények érdekében, és a döntései alátámasztására költséghatékonysági érveket kell tudnia felsorakoztatni. Az információbiztonsági vezető döntései alapjául iparági tanulmányok és összehasonlító elemzések szolgálhatnak, és mindezek mellett jól kell ismernie a szervezte biztonsággal kapcsolatos napi viselkedését is azért, hogy megfelelően tudja képviselni a szervezte biztonságos működését szolgáló stratégiai döntéseket és azok beillesztését a gyakorlatba.