Dátum:	2015. március 17.
Minősítés:	átadott
Fájlnév:	MKSZ_Információbiztonsági tanácsadás_Ajánlat_v0.5.doc
Verzió:	1.0
Készítette:	Dénes György

ÜZLETI AJÁNLAT
INFORMÁCIÓBIZTONSÁGI TANÁCSADÁS
TÁRGYÁBAN

MAGYAR KÁBELKOMMUNIKÁCIÓS SZÖVETSÉG (MKSZ)
SZÁMÁRA

Ref: KSZ-678/582/A

Budapest, 2015. március 17.

T a r t a l o m j e g y z é k

1. ELŐZMÉNYEK 3
2. A SZOLGÁLTATÓK ÁLTAL ELVÉGZENDŐ FELADATOK 4
2.1. SZERVEZET VEZETŐJÉNEK KÖTELEZETTSÉGEI 5
3. A HRK CONSULTING ÁLTAL ELVÉGZENDŐ FELADAT 6
3.1. ELVÁRÁSOK AZ AJÁNLATRA VONATKOZÓAN 6
3.2. TANÚSÍTÁSRA TÖRTÉNŐ FELKÉSZÍTÉS FELADATAI 7
4. PÉNZÜGYI AJÁNLATUNK 8
5. MÓDSZERTAN 8
5.1. MKSZ ELVÁRÁSAINAK VALÓ TÉTELES MEGFELELÉS 9
6. FIZETÉSI FELTÉTELEK 9
7. EGYÉB FELTÉTELEK 10

1. ELŐZMÉNYEK

A 2003. évi C. törvény az elektronikus hírközlésről változásai, különösen a 142. § az elektronikus hírközlési szolgáltatókra vonatkozóan jelentős információbiztonsági előírásokat tartalmaz.

A 142. § alapján számla kiállítására csak olyan informatikai rendszer felhasználásával kerülhet sor, amely biztosítja a díjak hibátlan kiszámítását végző rendszerelemek zártságát, és megakadályozza a számlázási rendszerhez történő jogosulatlan hozzáférést, valamint a számlázási információk észrevétlen módosítását. A számlázási rendszernek továbbá meg kell felelnie az általános információbiztonsági zártsági követelményeknek is. Ennek érdekében a szolgáltatónak adminisztratív, fizikai és logikai intézkedésekkel biztosítani kell az általános információbiztonsági zártsági követelmények teljesülését.

Az előző bekezdésben meghatározott követelményeknek való megfelelést a tanúsító szervezet által történő, a számlázási informatikai rendszerre vonatkozó tanúsítással kell igazolni. A számlázási rendszerre vonatkozó követelmények teljesülése kizárólag informatikai biztonsági funkciókat megvalósító szoftvertermékek és -rendszerek elfogadott hazai vagy nemzetközi informatikai biztonsági módszertanon alapuló tanúsítására akkreditált tanúsító szervezet által kiállított tanúsítvánnyal igazolható. A tanúsítvány a kiadását követő második naptári év utolsó napjáig érvényes.

Az elektronikus hírközlési szolgáltatás díjának elszámolása alapjául szolgáló számlázási rendszer információbiztonsági megfeleltetéséről a szolgáltató az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvénynek megfelelően és módon köteles gondoskodni.

A logikai védelmi intézkedések teljesítésének vizsgálata során a számlázási rendszer vizsgálatának a számlázó szoftveren túl a teljes, a számlázásban részt vevő rendszer technológiai vizsgálata szükséges, beleértve a számlázási folyamathoz szükséges összes releváns bemeneti adatot (pl. mérési, fogyasztási adatok) kezelő rendszerelemet. A vizsgálatnak ki kell terjednie a rendszerben alkalmazott számlázó szoftver termék konkrét beállításainak, telepítésének és üzemeltetésének ellenőrzésére is.

Amennyiben a számlázási rendszert üzemeltető szolgáltató komplex, sokfunkciós elektronikus információs rendszerének a számlázási rendszer integráns része, a számlák kiállításához közvetlenül nem tartozó rendszerelemek nem esnek a tanúsítás hatáskörébe.

A logikai védelmi intézkedések teljesítésének vizsgálata során a tanúsító szervezet figyelembe veheti a számlázási rendszer részét képező számlázó szoftver vagy komponenseinek meglévő terméktanúsítványait is. A logikai védelmi intézkedések számlázó szoftverre vonatkozó követelményeinek vizsgálata során a nyilvános, nemzetközi sérülékenységi adatbázissal nem rendelkező egyedi számlázó szoftverek esetén a vizsgálatnak ki kell terjednie a számlázó szoftver forráskódszintű elemzésére is.

A 142. §-ban hivatkozott, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényt (2013. évi L. tv.) a magyar Országgyűlés 2013. április 15-én fogadta el.

A tv. 5. §-a és 6. §-a szerint a tv. hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell:

- az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
- az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és a kockázatokkal arányos védelmét

Az elektronikus információs rendszernek az előbbiekben meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

- a megelőzést és a korai figyelmeztetést,
- az észlelést,
- a reagálást,
- a biztonsági események kezelését.

2. A SZOLGÁLTATÓK ÁLTAL ELVÉGZENDŐ FELADATOK

A 2013. évi L. törvény, illetve annak végrehajtási rendelete (77/2013. NFM rendelet) előírásai szerint a szolgáltatónak az alábbi feladatokat kell elvégeznie. A hírközlési szolgáltatók esetében az általuk üzemeltetett elektronikus információs rendszerek alatt az elektronikus hírközlésről szóló 2003. évi C. törvény 142. § (3) bekezdésében szereplő, a díjak hibátlan kiszámítását végző rendszerelemeket, vagyis a számlázó rendszert, illetve a számlázás folyamatában részt vevő egyéb rendszerelemeket (pl. tarifáló rendszer) kell érteni.

1. **Ki kell nevezni a szervezet elektronikus információs rendszereinek biztonságáért felelős személyt.**

Magyarázat: A törvény alapján felsőfokú végzettséggel és szakképzettséggel rendelkező személy nevezhető ki, a végrehajtási rendeletek alapján szerződéses viszony keretein belül a feladat ellátható.

2. **Be kell jelenteni a Hatóságnak az 1-es pontban kinevezett személy adatait.**

Magyarázat: A törvény hatályba lépését követő 60 napon belül meg kell küldeni a Nemzeti Elektronikus Információbiztonsági Hatóságnak a szervezet elektronikus információs rendszereinek biztonságáért felelős személye természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét és a végzettségét igazoló okiratokat.

3. **Be kell jelenteni a Hatóságnak a szervezet adatait.**

Magyarázat: *A törvény hatályba lépését követő 60 napon belül meg kell küldeni a Nemzeti Elektronikus Információbiztonsági Hatóságnak a szervezetnek a szervezet azonosításához szükséges adatait.*

4. **Meg kell küldeni a Hatóságnak a szervezet Informatikai Biztonsági Szabályzatát.**

Magyarázat: A törvény hatályba lépését követő 90 napon belül meg kell küldeni nyilvántartásba vétel céljából a Nemzeti Elektronikus Információbiztonsági Hatóságnak a szervezet Informatikai Biztonsági Szabályzatát.

5. **El kell végezni a szervezet elektronikus információs rendszereiben kezelt adatok biztonsági osztályba sorolását.**

Magyarázat: A törvény szerint a szolgáltató biztonsági besorolását az általa üzemeltetett elektronikus információs rendszerek biztonsági osztályai alapján kell megtenni. Az elektronikus információs rendszerek biztonsági osztályba sorolását a bizalmasság, sértetlenség és rendelkezésre állás szempontjából kell megtenni a 77/2013. (XII. 19.) NFM rendelet alapján.

6. **A szervezet biztonsági szintbe sorolása**

Magyarázat: A szolgáltató biztonsági besorolási szintje mindig az elektronikus információs rendszereinek a legmagasabb biztonsági osztálynak megfelelő fokozata.

7. **A szervezet biztonsági szintjének megfelelő informatikai biztonsági irányítási rendszer kialakítására cselekvési terv készítése.**

Magyarázat: A törvény által előírt szervezeti szintű biztonsági besorolást követően, ha a szervezet a törvényben meghatározott biztonsági szintet nem éri el, akkor 90 napon belül cselekvési tervet kell készítenie az előírt biztonsági szint elérésére.

A törvény alapján a szervezetnek lehetősége van az előírt biztonsági szint fokozatos elérésére. Ennek keretében a magasabb biztonsági szint elérésére – minden egyes szintet érintően, a következő magasabb szintre lépéshez – két év áll rendelkezésére.

Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, akkor az 1. szint eléréséhez szükséges intézkedéseket a lefolytatott vizsgálatot követő egy éven belül meg kell valósítani.

A tanúsítást végző szervezet álláspontja szerint a szervezetnek az adminisztratív védelem szempontjából 1-es, míg a fizikai védelem szempontjából 2-es szintű biztonsági besorolást kell elérnie.

2.1. Szervezet vezetőjének kötelezettségei

(1) A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:

a) biztosítja az elektronikus információs rendszerre irányadó biztonsági osztály tekintetében a jogszabályban meghatározott követelmények teljesülését,

b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a jogszabályban meghatározott követelmények teljesülését,

c) az elektronikus információs rendszer biztonsági osztálya és a szervezet biztonsági szintje alapján előírt követelményeknek megfelelően az **elektronikus információs rendszer biztonságáért felelős személyt nevez ki**, vagy bíz meg, aki azonos lehet a minősített adat védelméről szóló 2009. évi CLV. törvény szerinti biztonsági vezetővel,

d) kiadja a szervezet elektronikus információs rendszereire vonatkozó **informatikai biztonságpolitikáját**,

e) meghatározza a szervezet elektronikus információs rendszereinek **informatikai biztonsági stratégiáját**,

f) meghatározza a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat, illetve kiadja az **informatikai biztonsági szabályzatot**,

g) gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek **oktatásáról**, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,

h) **rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok** lefolytatása révén meggyőződik arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,

i) gondoskodik az elektronikus információs rendszer eseményeinek **nyomon követhetőségéről**,

j) biztonsági esemény bekövetkezésekor minden szükséges és rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a **biztonsági események kezeléséről**,

k) ha az elektronikus információs rendszer **létrehozásában**, **üzemeltetésében**, **auditálásában**, **karbantartásában** vagy **javításában közreműködőt vesz igénybe**, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek, ha a szervezet az **adatkezelési** vagy az **adatfeldolgozási tevékenységhez közreműködőt vesz igénybe**, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,

l) felelős az érintetteknek a biztonsági eseményekről és a lehetséges fenyegetésekről történő haladéktalan tájékoztatásáért,

m) megteszi az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

3. A HRK CONSULTING ÁLTAL ELVÉGZENDŐ FELADAT

3.1. Elvárások az ajánlatra vonatkozóan

Az MKSz elvárásai a HRK Consulting által benyújtandó ajánlattal kapcsolatosan az alábbiak:

1. Elkülönített ajánlatot kér a mikrovállalkozói kategóriára vonatkozóan, ahol a havonta kibocsátott számlák (előfizetők) száma 2000 alatti.
2. Elkülönített ajánlatot kér a kisvállalkozói kategóriára vonatkozóan, ahol a havonta kibocsátott számlák (előfizetők) száma 2000-5000 közötti.
3. Elkülönített ajánlatot kér a közepes vállalkozói kategóriára vonatkozóan, ahol a havonta kibocsátott számlák (előfizetők) száma 5000-50000 közötti.
4. Az 1.-3. pontban megjelölt eseteken belül külön-külön kéri az ajánlatot megadni arra az esetre, ha valaki egy már auditált vagy sérülékenységi adatbázissal rendelkező szoftverrel (pl. Ecosoft) rendelkezik, vagy ha ettől eltérő (pl. egyedi fejlesztésű) számlázó szoftverrel rendelkezik.
5. Külön kéri annak megjelölését, hogy az 1-3. pontok szerinti kategóriák esetében csoportos felkészítés lehetséges-e, valamint csoportos felkészítés esetén a résztvevők minimális és maximális számának megadását (ha van ilyen), a vállalt helyszínt (Bp, vidéki nagyvárosok), valamint az 1-3. pontok szerinti, egyéni felkészítésre vonatkozó díjaktól eltérő (csoportos kedvezményt tartalmazó) díjat.

6. Kéri annak leírását mindegyik esetre, hogy az auditra való felkészítés tartalma mit jelent: milyen dokumentummintákat bocsátanak a szolgáltatók rendelkezésére, milyen dokumentumminták egyediesítésében közreműködnek, stb.
7. Kérik külön megjelölni azt, hogy a 6. pont szerinti tevékenységen kívül a sikeres auditáláshoz milyen további felkészítő támogatás(oka)t nyújtanak, és ennek ellenértékét az 1.-3. szerint alapdíjak tartalmazzák-e (ha nem, milyen irányárral lehet számolni).
8. Kérik megjelölni minden esetben azt, hogy a felkészítési tevékenységért milyen mértékű felelősséget vállalnak (pl. eredménytelen auditnál díjmentesség, a szabályzatokra az auditor által előírt/elvárt esetleges módosítások ingyenessége, a díjfizetés csak az eredményes audit után esedékes, stb.).
9. Kérik megjelölni azt, hogy az adott ajánlatban a szövetség részéről milyen mértékű segítő/szervező tevékenységre számítanak.
10. Minden olyan, a HRK Consulting által fontosnak tartott további körülményt, amely az előzőekben nem szerepel, ugyanakkor a szolgáltatók részére az audit felkészítők közötti választásnál érdemi kihatással lehet.

3.2. Tanúsításra történő felkészítés feladatai

A tanúsításra történő felkészítés során, a fenti igények alapján a HRK Consulting az alábbi feladatokat kívánja elvégezni az MKSz tagszerveinek.

1. A szervezet adminisztratív védelme aktuális állapotának felmérése a végrehajtási rendelet által megadott szempontrendszer szerint, a nem megfelelőségek, hiányosságok feltárása, előre összeállított kérdőív alapján, ha szükséges, konzultációval.
2. A szervezet fizikai védelme aktuális állapotának felmérése a végrehajtási rendelet által megadott szempontrendszer szerint, a nem megfelelőségek, hiányosságok feltárása, előre összeállított kérdőív alapján, ha szükséges, konzultációval.
3. A számlázási rendszer, illetve az ahhoz kapcsolódó folyamatok információbiztonsági besorolása és felmérése a végrehajtási rendelet által megadott szempontrendszer szerint, a nem megfelelőségek, hiányosságok feltárása, előre összeállított kérdőív alapján, ha szükséges, konzultációval
4. Cselekvési terv összeállítása a hiányosságok megszüntetésére. A hiányosságok megszüntetése két részre bontható.
    a. egyrészt kizárólag a szervezet által elvégzendő feladatokkal kapcsolatos cselekvési terv, aminek elvégzésére javaslatokat tudunk tenni, illetve az elvégzését ellenőrizni, ezeket azonban elvégezni, végrehajtani nem áll módunkban
    b. másrészt a tanácsadó, jelen esetben a HRK Consulting által elvégzendő feladatok, melyek főleg az adminisztratív védelmi intézkedéseket jelentik, mint pl. az Információbiztonsági Politika (IBP), Információbiztonsági Stratégia (IBS), illetve az Informatikai Biztonsági Szabályzat (IBSZ) összeállítása
5. A számlázási rendszer, és annak környezete (hardver elemek, operációs rendszerek, adatbázis kezelők, jogosultságkezelés, stb.) vizsgálata az információbiztonsági zártsági követelmények szempontjából, a végrehajtási rendeletben meghatározott bizalmasság, sértetlenség, rendelkezésre állás információbiztonsági alapelvek mentén.
6. A tanúsítás felügyelete, támogatása.

7. A tanúsítás eredményeként talált esetleges további hiányosságok, nem megfelelőségek elhárítása a számlázási folyamat olyan területein, melyek nem tartoznak az adott szolgáltató kizárólagos hatáskörébe.

4. PÉNZÜGYI AJÁNLATUNK

A korábbi fejezetben bemutatott feladatok elvégzésére a HRK Consulting az alábbi árajánlatot teszi az MKSz elvárásainak megfelelően. Az alábbi árajánlatot azoknál a tagvállalatoknál tudjuk érvényesíteni, amelyek már auditált vagy sérülékenységi adatbázissal rendelkező szoftverrel (pl. Ecosoft) rendelkeznek. Ha ettől eltérő (pl. egyedi fejlesztésű) számlázó szoftverrel rendelkeznek, akkor a felmérés, és felkészítés egyedi alku tárgyát képezi.

	Feladat	**Vállalkozási díj [nettó Ft]**
1.	Adminisztratív védelem aktuális állapotának felmérése	300.000,- Ft
2.	Fizikai védelem aktuális állapotának felmérése	
3.	A számlázási rendszer, illetve az ahhoz kapcsolódó folyamatok információbiztonsági besorolása és felmérése	
4.	Cselekvési terv összeállítása a hiányosságok, nem megfelelőségek elhárítására	
5.	Cselekvési terv alapján az adminisztratív védelmi intézkedések, szabályozások elkészítése	
6.	Tanúsítás felügyelete, támogatása	
7.	Tanúsítás eredményeként talált esetleges további hiányosságok, nem megfelelőségek elhárítása	
8.	Sikeres tanúsítás	

5. MÓDSZERTAN

A számlázó rendszer biztonsági osztályának, illetve a szervezet biztonsági szintjének meghatározásához szükséges a szolgáltató által használt számlázó rendszer legfontosabb jellemzőinek számbavétele üzletkritikusság, biztonság (bizalmasság, sértetlenség, rendelkezésre állás) fókusszal. Az adatokat táblázatos formában célszerű összegyűjteni, amely első körben legalább a következő oszlopokat tartalmazza:

Rendszer (alkalmazás) megnevezése:

Adatgazda* beosztása, neve (ha nem a rendszergazda):

Mire használjuk (funkcionális leírás):

Ki használja:

Jogosultság kiosztása hogy történik:

Dokumentálása hogyan történik:

A rendszer által kezelt, tárolt adatkör meghatározása, kritikussága:

Bizalmassági szempontok rövid értékelése:

Sértetlenségi szempontok rövid értékelése:

Rendelkezésre állás szempontjának rövid értékelése:

Naplózás státusza:

Hardver, szoftver, hálózati környezet rövid leírása:

*Adatgazda beosztása, neve (annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik)

5.1. MKSz elvárásainak való tételes megfelelés.

- 1-3. pont: Tekintettel arra, hogy a szervezet adminisztratív-, fizikai-, illetve logikai biztonsági védelme felmérése kérdőíves formában történik, melynek értékelése erőforrás igénye lényegében független a szervezet méretétől, ezért az ajánlatunkban nem tettünk különbséget méret alapján.
- 4. pont: Az ajánlatunk ennek megfelelően tettük meg.
- 5. pont: Csoportos felkészítés olyan szinten lehetséges, hogy a felkészítés és a felmérés folyamatát, a felmérő kérdőív kitöltését a HRK Consulting bemutatja a résztvevőknek. A felmérő kérdőív kitöltése ezek alapján egyedi kell, hogy legyen.
- 6. pont: Ajánlatunk 3.2. fejezete bemutatja, milyen dokumentum alapú termékeket készítünk el, illetve hogyan ellenőrizzük a számlázó rendszerrel kapcsolatos folyamatoknak, és magának a rendszer komponenseknek a zártságra vonatkozó előírások teljesülését.
- 7. pont: Vállalkozási díjunk minden feladat elvégzésének ellenértékét tartalmazza, a számla kiállításának feltétele a sikeres tanúsítás.
- 8. pont: Számla kiállításának feltétele a sikeres tanúsítás.
- 9. pont: Amennyiben a szövetség tagvállalatai igénylik, hogy a felmérés előtt a HRK Consulting személyesen bemutassa a felmérés folyamatát, a felmérő kérdőív kitöltésének menetét, úgy a szövetség részéről kérjük ennek a bemutatónak megszervezését, illetve helyiség biztosítását. A bemutatót – amennyiben igény van rá – javaslatunk szerint regionális szinten kellene megtartani, minimum 5 szervezet részvételével.
- 10. pont: Véleményünk szerint minden lényeges információt beletettünk jelen ajánlatunkba.

6. FIZETÉSI FELTÉTELEK

A vállalkozási díj az elfogadott és aláírt teljesítésigazolás alapján, az elvégzett feladatok ellentételezésére benyújtott számla ellenében kerül kifizetésre banki átutalással, a számla kézhezvételétől számított 15 napon belül.

Amennyiben a szolgáltató a folyamatos IT biztonsági tanácsadási szolgáltatásunkat kívánja

igénybe venni, a teljesítésigazolás aláírására, illetve ennek alapján a számla kiállítására minden negyedév végén kerül sor. A felmerült utazási költségeket a Nemzeti Adó és Vámhivatal előírásai alapján, tételes elszámolással, a szolgáltatóval egyeztetve, a teljesítésigazolásra rávezetve számoljuk el.

7. EGYÉB FELTÉTELEK

A HRK Consulting jelen ajánlat alapján a szolgáltatóval történő szerződés megkötésének tényét titokvédelmi kötelezettségének megtartása mellett marketing tevékenységében hivatkozási referenciaként használhatja.

A jelen ajánlatban nem szabályozott kérdésekben a Polgári Törvénykönyv (1959. évi. IV. tv.) általános és a vállalkozásra vonatkozó különös rendelkezései az irányadóak. A Felek az esetleges vitás kérdések esetére a Pesti Központi Kerületi Bíróság kizárólagos illetékességében egyeznek meg.

Ajánlatunk a benyújtás napjától számított 30 napig érvényes, azonban e határidő elteltével sem zárkózunk el újabb ajánlat benyújtásától.

Budapest, 2015. március 17.

……

Farkas István

ügyvezető