

Nyilvántartási szám: ESZ/2020/3
Iktatószám: 8360-1/2020/PKF

ADÁSVÉTELI SZERZŐDÉS

amely létrejött egyrészről a

Intézmény neve:	Nemzeti Népegészségügyi Központ
Székhely:	1097 Budapest, Albert Flórián út 2-6.
Adószám:	15329530-2-43
Bankszámlaszám:	10032000-00281519-30005307
Képviseli:	Dr. Müller Cecília
Képviselő titulusa:	országos tisztifőorvos

mint vevő, (a továbbiakban: Vevő)

másrészről a(z)

Cég neve:	TIGRA Kft.
(konzorciumvezető, közbeszerzési vevőszolgálat):	1145 Budapest, Törökőr utca 2.
Székhely:	12218778-2-42
Adószám:	01-09-566107
Cégjegyzék szám:	10900059-00000003-31980015
Bankszámlaszám:	Vertán György
Képviseli:	ügyvezető
Képviselő titulusa:	

Cég neve:	ALPHA MACHINE Kft.
Székhely:	1123 Budapest, Táltos utca 1.
Adószám:	14707126-2-43
Cégjegyzék szám:	01-09-916104
Bankszámlaszám:	10918001-00000052-77850002
Képviseli:	Fejti Gábor
Képviselő titulusa:	ügyvezető

Cég neve:	Cyber Services Zrt.
Székhely:	1089 Budapest, Elnök utca 1.
Adószám:	24800282-2-42
Cégjegyzék szám:	01-10-047971
Bankszámlaszám:	10300002-10645794-49020010
Képviseli:	Frész Ferenc
Képviselő titulusa:	vezérigazgató

Cég neve:	DAMIT INFORMATIKA Kft.
Székhely:	6725 Szeged, Hópárdac utca 7. fszt. 3.
Adószám:	13596789-2-06
Cégjegyzék szám:	06-09-010221
Bankszámlaszám:	10400164-49555557-48571013
Képviseli:	Dorn András
Képviselő titulusa:	ügyvezető

Cég neve:	DIGITAL Kft.
Székhely:	6723 Szeged, Csongrádi sgt. 83.
Adószám:	10406115-2-06
Cégjegyzék szám:	06-09-000341
Bankszámlaszám:	10980006-00000004-20740003

h

Nyilvántartási szám: ESZ/2020/3
Iktatószám: 8360-1/2020/PKF

Képviseli: Fenyvesi József
Képviselő titulusa: ügyvezető

Cég neve: KÜRT Zrt.
Székhely: 1118 Budapest, Rétköz utca 5.
Adószám: 11780359-2-43
Cégjegyzék szám: 01-10-048723
Bankszámlaszám: 10102093-30661600-00000307
Képviseli: Kmetty József Béla
Képviselő titulusa: vezérigazgató

Cég neve: M&S Informatikai Zrt.
Székhely: 1136 Budapest, Pannónia u 17/a. a. ép. fszt. 4.
Adószám: 14409471-2-41
Cégjegyzék szám: 01-10-046107
Bankszámlaszám: 10300002-20222941-00003285
Képviseli: Mester László
Képviselő titulusa: igazgatótanácsi tag (vezető tisztségviselő)

Cég neve: RacioNet Zrt.
Székhely: 1117 Budapest, Hauszmann Alajos u. 3/A.
Adószám: 13846606-2-44
Cégjegyzék szám: 01-10-045565
Bankszámlaszám: 10102093-56990600-01000008
Képviseli: Balázs András
Képviselő titulusa: cégvezető

Cég neve: Visoft Kft.
Székhely: 1119 Budapest, Than Károly utca 17.
Adószám: 12978881-2-43
Cégjegyzék szám: 01-09-712967
Bankszámlaszám: 10918001-00000039-63630006
Képviseli: Bódis Gyula
Képviselő titulusa: ügyvezető

mint Eladó (a továbbiakban együtt: Eladó) között (a továbbiakban együtt: Felek) alulírott helyen és napon az alábbi feltételekkel.

1. A szerződés létrejöttének előzménye:

A Digitális Kormányzati Ügynökség Zártkörűen Működő Részvénytársaság (a továbbiakban: DKÜ Zrt.) a Nemzeti Hírközlési és Informatikai Tanácsról, valamint a Digitális Kormányzati Ügynökség Zártkörűen Működő Részvénytársaság és a kormányzati informatikai beszerzések központosított közbeszerzési rendszeréről szóló 301/2018. (XII. 27.) Korm. rendelet (a továbbiakban: DKÜ rendelet) 13. § (1) bekezdés a) pontja alapján a Vevő, mint Ajánlatkérő javára „2. rész: IT biztonságtechnikai megoldások és kapcsolódó szolgáltatások beszerzése – 2017 KM01ITBT17” beszerzése, a közbeszerzésekről szóló 2015. évi CXLI. törvény (a továbbiakban: Kbt.) 105. § (2) bekezdés c) pontja alapján az „Nemzeti Népegészségügyi Központ részére informatikai határvédelmi rendszer korszerűsítése az „EFOP-1.8.1-VEKOP-15-2016-00001 Komplex népegészségügyi szűrések” azonosítószámú projekt keretében” közbeszerzési eljárást folytatott le.

Felek rögzítik, hogy Vevő az EFOP-1.8.1-VEKOP-15-2016-00001 Komplex népegészségügyi szűrések projekt (a továbbiakban: Projekt) keretében 100 %-os támogatásban részesült a 2016. június 27. napján kelt, EFOP-1.8.1-VEKOP-15-2016-00001 számú Támogatási Szerződésben rögzítettek szerint.

Nyilvántartási szám: ESZ/2020/3
Iktatószám: 8360-1/2020/PKF

A Felek rögzítik, hogy a Közbeszerzési és Ellátási Főigazgatóság (KEF), (a továbbiakban: Beszerző) által TED 2017/S 247-517926 ill. KÉ-18977/2017 szám alatt, a központosított közbeszerzés hatálya alá tartozó Intézmények részére **IT biztonságtechnikai megoldások és kapcsolódó szolgáltatások beszerzése – 2017 KM01ITBT17** tárgyban lefolytatott központosított közbeszerzési keretmegállapodásos eljárás 1. része eredményeképpen a Beszerző és az abban részes Szolgáltatók között keretmegállapodás jött létre (a továbbiakban: KM).

KM azonosítószáma: KM01ITBT17

KM aláírásának dátuma: 2018. május 2.

KM időbeli hatálya: 2021. május 1.

KM keretösszege: 20.000.000.000 forint + Áfa.

A központosított közbeszerzési rendszerről, valamint a központi beszerző szervezet feladat- és hatásköréről szóló 168/2004. (V. 25.) Korm. rendelet (a továbbiakban: KEF rendelet), valamint a DKÜ rendelet 2019. október 31-i és november 1-jei módosításának következtében a DKÜ Zrt. a KM-ben jogutódként a Beszerző helyébe lépett.

Amennyiben az Eladó közös ajánlattevő, akkor felek rögzítik, hogy jelen szerződést a közbeszerzési eljárásban közös ajánlatot benyújtó – jelen szerződésben Eladóként megjelölt - ajánlattevők közösen teljesítik. A közös ajánlattevők egymás közti, illetve a Vevő közti viszonyát a jelen szerződés (a továbbiakban: szerződés) és az együttműködési megállapodás tartalmazza. A jelen szerződést aláíró Eladó, a(z) **TIGRA Kft.** a szerződést – meghatalmazás alapján – a(z) összes közös ajánlattevő nevében írja alá, így a jogviszony a Vevő és az Eladók között jön létre. A közös ajánlattevők kijelentik, hogy jelen szerződésből eredő kötelezettség teljesítéséért egyetemleges felelősséget vállalnak.

Eladó, jelen szerződés aláírásával kinyilvánítja, hogy ismeri és a szerződés teljesítése során figyelembe veszi, elfogadja és betartja a jelen szerződés tárgyát, annak megvalósítását érintő valamennyi jogszabályt, az egyébként rá vonatkozó etikai normákat, a KM-et, valamint a Szerződés mellékletét képező műszaki leírásban (1. számú melléklet) foglaltakat.

2. A szerződés tárgya, mennyisége:

2.1. A jelen szerződés a keretmegállapodásos eljárás 2. része eredményeképpen a Vevő – hivatkozott KM tárgyát képező termékekre vonatkozó - beszerzési igénye (hardver és szoftver adásvétel, és kapcsolt szolgáltatások ellátása) megvalósítására jött létre.

2.2. A jelen szerződés alapján a Vevő megrendeli, az Eladó pedig elvállalja egy új informatikai **határvédelmi rendszer kialakítását (tűzfal és levelezőszűrő rendszer)**, loggyűjtő-logelemző szoftver (a továbbiakban: **Rendszerek**) szállítását, ezen belül hardver eszközök és licencek szállítását, bevezetési szolgáltatások nyújtását, követési szolgáltatások nyújtását, valamint gyártói támogatás biztosítását az alábbiakban, valamint az „Ajánlattételi felhívás és egyéb közbeszerzési dokumentum”-ban foglaltak szerint.

2.3. A Vevő az ajánlattételi felhívást és a közbeszerzési dokumentumot a KM01ITBT17 számon nyilvántartott keretmegállapodásban részes valamennyi Ajánlattevő részére a DKÜ Rendszeren keresztül térítésmentesen rendelkezésre bocsátotta.

2.4. Az Eladó feladata a bevezetési projekt végrehajtása során az alábbi dokumentumok és projekttermékek leszállítása:

- Rendszerterv
- Implementációs dokumentum
- Üzemeltetési kézikönyv
- Tesztelési terv
- Tesztelési forgatókönyvek
- Tesztelési jegyzőkönyvek
- Mentési-, Üzletfolytonossági-, valamint IT katasztrófa elhárítási terv a határvédelmi és a loggyűjtő-logelemző rendszerre vonatkozóan.

Nyilvántartási szám: ESZ/2020/3

Iktatószám: 8360-1/2020/PKF

2.5. A Vevő a szerződés alapján – a jelen szerződés szerinti ellenszolgáltatás megfizetésének feltételével – a Rendszerek átadásával egyidejűleg időbeli korlátozás nélküli, nem kizárólagos felhasználási jogot (licenszet) szerez valamennyi a jelen szerződés keretében átadott Rendszerre és annak minden szoftverére és/vagy szoftverelemére.

2.6. A Vevő a felhasználási jogát (licenszt) az Európai Unió területén belül gyakorolhatja. A felhasználási jog (licenz) kiterjed ugyanakkor arra, hogy a Vevő a szoftvereket saját informatikai rendszerében a megrendelt licenyszámban és korlátlan alkalommal telepítse, üzembe helyezze és használatát munkavállalói számára szabadon – további díjazás nélkül – átengedje. A felhasználási jog magában foglalja azt a jogot, hogy a Vevő az átadás-átvételi jegyzőkönyv Vevő általi aláírásától számított 36 hónapon keresztül a mindenkor legfrissebb szoftver verziót használhatja (szoftverkövetés).

2.7. A jelen szerződésben meghatározott szállítást és számlakiállítást a **TIGRA Kft.** teljesíti.

2.8. Az Eladó elfogadja és megerősíti, hogy a jelen szerződés részére eredménykötelmet eredményez, mely alapján a szerződést kizárólag akkor teljesítette, ha a jelen szerződés szerinti valamennyi feladatát elvégezte, függetlenül attól, hogy ezt mekkora humánerőforrás ráfordítással érte el. Ebből következően az Eladó nem mentesül a szerződés teljesítésének kötelezettsége alól akkor sem, ha az 1. számú mellékletben előírt szolgáltatásokra jelzett időkereteket a teljesítés során kimerítette.

3. A szerződés részteljesítési és teljesítési határideje:

3.1. Felek megállapodnak abban, hogy az Eladó a szerződés megkötésétől számított 30 napon belül köteles részletes Rendszertervet készíteni és azt átadni a Vevő részére. Vevő a Rendszertervet az átvételtől számított 10 napon belül megvizsgálja és ennek eredményétől függően jóváhagyja vagy az esetleges kifogásainak ismertetésével együtt javításra visszaadja azt az Eladónak. Utóbbi esetben az Eladó 5 napon belül köteles a Rendszertervet kijavítva átadni a Vevőnek. A Felek a Rendszerterv tekintetében akkor tekintik megtartottnak a határidőket, ha az Eladó a jelen pont szerinti 30 és 5 napos határidőket teljesíti.

3.2. Az 1. sz. melléklet szerinti termékek (árak) és szolgáltatások tekintetében a Vevő részére történő átadásának (szállításának/értékesítésének) határideje: **a szerződéskötéstől számított legkésőbb 360 napon belül**, a 3.3. pontban meghatározott részteljesítési határidők betartása mellett, melyről Felek részletes átadás-átvételi jegyzőkönyvet készítenek.

3.3. A termékek leszállítására és a szolgáltatások nyújtására vonatkozó határidők az alábbiak:

Részteljesítési határidők:

Termék / szolgáltatás	Teljesítési határidő (naptári napokban számítva)	Részteljesítés
Hardverek és licencek szállítása, az átadástól számított 3 éves gyártói garancia és gyártói támogatás biztosításával, valamint jóváhagyott rendszerterv elkészítése a szerződésben foglaltak szerint	a szerződéskötéstől számított 60 nap	1. részteljesítés
Tűzfal és levelezőszűrő eszközökhöz kapcsolódó implementációs szolgáltatások teljesítése, az eszközök éles üzemre állítása	a szerződéskötéstől számított 180 nap	2. részteljesítés

SIEM rendszerhez kapcsolódó implementációs szolgáltatások teljesítése, rendszer éles indítása	a szerződéskötéstől számított 180 nap	3. részteljesítés
Követési szolgáltatások (mérnöki időkeret biztosítása) valamennyi fent említett rendszerhez (finomhangolás, tanácsadás)	Minden rendszer esetén az éles üzembe állástól számított 180 napon át folyamatosan.	4-5. részteljesítés

Az ajánlatkérő előteljesítést elfogad, előzetes egyeztetés alapján.

3.4. A Vevő a jelen szerződés teljesítését teljesítésigazolás kiállításával írásban ismeri el. Ennek a teljesítés megtörténte mellett az is feltétele, hogy Eladó Vevő részére átadja a gyártói garanciát igazoló okiratot papír alapon vagy elektronikus formában vagy egyéb megfelelő tájékoztatást arról, hogy a garancia megléte az interneten pontosan hol ellenőrizhető.

4. A teljesítés helye:

A Vevő által megjelölt magyarországi cím:
H-1097 Budapest, Albert Flórián út 2-6.

5. A jótállás terjedelme és kezdete:

5.1. Az Eladó jótáll azért, hogy az átadott Rendszer alkalmas a jelen szerződés alapján meghatározott valamennyi minőségi és funkcionális követelménynek megfelelő, rendeltetésszerű és zavartalan üzemszerű használatra és működésre, ennek megfelelően működik is, továbbá a Rendszer és annak bármely eszköze, alkatrésze, szoftver- és hardvereleme mentes mindenfajta gyártási, tervezési, fejlesztési (konstrukciós), anyagbeli, kivitelezési hibától.

5.2. A jótállás kezdete a termékek átadás-átvételét követő nap. Az Eladó jótállási kötelezettségének úgy is megfelelhet, hogy az átadott termékekhez – a jelen szerződésnek mindenben megfelelő tartalmú – gyártói garanciát biztosít azzal, hogy amennyiben a gyártó a vállalt jótállási kötelezettségének nem vagy nem megfelelően tesz eleget, akkor az Eladó más módon köteles jótállási kötelezettségének eleget tenni.

5.3. A jótállásra egyebekben a KM-ben foglaltak irányadók.

6. Gyártói garancia

6.1. Az Eladó kötelezettséget vállal arra, hogy legkésőbb a teljesítés elismeréséig olyan okiratot ad át a Vevő részére, melyben a gyártó vagy a gyártó által erre feljogosított harmadik személy a Vevő részére - a jelen szerződésben meghatározott tartalommal és valamennyi termékre kiterjedően - jótállást vállal (a továbbiakban: gyártói garancia). Ennek elmulasztása esetén Vevő megtagadhatja a teljesítés elismerését.

6.2. A gyártói garancia pontos tartalma:

Minimum 24 órában a hét minden napján (24x7) elérhető technikai támogatás nyújtása és hardver csere bejelentésének biztosítása azonnali ügyintézésel, következő napi küldéssel (Next-day Delivery).

Hozzáférés biztosítása firmware- és szoftverfrissítésekhez, a beszerzett eszközök teljes szoftver és hardver tekintetében. Hozzáférés a technikai portálhoz és dokumentációkhoz.

6.3. A gyártói garanciának a teljesítés Vevő általi elismerésétől számított 36 hónap lejártáig érvényesnek kell lennie.

Nyilvántartási szám: ESZ/2020/3

Iktatószám: 8360-1/2020/PKF

6.4. A gyártói garanciának nyílt interneten ellenőrizhetőnek kell lennie. Az Eladó köteles gondoskodni a gyártói garancia érvényesítéséhez szükséges minden adminisztratív feladat elvégzéséről, különösen ideértve a szükséges internetes regisztrációt.

7. A fizetendő ellenérték:

7.1. A 2. pont szerinti valamennyi feladat hiánytalan és hibátlan teljesítéséért az Eladót összesen **149.116.547 Ft + ÁFA** vételár (mely tartalmazza a szerzői jogról szóló 1999. évi LXXVI. törvény 16. § (4) bekezdésében meghatározott felhasználási díjat) (a továbbiakban: teljes ellenszolgáltatás) illeti meg, mely az alábbiakban meghatározott rendben, a szerződés 3.3 pontjában rögzített feladatok Vevő általi elismerését követően (teljesítés igazolás) válik esedékessé.

Alapmennyiségre vonatkozó számlázási rend:

Termék / szolgáltatás	Számlázás rendje
Hardver és licenck (3 éves gyártói garancia biztosításával), Jóváhagyott Rendszerterv elkészítése a szerződésben foglaltak szerint	1. részszámla: Teljesítés-igazolás alapján, 30 nap fizetési határidővel. A teljesítés-igazolás elválaszthatatlan részét képezi a gyártói garancia igazolásának átadása. A gyártói garanciának a nyílt interneten ellenőrizhetőnek kell lennie.
Tűzfal és levelezőszűrő eszközkhöz kapcsolódó implementációs szolgáltatások teljesítése, az eszközök éles üzemre állítása	2. részszámla: A sikeres éles indítást követően számlázható, 30 nap fizetési határidővel
SIEM rendszerhez kapcsolódó implementációs szolgáltatások teljesítése, rendszer éles indítása	3. részszámla: A sikeres éles indítást követően számlázható, 30 nap fizetési határidővel
Követési szolgáltatások valamennyi fent említett rendszerhez (finomhangolás, tanácsadás)	4-5. részszámla Két részletben: 1-90, illetve 91-180. napokra, igazolt munkalapok alapján, 30 nap fizetési határidővel.

7.2. Az egyes részszámlákhoz tartozó teljesítések ellenértékeit a szerződés 1. számú melléklete tartalmazza.

7.3. A teljes ellenszolgáltatás tartalmazza a teljesítéssel kapcsolatos valamennyi költséget, különösen ideértve a felhasználói jog és a gyártói garancia ellenértékét, a kiszállítás díját, a behozatallal, a forgalomba hozatallal kapcsolatban felmerülő összes költséget (vám, adók, díjak, illetékek, egyéb), de nem tartalmazza a közbeszerzési díjat.

7.4. Tekintettel arra, hogy a jelen szerződés eredménykötelmet ír elő az Eladó részére, Felek a teljes ellenszolgáltatást átalánydíjnak tekintik, melynek összegét nem befolyásolja az, hogy az Eladó a szerződés teljesítését ténylegesen mekkora humán erőforrás ráfordítás mellett biztosítja.

7.5. A közbeszerzési díjat a Vevő a DKÜ rendelet 14. § (2) bekezdésének d) pontja alapján közvetlenül az eljárást lefolytató DKÜ Zrt. részére fizeti meg. A közbeszerzési díj alapja a KM alapján lefolytatott közbeszerzési eljárás esetén a létrejövő visszerthes szerződés általános forgalmi adó nélkül számított értéke, mértéke 2% + Áfa.

8. Fizetési feltételek:

8.1. Az esedékessé vált ellenszolgáltatásnak Vevő által történő kiegyenlítése az igazolt teljesítést követően, a Kbt. 135. § (1) és (4) bekezdésében meghatározott szabályok szerint, az adott részszámla igazolt kézhezvételétől számított 30 napon belül történik.

8.2. Az Eladó köteles az adott részszámlát a teljesítés elismerésétől számított 15 napon belül kiállítani, majd a Vevő részére eljuttatni. Az egyes részszámlához a Kbt. 135. §-ában meghatározott iratokat mellékelni kell.

8.3. A részszámlákon csak a jelen keretmegállapodás és az adott teljesítés hatálya alá tartozó termékek és szolgáltatások szerepelhetnek.

8.4. Az Eladó a jelen egyedi szerződésből eredő követelését nem engedményezheti harmadik személyre.

8.5. Késedelmes fizetés esetén a Vevő a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.) 6:155. § (1) bekezdése szerinti késedelmi kamatot fizet az Eladónak.

8.6. Az Eladó a szerződés teljesítése során előleget nem kérhet, és az előre fizetés sem megengedett.

8.7. Az Eladó a Kbt. 136. § (1) bekezdése szerint:

a) nem fizethet, illetve számolhat el a szerződés teljesítésével összefüggésben olyan költségeket, amelyek a Kbt. 62. § (1) bekezdés k) pont ka)-kb) alpontjai szerinti feltételeknek nem megfelelő társaság tekintetében merülnek fel, és amelyek az Eladó adóköteles jövedelmének csökkentésére alkalmasak;

b) a szerződés teljesítésének teljes időtartama alatt tulajdonosi szerkezetét a Vevő számára megismerhetővé teszi és a Kbt. 143. § (3) bekezdése szerinti ügyletekről a Vevőt haladéktalanul értesíti;

8.8. Amennyiben külföldi adóilletőségű úgy köteles a szerződéshez arra vonatkozó meghatalmazást csatolni, hogy az illetősége szerinti adóhatóságtól a magyar adóhatóság közvetlenül beszerezhet a nyertes ajánlattevőre vonatkozó adatokat az országok közötti jogsegély igénybevétele nélkül.

8.9. Eladó a számlát az alábbiak szerint köteles kiállítani:

- o a számla szabályszerű kiállítása után az Eladó a számlát a Vevő nevére és címére (cím: 1097 Budapest, Albert Flórián út. 2-6.) küldi meg,
- o a számlán szerepeltetni szükséges a szállított termékek megnevezése, VTSZ/SZJ száma mellett a Vevő által megadott belső azonosításra szolgáló szerződés számot, valamint fizetési határidőként 30 napot,
- o a számlán fel kell tüntetni a bankszámlaszámot, a bank nevét, valamint az adószámot,
- o a számlán fel kell tüntetni a „számla” elnevezést,
- o a számlának meg kell felelnie az általános forgalmi adóról szóló 2007. évi CXXVII. törvény (Áfa tv.) 169. § szerinti előírásoknak,
- o a számlán fel kell tüntetni az alábbi projekt beazonosítására szolgáló információkat az alábbi módon:
 - EFOP-1.8.1-VEKOP-15-2016-00001 „Komplex népegészségügyi szűrések”
- o Eladó Vevő teljesítésigazolásának kiállítását követően jogosult projektenként számlát kiállítani.

9. Szerződésszegés:

9.1. Felek megállapodnak abban, hogy a 3.3. pont szerinti teljesítési határidők elmulasztása esetén a Vevőt késedelmi kötbér illeti meg. Hibás teljesítés esetén a Vevő szintén kötbérre jogosult. A késedelmi és a hibás teljesítési kötbér alapja a nem teljesített, a késedelmesen vagy hibásan teljesített termék nettó vételára, illetve szolgáltatás nettó díja.

9.2. Késedelmi kötbér mértéke: a késedelem 1-10. napja alatt napi 0,5 %, a késedelem 11. napjától napi 1 % mértékű. A késedelmi kötbér maximális mértéke 20 %.

9.3. Hibás teljesítési kötbér mértéke: a hibás teljesítés 1-10. napja alatt napi 0,5 %, a 11. napjától napi 1 %. A hibás teljesítési kötbér maximális mértéke 20 %. Hibás teljesítésnek minősül, amennyiben bármelyik átadott termék és/vagy a Rendszer nem használható rendeltetészerűen, valamint az is, ha az Eladó nem vagy nem az előírt tartalommal bocsátja Vevő rendelkezésére a jelen szerződés 6. pontja szerinti gyártói garanciát.

Nyilvántartási szám: ESZ/2020/3

Iktatószám: 8360-1/2020/PKF

9.4. Meghiúsulási kötbér mértéke: a 7.1 pont szerinti – áfa nélkül számított – teljes ellenszolgáltatás 25 %-a.

9.5. Jelen szerződés meghiúsultnak tekintendő, amennyiben a Vevő az Eladó súlyos szerződésszegése miatt jelen szerződést azonnali hatállyal felmondja, a Vevő jelen szerződéstől az Eladó súlyos szerződésszegése miatt eláll, az Eladó 25 napot meghaladó késedelembe esik, illetve az Eladó olyan mértékű hibás teljesítése esetén, amely kapcsán a Vevő már nem érdekelt a teljesítés elfogadásában.

9.6. A Vevő jogosult az esedékessé vált kötbér összegét a kötbérrel érintett ellenszolgáltatásból visszatartani a Kbt. vonatkozó szabályainak betartásával.

9.7. A kötbérigények érvényesítése nem zárja ki a szerződésszegésből eredő egyéb igények érvényesítésének lehetőségét.

9.8. Felek Eladó részéről súlyos szerződésszegésnek tekintik különösen:

- amennyiben a késedelmi kötbér eléri a maximumot;
- amennyiben a hibás teljesítési kötbér eléri a maximumot;
- Eladó egyéb, meghiúsulási kötbérfizetési kötelezettséget keletkeztető magatartása;
- Eladó jelen szerződésen alapuló kötelezettségeit olyan jelentős mértékben megszegte, hogy ennek következtében Vevőnek a további teljesítés nem áll érdekében
- a titoktartási kötelezettség megszegése;
- Eladó a teljesítést jogos ok nélkül megtagadja,
- Vevő bármilyen módon megtéveszti Eladót, vagy valótlan adatokat szolgáltat.

Eladó súlyos szerződésszegése esetén Vevő jogosult meghiúsulási kötbér érvényesítésére, továbbá a szerződést azonnali hatállyal felmondhatja, vagy attól elállhat.

9.9. Felek rögzítik, hogy bármely nem szerződésszerű szolgáltatási teljesítés jogi fenntartás nélküli elfogadása a Vevő részéről nem értelmezhető joglemondásként azon igényekről, amelyek a Vevőt a szerződésszegés következményeként megilletik.

10. Felek közötti kapcsolattartás

10.1. Jelen szerződésben Felek szakmai kapcsolattartásra kijelölt képviselői:

Vevő részéről kapcsolattartásra jogosult	
Neve:	
Beosztása:	
Levelezési címe:	
Telefonszáma:	
Mobiltelefon száma:	
e-mail címe:	

Eladó részéről kapcsolattartásra jogosult	
Neve:	
Beosztása:	
Levelezési címe:	
Telefonszáma:	
Mobiltelefon száma:	
e-mail címe:	

Nyilvántartási szám: ESZ/2020/3

Iktatószám: 8360-1/2020/PKF

10.2. Jelen szerződésben Megrendelő részéről teljesítés igazolására jogosult személy:

Vevő részéről teljesítés igazolására jogosult	
Neve:	Dr. Müller Cecília
Beosztása:	országos tisztifőorvos
Levelezési címe:	1097 Budapest, Albert Flórián út 2-6.
Telefonszáma:	
Mobiltelefon száma:	
e-mail címe:	tisztifoorvos@nnk.gov.hu

10.3. Felek jelen pontban meghatározott kapcsolattartóik útján tartják a szerződés teljesítése során a kapcsolatot. Bármelyik Fél jogosult a 10.1., 10.2. pontban meghatározott kapcsolattartója/teljesítésigazolója személyét megváltoztatni. Felek megállapodnak, hogy a kapcsolattartók, teljesítésigazoló személyében bekövetkező változás nem igényel szerződésmódosítást, elegendő arról a másik Felet írásban tájékoztatni. A kapcsolattartó/teljesítésigazoló személyében bekövetkezett változás a másik Féllel való szerződésszerű közléstől hatályos. A kapcsolattartó személyek a szerződésmódosításra nem jogosultak.

10.4. Felek rögzítik, hogy minden, jelen szerződés teljesítésével kapcsolatos nyilatkozatot vagy egyéb értesítést (a továbbiakban: értesítés) szerződésszerűen küldenek meg egymásnak. Szerződésszerű megküldésnek minősül, az írásban és

- írásban igazolt személyes átadással,
- tértivevényes ajánlott levélben,
- az olvasásról visszaigazolt e-mailben vagy
- visszaigazolt telefax útján – megküldött értesítés.

10.5. Az e-mail vagy telefax útján történő kézbesítés esetén az értesítés akkor válik joghatállyossá, amikor a címzett azt igazoltan kézhez vette, arról automatikus vagy kifejezett visszaigazolás érkezett. A tértivevényes ajánlott postai küldeményt a kézbesítés megkísérlésének napján kézbesítettnek kell tekinteni, ha a címzett az átvételt megtagadta. Ha a kézbesítés azért volt eredménytelen, mert a címzett az iratot nem vette át (az a másik félhez nem kereste jelzéssel érkezett vissza), az iratot – az ellenkező bizonyításáig – a postai kézbesítés második megkísérlésének napját követő ötödik munkanapon kell kézbesítettnek tekinteni.

10.6. Felek megállapodnak, hogy a postai utat kizárólag a szerződésszegéssel, valamint a jelen szerződés megszüntetésével kapcsolatos értesítések megküldésére veszik igénybe. Jelen pontban meghatározott esetekben azonban a kézbesítés kizárólag postai úton (tértivevényes ajánlott levélben) vagy írásban igazolt személyes átadással történhet.

10.7. Felek rögzítik, hogy rendelkeznek az adatvédelmi jogszabályok által előírt felhatalmazással a jelen szerződésben rögzített kapcsolattartói személyes adatok kezelésére. Felek kijelentik, hogy a szükséges és előírt, előzetes tájékoztatást megadták a jelen szerződésben megnevezett munkavállalóiknak arról, hogy személyes adatukat (név, e-mail, adott esetben a hozzájuk köthető telefonos, faxos elérhetőség) a jelen szerződéssel összefüggésben, a Felek közötti kapcsolattartás érdekében, a jelen szerződés megszűnésének időpontjáig – amennyiben a szerződés időtartama alatt a kapcsolattartó személye változik, úgy e változás hatályba lépéséig - az őket foglalkoztató Fél a fentebb írt körben és célból használhatja, és a másik Félnek ugyanezen célból és feltételekkel történő használat érdekében továbbíthatja. Felek kijelentik, hogy a munkavállalók jelen pontban hivatkozott adatkezelésről szóló tájékoztatásában kitértek arra, hogy a szerződésre vonatkozó kötelező iratmegőrzés időtartama alatt fenti személyes adataik a Felek dokumentumkezelő rendszerében eltárolásra, illetve jogszabály által szabályozott hatósági, bírósági eljárás során az eljáró szerv részére megküldésre kerülhetnek.

Nyilvántartási szám: ESZ/2020/3

Iktatószám: 8360-1/2020/PKF

Felek rögzítik, hogy a jelen szerződés időtartama alatt, valamint azt követően is, kölcsönösen betartják a hatályos magyar és európai uniós adatvédelmi szabályokat, ideértve különösen, de nem kizárólagosan az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény („Infotv.”), valamint a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679. számú rendelet („GDPR”) rendelkezéseit.

11. Egyéb rendelkezések

11.1. A Felek rögzítik, hogy az egyedi szerződés kizárólag a Kbt. 141. §-a alapján módosítható.

11.2. a Vevő a szerződést felmondja – ha szükséges olyan határidővel, amely lehetővé teszi, hogy a szerződéssel érintett feladata ellátásáról gondoskodni tudjon –, ha

- az Eladóban közvetetten vagy közvetlenül 25%-ot meghaladó tulajdoni részesedést szerez valamely olyan jogi személy vagy személyes joga szerint jogképes szervezet, amely tekintetében fennáll a Kbt. 62. § (1) bekezdés k) pont kb) alpontjában meghatározott feltétel;
- az Eladó közvetetten vagy közvetlenül 25%-ot meghaladó tulajdoni részesedést szerez valamely olyan jogi személyben vagy személyes joga szerint jogképes szervezetben, amely tekintetében fennáll a Kbt. 62. § (1) bekezdés k) pont kb) alpontjában meghatározott feltétel.

11.3. A szerződő Felek tudomásul veszik, hogy a vonatkozó jogszabályok és megállapodások szerinti illetékes ellenőrző szervezetek feladat- és hatáskörüknek megfelelően jelen szerződés alapjául szolgáló közbeszerzési eljárást és jelen szerződés teljesítését ellenőrizhetik, részükre a jogszabály szerinti információ megadása üzleti titokra való hivatkozással nem tagadható meg. Az illetékes ellenőrző szervezetek ellenőrzése, helyszíni vizsgálata esetén Eladó köteles minden segítséget Vevő részére megadni, az ellenőrzés hatékonysága Vevő kötelezettségeinek megfelelő teljesítése érdekében.

11.4. Eladót titoktartási kötelezettség terheli a Keretmegállapodás VIII. pontja szerint. Eladó a tevékenysége során a tudomására jutott valamennyi információ, a Vevő adatbázisában szereplő harmadik személyre, ügyletre vonatkozó adatot köteles titokként kezelni.

11.5. A jelen szerződésben nem szabályozott kérdésekben, valamint bármely, a teljesítéssel kapcsolatos ellentmondás esetén a hivatkozott KM, illetve mellékletei vonatkozó rendelkezései, továbbá Magyarország mindenkor hatályos jogszabályai irányadók. Jelen szerződés a KM-ban meghatározottakkal ellentétes rendelkezéseket nem tartalmazhat.

11.6. Jelen szerződés elválaszthatatlan részét képezi a Beszerző és az Eladó között létrejött fent hivatkozott KM, és az alábbi mellékletek:

1. sz. melléklet: termék/szolgáltatás lista
2. sz. melléklet: Eladó átláthatósági nyilatkozata (minta)
3. sz. melléklet: KM teljesülésgazolás
4. sz. melléklet: a közbeszerzési dokumentumok (felhívás, műszaki leírás, valamint kiegészítő tájékoztatások)

11.7. Az Eladó a jelen egyedi szerződés aláírásával kijelenti, hogy a nemzeti vagyronról szóló 2011. évi CXCVI. törvény 3. § (1) bekezdés 1. pontja szerinti átlátható szervezetnek minősül. Az Eladó tudomásul veszi, hogy a jelen nyilatkozatban foglaltak változásáról - a változás bekövetkeztétől számított 8 napon belül – köteles a Vevőt írásban értesíteni. Az Eladó tudomásul veszi továbbá, hogy a valótlán tartalmú nyilatkozat alapján létrejött szerződést a Vevő jogosult azonnali hatállyal felmondani, vagy attól elállni.

11.8. Felek megállapodnak, hogy jelen szerződésből eredő esetleges vitás kérdéseiket elsősorban peren kívüli tárgyalás és egyeztetés útján kívánják rendezni. Az egyeztetés eredménytelensége esetén a

Nyilvántartási szám: ESZ/2020/3
Iktatószám: 8360-1/2020/PKF

Felek alávetik magukat Polgári Perrendtartásról szóló 2016. évi CXXX. tv. szerint hatáskörrel és illetékességgel rendelkező bíróság kizárólagos illetékességének.

A szerződést Felek áttanulmányozás és értelmezés után, mint szándékukkal és ügyleti akaratukkal mindenben megegyezőt 4 eredeti példányban jóváhagyólag írják alá.

Dátum: Budapest, 2020. 02. 24.

Dátum: Budapest, 2020. 02. 26.


Dr. Müller Cecília
országos tisztifőorvos
Nemzeti Népegészségügyi Központ
2020 FEBR 24


Vertán György
ügyvezető
1115 Bp., Bartók Béla út 105-113.
a **TIGRA Kft., ALPHA** száma: 12218778-2-42
MACHINE Kft., Cyber Services száma: 01-09-566107
Zrt., DAMIT INFORMATIKA
Kft., DIGITAL Kft., KÜRT
Zrt., M & S Zrt., RacioNet Zrt.
és Visoft Kft.
közös Ajánlattevők nevében

Pénzügyi ellenjegyző: 

20. 02. 23

MŰSZAKI LEÍRÁS

Nemzeti Népegészségügyi Központ részére informatikai határvédelmi rendszer korszerűsítése az „EFOP-1.8.1-VEKOP-15-2016-00001 Komplex népegészségügyi szűrések” azonosítószámú projekt keretében”

1. Háttér

Az EFOP-1.8.1-VEKOP-15-2016-00001 számú "Komplex Népegészségügyi Szűrések" elnevezésű kiemelt projekt Beszerzési, IT és kommunikációs pillérének IT alprojektje keretében megvalósuló informatikai fejlesztésének legfőbb célja, hogy országos, népegészségügyi célú, szervezett onkológiai szűrések (méhnyak-, emlő-, vastagbél-szűrés) informatikai támogatása a jelen kor igényeinek megfelelően megvalósuljon. A cél eléréséhez az informatikai alkalmazásfejlesztésen túl kiemelt figyelmet kell fordítani az információbiztonsági és adatvédelmi előírásokra is. Ajánlatkérő meglévő határvédelmi eszközei a fizikai és technológiai avulást elérték, loggyűjtő-elemző (SIEM) rendszerét pedig törvényben előírtaknak megfelelően szükséges fejleszteni. A Nemzeti Népegészségügyi Központ IT infrastruktúrájának biztonságos üzemeltetése, különösen pedig az országos szakrendszerekben tárolt személyes, különlegesen személyes és egészségügyi adatok védelme érdekében szükséges a határvédelmi eszközök teljes cseréje, továbbá loggyűjtő-elemző (SIEM) rendszerek beszerzése. Ajánlatkérő nem rendelkezik e rendszerek bevezetéséhez és támogatásához szükséges szabad kapacitással, ezért az eszközök és szoftver licencek beszerzésén túl bevezetési és követési szolgáltatások nyújtása is szükséges.

2. Bevezetendő rendszerek felsorolása

Nyertes Ajánlattevő feladatai:

- Redundáns levélszemét-szűrőpár szállítása és beüzemelése (ide értve a beállítások migrálását, a szabályok konszolidációját a jelenlegi rendszerből és az üzemeltetői betanítást), gyártói garancia biztosításával a leszállított eszközök átadástól számított 3 év időtartamra. A gyártói garancián túlmenően mérnöki időkeret biztosítása finomhangolási és konzultációs célokra.
- Redundáns tűzfalpár szállítása és beüzemelése (ide értve a beállítások migrálását, a szabályok konszolidációját a jelenlegi rendszerből és az üzemeltetői betanítást), gyártói garancia biztosításával a leszállított eszközök átadástól számított 3 év időtartamra. A gyártói garancián túlmenően mérnöki időkeret biztosítása finomhangolási és konzultációs célokra.
- SIEM loggyűjtő és logelemző szállítása és beüzemelése (ide értve az üzemeltetői betanítást), gyártói garancia biztosításával a leszállított eszközök átadástól számított 3 év időtartamra. A gyártói garancián túlmenően mérnöki időkeret biztosítása finomhangolási és konzultációs célokra.

Részletes műszaki tartalom

3. Az alapmennyiségként szállítandó rendszerekkel kapcsolatos általános követelmények:

- Hardver elemek esetében 3 év cseregarancia biztosítása szükséges 7x24 bejelentési lehetőséggel.
- Szoftver elemek esetében 3 év terméktámogatás, mely kiterjed valamennyi szoftver verzió frissítés használatának jogára; a hét minden napján 24 órában (7x24) korlátozás nélkül igénybe vehető távoli segítségnyújtásra hibaelhárítás céljára; valamint ahol ez külön meg van jelölve, ott a gyártó által nyújtott szignatúra frissítések, felhő alapú hozzáférések használati jogára.
- A rendszerek tervezése, szállítása, telepítése és támogatása során kiemelt figyelmet kell fordítani az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény előírásaira, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló a 41/2015. (VII. 15.) BM rendelet (továbbiakban: technológiai vhr) 5-ös biztonsági osztályára előírt követelmények teljesítésére.
- A részletes információbiztonsági követelmények a jelen melléklet 8. pontjában kerültek meghatározásra, oly módon, hogy elsőként azok a követelmények kerültek azonosításra, melyet valamennyi szállítandó rendszernek teljesítenie kell, majd az érintett rendszerre vonatkozó releváns, többletkövetelmények kerültek meghatározásra.

4. Tűzfal rendszer részletes követelményei

4.1. Tűzfal rendszerrel szemben támasztott műszaki követelmények

- Célhardveres, rack szekrénybe szerelhető kialakítás
- Klaszterezett, hibatűrő kialakítás
- Redundáns, menet közben cserélhető tápegységek
- Minimum 400 GB SSD belső tárhely kapacitás
- Minimum portszámok (eszközönként), szállítandó optikai modulok (eszközönként)
 - 32 darab 1GE RJ45 (rész) port
 - 10 darab 10GE SFP+ port
 - 2 darab 10GE port hardveres bypass támogatással
 - Dedikált menedzsment és HA port
 - 2 darab 10GE-SR SFP+ optikai modul szállítandó
 - A portok száma dinamikusan növelhető legyen igény szerint a későbbiekben a tűzfalról menedzselhető switch-ek segítségével
- Minimális teljesítményadatok (eszközönként)
 - 10 Gbps IPS teljesítmény
 - 50 Gbps IPsec VPN teljesítmény (512 byte csomagméret, AES256-SHA256 mellett mérve)
 - 5 Gbps SSL VPN teljesítmény

- 5 Gbps szűrési teljesítmény valamennyi szűrési technológia egyidejű használata mellett (hagyományos tűzfal funkciók, alkalmazás felismerés és szűrés, behatolásdetektálás, rosszindulatú kódok szűrése)
- 500k new session/second (TCP)
- 20M concurrent session (TCP)
- Elvárt biztonsági funkciók
 - AD/LDAP integrált és házirend alapú szűrések, pl:
 - URL szűrés folyamatosan frissülő kategorizált és reputációs adatbázis alapján
 - Rosszindulatú kódok szűrése (vírus, botnet, mobil kód, stb.)
 - Behatolásdetektálás és inline blokkolás folyamatosan frissülő támadási minta adatbázis segítségével
 - Folyamatosan frissülő alkalmazási minta adatbázis
 - Erős felhasználó azonosítás támogatása a gyártó saját token megoldásával
 - 2 darab token szállítandó az eszközökkel együtt az adminisztrátori hozzáférés biztonságossá tételéhez, a rendszer 5000 tokenig bővíthető legyen hardver csere nélkül
 - Távoli hozzáférés biztosítása beépített SSL VPN portál megoldás segítségével
 - Ne legyen felhasználó szám licenc korlátozás a megoldásban, vagy ha van, akkor minimum 5000 egyidejű felhasználót engedélyezzen.

4.2.A tűzfal rendszer telepítése során a Vállalkozó által nyújtandó szolgáltatások

- Tervezés
 - Helyszíni konzultáció, informatikai rendszer, célok megismerése
 - Írásos rendszerterv készítése
- Telepítés
 - Ajánlatkérő meglévő FortiGate és McAfee rendszeréből szabályok exportálása
 - Szabályok validálása, optimalizálása
 - Szabályok áttöltése, implementálása az új leszállítandó megoldásba
 - Előre telepített riportok bemutatása, felhasználói igények szerinti további egyedi riportok konfigurálása
 - Mentés beállítása, rendszer konfiguráció mentése, visszaállítási lépések ismertetése
- Dokumentáció
 - A telepítés és konfigurálás lépéseinek dokumentálása melynek segítségével reprodukálható a tűzfal rendszer
- Oktatás
 - Tantermi körülmények között, az NNK telephelyén üzemeltetői oktatás tartása, hivatalos gyártói tematika alapján minimum 5 fő részére legalább 3 nap terjedelemben. Az oktatás végére a résztvevőknek a tűzfal rendszer telepítésével, üzemeltetésével kapcsolatos valamennyi lépéssel meg kell ismerkedniük. Az oktatási anyagot online és offline is rendelkezésre kell bocsátani.
- Támogatás

- Az Ajánlattevőnek az átadott rendszert 6 hónapon keresztül kiemelten kell támogatnia, az alábbiak szerint:
 - Korlátlan távoli segítségnyújtás (email, telefon, remote desktop) munkaidőben a hibaelhárításhoz
 - Szükség esetén helyszíni kiszállás és konzultáció, segítség a rendszer finomhangolásában, a telepítés kiterjesztésében

5. Levélszűrő rendszer részletes követelményei

5.1. Levélszűrő rendszerrel szemben támasztott műszaki követelmények

- A megoldás eszköz alapú legyen.
- Rendelkezzen legalább 24GB email tárhellyel és 60GB karantén tárhellyel.
- A megoldás rendelkezzen tükrözött merevlemezekkel.
- Tudjon kezelni legalább 500 domaint és 1000-5000 felhasználói fiókot.
- A megoldásnak a karantén leveleket tárolnia kell magán az eszközön, vagy tovább küldenie egy rendszergazda által menedzselt email fiókba.
- A megoldás legalább 22 féle napi riportot tudjon készíteni igény szerint és azt a rendszergazdának elküldeni.
- A megoldás rendelkezzen helyi vírus- és spam definíciós adatbázissal.
- A megoldásnak lehetőséget kell nyújtania felhő alapú előszűrésre.
- A megoldásnak lehetőséget kell nyújtania felhő alapú menedzselhetőségre.
- Az opcionális felhő alapú védelem rendelkezzen vírus, spam, phishing szűréssel, sandbox alapú csatolmányszűréssel, URL szűréssel.
- A fizikai eszköz elérhetetlensége esetén a felhő alapú szűrőnek 4 napig tárolnia kell a felgyülemelő emaileket, vagy amíg a fizikai eszközzel helyre nem áll a kapcsolat.
- A megoldásnak lehetőséget kell nyújtani egyéni fekete/fehér lista készítésére a felhasználó számára.
- A megoldásnak lehetőséget kell nyújtani a rendszergazdának, hogy emaileket blokkoljon a fejléc/tárgy/levéltörzsben reguláris kifejezések és szavak alapján.
- A megoldás blokkolhassa a csatolmányokat fájl típus, vagy kiterjesztés alapján.
- A megoldásnak blokkolnia kell azokat a válasz üzeneteket (NDR) amelyek hamisított címről és nem a saját rendszerétől származnak.
- A megoldásnak tudnia kell titkosítani kimenő leveleket.
- A megoldásnak tudnia kell blokkolni vagy titkosítani kimenő leveleket, ha azok érzékeny információt tartalmaznak.
- Email szabályok kikényszerítése emailben található karakterkészlet alapján.
- A megoldásnak tudnia kell a küldő IP címének DNS visszaellenőrzését, meghatározni az eredeti küldő domaint és a blokkolni a tipikusan spammelő IP-ről érkező emaileket.
- Lehetőség legyen a levélben található URL címének visszaellenőrzése alapján szabályokat létrehozni az ismert spammer domainek kiszűrésére.
- A megoldásnak meg kell akadályoznia, hogy rövid idő alatt nagy mennyiségű spam érkezzon egy IP címről.

- A megoldás támogassa az SNMP monitorozást és figyelmeztetéseket, valamint API segítségével a megváltoztatható legyen a konfiguráció anélkül, hogy be kelljen lépni az eszközre.
- 3 év gyártói terméktámogatás és előfizetés a frissítésekre
- 3 év következő munkanapi cseregarancia

5.2.A levélszűrő rendszer telepítése során a Vállalkozó által nyújtandó szolgáltatások

- Tervezés
 - Helyszíni konzultáció, informatikai rendszer, célok megismerése
 - Írásos rendszerterv készítése
- Telepítés
 - Ajánlatkérő meglévő McAfee rendszeréből szabályok exportálása
 - Szabályok validálása, optimalizálása
 - Szabályok áttöltése, implementálása az új leszállítandó megoldásba
 - Előre telepített riportok bemutatása, felhasználói igények szerinti további egyedi riportok konfigurálása
 - Mentés beállítása, rendszer konfiguráció mentése, visszaállítási lépések ismertetése
- Dokumentáció
 - A telepítés és konfigurálás lépéseinek dokumentálása melynek segítségével reprodukálható a levelező szűrő rendszer
- Oktatás
 - Tantermi körülmények között, az NNK telephelyén üzemeltetői oktatás tartása, hivatalos gyártói tematika alapján minimum 5 fő részére legalább 2 nap terjedelemben. Az oktatás végére a résztvevőknek az email szűrő rendszer telepítésével, üzemeltetésével kapcsolatos valamennyi lépéssel meg kell ismerkedniük. Az oktatási anyagot online és offline is rendelkezésre kell bocsátani.
- Támogatás
 - Az Ajánlattevőnek az átadott rendszert 6 hónapon keresztül kiemelten kell támogatnia, az alábbiak szerint:
 - Korlátlan távoli segítségnyújtás (email, telefon, remote desktop) munkaidőben a hibaelhárításhoz
 - Szükség esetén helyszíni kiszállás és konzultáció, segítség a rendszer finomhangolásában, a telepítés kiterjesztésében

6. Logelemző (SIEM) rendszer részletes követelmények

6.1.Logelemző (SIEM) rendszerrel szemben támasztott műszaki követelmények

- A SIEM architektúrának támogatnia kell a rendszer komponensek elosztott telepítését a rendelkezésre állás és a skálázhatóság érdekében. Minimum az alábbi funkciók elválasztása lehetséges kell legyen:
 - központi intelligencia

- eseménygyűjtés
 - parse funkciók
 - riport és riasztások funkciók.
- Az események archiválása megvalósítható legyen egy közös NFS tárhelyen.
- Telepítése támogassa az elterjedt virtuális környezeteket.
- A redundáns működés és az erőforrások bővítése 3rd gyártó nélkül, a gyártó saját megoldásaival megvalósítható legyen.
- Az események összegyűjtése és elemzése kapcsán a rendszernek képesnek kell lennie kliens program telepítése nélkül a Syslog, Microsoft WMI, SNMP v2/v3 eseményeket fogadni és feldolgozni. A kezelőfelületen legyen lehetőség a parserek módosítására, egyedi parserek készítésére és tesztelésére.
- Microsoft és/vagy Unix/Linux alapú rendszereken futó, többlet funkciókat biztosító kliens programmal szemben elvárás, hogy az legyen központosított menedzselhető, működése policy alapú.
- A telepített agent tegye lehetővé a kliensekről való események összegyűjtését, előfeldolgozását és titkosított továbbítását a központi elem felé.
- Rendelkezzen olyan képességekkel, mely a beérkezett, illetve importálható eseménytípusokat automatikusan operációs rendszerek, funkciók, szolgáltatások, hálózati elhelyezkedésük, futtatott szoftverek szerint csoportosítsa, és kereshető adatbázisba tárolja le.
- Képes legyen konfigurációs fájlok módosításainak monitorozására például SSH vagy TELNET protokollal, a változások megjelenítésére.
- Az incidensek kezelésére legyen saját, beépített, vagy integrálható Ticketing rendszere.
- Az incidensek kezelésére legyen lehetőség automatikus megelőző intézkedések implementálására.
- Rendelkezzen UEBA (user and entity behavior analytics) képességekkel.
- A valós idejű riasztásokat és riportokat ténylegesen készítse valós időben. Nem elfogadható az események parsolása és tárolása utáni korreláció vizsgálat, riasztás küldés. A SIEM megoldásnak a riasztások kiküldését, korrelációk még az események lemezre (storage) írása előtt, memóriában kell megvalósítania.
- A SIEM megoldás valósítsa meg a SOC és NOC intelligenciát és legyen képes ezen események között keresztkorrelációs lekérdezésekre, riasztásokra.
- Rendelkezzen a gyártó által előfizethető és napi szinten frissíthető sérülékenységi adatbázissal, egyéb blacklist IP-k, Blacklist domain-ek listájával. A gyártói támogatáson felül legyen alkalmas a STIX/TAXII formátumban betölthető adatok küldésére illetve fogadására.
- Minimálisan elvárt eseményfogadási- és feldolgozási sebesség: 2500 EPS.

6.2.A logelemző (SIEM) rendszer telepítése során a Vállalkozó által nyújtandó szolgáltatások

- Tervezés
 - Helyszíni konzultáció, a logforrások, informatikai rendszer, célok megismerése
 - Írásos rendszerterv készítése
- Telepítés

- Egy tetszőleges Windows szerverre való klienstelepítés, Agent kommunikáció konfigurálása, egy policy létrehozása;
- Igény szerint helyi csoportok, felhasználók létrehozása, jogosultságuk beállítása;
- A logforrások IP tartományainak és IP címeinek definiálása;
- Lekérdezések, CMDB/Asset Management ellenőrzés és bemutatás és oktatás
- Beépített szabályok, riasztások, megelőző intézkedések, hibajegyek bemutatása, egyedi szabályok létrehozása igény szerint;
- Előre telepített riportok bemutatása, felhasználói igények szerinti további egyedi riportok konfigurálása;
- Dashboard konfigurálása;
- A Megrendelő szakembereinek felkészítése a rendszer komponenseinek teljes körű telepítésére („roll-out”);
- Mentés beállítása, rendszer konfiguráció mentése, visszaállítási lépések ismertetése;
- Dokumentáció
 - A telepítés és konfigurálás lépéseinek dokumentálása melynek segítségével reprodukálható a SIEM rendszer.
- Oktatás
 - Tantermi körülmények között, az NNK telephelyén üzemeltetői oktatás tartása, hivatalos gyártói tematika alapján minimum 5 fő részére legalább 5 nap terjedelemben. Az oktatás végére a résztvevőknek a SIEM rendszer telepítésével, üzemeltetésével kapcsolatos valamennyi lépéssel meg kell ismerkedniük. Az oktatási anyagot online és offline is rendelkezésre kell bocsátani.
- Támogatás
 - Az Ajánlattevőnek az átadott rendszert 6 hónapon keresztül kiemelten kell támogatnia, az alábbiak szerint:
 - Korlátlan távoli segítségnyújtás (email, telefon, remote desktop) munkaidőben a hibaelhárításhoz
 - Szükség esetén helyszíni kiszállás és konzultáció, segítség a rendszer finomhangolásában, a telepítés kiterjesztésében

6.3.A megajánlott megoldás méretezéshez szükséges információk

Microsoft alapú szerverek	Microsoft tartományvezérlő szerver (4 db), Microsoft alkalmazás szerver (50 db), Microsoft Exchange Server (4 db), Microsoft Web szerver (25 db), Microsoft DNS szerver (4 db), Microsoft SQL adatbázis szerver (4 db), DHCP szerver (4 db)
Linux alapú szerverek	Linux szerver (50 db), Linux adatbázis szerver (MYSQL), WEB server (Apache, Tomcat...) (10 db)

Egyéb:	VMware (15 db), Oracle 11G, Oracle 19C adatbázis szerverek.
Hálózati eszközök:	Tűzfal (2 db) Netflow-t küldő switch (1 db) Egyéb Switch (50 db) Antispam appliance (2 db)
Kliens végpontok:	Különböző Microsoft Windows 950 db

7. Valamennyi rendszer esetén elkészítendő dokumentumok, projekttermékek

Nyertes Ajánlattevő feladata a projekt végrehajtása során, az összes bevezetendő eszköz és szolgáltatás tekintetében, az alábbi dokumentumok és projekttermékek leszállítása:

- Rendszerterv
- Implementációs dokumentum
- Üzemeltetési kézikönyv
- Tesztelési terv
- Tesztelési forgatókönyvek
- Tesztelési jegyzőkönyvek
- Mentési-, Üzletfolytonossági-, valamint IT katasztrófa elhárítási terv a projekt során bevezetendő összes rendszerre vonatkozóan.
- Online és Offline oktatási dokumentáció gyártói tematika alapján a 3 témakörre összesen 10 nap keretben.
- Oktatásokról készült jegyzőkönyvek

8. Információbiztonsági követelmények

A jelen fejezetben a technológiai vhr 5-ös biztonsági osztályára vonatkozó adminisztratív és logikai védelmi intézkedések találhatóak, melyeket valamennyi szállítandó rendszer esetében teljesíteni kell. A védelmi intézkedéseket a tervezés fázisában előzetesen az Megrendelő információbiztonsági felelőssével egyeztetni kell és el kell vele fogadtatni a rendszertervet.

A fejezetben alkalmazott számozás megegyezik a technológiai vhr 4. sz. mellékletében alkalmazott számozással.

8.1.Valamennyi rendszerre vonatkozó információbiztonsági követelmények

3.1.3. Rendszer és szolgáltatás beszerzés

3.1.3.4. Az elektronikus információs rendszerre vonatkozó dokumentáció²

3.1.3.4.1. Az érintett szervezet:

² Az Ajánlattételi felhívás és egyéb közbeszerzési dokumentum 3-as pontjában felsorolt dokumentációk fedjék le a jelen pontban felsorolt tartalmi elemeket.

3.1.3.4.1.1. ha hatókörébe tartozik, megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre, vagy rendszerszolgáltatásra vonatkozó adminisztrátori dokumentációt, amely tartalmazza:

3.1.3.4.1.1.1. a rendszer, rendszerelem vagy rendszer szolgáltatás biztonságos konfigurálását, telepítését és üzemeltetését,

3.1.3.4.1.1.2. a biztonsági funkciók hatékony alkalmazását és fenntartását,

3.1.3.4.1.1.3. a konfigurációval és az adminisztratív funkciók használatával kapcsolatos, a dokumentáció átadásakor ismert sérülékenységeket;

3.1.3.4.1.2. megköveteli és birtokába veszi az elektronikus információs rendszerre, rendszerelemre vagy rendszerszolgáltatásra vonatkozó felhasználói dokumentációt, amely tartalmazza:

3.1.3.4.1.2.1. a felhasználó által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját,

3.1.3.4.1.2.2. a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságos használatának módszereit,

3.1.3.4.1.2.3. a felhasználó kötelezettségeit a rendszer, rendszerelem vagy rendszerszolgáltatás biztonságának a fenntartásához;

3.1.3.4.1.3. gondoskodik arról, hogy az információs rendszerre vonatkozó – különösen az adminisztrátori és fejlesztői – dokumentáció jogosulatlanok számára ne legyen megismerhető, módosítható;

3.1.3.4.1.4. gondoskodik a dokumentációknak az érintett szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismerésről.

3.1.4. Üzletmenet- (üzymenet-) folytonosság tervezése

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

3.1.4.2.1. Az érintett szervezet:

3.1.4.2.1.1. megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az elektronikus információs rendszerekre vonatkozó üzletmenet-folytonossági tervet;

3.1.4.2.1.2. összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;

3.1.4.2.1.3. meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszerhez kapcsolódó üzletmenet-folytonossági tervet;

3.1.4.2.1.4. az elektronikus információs rendszer vagy a működtetési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet;

3.1.4.2.1.5. tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket;

3.1.4.2.1.6. gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető, módosítható;

3.1.4.2.1.7. meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;

3.1.4.2.1.8. rendelkezik a helyreállítási feladatokról, a helyreállítási prioritásokról és mértékekről;

3.1.4.2.1.9. jelöli a vészhelyzeti szerepköröket, felelőségeket, a kapcsolattartó személyeket;

3.1.4.2.1.10. fenntartja a szervezet által előzetesen definiált alapszolgáltatásokat, még az elektronikus információs rendszer összeomlása, kompromittálódása vagy hibája ellenére is;
3.1.4.2.1.11. kidolgozza a végleges, teljes elektronikus információs rendszer helyreállításának tervét úgy, hogy az nem ronthatja le az eredetileg tervezett és megvalósított biztonsági védelmeket.

3.1.4.8. Az elektronikus információs rendszer mentései

3.1.4.8.1. Az érintett szervezet:

3.1.4.8.1.1. meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.2. meghatározott gyakorisággal elmenti az elektronikus információs rendszerben tárolt rendszerszintű információkat, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.3. meghatározott gyakorisággal elmenti az elektronikus információs rendszer dokumentációját, köztük a biztonságra vonatkozókat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal;

3.1.4.8.1.4. megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a másodlagos tárolási helyszínen.

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

Az érintett szervezet gondoskodik az elektronikus információs rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

3.3.2. Tervezés

3.3.2.2. Rendszerbiztonsági terv³

3.3.2.2.1. Az érintett szervezet, ha az elektronikus információs rendszer tervezése a hatókörébe tartozik, az elektronikus információs rendszerhez rendszerbiztonsági tervet készít, amely:

3.3.2.2.1.1. összhangban áll szervezeti felépítésével vagy szervezeti szintű architektúrájával;

3.3.2.2.1.2. meghatározza az elektronikus információs rendszer hatókörét, alapfeladatait (biztosítandó szolgáltatásait), biztonságkritikus elemeit és alapfunkcióit;

3.3.2.2.1.3. meghatározza az elektronikus információs rendszer és az általa kezelt adatok jogszabály szerinti biztonsági osztályát;

3.3.2.2.1.4. meghatározza az elektronikus információs rendszer működési körülményeit és más elektronikus információs rendszerekkel való kapcsolatait;

3.3.2.2.1.5. a vonatkozó rendszerdokumentáció keretében foglalja az elektronikus információs rendszer biztonsági követelményeit;

3.3.2.2.1.6. meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket és intézkedés bővítéseket, végrehajtja a jogszabály szerinti biztonsági feladatokat;

3.3.2.2.1.7. gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyi és szerepkörökben dolgozók megismerjék (ideértve annak változásait is);

³ Az Ajánlattételi felhívás és egyéb közbeszerzési dokumentum 3-as pontjában felsorolt dokumentációk fedjék le a jelen pontban felsorolt tartalmi elemeket.

3.3.2.2.1.8. belső szabályozásában, vagy a rendszerbiztonsági tervben meghatározott gyakorisággal felülvizsgálja az elektronikus információs rendszer rendszerbiztonsági tervét;
3.3.2.2.1.9. frissíti a rendszerbiztonsági tervet az elektronikus információs rendszerben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén;

3.3.2.2.1.10. elvégzi a szükséges belső egyeztetéseket;

3.3.2.2.1.11. gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető, módosítható.

3.3.3. Rendszer és szolgáltatás beszerzés

3.3.3.3. Funkciók, portok, protokollok, szolgáltatások

Az érintett szervezet megköveteli, hogy a szolgáltató meghatározza a szolgáltatások igénybevételéhez szükséges funkciókat, protokollokat, portokat és egyéb szolgáltatásokat.

3.3.6. Konfigurációkezelés

3.3.6.2. Alapkonfiguráció

3.3.6.2.1. Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.

3.3.6.5.4. Aláírt elemek

A szervezet által meghatározott szoftver- és az úgynevezett firmware (vezérlőeszköz) elemek esetében meg kell akadályozni az elemek telepítését, ha azok nincsenek digitálisan aláírva ismert és jóváhagyott tanúsítvány alkalmazásával.

3.3.6.6. Konfigurációs beállítások

3.3.6.6.1. Az érintett szervezet:

3.3.6.6.1.1. meghatározza a működési követelményeknek még megfelelő, de a biztonsági szempontból a lehető leginkább korlátozott módon - a „szükséges minimum” elv alapján - az elektronikus információs rendszerben használt információtechnológiai termékekre kötelező konfigurációs beállítást, és ezt ellenőrzési listaként dokumentálja;

3.3.6.6.1.2. elvégzi a konfigurációs beállításokat az elektronikus információs rendszer valamennyi elemében;

3.3.6.6.1.3. a meghatározott elemek konfigurációs beállításában azonosít, dokumentál és jóváhagy minden eltérést;

3.3.6.6.1.4. figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait, az érintett szervezet belső szabályzataival és eljárásaival összhangban.

3.3.6.7. Legszűkebb funkcionális

3.3.6.7.1. Az érintett szervezet:

3.3.6.7.1.1. az elektronikus információs rendszert úgy konfigurálja, hogy az csak a szükséges szolgáltatásokat nyújtsa;

3.3.6.7.1.2. meghatározza a tiltott, vagy korlátozott, nem szükséges funkciók, portok, protokollok, szolgáltatások, szoftverek használatát.

3.3.9. Azonosítás és hitelesítés⁴

3.3.9.2. Azonosítás és hitelesítés

3.3.9.2.1. Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a szervezet felhasználóit, a felhasználók által végzett tevékenységet.

⁴ Jelen fejezetben foglalt követelmények teljesítésétől annak függvényében lehet részben vagy teljes egészében eltekinteni, hogy ha a szállított rendszer Active Directory integrált azonosítást és hitelesítést fog alkalmazni.

3.3.9.2.2. Hálózati hozzáférés privilegizált fiókokhoz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a különleges jogosultsághoz kötött - úgynevezett privilegizált - felhasználói fiókokhoz való hálózaton keresztüli hozzáféréshez.

3.3.9.5. A hitelesítésre szolgáló eszközök kezelése

3.3.9.5.1. Az érintett szervezet:

3.3.9.5.1.1. ellenőrzi a hitelesítésre szolgáló eszközök kiosztásakor az eszközt átvevő egyén, csoport, szerepkör vagy eszköz jogosultságát;

3.3.9.5.1.2. meghatározza a hitelesítésre szolgáló eszköz kezdeti tartalmát;

3.3.9.5.1.3. biztosítja a hitelesítésre szolgáló eszköz tervezett felhasználásának megfelelő jogosultságokat;

3.3.9.5.1.4. dokumentálja a hitelesítésre szolgáló eszközök kiosztását, visszavonását, cseréjét, az elvesztett, vagy a kompromittálódott, vagy a sérült eszközöket;

3.3.9.5.1.5. megváltoztatja a hitelesítésre szolgáló eszközök alapértelmezés szerinti értékét az elektronikus információs rendszer telepítése során;

3.3.9.5.1.6. meghatározza a hitelesítésre szolgáló eszközök minimális és maximális használati idejét, valamint ismételt felhasználhatóságának feltételeit;

3.3.9.5.1.7. a hitelesítésre szolgáló eszköz típusra meghatározott időnként megváltoztatja vagy frissíti a hitelesítésre szolgáló eszközöket;

3.3.9.5.1.8. megvédi a hitelesítésre szolgáló eszközök tartalmát a jogosulatlan felfedéstől és módosítástól;

3.3.9.5.1.9. megköveteli a hitelesítésre szolgáló eszközök felhasználóitól, hogy védjék eszközeik bizalmasságát, sértetlenségét;

3.3.9.5.1.10. lecseréli a hitelesítésre szolgáló eszközt az érintett fiókok megváltoztatásakor.

3.3.9.5.2. Jelszó (tudás) alapú hitelesítés

3.3.9.5.2.1. Az érintett szervezet:

3.3.9.5.2.1.1. a jelszóra a következő elvárásokat érvényesíti: kis- és nagybetűk megkülönböztetése; a karakterek számának meghatározása; a kisbetűk, nagybetűk, számok és speciális karakterek, és minimális jelszóhosszúság;

3.3.9.5.2.1.2. meghatározott szám karakterváltozást kényszerít ki új jelszó létrehozásakor;

3.3.9.5.2.1.3. a jelszavakat nem tárolja (ide nem értve az irreverzibilis kriptográfiai hasító függvényrel a jelszóból képzett hasító érték tárolást) és nem továbbítja;

3.3.9.5.2.1.4. a jelszavakra minimális és maximális élettartam korlátozást juttat érvényre úgy, hogy meghatározott számú új jelszóig megtiltja a jelszavak ismételt felhasználását, és a rendszerbe első lépést lehetővé tevő ideiglenes jelszó lecserélésére kötelez.

3.3.9.5.3. Birtoklás alapú hitelesítés

3.3.9.5.3.1. Az érintett szervezet:

3.3.9.5.3.1.1. az elektronikus információs rendszer hardver token alapú hitelesítése esetén olyan mechanizmusokat alkalmaz, amely megfelel az érintett szervezet által meghatározott minőségi követelményeknek, vagy

3.3.9.5.3.1.2. az elektronikus információs rendszer nyilvános kulcsú infrastruktúra alapú hitelesítés esetén:

3.3.9.5.3.1.2.1. ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is;

3.3.9.5.3.1.2.2. kikényszeríti a megfelelő magánkulcshoz való jogosult hozzáférést;

3.3.9.5.3.1.2.3. összekapcsolja a hitelesített azonosságot az egyéni vagy csoport fiókkal;

3.3.9.5.3.1.2.4. megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlanc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

3.3.9.6. A hitelesítésre szolgáló eszköz visszacsatolása

Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

3.3.10. Hozzáférés ellenőrzése⁵

3.3.10.2. Felhasználói fiókok kezelése

3.3.10.2.1. Az érintett szervezet:

3.3.10.2.1.1. meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait, és ezek típusait;

3.3.10.2.1.2. kijelöli a felhasználói fiókok fiókkezelőit;

3.3.10.2.1.3. kialakítja a csoport- és szerepkör tagsági feltételeket;

3.3.10.2.1.4. meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit;

3.3.10.2.1.5. létrehozza, engedélyezi, módosítja, letiltja és eltávolítja a felhasználói fiókokat a meghatározott eljárásokkal vagy feltételekkel összhangban;

3.3.10.2.1.6. ellenőrzi a felhasználói fiókok használatát;

3.3.10.2.1.7. értesíti a fiókkezelőket, ha:

3.3.10.2.1.7.1. a felhasználói fiókokra már nincsen szükség,

3.3.10.2.1.7.2. a felhasználók kiléptek vagy áthelyezésre kerültek,

3.3.10.2.1.7.3. az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak;

3.3.10.2.1.8. feljogosít az elektronikus információs rendszerhez való hozzáférésre:

3.3.10.2.1.8.1. az érvényes hozzáférési engedély,

3.3.10.2.1.8.2. a tervezett rendszerhasználat,

3.3.10.2.1.8.3. az alapfeladatok és funkcióik alapján;

3.3.10.2.1.9. meghatározott gyakorisággal felülvizsgálja a felhasználói fiókokat, a fiókkezelési követelményekkel való összhangot;

3.3.10.2.1.10. kialakít egy folyamatot a megosztott vagy csoport felhasználói fiókokhoz tartozó hitelesítő eszközök vagy adatok újra kibocsátására (ha ilyet alkalmaznak), a csoport tagjainak változása esetére.

3.3.10.2.3. Ideiglenes fiókok eltávolítása

Meghatározott időtartam letelte után az elektronikus információs rendszer automatikusan eltávolítja, vagy letiltja az ideiglenes vagy kényszerhelyzetben létrehozott felhasználói fiókokat, vagy egyes kijelölt felhasználói fiók típusokat.

3.3.10.2.4. Inaktív fiókok letiltása

Az elektronikus információs rendszer automatikusan letiltja az inaktív fiókokat meghatározott időtartam letelte után.

3.3.10.2.5. Automatikus naplózás

⁵ Jelen fejezetben foglalt követelmények teljesítésétől annak függvényében lehet részben vagy teljes egészében eltekinteni, hogy ha a szállított rendszer Active Directory integrált azonosítást és hitelesítést fog alkalmazni.

Az elektronikus információs rendszer automatikusan naplózza a fiókok létrehozásával, módosításával, engedélyezésével, letiltásával és eltávolításával kapcsolatos tevékenységeket, és értesíti ezekről a meghatározott személyeket vagy szerepköröket.

3.3.10.2.6. Kiléptetés

Meghatározott időtartamú várható inaktivitás, vagy egyéb előre meghatározott esetekben ki kell léptetni a felhasználót.

3.3.10.3. Hozzáférés ellenőrzés érvényesítése

Az elektronikus információs rendszer a megfelelő szabályzatokkal összhangban érvényesíti a jóváhagyott jogosultságokat az információkhoz és a rendszer erőforrásaihoz való logikai hozzáféréshez.

3.3.10.6. Legkisebb jogosultság elve

3.3.10.6.1. Az elektronikus információs rendszer a legkisebb jogosultság elvét alkalmazza, azaz a felhasználók - vagy a felhasználók tevékenysége - számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi.

3.3.10.6.2. Jogosult hozzáférés a biztonsági funkciókhoz

Az érintett szervezet hozzáférési jogosultságokat biztosít a meghatározott biztonsági funkciókhoz és biztonságkritikus információkhoz.

3.3.10.6.3. Nem privilegizált hozzáférés a biztonsági funkciókhoz

Az érintett szervezet kötelezővé teszi, hogy a szervezet meghatározott biztonsági funkciókhoz vagy biztonságkritikus információkhoz hozzáférési jogosultsággal rendelkező felhasználói a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett privilegizált - fiókjukat vagy szerepkörüket használják.

3.3.10.6.4. Privilegizált fiókok

Az érintett szervezet az elektronikus információs rendszer privilegizált fiókjait meghatározott személyekre vagy szerepkörökre korlátozza.

3.3.10.6.5. Privilegizált funkciók használatának naplózása

Az elektronikus információs rendszer naplózza a privilegizált funkciók végrehajtását.

3.3.10.6.7. Hálózati hozzáférés a privilegizált parancsokhoz

A meghatározott privilegizált parancsok hálózaton keresztüli elérését csak meghatározott üzemeltetési szükséghelyzetben lehet engedélyezni, és az ilyen hozzáférések indoklását dokumentálni kell a rendszerbiztonsági tervben. Privilegizált parancsok csak meghatározott munkaállomásokról, terminálokról, szegmensekről és IP címekről adhatóak ki, mely munkaállomások/terminálok helyiségei fizikai hozzáférés szempontjából normáltól eltérő szintű besorolást kapnak.

3.3.10.7. Sikertelen bejelentkezési kísérletek

3.3.10.7.1. Az elektronikus információs rendszer:

3.3.10.7.1.1. az érintett szervezet által meghatározott esetszám korlátot alkalmaz a felhasználó meghatározott időtartamon belül egymást követő sikertelen bejelentkezési kísérleteire;

3.3.10.7.1.2. amennyiben a sikertelen bejelentkezési kísérletekre felállított esetszám korlátot a felhasználó túllépi, automatikusan zárolja a felhasználói fiókot, vagy csomópontot meghatározott időtartamig, vagy meghatározott módon késlelteti a következő bejelentkezési kísérletet.

3.3.10.9. Egyidejű munkaszakasz kezelés

Az érintett szervezet az elektronikus információs rendszerben meghatározott számra korlátozza az egyidejű munkaszakaszok számát, a meghatározott fiókok vagy fiók típusok számára külön-külön.

3.3.10.10. A munkaszakasz zárolása

3.3.10.10.1. Az érintett szervezet:

3.3.10.10.1.1. meghatározott időtartamú inaktivitás után, vagy a felhasználó erre irányuló lépése esetén a munkaszakasz zárolásával megakadályozza az elektronikus információs rendszerhez való további hozzáférést;

3.3.10.10.1.2. megtartja a munkaszakasz zárolását mindaddig, amíg a felhasználó a megfelelő eljárások alkalmazásával nem azonosítja és hitelesíti magát újra.

3.3.10.10.2. Képernyőtakarás

A munkaszakasz zárolásakor a képernyőn korábban látható információt egy nyilvánosan látható képpel (vagy üres képernyővel), vagy a bejelentkezési felülettel - ami a zároló személy nevét is tartalmazhatja - kell eltakarni.

3.3.10.11. A munkaszakasz lezárása

Az elektronikus információs rendszer automatikusan lezárja a munkaszakaszt az érintett szervezet által meghatározott feltételek vagy munkaszakasz szétkapcsolást igénylő események megtörténte után.

3.3.10.12. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

3.3.10.12.1. Az érintett szervezet:

3.3.10.12.1.1. kijelöli azokat a felhasználói tevékenységeket, amelyeket az elektronikus információs rendszerben azonosítás vagy hitelesítés nélkül is végre lehet hajtani;

3.3.10.12.1.2. dokumentálja és indokolja a rendszerbiztonsági tervben, vagy más szabályzatban az azonosítás vagy hitelesítés nélkül is végrehajtható felhasználói tevékenységeket.

3.3.12. Naplózás és elszámoltathatóság

3.3.12.2. Naplózható események

3.3.12.2.1. Az érintett szervezet:

3.3.12.2.1.1. meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét;

3.3.12.2.1.2. egyeztet a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;

3.3.12.2.1.3. megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

3.3.12.3. Naplóbejegyzések tartalma

3.3.12.3.1. Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

3.3.12.4. Napló tárhelykapacitás

Az érintett szervezet a naplózásra elegendő méretű tárhelykapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

3.3.12.5. Naplózási hiba kezelése

3.3.12.5.1. Az elektronikus információs rendszer:

3.3.12.5.1.1. naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek;

3.3.12.5.1.2. elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítást, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítást.

3.3.12.5.2. Naplózási tárhely ellenőrzés

Az elektronikus információs rendszer figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a beállított maximális naplózási tárhely előre meghatározott részét.

3.3.12.8. Időbélyegek

3.3.12.8.1. Az elektronikus információs rendszer:

3.3.12.8.1.1. belső rendszerórát használ a naplóbejegyzések időbélyegeinek előállításához;

3.3.12.8.1.2. időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidejűhöz - úgynevezett GMT - rendelhető módon, megfelelően az érintett szervezet által meghatározott időmérési pontosságnak.

3.3.12.8.2. Szinkronizálás

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórát egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórát a hiteles külső időforrással.

3.3.12.9. A naplóinformációk védelme

3.3.12.9.1. Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

3.3.12.9.2. Hozzáférés korlátozása

A naplófunkciók kezelésére csak az érintett szervezet által meghatározott, privilegizált felhasználók jogosultak.

3.3.12.12. Naplógenerálás

3.3.12.12.1. Az elektronikus információs rendszer:

3.3.12.12.1.1. biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.12.2. pontban meghatározott, naplózható eseményekre;

3.3.12.12.1.2. lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire;

3.3.12.12.1.3. naplóbejegyzéseket állít elő a 3.3.12.2. pont szerinti eseményekre a 3.3.12.3. pontban meghatározott tartalommal.

3.3.13. Rendszer- és kommunikációvédelem

3.3.13.3. Biztonsági funkciók elkülönítése

Az elektronikus információs rendszer elkülöníti a biztonsági funkciókat a nem biztonsági funkcióktól.

3.3.13.7. Az adatátvitel bizalmassága

3.3.13.7.1. Az elektronikus információs rendszer védje meg a továbbított információk bizalmasságát.

3.3.13.7.2. Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk jogosulatlan felfedése ellen, kivéve, ha az átvitel más, az érintett szervezet által meghatározott alternatív fizikai ellenintézkedéssel védett.

3.3.13.8. Az adatátvitel sértetlensége

3.3.13.8.1. Az elektronikus információs rendszer megvédi a továbbított információk sértetlenségét.

3.3.13.8.2. Kriptográfiai vagy egyéb védelem

Az elektronikus információs rendszer kriptográfiai mechanizmusokat alkalmaz az adatátvitel során az információk megváltozásának észlelésére, ha az átvitel nincsen más alternatív fizikai intézkedésekkel védve.

3.3.13.11. Kriptográfiai védelem

Az elektronikus információs rendszer szabványos, egyéb jogszabályokban biztonságosnak minősített kriptográfiai műveleteket valósít meg.

8.2.Tűzfalrendszerre vonatkozó információbiztonsági többletkövetelmények

A szállítandó tűzfal rendszernek biztosítania és támogatnia kell a technológiai vhr következő pontjaiban foglalt adminisztratív és logikai védelmi intézkedéseket, illetve úgy kell tervezni és konfigurálni az eszközöket, hogy a lenti követelmények is teljesüljenek:

3.1.6. Emberi tényezőket figyelembe vevő - személy – biztonság

3.1.6.9. Viselkedési szabályok az interneten

3.1.6.9.1. Az érintett szervezet:

3.1.6.9.1.1. tiltja és számon kéri a szervezettel kapcsolatos információk nyilvános internetes oldalakon való illegális közzétételét;

3.1.6.9.1.2. tiltja a belső szabályzatában meghatározott, interneten megvalósuló tevékenységet (pl.: chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták, stb.);

3.1.6.9.1.3. tilthatja a közösségi oldalak használatát, magánpostafiók elérését, és más, a szervezettől idegen tevékenységet.

3.3.9. Azonosítás és hitelesítés

3.3.9.2.6. Távoli hozzáférés - külön eszköz

Az elektronikus információs rendszer többtényezős hitelesítést alkalmaz a felhasználói fiókokhoz való távoli hozzáféréshez, és az egyik hozzáférést megelőző tényező egy, az elektronikus információs rendszertől elkülönülő olyan eszköz, amelyen a meghatározott biztonsági követelmények teljesülnek.

3.3.10. Hozzáférés ellenőrzése

3.3.10.13.2. Ellenőrzés

Az elektronikus információs rendszer figyelmeztet és ellenőrzi a távoli hozzáféréseket.

3.3.10.13.3. Titkosítás

Kriptográfiai mechanizmusokat kell alkalmazni a távoli hozzáférés munkaszakaszok bizalmasságának és sértetlenségének a védelmére.

3.3.10.13.4. Hozzáférés ellenőrzési pontok

Minden távoli hozzáférést felügyelt hozzáférés ellenőrzési ponton keresztül kell irányítani az elektronikus információs rendszerben.

3.3.11. Rendszer- és információsértetlenség

3.3.11.4. Kártékony kódok elleni védelem⁶

3.3.11.4.1. Az érintett szervezet:

3.3.11.4.1.1. az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;

3.3.11.4.1.2. frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

3.3.11.4.1.3. konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem eszköze:

3.3.11.4.1.3.1. rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtja végre a külső forrásokból származó fájlok valós idejű ellenőrzését a

⁶ A web böngészés szolgáltatás esetében értelmezendő.

végpontokon, a hálózati belépési, vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

3.3.11.4.1.3.2. a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt; és riassza a rendszeradminisztrátort, és az érintett szervezet által meghatározott további személy(ek)e)t;

3.3.11.4.1.4. ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

3.3.11.4.2. Központi kezelés

Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.4.3. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.5. Az elektronikus információs rendszer felügyelete

3.3.11.5.1. Az érintett szervezet:

3.3.11.5.1.1. felügyeli az elektronikus információs rendszert, hogy észlelje a kibertámadásokat, vagy a kibertámadások jeleit a meghatározott figyelési céloknak megfelelően, és feltárja a jogosulatlan lokális, hálózati és távoli kapcsolatokat;

3.3.11.5.1.2. azonosítja az elektronikus információs rendszer jogosulatlan használatát;

3.3.11.5.1.3. felügyeleti eszközöket alkalmaz a meghatározott alapvető információk gyűjtésére; és a rendszer ad hoc területeire a potenciálisan fontos, speciális típusú tranzakcióknak a nyomon követésére;

3.3.11.5.1.4. védi a behatolás-felügyeleti eszközökből nyert információkat a jogosulatlan hozzáféréssel, módosítással és törléssel szemben;

3.3.11.5.1.5. erősíti az elektronikus információs rendszer felügyeletét minden olyan esetben, amikor fokozott kockázatra utaló jelet észlel;

3.3.11.5.1.6. meghatározott gyakorisággal biztosítja az elektronikus információs rendszer felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek.

3.3.11.5.2. Automatizálás

Automatizált eszközöket kell alkalmazni az események közel valós idejű vizsgálatának támogatására.

3.3.11.5.3. Felügyelet

Az elektronikus információs rendszer felügyelje a beérkező és kimenő adatforgalmat a szokatlan vagy jogosulatlan tevékenységekre, vagy körülményre tekintettel.

3.3.11.5.4. Riasztás

Az elektronikus információs rendszer riassza az érintett szervezet illetékes személyeit, csoportjait, amikor veszélyeztetés vagy lehetséges veszélyeztetés előre meghatározott jeleit észleli.

3.3.13. Rendszer- és kommunikációvédelem

3.3.13.5. Túlterhelés - szolgáltatás megtagadás alapú támadás - elleni védelem

Az elektronikus információs rendszer véd a túlterheléses (ügynevezett szolgáltatás megtagadás) jellegű támadásokkal szemben, vagy korlátozza azok kihatásait a megtagadás jellegű támadások listája alapján, a meghatározott biztonsági intézkedések bevezetésével.

3.3.13.6. A határok védelme

3.3.13.6.1. Az elektronikus információs rendszer:

3.3.13.6.1.1. felügyeli és ellenőrzi a külső határain történő, valamint a rendszer kulcsfontosságú belső határain történő kommunikációt;

3.3.13.6.1.2. a nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól;

3.3.13.6.1.3. csak az érintett szervezet biztonsági architektúrájával összhangban elhelyezett határvédelmi eszközökön felügyelt interfészeken keresztül kapcsolódik külső hálózatokhoz vagy külső elektronikus információs rendszerekhez.

3.3.13.6.2. Hozzáférési pontok

Az érintett szervezet korlátozza az elektronikus információs rendszer külső hálózati kapcsolatainak a számát.

3.3.13.6.3. Külső kommunikációs szolgáltatások

3.3.13.6.3.1. Az érintett szervezet:

3.3.13.6.3.1.1. felügyelt interfészt működtet minden külső infokommunikációs szolgáltatáshoz;

3.3.13.6.3.1.2. minden felügyelt interfészhez forgalomáramlási szabályokat alakít ki;

3.3.13.6.3.1.3. védi az összes interfésznél az átvitelre kerülő információk bizalmasságát és sértetlenségét;

3.3.13.6.3.1.4. dokumentál minden kivételt a forgalomáramlási szabályok alól, a kivételt alátámasztó alapeladattal és az igényelt kivétel időtartamával együtt;

3.3.13.6.3.1.5. meghatározott gyakorisággal áttekinti a forgalomáramlási szabályok alóli kivételeket, és eltávolítja azokat a kivételeket, amelyeket közvetlen alapeladat már nem indokol.

3.3.13.6.4. Alapeseti visszautasítás

Az elektronikus információs rendszer a felügyelt kapcsolódási pontjain tilt, és csak kivételként engedélyez hálózati forgalmat.

3.3.13.6.5. Távoli készülékek megosztott csatornahasználatának tiltása

A távoli készülékkel kapcsolatban álló elektronikus információs rendszer meggátolja, hogy a készülék egyidejűleg helyi kapcsolatokat létesítsen a rendszerrel.

3.3.13.6.8. Rendszerelemek elkülönítése

Az érintett szervezet határvédelmi mechanizmusokat alkalmaz azoknak az elektronikus információs rendszerelemeknek az elkülönítésére, amelyek a meghatározott alapeladatokat és alapfunkciókat támogatják.

3.3.13.14. Mobilkód korlátozása

3.3.13.14.1. Az érintett szervezet:

3.3.13.14.1.1. meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat;

3.3.13.14.1.2. használati korlátozásokat vezet be, vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra;

3.3.13.14.1.3. engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

8.3.A levélszűrő rendszerrel szemben támasztott információbiztonsági többletkövetelmények

A szállítandó levélszűrő rendszernek biztosítania és támogatnia kell a technológiai vhr következő pontjaiban foglalt adminisztratív és logikai védelmi intézkedéseket, illetve úgy kell tervezni és konfigurálni az eszközöket, hogy a lenti követelmények is teljesüljenek:

3.3.11. Rendszer- és információsértetlenség

3.3.11.4. Kártékony kódok elleni védelem⁷

3.3.11.4.1. Az érintett szervezet:

3.3.11.4.1.1. az elektronikus információs rendszerét annak belépési és kilépési pontjain védi a kártékony kódok ellen, felderíti és megsemmisíti azokat;

3.3.11.4.1.2. frissíti a kártékony kódok elleni védelmi mechanizmusokat a konfigurációkezelési szabályaival és eljárásaival összhangban minden olyan esetben, amikor kártékony kódirtó rendszeréhez frissítések jelennek meg;

3.3.11.4.1.3. konfigurálja a kártékony kódok elleni védelmi mechanizmusokat úgy, hogy a védelem csökkönjen;

3.3.11.4.1.3.1. rendszeres ellenőrzéseket hajtson végre az elektronikus információs rendszeren, és hajtson végre a külső forrásokból származó fájlok valós idejű ellenőrzését a végpontokon, a hálózati belépési, vagy kilépési pontokon, a biztonsági szabályzatnak megfelelően, amikor a fájlokat letöltik, megnyitják, vagy elindítják,

3.3.11.4.1.3.2. a kártékony kód észlelése esetén blokkolja vagy helyezze karanténba azt; és riassza a rendszeradminisztrátort, és az érintett szervezet által meghatározott további személy(ek)et;

3.3.11.4.1.4. ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az elektronikus információs rendszer rendelkezésre állására.

3.3.11.4.2. Központi kezelés

Az elektronikus információs rendszer központilag kezeli a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.4.3. Automatikus frissítés

Az elektronikus információs rendszer automatikusan frissíti a kártékony kódok elleni védelmi mechanizmusokat.

3.3.11.9. Kéretlen üzenetek elleni védelem

3.3.11.9.1. Az érintett szervezet:

3.3.11.9.1.1. kéretlen üzenetek - úgynevezett levélszemét - elleni védelmet valósít meg az elektronikus információs rendszer belépési és kilépési pontjain, a levélszemét észlelése és kiszűrése érdekében;

3.3.11.9.1.2. új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat, összhangban a konfigurációkezelési szabállyal és eljárásrenddel.

3.3.11.9.2. Központi kezelés

Az érintett szervezet központi beállításokkal irányítja a levélszemét elleni védelmet.

3.3.11.9.3. Frissítés

Az elektronikus információs rendszer automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat azok újabb verzióival.

3.3.13.14. Mobilkód korlátozása

3.3.13.14.1. Az érintett szervezet:

⁷ Az elektronikus levelezési szolgáltatás vonatkozásában

- 3.3.13.14.1.1. meghatározza az elfogadható és a nem elfogadható mobilkódokat és mobilkód technológiákat;
- 3.3.13.14.1.2. használati korlátozásokat vezet be, vagy megvalósítási útmutatót bocsát ki az elfogadható mobilkódokra és mobilkód technológiákra;
- 3.3.13.14.1.3. engedélyezi, felügyeli és ellenőrzi a mobilkódok használatát az elektronikus információs rendszeren belül.

8.4. Logelemző (SIEM) rendszerrel szemben támasztott információbiztonsági követelmények

A szállítandó logelemző (SIEM) rendszernek biztosítania és támogatnia kell a technológiai vhr következő pontjaiban foglalt adminisztratív és logikai védelmi intézkedéseket, illetve úgy kell tervezni és konfigurálni az eszközöket, hogy a lenti követelmények is teljesüljenek:

3.1.5 A biztonsági események kezelése

3.1.5.2. Automatikus eseménykezelés

Az érintett szervezet automatizált mechanizmusokat alkalmaz az eseménykezelési eljárások támogatására.

3.1.5.3. Információ korreláció

Az érintett szervezet összekapcsolja a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és reagálásokra.

3.1.5.4. A biztonsági események figyelése

Az érintett szervezet nyomon követi és dokumentálja az elektronikus információs rendszer biztonsági eseményeit.

3.1.5.5. Automatikus nyomon követés, adatgyűjtés és vizsgálat

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.

3.1.5.6.2. Automatizált jelentés

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események jelentését.

3.1.5.7.2. Automatizált támogatás

Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk és a támogatás rendelkezésre állását.

3.3.12. Naplózás és elszámoltathatóság

3.3.12.3.3. Központi kezelés

Az elektronikus információs rendszer biztosítja a meghatározott rendszerelemek által generált naplóbejegyzések tartalmának központi kezelését és konfigurálását.

3.3.12.5.3. Valós idejű riasztás

Az elektronikus információs rendszer riasztást küld, ha a meghatározott, valós idejű riasztást igénylő hibaesemények listája szerint valamely esemény megtörténik.

3.3.12.6. Naplóvizsgálat és jelentéskészítés

3.3.12.6.1. Az érintett szervezet:

3.3.12.6.1.1. rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából;

3.3.12.6.1.2. jelenti ezeket a meghatározott személyeknek, vagy szerepköröknek.

3.3.12.6.2. Folyamatba illesztés

Az érintett szervezet automatikus mechanizmusokat használ a naplóbejegyzések vizsgálatának, elemzésének és jelentésének átfogó folyamattá integrálására, amely a veszélyes, vagy tiltott tevékenységekre és történésekre reagál.

3.3.12.6.3. Összegzés

Az érintett szervezet megvizsgálja és összefüggésbe hozza a különböző adattárakban található naplóbejegyzéseket, a teljes érintett szervezetre kiterjedő helyzetfelmérés érdekében.

3.3.12.6.4. Felügyeleti képességek integrálása

Az érintett szervezet egyesíti a naplóbejegyzések vizsgálatát a sebezhetőség ellenőrzési információkkal, a teljesítmény adatokkal, az elektronikus információs rendszer felügyeletéből származó információkkal, vagy egyéb forrásokból begyűjtött adatokkal vagy információkkal.

3.3.12.6.5. Összekapcsolás a fizikai hozzáférési információkkal

Az érintett szervezet összefüggésbe hozza a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert információkkal.

3.3.12.7. Naplósökkentés és jelentéskészítés

3.3.12.7.1. Az elektronikus információs rendszer:

3.3.12.7.1.1. lehetőséget biztosít naplósökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplótisztítási és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;

3.3.12.7.1.2. nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

3.3.12.7. Naplósökkentés és jelentéskészítés

3.3.12.7.1. Az elektronikus információs rendszer:

3.3.12.7.1.1. lehetőséget biztosít naplósökkentésre és jelentés készítésére, amely támogatja az igény esetén végzendő naplóáttekintési, naplótisztítási és jelentéskészítési követelményeket és a biztonsági eseményeket követő tényfeltáró vizsgálatait;

3.3.12.7.1.2. nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

3.3.12.7.2. Automatikus feldolgozás

Az elektronikus információs rendszer biztosítja, hogy a fontos naplóbejegyzéseket automatikusan fel lehessen dolgozni.

3.3.12.9.4. Kriptográfiai védelem

Kriptográfiai mechanizmusokat kell alkalmazni a naplóinformáció és a napló kezelő eszköz sértetlenségének védelmére.

3.3.12.10. Letagadhatatlanság

Az elektronikus információs rendszer védelmet biztosít az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.

3.3.12.11. A naplóbejegyzések megőrzése

Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

9. A beszerzendő licencek, eszközök és szolgáltatások mintakonfigurációja az ITBT2017 szerint:

Sorszám	Megnevezés (árlista szerint)	cikk azonosító	Jelleg	Mennyiség	Egység
1.	FortiGate-2500E 10 x 10GE SFP+ slots, 2 x 10GE bypass SFP+ (LC Adapter), 34 x GE RJ45 ports (including 32 x ports, 2 x management/HA ports), SPU NP6 and CP9 hardware accelerated, 480GB SSD onboard storage	FTNT-FGx2500E-B	hardver	2	db
2.	FortiGate-2500E 1 Year UTM Bundle (24x7 FortiCare plus Application Control, IPS, AV, Botnet IP/Domain, Web Filtering and Antispam Services)	FTNT-FC-10-02K5Ex950-02-12-C	gyártói támogatás	6	db
	Barracuda Email Security Gateway 400	BSFI400A	hardver	2	db
4.	Barracuda Email Security Gateway Appliance 400 Energize Updates Subscription 1 Month	BSFI400A-E	gyártói támogatás	72	db
5.	Barracuda Email Security Gateway Appliance 400 Instant Replacement Subscription 1 Month	BSFI400A-H	gyártói támogatás	72	db
6.	FortiSIEM 50 devices and 500 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	FTNT-FSMxAIO-BASE-B	licenc	1	db
7.	FortiSIEM Add 25 devices and 250 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	FTNT-FSMxAIO-25-UG-B	licenc	1	db
8.	FortiSIEM Add 100 devices and 1000 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	FTNT-FSMxAIO-100-UG-B	licenc	1	db

9.	FortiSIEM 100 Advanced Windows Agents for perpetual license. Each Windows Agent requires a device license. Does not include Maintenance & Support	FTNT-FSMxWIN-ADV-100-UG-B	licenc	1	db
10.	EPS Add Add 1 EPS Perpetual for Non-MSP/MSSP's	FTNT-FSMxEPS-100-UG-B	licenc	1000	db
11.	FortiCare 1 Year 24x7 FortiCare Contract (1 - 300 points) for FortiSIEM Software deployments. 1 device or 2 End points or 3 Windows Agents equals 1 point.	FTNT-FC4-10-FSM9x248-02-12-C	gyártói támogatás	3	db
12.	Subscription license for the FortiGuard Indicator of Compromise (IOC).	FTNT-FC-10-L200Fx149-02-12-E	licenc	50	db
13.	Terméktámogatás - konfigurálás (vezető rendszermérnök)	ITBT_SZOLG12	implementáció és támogatási szolgáltatás	1400	óra

2 RÉSZLETES AJÁNLAT

Alulírott **Vertán György** mint a **TIGRA Kft.** (székhely: 1145 Budapest, Törökőr utca 2.) cégjegyzésre jogosult képviselője, valamint az **ALPHA MACHINE Kft.** (székhely: 1123 Budapest, Táltos utca 1.), a **Cyber Services Zrt.** (székhely: 1089 Budapest, Elnök utca 1.), a **DAMIT INFORMATIKA Kft.** (székhely: 6725 Szeged, Hópárdac utca 7. fszt. 3.), a **DIGITAL Kft.** (székhely: 6723 Szeged, Csongrádi sgt. 83.), a **KÜRT Zrt.** (székhely: 1118 Budapest, Rétköz utca 5.), az **M & S Zrt.** (székhely: 1136 Budapest, Pannónia utca 17/a. a. ép. fszt. 4.), a **RacioNet Zrt.** (székhely: 1117 Budapest, Hauszmann Alajos u. 3/A.) és a **Visoft Kft.** (székhely: 1119 Budapest, Than Károly utca 17.) közös Ajánlattevők nevében kötelezettségvállalásra jogosult képviselője a **Nemzeti Népegészségügyi Központ** mint Ajánlatkérő által indított „**Nemzeti Népegészségügyi Központ részére informatikai határvédelmi rendszer korszerűsítése az „EFOP-1.8.1-VEKOP-15-2016-00001 Komplex népegészségügyi szűrések” azonosítószámú projekt keretében**” tárgyú közbeszerzési eljárás közös Ajánlattevőjeként a következő részletes ajánlatot tesszük:

Cikkszám	Megnevezés	Mennyiség	Megajánlott termék cikkszám	Megajánlott termék megnevezése	Nettó ajánlati egységár (nettó Ft)	Nettó ajánlati ár összesen (közbeszerzési díj nélkül) /Nettó ajánlati egységár * Mennyiség/
FTNT-FGx2500E-BA2:A14	FortiGate-2500E 10 x 10GE SFP+ slots, 2 x 10GE bypass SFP+ (LC Adapter), 34 x GE RJ45 ports (including 32 x ports, 2 x management/HA ports), SPU NP6 and CP9 hardware accelerated, 480GB SSD onboard storage	2	FTNT-FGx2500E-BA2:A14	FortiGate-2500E 10 x 10GE SFP+ slots, 2 x 10GE bypass SFP+ (LC Adapter), 34 x GE RJ45 ports (including 32 x ports, 2 x management/HA ports), SPU NP6 and CP9 hardware accelerated, 480GB SSD onboard storage	11709225	23418450
FTNT-FC-10-02K5Ex950-02-12-C	FortiGate-2500E 1 Year UTM Bundle (24x7 FortiCare plus Application Control, IPS, AV, Botnet	6	FTNT-FC-10-02K5Ex950-02-12-C	FortiGate-2500E 1 Year UTM Bundle (24x7 FortiCare plus Application Control, IPS, AV, Botnet	6919088	41514528

	IP/Domain, Web Filtering and Antispam Services)			IP/Domain, Web Filtering and Antispam Services)		
BSFI400A	Barracuda Email Security Gateway 400	2	BSFI400A	Barracuda Email Security Gateway 400	2017978	4035956
BSFI400A-E	Barracuda Email Security Gateway Appliance 400 Instant Replacement Subscription 1 Month	72	BSFI400A-E	Barracuda Email Security Gateway Appliance 400 Instant Replacement Subscription 1 Month	55453	3992616
BSFI400A-H	Barracuda Email Security Gateway Appliance 400 Instant Replacement Subscription 1 Month	72	BSFI400A-H	Barracuda Email Security Gateway Appliance 400 Instant Replacement Subscription 1 Month	36379	2619288
FTNT-FSMxAIO-BASE-B	FortiSIEM 50 devices and 500 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	1	FTNT-FSMxAIO-BASE-B	FortiSIEM 50 devices and 500 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	5510882	5510882
FTNT-FSMxAIO-25-UG-B	FortiSIEM Add 25 devices and 250 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	1	FTNT-FSMxAIO-25-UG-B	FortiSIEM Add 25 devices and 250 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	2755571	2755571
FTNT-FSMxAIO-100-UG-B	FortiSIEM Add 100 devices and 1000 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	1	FTNT-FSMxAIO-100-UG-B	FortiSIEM Add 100 devices and 1000 EPS all-in-one perpetual license for Non-MSP/MSSP's. Does not include Maintenance & Support	9641376	9641376

FTNT-FSMxWIN-ADV-100-UG-B	FortiSIEM 100 Advanced Windows Agents for perpetual license. Each Windows Agent requires a device license. Does not include Maintenance & Support	1	FTNT-FSMxWIN-ADV-100-UG-B	FortiSIEM 100 Advanced Windows Agents for perpetual license. Each Windows Agent requires a device license. Does not include Maintenance & Support	3622574	3622574
FTNT-FSMxEPS-100-UG-B	EPS Add Add 1 EPS Perpetual for Non-MSP/MSSP's	1000	FTNT-FSMxEPS-100-UG-B	EPS Add Add 1 EPS Perpetual for Non-MSP/MSSP's	3122	3122000
FTNT-FC4-10-FSM9x248-02-12-C	FortiCare 1 Year 24x7 FortiCare Contract (1 - 300 points) for FortiSIEM Software deployments. 1 device or 2 End points or 3 Windows Agents equals 1 point.	3	FTNT-FC4-10-FSM9x248-02-12-C	FortiCare 1 Year 24x7 FortiCare Contract (1 - 300 points) for FortiSIEM Software deployments. 1 device or 2 End points or 3 Windows Agents equals 1 point.	4254052	12762156
FTNT-FC-10-L200Fx149-02-12-E	Subscription license for the FortiGuard Indicator of Compromise (IOC).	50	FTNT-FC-10-L200Fx149-02-12-E	Subscription license for the FortiGuard Indicator of Compromise (IOC).	190423	9521150
ITBT_SZOLG12	Terméktámogatás - konfigurálás (vezető rendszermérnök)	1400	ITBT_SZOLG12	Terméktámogatás - konfigurálás (vezető rendszermérnök)	19000	26600000
Nettó ajánlati ár mindösszesen (közbeszerzési díj nélkül):						149.116.547

Budapest, 2019. november 20.

.....
Vertán György

ügyvezető

a TIGRA Kft., ALPHA MACHINE Kft., Cyber Services Zrt., DAMIT INFORMATIKA Kft., DIGITAL Kft., KÜRT Zrt., M & S Zrt., RacioNet Zrt. és Visoft Kft.
a közös Ajánlattevők nevében

A KERETMEGÁLLAPODÁS TELJESÜLÉSÉNEK ÖSSZESÍTÉSE

Keretmegállapodás megtekintése

Keretmegállapodás adatai	Teljesülési összegek	Szerződések	Devizák	Termékkategóriák	Excel export
IT biztonságtechnikai megoldások és kapcsolódó szolgáltatások beszerzése - KM01ITBT17					
KM keretösszege	Eljárás teljesülése (Visszaigazolt megrendelések) (nettó Ft)	Eljárás teljesülése (%)			
20 000 000 000	8 664 511 926,538	43,32			