Elosztott Kormányzati IT-hálózatbiztonsági Csapdarendszer

Ismertető a befogadó intézmények részére

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET

Tartalom

Bevezetés, trendek

Az intelligens digitális eszközök (számítógép, okostelefon, tablet, stb.) és az internet használata napjainkra teljesen általánossá vált. Ezekre épülve mind társadalmi, közösségi és gazdasági szinten új kapcsolati viszonyok, folyamatok alakultak ki.

Az elektronikus levelezés mellett az interaktív közösségi oldalakon folyó kommunikáció került előtérbe, az elektronikus közigazgatás az élet egyre nagyobb területein nyújt kényelmesebb és gyorsabb ügyintézést és az online kereskedelem is egyre nagyobb szeletet hasít ki a teljes kereskedelmi forgalomból. Ezen tendenciák további erősödését jelzik előre a gazdasági/társadalmi kutatóintézetek.

A digitális információcsere már nem csak ember és ember között zajlik, hanem kiterjed a gépek, eszközök adatcseréjére is. Az IoT (Internet of Things) szintén új kihívások elé néz. Az IoT eszközök elterjedésével az internet az ipari folyamatokba is beszivárgott, ezzel új lehetőségeket nyitott az ipari gazdaság számára. Az átalakulási folyamatok új digitális ipari struktúrák kidolgozását teszik szükségessé, azért, hogy a digitalizáció minél jobban kihasználható legyen.

Ám a jól kiépített informatikai infrastruktúrát nem csak legális célok megengedett módon történő elérésére használják. Egyre jobban látható tény, hogy a digitalizáció terjedésével a kiberbűnözés is erősödik, és egyre nagyobb károkat okoz. Ennek kifejlődtek olyan speciális területei, melyek már túllépnek az „egyszerű" bűnözés keretein: ilyenek a kiberterrorizmus és a kiberhadviselés. Ezek különösen nagy károkat okozhatnak, ha célpontjukat a kritikus infrastruktúrák elemei közül választják. Létfontosságú infrastruktúrákhoz azok a fizikai és információs-technológiai berendezések és hálózatok, valamint szolgáltatások és eszközök tartoznak, amelyek összeomlása vagy megsemmisülése súlyos következményekkel járhat a polgárok egészsége, védelme, biztonsága és gazdasági jóléte, illetve a tagállamok kormányainak hatékony működése szempontjából.

Könnyen belátható, hogy az ezen rendszereket érő sikeres támadások társadalmi hatása nagyon súlyos, így ezek védelme alapvetően fontos, kiemelt jelentőségű feladat.

A támadási célból kifejlesztett káros kódok azonban jellemzően nem „csereszabatosak", tehát nem kompatibilisek bármely operációs rendszerrel. Így a támadók egyik legelső és

alapvető feladata kideríteni, hogy a kiszemelt hálózatban milyen operációs rendszerek, szolgáltatások és egyéb programok, illetve programverziók találhatók. Ennek alapján dől el, hogy hol, mikor, és milyen technikával érdemes kezdeni a behatolási kísérleteket – sok esetben egy-egy rosszul beállított tűzfal vagy magára hagyott (biztonsági frissítéseket nélkülöző) alkalmazás siet ebben a támadó segítségére.

A sikeres támadás előfeltétele a célponti rendszer letapogatása, az esetleges gyenge pontok, biztonsági rések és hiányosságok, valamint a szűk keresztmetszetek feltérképezése. Ez az „előkészületi, letapogató fázis" azonban jellemző hálózati forgalmat generál (függetlenül a célba vett gépek operációs rendszerétől), így adott a lehetőség a megtámadott rendszer üzemeltetői számára, hogy forgalomfigyeléssel és elemzéssel felismerjék a támadási kísérleteket, és megtegyék a szükséges (akár automatizált) intézkedéseket rendszerük védelme érdekében.

Egy másik támadási stratégia szerint azonban elmaradhat a letapogatási fázis: ez esetben a támadók mellőzik az előzetes vizsgálatot, és feltételezik, hogy a megtámadott gépek az általuk terjesztett káros kódnak megfelelő és kihasználható paraméterekkel rendelkeznek. Ilyenkor azonban nem egy-egy jól definiált számítógépet céloznak meg, hanem teljes gép csoportokat, illetve tartományokat – bízva abban, hogy ezekben majd megfelelő célpont is akad. Az ilyen stratégia mentén végrehajtott támadások azonban szintén jellegzetes hálózati forgalmat eredményeznek.

Mindkét fenti esetben látható tehát, hogy mennyire kiemelt jelentőségű a kritikus infrastruktúra elemek hálózati forgalmának figyelemmel kísérése és elemzése az üzemeltetők által, mert ez alapján jó eséllyel felismerhető a hálózaton zajló illegális tevékenység, végső soron pedig megelőzhető és megakadályozható a sikeres behatolás.

A honeypot célja

A csapda rendszerek elsődleges célja az, hogy – valós működést szimulálva – elhitessék a támadókkal, hogy éles szolgáltatást nyújtó rendszert sikerült elérniük. Mindeközben azonban a jól felépített csapda rendszerek a támadó valamennyi tevékenységét letapogatják, módszeresen összegyűjtik, rögzítik és naplózzák. Tekintettel arra, hogy a csapda rendszer valójában nem működtet „igazi" szolgáltatást, a rajta észlelt

valamennyi tevékenység jogtalannak minősíthető, azaz potenciális támadásként fogható fel. A csapda rendszerek tehát lényegében arra szolgálnak, hogy a támadók saját magukat leplezzék le egy olyan álcázott környezetben, ahol minden tevékenységük nyomot hagy.

A szisztematikusan összegyűjtött támadási kísérletek rendszerezett adatai alapján aztán egyrészt azonosíthatók és lekérdezhetők a támadók által felhasznált internetes erőforrások (számítógépek, illetve szerverek) forrás címei, másrészt pedig – különböző elemző algoritmusok segítségével – felfedezhető a behatolási módszerek alkalmazási trendjeinek aktuális alakulása, valamint következtetések vonhatók le az internetre épülő szolgáltatások hátterét nyújtó szoftverkörnyezet esetleges gyenge pontjairól, illetve sebezhetőségeiről.

A csapdarendszerek által feltárt információk akár közvetlenül, akár automatizáltan is hasznosíthatóak lehetnek.

A rögzített adatok, támadási mintázatok elemzésének révén eleddig ismeretlen támadási módszerek is felismerhetőek és megtanulhatóak, ami elengedhetetlenül szükséges a további biztonsági intézkedések megtételéhez.

A GovProbe rendszer

Az elosztott kormányzati IT-hálózatbiztonsági csapdarendszer (GovProbe) egy központi adatgyűjtő, kiértékelő elemből, valamint az azzal kapcsolatban álló, a külső támadó számára valósnak látszó hálózati szolgáltatásokat szimuláló célpont rendszerekből (szenzorok) áll, ami az aktív támadási próbálkozások során keletkező adatok és mintázatok rögzítését teszi lehetővé.

A rendszer által rögzített támadási adatok betekintést nyújtanak a rendszer által védett kritikus infrastruktúrákat érő kibertámadások előkészítési, információgyűjtési, valamint terjedési folyamataiba is. A rendszer segítségével felderíthetőek a hálózatokon belüli, illetve kívülről érkező letapogatási és zero-day (a nyilvánosság számára ismeretlen) sérülékenységeket kihasználó aktivitások.

Speciális kiépítése és alapvetően passzív hálózati elhelyezése következtében a csapda rendszer olyan információkhoz juttatja a kiberbiztonsági incidensek feltárását végző

elemzőket, melyek más, jellemzően vonalra épülő biztonsági rendszerek (például IDS/IPS, Network Tap) esetén természetszerűleg nem érhetők el.

Az Elosztott Kormányzati IT-hálózatbiztonsági Csapdarendszer központosított felügyeleti szolgáltatásai révén a Nemzeti Korrupcióellenes Program alapelveivel összhangban preventív (megelőző) passzív eszközökkel jelentősen hozzájárul a korrupció elleni eredményes fellépéshez azáltal, hogy a nemzeti adatvagyont, illetve az állampolgárok személyes adatait kezelő rendszerek észlelési képességének javításával, valamint korrupciós szempontból érzékeny rendszerek biztonságának erősítésével javítja a közigazgatás intézményeinek működésébe, elektronikus adatok kezelésébe vetett közbizalmat. A megvalósított védelem preventív és detektív jellegű, hiszen a kialakításra kerülő rendszer alapvetően passzív működésű.

A rendszer jelenlegi fázisában számos hálózat menedzsment protokoll megjelenítésére képes, illetve több magas interakciójú sandbox csapdával rendelkezik. A konkrét elérhető szolgáltatásokról és sandbox csapdák típusáról munkatársaink tudnak bővebb információt adni.

A kutatási céllal működtetett, nyílt elérésű csapdákon keletkező információkra alapozott vizsgálatok eredményeiből a csatlakozott intézmények részére minden héten heti jelentést készítünk. A dokumentum az automatikusan előállított statisztikai kimutatások mellett az NKI munkatársai által végzett mélyebb elemzések eredményeit tartalmazza. A védendő intézmény produktív hálózatában elhelyezett csapdákon észlelt eseményeket automatizált rendszerünk küldi meg ütemezetten az adott intézmény részére, harmadik félhez még anonimizáltan sem kerülnek.

Logikai és fizikai architektúra

A projekt keretén belül szenzornak nevezzük az olyan virtuális gépet, amely egymástól elszigetelt csapda környezeteket futtat abból a célból, hogy a rosszindulatú, támadási és behatolási kísérletek észlelhetővé váljanak. Egy szenzor egy vagy több csapda rendszert is futtathat. A szenzorok a begyűjtött információkat VPN kapcsolaton keresztül a központi adattárba továbbítják.

Az egyes szenzorok fizikai környezetét biztosító hardverelemet szondának nevezzük. A projekt keretein belül a szondák (jelen dokumentum keletkezésekor) 1U magas

meghatározott típusú szerver számítógépek, melyek virtualizációs környezetben futtatják az egyes szenzor példányokat.

Az egyes szondák, szenzorok és csapdák konfigurálása távolról, a csapdarendszer központból történik. Tekintettel arra, hogy az egyes szenzorokra kerülő szoftverek automatikusan a központból töltődnek le, így azok frissítése is könnyen elvégezhető távolról. Az említett szoftver környezetek tartalmazzák a szenzorok futtatásához szükséges teljes operációs rendszert, kiegészítve ezt az adott szenzoron futtatandó csapdarendszerekkel is.

Hardver telepítés

A kihelyezést megelőzően a Nemzeti Kiberbiztonsági Intézet szakemberei az erre vonatkozó külön dokumentáció alapján elvégzik a szonda egységek alapkonfigurációját, így azok már megfelelő hardveres beállításokkal, előre telepített alapszoftverekkel érkeznek meg a kihelyezés helyszínére. Az eszköz elhelyezéséhez 1U méretű, szabad, szabványos 19 colos rack szekrény helyre van szükség, első és hátsó szerelősínnel, legalább 1000mm mélységgel.

A szondák áramellátását a beépített redundáns tápegység végzi, amelyeket egy-egy független PDU-ba kell bekötni. Az eszköz villamos betáplálásához 2 darab, egyenként legalább 550W szabad kapacitással rendelkező 240V szokványos hálózati villamos betáplálási lehetőségre (az egység két darab, IEC C14 szabványos tápcsatlakozóval rendelkezik) van szükség. A szondák hálózatba kötéséhez ezen felül kettő darab, megfelelő hosszúságú, legalább Cat5, illetve Cat5e típusú patch kábelre van szükség, a következő szakaszban részletezettek szerint.

Hálózati telepítés - fizikai kábelezés, Layer 2 telepítés

A szonda egységek a telepítés szempontjai alapján három darab lényegi, eltérő célú fizikai hálózati interfésszel rendelkeznek:

Interfész	Típus	Feladatkör
iDRAC	1GBase-T	Hardver monitoring és menedzsment (Dell iDRAC)
Gb1	1GBase-T	Csapdarendszer elsődleges hálózati interfész

Gb2	1GBase-T	Konfigurációs interfész

A rendszer számára minden felsorolt interfészen egységesen biztosítani kell a szokványos TCP/IP hálózati ARP protokoll megfelelő működését.

Az iDRAC interfészt a telepítés helyszínén elérhető hardver menedzsment hálózatba kell csatlakoztatni. Az interfész tetszőleges VLAN konfigurációt támogat, MAC címe előre ismert. Az interfész javasolt hozzáférési sebessége legalább 100 MBps FastEthernet (auto negotiation, MDX támogatott), az ennek megfelelő (legalább Cat5) típusú kábelezéssel.

A Gb1 interfészt a telepítés helyszínén a védendő kritikus infrastruktúra hálózatba kell csatlakoztatni. Az interfészen az eszközön futó virtuális gépeket a külvilággal összekapcsoló virtuális switch üzemel. A központi, dinamikus konfiguráció miatt az interfészen megjelenő forrás MAC címek előre nem ismertek.

A csapdarendszer LAN funkcióinak (pl.: ARP és DHCP letapogatások és támadások felderítése) hatékony működéséhez a Gb1 interfész esetén – a védett hálózat kiépítésétől függően – lehetővé kell tenni a szokványos helyi számítógépként történő Ethernet csomag lehallgatás funkciók működését. Ezen szolgáltatás támogatására a Gb1 interfészhez csatlakozó switch port ún. „promiscuous" módba kapcsolható, ügyelve arra, hogy *ez a rendszer magasabb szintű adatforgalmazási képességeit (TCP/IP kliens/szerver) ne befolyásolja*. Javasolt hozzáférési sebessége legalább 1 GBps GigabitEthernet (auto negotiation, MDX támogatott), az ennek megfelelő (legalább Cat5e) típusú kábelezéssel.

A Gb2 interfészt a telepítés helyszínén *nem szükséges csatlakoztatni*, ezen interfész célja a virtuális gépet futtató környezet helyszíni szervizelési lehetőségének biztosítása. Javasolt hozzáférési sebessége legalább 100 MBps FastEthernet (auto negotiation, MDX támogatott), az ennek megfelelő (legalább Cat5) típusú kábelezéssel.

Virtuális telepítés

Egyes esetekben a befogadó intézmény számára testhezállóbb a virtuális szerverek kezelése. A GovProbe Honeypot képes virtualizált környezetben is működni. Az előzetes egyeztetések után a Nemzeti Kiberbiztonsági Intézet szakemberei konfigurálnak és

előállítanak egy .iso képfájlt amelyet átadnak a befogadó intézmény üzemeltetési csoportjának telepítésre.

A virtuális gép erőforrásai nagyban függenek a kért csapdakörnyezet méretétől, csapdák típusától, és a várható terheltségtől. A tervezett gépigény az egyeztetések során kerül kiszámításra, melyhez a dokumentum alján található „Virtuális honeypot csapdák erőforrás számítása" szekcióban található az útmutató.

Logikai kiépítés, IP hálózati telepítés

A rendszer architekturális kiépítéséből következően a szondák csak olyan hálózati környezetben tudnak működni, amely biztosítja számukra a VPN kapcsolat felépítésének hálózati feltételeit. A csapdarendszer központi menedzsment funkciók működőképességének biztosítására a szonda eszköz kitelepítését megelőzően központi hálózati konfiguráció, valamint ehhez a befogadó környezet részéről az IP hálózati alapkonfiguráció paramétereinek megadása szükséges, az alábbiak szerint.

Az eszköz hardver monitoring és menedzsment céljára az iDRAC interfész IP konfigurációja és (legalább) helyi elérhetőségének biztosítása szükséges. Mivel az erre a célra biztosított, beágyazott menedzsment felület nem rendelkezik fejlett hálózati védelmi funkciókkal, az iDRAC interfészt tilos az interneten keresztül elérhetővé tenni, annak egy védett hálózatot kell biztosítani.

Mivel a csapdarendszer központi menedzsment funkciói nem terjednek ki az iDRAC interfész kezelésére, az alrendszer céljára egy (legalább) lokális hálózati IP cím biztosítása szükséges, a hozzá tartozó szokványos IP paraméterekkel együtt (alhálózat, alhálózati maszk, alapértelmezett átjáró). Az iDRAC támogatja a DHCP-t, valamint a statikus IP konfigurációt is.

Az iDRAC részére további szokványos helyi hálózati szolgáltatások (például: DNS, NTP, SMTP, SNMP, Syslog) hozzáférése biztosítható, ez azonban nem feltétele a rendszer megfelelő működésének.

Csapdarendszer funkciók

A csapdarendszer elsődleges funkcióinak megvalósítása érdekében a Gb1 interfész IP konfigurációja, helyi elérhetőségének biztosítása, valamint a csapdarendszer központ

irányába történő adattovábbítás lehetőségének biztosítása szükséges. Adatérzékelési képességei szempontjából a Gb1 interfész, illetve az ezen konfigurált IP címek helyi hálózati szempontból történő elhelyezkedése kritikus jelentőségű. A lehetséges elhelyezések, illetve ezek főbb jellemzői:

LAN elhelyezés

Amennyiben a szonda eszközt egy helyi irodai hálózatban helyezzük el, lehetőség nyílik a kliensek (pl.: Windows munkaállomások), illetve az ezeket befogadó hálózat kompromittálása esetén előálló támadási minták érzékelésére. Az elhelyezés hátránya, hogy a legtöbb jelenlegi csapda funkció egy irodai hálózatban idegen, így megnövekszik annak valószínűsége, hogy egy támadó felismeri a csapdarendszer jelenlétét. A magas szinten védett hálózatok esetén további nehézséget jelenthet a csapda központ irányú VPN kapcsolat kiépítését lehetővé tevő tűzfal szabályok implementációja.

DMZ elhelyezés

A szonda eszköz elsődlegesen az egyéb helyi, illetve távoli kiszolgálók lokális hálózati környezetében történő elhelyezésre készült. A munkaállomásokat veszélyeztető, LAN típusú támadások a kiszolgálók számára dedikált hálózati környezetben szintén jelentőséggel bírnak, ezt kiegészítve az egyes csapda funkciók az ilyen környezetben elvárt virtuális szolgáltatások segítségével hatékonyan, kevés fals pozitív esemény rögzítése mellett nyújtanak lehetőséget a potenciális támadások felderítésére.

Nyílt hálózati elhelyezés

A szonda eszköz, fejlett védelmi funkcióinak alapján, alkalmas nagy forgalmú, részben-, illetve teljesen nyílt hálózatok (mint például az NTG, illetve az Internet) környezetében történő működésre is. A nyílt elhelyezés hátránya, hogy a projekt által elsődlegesen célzott kritikus hálózati környezeteket védő berendezések (Tűzfal, IPS) által a továbbiakban nagy biztonsággal kiszűrt támadási, automatizált letapogatási kísérletek számos fals pozitív érzékelési eseményt eredményezhetnek.

A csapdarendszer a központi menedzsment funkcióit, valamint az elsődleges érzékelési funkciókat is az erre a célra dedikált hálózati interfészen valósítja meg.

A központi menedzsment céljára a rendszer egy dedikált virtuális gépet futtat, melynek egy darab önálló IP cím biztosítása szükséges. A rendszer ezen az IP címen bemenő TCP vagy UDP kapcsolatokat nem fogad, kimenő irányban kizárólag a csapdarendszer központ VPN kiszolgálója felé épít fel kapcsolatot, meghatározott TCP és UDP portokon.

A csapdarendszer elsődleges érzékelési funkcióit megvalósító egy vagy több szenzor példány (virtuális gép) számára önálló IP cím(ek) biztosítása szükséges. A rendszer ezen IP címeken különböző virtuális (csapda) szolgáltatásokat nyújt a helyi- illetve távoli IP forrásokból érkező letapogatási kísérletek, potenciális támadók számára. A csapda funkciók megfelelő működéséhez a szenzor példányokhoz rendelt IP címek irányába a lehető legnagyobb mértékben megengedő routing, illetve tűzfal szabályok („allow all from any") konfigurációja szükséges. A rendszer ezen IP címek esetében, a központi menedzsmentnél leírtakkal azonos módon, a csapdarendszer központi VPN kiszolgálóhoz csatlakozik.

A VPN kapcsolat működőképességének biztosítása érdekében a megadott kimenő forgalmat a megfelelő routing, illetve tűzfal beállításokkal biztosítani kell. Mivel a rendszer megfelelően kezeli a forrás címre vonatkozó hálózati címfordítást (SNAT), így ennek alkalmazása a csapdarendszer esetén megengedett.

A csapdarendszer funkciókat megvalósító virtuális gépek a további szokványos helyi hálózati szolgáltatásokat (például: DNS, NTP, SMTP, SNMP, Syslog) is a VPN kapcsolaton keresztül, a csapda rendszer központja felől veszik igénybe. A felsorolt esetekben a csapdarendszer támogatja a DHCP-t és a statikus IP konfigurációt is.

Az alábbi táblázat a jelen szakaszban leírt környezeti paramétereket foglalja össze:

Szonda funkció	IP címek (db)	Bejövő IP kapcsolatok	Kimenő IP kapcsolatok
központi menedzsment	1	nincsenek (deny all)	csak VPN
szenzor példány(ok)	legalább 1	bárhonnan bármi (allow all from any)	csak VPN
központi menedzsment	1	nincsenek (deny all)	csak VPN

Ellenőrző lista

A kitelepítést megelőzően a befogadó környezet üzemeltetői részéről a szonda egységek előkészítő konfigurációjához átadandó információk:

- **iDRAC hálózat paraméterei:** IP cím, hálózati maszk, átjáró, esetleges VLAN beállítások.
- **Csapdarendszer IP hálózat paraméterei:** hálózati maszk, átjáró, IP címek (szondánként 1 darab + központi menedzsment számára 1 darab).

A befogadó környezet további szükséges feltételei a sikeres kitelepítéshez:

1) 1U méretű, szabad, szabványos 19 colos, rack szekrény hely első és hátsó szerelősínnel, legalább 1000mm mélységgel.
2) 2 darab, egyenként legalább 550W szabad kapacitással rendelkező 240V szokványos hálózati villamos betáplálási lehetőség (az egység két darab, IEC C14 szabványos tápcsatlakozóval rendelkezik).
3) 1 darab management hálózati patch csatlakozás (legalább Cat5).
4) 1 darab csapdarendszer hálózati patch csatlakozás (legalább Cat5e).
5) Az előzetesen átadott hálózati paramétereknek megfelelő fizikai és logikai működés biztosítása a helyi hálózati környezetben (Switching, Routing, ARP, esetlegesen DHCP elvárt működése).
6) A csapdarendszer szenzorok számára biztosított IP címekre irányuló hálózati (tűzfal) konfiguráció: a védett környezetből, illetve az Internet felől, illetve bármilyen forráscímről a lehető leginkább megengedő („allow all from any") típusú szabályok felvétele.
7) A csapdarendszer központ elérését lehetővé tevő IP hálózati (tűzfal) konfiguráció: a központi VPN kiszolgáló meghatározott TCP/UDP portjaira irányuló elérésének engedélyezése a szenzorok, illetve a központi menedzsment funkció számára megadott IP címekről.

Virtuális honeypot csapdák erőforrás számítása

A virtuális gép erőforrásai nagyban függenek a kért csapdakörnyezet méretétől, csapdák típusától, és a várható terheltségtől. Ugyanakkor az alábbi táblázat alapján meg lehet becsülni a szükséges várható erőforrásokat, mely az optimális működéshez szükséges:

Csapda típusa	Interaktív	Nem interaktív
vCPU	1	1/3
MEM	1024MB	500MB
Csapda típusa	Interaktív	Nem interaktív

A fentiek alapján – és a korábbi tapasztalataink alapján – egy átlagos Honeypot infrastruktúra üzemeltetéséhez az alábbi erőforrások szükségesek:

Átlag infrastruktúra összetétele

- 1 db operációs rendszer
- 5 db nem interaktív szonda
- 1 db interaktív szonda

A táblázatra figyelemmel egy infrastruktúra erőforrás igénye az alábbi:

- **Nem interaktív**
  - vCPU: 1/3 X 5 = 5/3 vCPU igény, tehát összesen 2 CPU
  - Memória: 5 X 500 MB, tehát összesen 2,5 GB igény
- **Interaktív**
  - vCPU 1
  - Memória: 1 GB

Háttértár: 50 GB

Így a teljes erőforrás igény, a szondákat futtató operációs rendszerrel együtt ajánlottan: 2 vCPU, 7 GB memória és 75 GB háttértár.[1]

Esetenként komplexebb infrastruktúrára van igény, mely következőképpen épülhet fel:

- 1 db operációs rendszer
- 15 db nem interaktív szonda
- 3 db interaktív szonda

A táblázatra figyelemmel egy ilyen infrastruktúra erőforrás igénye az alábbi:

- **Nem interaktív**
    - vCPU: 1/3 X 15 = 15/3 vCPU igény, tehát összesen 5 CPU
    - Memória: 15 X 500 MB, tehát összesen 7,5 GB igény
- **Interaktív**
    - vCPU 3
    - Memória: 3 GB

Háttértár: 75 GB

Így a teljes erőforrás igény, a szondákat futtató operációs rendszerrel együtt ajánlottan: 10 vCPU, 14 GB memória és 100 GB háttértár.[2]

Amennyiben sandbox kerülne telepítésre, az a számított infrastruktúrán túl további 1 db vCPU, 2048 MB RAM erőforrás hozzáadása indokolt.

[1] Az értékeket felfelé kerekítéssel szükséges számítani
[2] Az értékeket felfelé kerekítéssel szükséges számítani

OS	Minimum	Ajánlott
VCPU	1	2
RAM (MB)	1536	3072
Disk (GB)	5	25

Végső erőforrásigény (Átlag)	Minimum	Ajánlott
VCPU	4 db	5 db
RAM	5 GB	7 GB
DISK	55 GB	75 GB

Csapda típus (interakció szint szerint)	Interaktív	Nem interaktív
VCPU	1	0,3
MEM (MB)	1024	500

Végső erőforrásigény (Komplex)	Minimum	Ajánlott
VCPU	9 db	10 db
RAM	12 GB	14 GB
DISK	80 GB	100 GB

Csapdarendszer összeállítás (infrastruktúra)	Átlag	Komplex
Interaktív esetén (VCPU)	1	3
Nem interaktív esetén (VCPU)	5	15
Disk (GB)	50	75

Végső erőforrásigény (Komplex, Sandbox)	Minimum	Ajánlott
VCPU	10 db	11 db
RAM	14 GB	16 GB
DISK	80 GB	100 GB

Kérdés esetén keressen minket az alábbi elérhetőségeink egyikén!

Általános kérdések esetén:
titkarsag@nki.gov.hu

Hatósági kérdések esetén:
hatosag@nki.gov.hu

Incidensbejelentéssel kapcsolatos kérdések esetén:
csirt@nki.gov.hu

Csatlakozással kapcsolatos kérdések esetén:
edt@nki.gov.hu

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET