10.17625/NKE.2021.018

- 2020 -

NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA

Jéri Tamás

A Kritikus Internetes Szolgáltatások biztonsági kérdései a védelmi szférában

Doktori (PhD) értekezés

Témavezető:

Prof. Dr. Kovács László dandártábornok (DSc)
egyetemi tanár

BUDAPEST, 2020.

Tartalomjegyzék

Bevezetés

„Információs társadalomban élünk. A napi gazdasági folyamatokhoz, életvitelünkhöz, hétköznapjainkhoz, munkánkhoz kapcsolódó – információkat hordozó – adatok, gyakran valahol a kibertérben, folyamatos elérhetőség biztosítása mellett szervereken tárolódnak. Az informatikai hálózatok előnyeit kiaknázva, mind a költségvetési, mind a piaci szegmensnek érdeke az elektronikus adattárolás, továbbá a már elektronikusan tárolt adatok centralizálása. A kialakult helyzet eredményeként többek között a 'pénz/értékpapír forgalom', 'levelezés', 'repülőjegy', 'ügyintézés' szavak jelentése napjainkra átértékelődött és még hosszasan lehetne sorolni azokat a fogalmakat melyek informatikai szolgáltatásként jelennek meg." [1]

A napi híradásokba ma már természetes, hogy bekerül, ha valamelyik pénzintézet on-line banki rendszere meghibásodik, vagy fennakadásokkal üzemel, ha a legnagyobb közösségi oldalak valamelyikében működési zavarok keletkeznek, ha a tőzsde informatikai rendszerének hibája miatt a kereskedelmet – egyszerűen – fel kell függeszteni, vagy ha az országos járványügyi tájékoztató portál terheléses támadás miatt elérhetetlenné válik. Az online, elektronikus ügyintézési és bevallási rendszer leállásán bosszankodnak, ha az valamelyik határidős jelentés napján mondja fel a szolgálatot, mert esetleg túlterhelődik; elszomorító, ha nem működik a közüzemi bejelentési rendszer, ahol az állampolgárok az energia felhasználásukat adhatják meg, hogy fogyasztásuknak megfelelő számlát kapjanak; idegesítő, ha adott településre vonatkozóan nem működik a hulladékkezelő információs rendszere és nem követhető nyomon az elszállítás rendje. A vásárlás, mint tevékenység teljesen átértékelődött. Otthon, informatikai eszközön állítható össze a virtuális kosár tartalma, véglegesíthető a rendelés, kivitelezhető a fizetés és nyomon követhető a világ bármelyik részéről érkező csomag útvonala, amelyet a vásárló kedve szerint, akár lakásának ajtajában rak le a csomagküldő szolgálat. Komplex, internetes szolgáltatások egybefésült rendszere az elektronikus vásárlás, amelynek eredményeként, az otthon ülve, kényelmesen is kivitelezhetővé válik.

A 2019. év végén Kínában megjelenő, majd az egész világon elterjedő COVID-19[1] járvány is megmutatta, hogy mekkora előnyt jelent az internetes szolgáltatások jelenléte és alkalmazhatósága, hogy mit jelent úgy karanténban lenni, hogy közben a kommunikáció, a tájékozódás, az ügyintézés és a vásárlás szinte változatlanul – internetes informatikai szolgáltatásoknak köszönhetően – biztosított. Magyarországon egy egyszerű, megalapozott döntéssel napok alatt bevezetésre került a digitális tanrend, amely keretében a diákok és a

[1] Vírusos, légúti, illetve légzőszervi megbetegedés, amelyet a SARS-CoV-2 nevű koronavírus okoz.

tanárok otthonaikból valósították meg a képzést, oktatást, az egymástól elválasztott családok pedig leggyakrabban video-megosztó oldalakon tartották a kapcsolatot szeretteikkel. Az egyetlen hivatalos, központi tájékoztató rendszer is az interneten kapott helyett, külön weblapot hoztak létre erre a célra, ahol az olvasók folyamatosan naprakész információkat kaphattak.
Ugyan kevésbé örvendetes, ha valamilyen objektív felelősség alá tartozó, közúti szabálytalanság elkövetése miatt kap valaki rendőrségi levelet, viszont annak tényszerűségét az értesítő dokumentumban megtalálható internetes hivatkozásra [2] belépve tekintheti meg az illető. A szabálytalanságot elkövető állampolgároknak joguk van megtudni, hogy mikor és mit vétettek, amelyre utazgatás és várakozás nélkül, az internetet felhasználva nyílik lehetőségük.
„Mára gyakorlatilag elvárássá vált az államigazgatás területén az elektronikus ügyintézés kiterjesztése, hogy a munkavégzéssel, a szolgálati tevékenységgel kapcsolatban szakszerű, hatékony és szükség esetén gyors segítséget kapjanak a munkavállalók az arra hivatott szakterületektől.
Az ügyfélszolgálati rendszer mára már mindenhonnan elérhető, használatáról és működéséről írásban tájékoztattuk a személyi állományt.” [3] Az idézett szöveget Ballainé Krikker Zsuzsanna ezredes, a HM Védelemgazdasági Hivatal Központi Illetményszámfejtő és Rendszerüzemeltető Igazgatóságának akkori igazgatója mondta 2017.03.27-én.
A fentiekben felsorolt példák csak szemléltető jellegűek, hisz életünk minden területéről hosszasan tudnánk sorolni azokat az interneten elérhető szolgáltatásokat, amelyek egyszerűen ma már megkerülhetetlenek. Természetes, hogy bizonyos internetes szolgáltatások jelenléte, vagy azok hiánya befolyásolja a mindennapokat, ugyanakkor a társadalom együtt él velük, azok alkalmazása az élet részévé vált.
Talán elképzelni sem tudjuk, hogy mi történne, ha ezek a létfontosságú vált internetes szolgáltatások hirtelen megállnának, vagy eltűnnének. A válasz egyszerű, valószínűleg bábeli zűrzavar támadna, azonnal információhiány lépne fel és egyszerűen felfordulna a világ.

A tudományos életben és a híradásokban a kritikus infrastruktúra [4], vagy a kritikus információs infrastruktúra [5] fogalmával találkozhattak az érdeklődők, viszont mellettük olyan internetes szolgáltatásoktól is függnek mindennapjaink, amelyek elérhetetlenné válása következménnyel jár, és igazán megmutatja, hogy valójában azok is kritikus szolgáltatások.
„A világháló használóinak növekedésével, mindenkinek érdeke olyan, interneten elérhető szolgáltatások működtetése, amelyek alkalmazásával az emberi energia és idő ráfordítás csökkenthető, ugyanakkor a rendelkezésre állás növelhető és összességében valamilyen profit

képezhető.” [1] Ezen szolgáltatások olyannyira jelen vannak, hogy az élet minden területén, még a védelmi szférában is felbukkantak, ugyanakkor hivatalosan eddig nem kerültek definiálásra, ezért jelen értekezésben – jelentőségük miatt – tudományosan is megközelítésre kerülnek.

Védelmi szféra alatt Magyarország Alaptörvénye 51. cikkének (3) bekezdésében szereplő – és az irányadó törvényekben[2] [3] részletezett – Magyar Honvédség, valamint rendvédelmi szervek fogalomkörébe tartozó szervezetek összességét-, továbbá a Nemzeti Adó- és Vámhivatalról szóló törvényben[4] definiált szervezet együttesét értem. A továbbiakban feltüntetett rendvédelmi kifejezést egyenértékűnek tekintem a védelmi szféra fogalmával.

A tudományos probléma

Az információtechnológia fejlődése a védelmi szféra minden ágában kivétel nélkül kikényszeríttette a gyors és hatékony eszközök és alkalmazások használatát, amelyek a napi munkavégzés részévé és létfontosságú adathordozóvá váltak. A megjelent internetes szolgáltatások hasonlóan a társadalomban alkalmazott internetes szolgáltatásokhoz, beivódtak a szervezetek, szervek életébe, nélkülük az alaptevékenységek ellátása is veszélybe kerülne, így joggal nevezhetjük azokat is létfontosságú szolgáltatásoknak[5]. Problémaként jelentkezik ugyanakkor, hogy ezeknek a rendszereknek és szolgáltatásoknak sem a feltérképezése, sem a védelme nem megoldott teljes körűen.

1. Jogszabályi kötelezettségek

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló **2013. évi L.** törvény, az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló **2015. évi CCXXII.** törvény, valamint a törvények végrehajtási rendeletei előírják, a társadalom pedig elvárást támaszt a közigazgatási szervek, így a védelmi szféra számára is:

- az elektronikus információbiztonsággal kapcsolatos szabályok kerüljenek minden körülmény között betartásra [6];

---

[2] 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról

[3] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

[4] 2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról

[5] Lásd: 1. fejezetben

- az ügyek lehetőleg papírmentesen, elektronikusan intéződjenek [7];
- az információk legyenek naprakészek, felhasználóbarát formában gyorsan-, könnyedén-, és állandóan elérhetők.

Ezeknek az elvárásoknak a teljesítése egészen mást jelent egy épület falai között, vagy a kibertérben. Az utóbbi nyilvánvalóan másfajta kihívást és nyomást jelent az érintett szervezetekre nézve, ugyanakkor egyben jelenthet késztetést is a kor vívmányainak kihasználására vonatkozóan. A megvalósítás jár néhány további megoldandó problémával is, hisz úgy kell szavatolni az információbiztonságot az interneten, hogy

- a szervezet informatikai rendszerében tárolt adatok hitelesen, csak és kizárólag a szükséges mértékben-, és állandó rendelkezésre állás mellett legyenek elérhetők;
- az állampolgároktól bármely időpontban indított ügyintézési folyamat a szervezet informatikai rendszerében is tárolódjon és a befelé érkező információk elérjenek az érintettekhez.

Tekintettel arra, hogy a rendvédelmi szervezetek, vagy azok szervei is eltérően működnek, nagyon nehéz általánosítani, ezért a legtöbb esetben külön alkalmazás fejlesztésre van szükség. Azonnal adódik a kérdés, hogy az internetre készülő fejlesztést ki végezze? Egy szervezeten kívüli, erre szakosodott vállalkozás jó megoldás lehet, viszont a sok kötöttségnek ára van, azt ki kell fizetni, ráadásul az elindított szolgáltatást fenn is kell tartani; a szükséges, igény szerinti módosításokat el kell végeztetni, aminek általában újra ára van. A szervezeten belüli fejlesztés olcsóbb lehet, viszont rendelkezésre kell állnia a megfelelő szakember gárdának, amely jelenti a fejlesztőket, az üzemeltetőket és a további szükséges személyzetet egyaránt.

Az aktuális helyzet szerint, ezen jogszabályi kötelezettségeknek való megfelelés nehéz falat, a fejlesztések csak komoly energiaráfordítással érhetők el. Leginkább a „jobb félni, mint megijedni” elvet követve, mindenki a legegyszerűbb módon próbál megfelelni az elvárásoknak. Lehetőség szerint keresik a kész, már kipróbált és a biztonság tekintetében is bizonyított termékeket, amelyekhez gyakran inkább az életszerűt igazítják, mintsem az életszerűséghez fejlesztést végezzenek. A szervezetek gyakorlata teljesen eltérő, amelyre a törvény által előírt elektronikus ügyintézés is jó példa. Van olyan szervezet, amelyik tényleges ügyintézést fejlesztett az internetre, és az állampolgár otthonából, azonnali végeredménnyel, ténylegesen képes megoldani a problémáját, de a legtöbb esetben az elektronikus ügyintézés „csak” egy hitelesített elektronikus űrlap szervezet részére történő megküldését jelenti, amelyet iktatást követően a falakon belül dolgoznak fel, majd a végeredményről másik, hivatalos csatornán

adnak visszajelzést a beküldő részére. Bizonyos tekintetben mindkét esetben elektronikus ügyintézésről van szó, valójában azonban óriási különbség van a két eljárás között.
A kapott, vagy vállalt kötelezettségből eredő internetes szolgáltatások fő problémája, hogy azoknak lehetőleg minden körülmény között, állandó rendelkezésre állással, biztonságosan működniük kell, amelyhez számos ajánlást be kell tartani.

2. Az internetben rejlő lehetőségek kihasználása

Az internet használatának kellemesebb oldala, hisz sokkal könnyebb mások által kifejlesztett alkalmazásokat igénybe venni, mint sajátot készíteni. Van olyan szervezet, amelyik saját programot fejlesztve, saját szerverén keresztül, dinamikusan frissülő tartalommal jeleníti meg a közvéleménynek szánt információkat, viszont van olyan is, amelyik közösségi oldalt használva dobja be a hírfolyamba az aktuális információkat és ad tájékoztatást. Mindkét megoldás információ-szolgáltatás, azonban itt is óriási a különbség a két eljárás között. A közösségi média valójában egy másik fél internetes szolgáltatásának az igénybevétele, amelyik fél a hozzá eljuttatott adatok tulajdonosává válik, és cserében – állítása szerint – gondoskodik az adatok megőrzéséről és a megfelelő információbiztonság megteremtéséről.

Ma már szinte mindenki talál kedvére való – akár – ingyenes szolgáltatást az interneten, amibe örömét, vagy kedvét leli, amely érdeklődési körébe tartozik, vagy egyszerűen csak valamilyen okból hasznos rá nézve, amely körbe természetesen a védelmi szféra is beletartozik.
Ezen internetes szolgáltatások egyik része szabadon-, másik része feltételhez kötötten használható, továbbá előfordulnak fizetős, vagy ingyenes formában elérhető szolgáltatások egyaránt. A pénzügyi források mindenhol fontosak, így a többség inkább a költségtakarékos megoldásokat keresi, megelőlegezve a bizalmat a szolgáltatásoknak. Az igénybe vevők köre is összetett, hisz az lehet a védelmi szféra bármely személyi állománya, de lehet egy rendvédelmi szervezet is. Az igénybevétel történhet saját elhatározás alapján, vagy kötelezettségből, amely szolgáltatás származhat a védelmi szférából, vagy azon kívülről. Adott szervezet, vagy szerv hozhat létre önmagának is szolgáltatásokat, amelyet azután saját állománya részére biztosíthat. Tipikus példája ennek a vállalati elektronikus levelezés világhálón elérhető formája, vagy a virtuális magánhálózat kialakítása, otthoni munkavégzés biztosítása céljából. Érzékelhető, hogy az internetes szolgáltatások igénybevételében viszonylag nagy a mozgástér, amely egyaránt jelenthet frappáns problémamegoldást, de jelenthet kockázatot, veszélyt is.

Az internetben rejlő lehetőségek kihasználásának egyik lehetséges problémája az ellenőrizetlen szolgáltatás felhasználás, amely kártékony programok rendszerbe jutását, vagy jogosulatlan rendszerbe lépést vonhat magával, másik lehetséges problémája a túlzott-, vagy megbízhatatlan szolgáltatás igénybevétel, amely annyira erős kötődést eredményezhet, hogy kimaradás, leállás esetén hátrányosan érinti az adott szervezetet.

Összegezve a következő tudományos problémák azonosíthatók:

- a létfontosságú internetes szolgáltatások témaköre – fontossága ellenére – eddig nem került tudományosan feldolgozásra, sem általánosságban sem a védelmi szférában;
- jelenleg nincs olyan iránymutatás, vagy ajánlás, amely rögzítené, hogy mit kell tenni együtt az internetes informatikai szolgáltatások biztonságáért és nagyfokú rendelkezésre állásáért;
    - a védelmi szféra internetes szolgáltatásainak bevezetése elsősorban a várható eredményekre koncentrál, ugyanakkor az esetleges leállás, vagy kimaradás esetére nem készül hatástanulmány, a megelőzés másodlagos szempont;
    - az alkalmazott internetes szolgáltatások egyenrangúak, nincsenek közülük kiemelve azok a kritikusnak tekinthető szolgáltatások, amelyek az átlagnál is nagyobb, folyamatos figyelmet érdemelnek;
    - a feltételezett Kritikus Internetes Szolgáltatásokra vonatkozó üzemeltetési hatáskörök nincsenek definiálva, a szolgáltatások súly-, és gócpontjai nem ismertek;
    - a futó internetes szolgáltatások működésképtelensége esetén az elhárítás öntevékeny, ad-hoc jellegű (mindenki a saját hatásköre szerint).
- az internetes informatikai szolgáltatások igénybevétele nem szabályozott, nincsen rá általános ajánlás, vagy iránymutatás annak ellenére, hogy folyamatos kockázatvállalást jelent.

Kutatási célkitűzések

1. Rá kívánok mutatni a kritikus internetes szolgáltatás jelenségre, létezésre.

2. Célom definiálni a kritikus internetes szolgáltatás (a továbbiakban: KRISZ) fogalmát, bemutatni felépítését, továbbá megvizsgálni működésének aspektusait, áttekinteni az általános és a hazai rendvédelmi alkalmazását.

3. Bizonyítani kívánom, hogy az infrastruktúrák, vagy az információs infrastruktúrák mellett internetes szolgáltatások is lehetnek kritikusak, hiszen egy infrastruktúra működése önmagában még nem jelent garanciát a szolgáltatás működésére.
4. Szeretném megvizsgálni a kritikus infrastruktúrákkal és a kritikus információs infrastruktúrákkal kapcsolatos összefüggéseket, továbbá a kritikusnak vélt internetes szolgáltatások gyakorlati alkalmazásához kívánom bemutatni azokat a módszereket és ajánlásokat, amelyek az információbiztonság betartása mellett hozzásegítenek a folyamatos rendelkezésre állás megvalósításához.
5. Javaslatokat kívánok adni a kritikusnak vélt internetes szolgáltatások biztonságos igénybevételéhez, működtetéséhez.

A kutatási célkitűzéseket az alábbi részcélokra bontott kutatómunkával kívánom elérni:

- A Kritikus Internetes Szolgáltatások létezésének és érzékelhető jelenlétének feltárása, valamint az információs infrastruktúrákkal kapcsolatos összefüggések vizsgálata
  - KRISZ definiálása;
  - KRISZ feltárása általánosságban és a védelmi szférában.

- Kritikus Internetes Szolgáltatások összetétele, elemeinek vizsgálata, a szolgáltatás-nyújtás veszélyeinek-, és a helyes alkalmazásrendnek a bemutatása
  - KRISZ felépítése, alrendszerei;
  - KRISZ leggyakoribb előfordulásai, rendszerei, biztonságos üzemeltetése;
  - KRISZ védelmi ajánlásai.

Kutatási hipotézisek megfogalmazása

A tudományos probléma és a kutatási célkitűzések megfogalmazása után az alábbi hipotéziseket állítom fel:

- A kritikus infrastruktúrák és a kritikus információs infrastruktúrák mellett hipotézisem szerint Kritikus Internetes Szolgáltatások is léteznek. Ezen feltételezésem tudományos megalapozása a Kritikus Internetes Szolgáltatás elméleti megközelítése, definiálása, valamint a definíció mögötti tartalom körül határolása után lehetséges;
- Feltételezésem szerint a Kritikus Internetes Szolgáltatások kialakulásának vizsgálata a létezés ténye mellett magyarázatát adja annak is, hogy az internetes szolgáltatások miként tudnak létfontosságúvá, kritikussá válni a társadalom különböző szereplőinek.

A kialakulás lehetséges módjai feltárják azokat a részleteket, amelyek tisztázzák a KRISZ-hez kapcsolódó szerepeket, valamint azok jelentőségét;

- Meglátásom szerint a KRISZ védelmi szférán belüli vizsgálatához a tényfeltáró megállapítások mellett az érintettek megkérdezése vezethet eredményre. Egy kellő részletességgel megfogalmazott, majd precízen feldolgozott kérdőív bizonyíthatja a KRISZ rendvédelmi létezését és előfordulásait. Feltételezésem szerint az internetes szolgáltatások rendvédelmi igénybevétele oly mértékű, hogy azok közül egyesek kiesése a szervezetek alaprendeltetéséhez köthető folyamatokat, a személyek munkavégzését, vagy munkakörök ellátását akadályozná;
- Véleményem szerint a KRISZ rendvédelmi működtetése kötelezettségből, vagy társadalmi elvárásból adódóan megkerülhetetlen feladat, amely a szervezetek legkülönbözőbb szintjein megjelenik. A folyamatos működést a stabil háttérszolgáltatások esetén is befolyásolja egy kibertámadás, amelynek lehetőségét a biztonság vizsgálatával lehetséges feltérképezni. Hipotézisem szerint, amennyiben fellelhetők támadási-, vagy gyenge pontok a KRISZ-ben, úgy bizonyított a védekezés szükségessége;
- Megítélésem szerint hiányzik az az általános érvényű eljárásrend, amelynek betartása jelentős segítséget jelent az internetes szolgáltatások nagy rendelkezésre állással bíró, biztonságos üzemeltetéséhez, illetve elősegíti az igénybe veendő létfontosságú internetes szolgáltatások rendelkezésre állását;

Kutatási módszerek

Az értekezésem elkészítéséhez az alábbi kutatási módszereket alkalmaztam:

- irodalomkutatás: a vonatkozó releváns nemzetközi és hazai szakirodalom, jogszabályok és egyéb dokumentumok kutatása, tanulmányozása, feldolgozása;
- kérdőívből kinyert adatok összehasonlító elemzése;
- általánosítás, mint vizsgálati módszer;
- logikai elemzés: a feltárt adatok feldolgozása, elemzése, értékelése, ebből a következtetések levonása után, javaslatok megfogalmazása;
- empirikus kutatások: saját megszerzett szakmai tapasztalatok felhasználása, leírása;
- konferenciákon, konzultációkon, rendezvényeken való részvétel, javaslatok kidolgozása;

- eredmények publikálása: kutatási eredmények feldolgozása, cikkek, egyetemi jegyzet fejezetek formájában történő publikálása, valamint konferenciákon és oktatásban történő előadása.

Az értekezés felépítése

A fentieknek megfelelően az értekezésemet négy fejezetben, elméleti és gyakorlati témakörök szerint építem fel:

Az első fejezetben a KRISZ elméletével kívánok foglalkozni. Értelmezni kívánom a Kritikus Internetes Szolgáltatásokat, vizsgálni kívánom azok felépítését és megvalósulásának aspektusait, valamint az irányukba kialakuló kötődéseket kívánom áttekinteni.

A védelmi szférában végzett felmérés alapján vizsgálni kívánom a személyi állomány, valamint a szervezetek által igénybe vett-, és a szervezetek által nyújtott internetes szolgáltatásokat, továbbá a szolgáltatások leállásának, kimaradásának esetleges hatásait, következményeit.

A második fejezetben a KRISZ felépítésével, működésének összetételével, alrendszeri összefüggéseivel és az adatbáziskezelők, mint – általában – háttérszolgáltatók szerepével fogok foglalkozni, továbbá át kívánom tekinteni az adatbáziskezelők biztonsági szerepét és helyzetét. Rá szeretnék mutatni arra, hogy mit jelent rendszerszintű megközelítésben, ha valamelyik alrendszeri elem nem látja el funkcióját, vagy támadási célponttá válik.

A harmadik fejezetben a KRISZ gyakorlati megvalósításával, biztonsági és rendelkezésre állási kérdéseivel, a Web szerepével, az elektronikus levelezés KRISZ-t érintő kérdéseivel, valamint a KRISZ biztonságos üzemeltetésével kívánok foglalkozni.

Az utolsó, negyedik fejezetben gyakorlati ajánlást kívánok tenni a KRISZ biztonságos üzemeltetésére és igénybevételére.

1. FEJEZET
Kritikus Internetes Szolgáltatások

A Kritikus Internetes Szolgáltatások témakörének célzott, nagyobb terjedelmű, tudományos feldolgozására a korábbiakban nem került sor; ebben a fejezetben az elméleti megközelítés és a gyakorlati felmérés egyaránt szerepet kap. Az elmélet alapja a korábbiakban definiált infrastrukturális megközelítés, amely alapvető támogatói környezete az internetes szolgáltatásoknak, a felmérés helye pedig a teljes rendvédelmi spektrum. Az elméleti megközelítés és a gyakorlati terepről származó információk összevetése lehetőséget ad a hipotézisek és a feltételezések alátámasztására.

1.1 A Kritikus Internetes Szolgáltatások elmélete

A Kritikus Internetes Szolgáltatások a kritikus infrastruktúrákkal és a kritikus információs infrastruktúrákkal szorosan összefüggő, a világhálón megjelenő szolgáltatások rendszere. Jelen fejezet célja definiálni a Kritikus Internetes Szolgáltatás fogalmát és bemutatni felépítését, továbbá megvizsgálni működésének aspektusait, áttekinteni az általános alkalmazásának lehetőségeit.

1.1.1 A Kritikus Internetes Szolgáltatás értelmezése

Figyelembe véve, hogy az internetes szolgáltatások létezése háttéreszközök rendelkezésre állása nélkül lehetetlen, a KRISZ bemutatása és definiálása előtt szükséges értelmezni az infrastruktúrák kritikusságát.

A legkorábbi, 2008-as meghatározás alapján kritikus infrastruktúra (továbbiakban: KI):

„Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek **meghibásodása**, **kiesése** vagy **megsemmisítése**, működésük **megzavarása közvetlenül** vagy **közvetetten**, **átmenetileg** vagy **hosszútávon** súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére." [8] Ez a definíció véleményem szerint ma is helytálló és finomítása alkalmas a KI részeként működő egységek meghatározására.

„A XXI. század új típusú kihívásainak rendszerében a 2001. szeptember 11-i támadások következményeképpen Európában is erőteljesebben megjelent a kritikus infrastruktúrák védelmének kérdésköre.” [9] A Katasztrófavédelem honlapján is megtalálható Kormányrendelet hivatkozása alapján:

„25. *Kritikus infrastruktúra:* Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.” [4] Egy jogszabályban is megjelent, tömörebb formájú, modernebb definíció, amely nagy átfedést mutat a 2008-ban megalkotott szöveggel.

Információs rendeltetésű Infrastruktúrák (továbbiakban: II):

„Olyan állandóhelyű vagy mobil létesítmények, eszközök, rendszerek, hálózatok, illetve az általuk nyújtott szolgáltatások összessége, melyek az információs társadalom működéséhez szükséges **információk megszerzését, előállítását, tárolását, elosztását, szállítását** és **felhasználását** teszik lehetővé. Az információs infrastruktúra a fizikai építményekből, berendezésekből, illetve az azokat szakszerűen működtetni tudó szakszemélyzetből áll, mely egy tudatosan tervezett, szervezett és megépített mesterséges környezet az információk feldolgozására, továbbítására vagy felhasználására." [10] Véleményem szerint a technikai fejlődéstől független, ma is aktuális meghatározás, amely megfelelően körül határolja az II fogalmát.

Kritikus Információs Infrastruktúrák (továbbiakban: KII):

„A kritikus infrastruktúrák védelmére vonatkozó európai programról szóló **zöld könyv** szerint: kritikus információs infrastruktúrák közé azokat kell sorolni, amelyek önmaguk is kritikus infrastruktúráknak minősülnek, vagy az infrastruktúrák működése szempontjából fontosak (pl.: távközlési hálózat, számítógép hardver/szoftver, internet, műholdak stb.)." [10]

Az Európai Bizottság 2005. novemberében közreadott anyaga [11] és a Zrínyi Miklós Nemzetvédelmi Egyetem Információs Műveletek és Elektronikai Hadviselés Tanszék kutatói és szakemberei által készített tanulmány szerint:

„A kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából (távközlés, számítógépek és szoftver, internet, műholdak

stb.)” [12] Ebben az egyébként szintén helytálló megfogalmazásban érzékelhető a KI és az II definícióiból származó levezetés, amely így értelemszerűen együttesen értelmezendő.

„Az információs rendeltetésű infrastruktúrák a definíciójukban megfogalmazott funkcióikat gyakran internethez kapcsolással érik el, mely részben a végfelhasználók-, részben pedig az azokat működtető apparátus jól felfogott gazdasági vagy társadalmi érdeke.” [1]

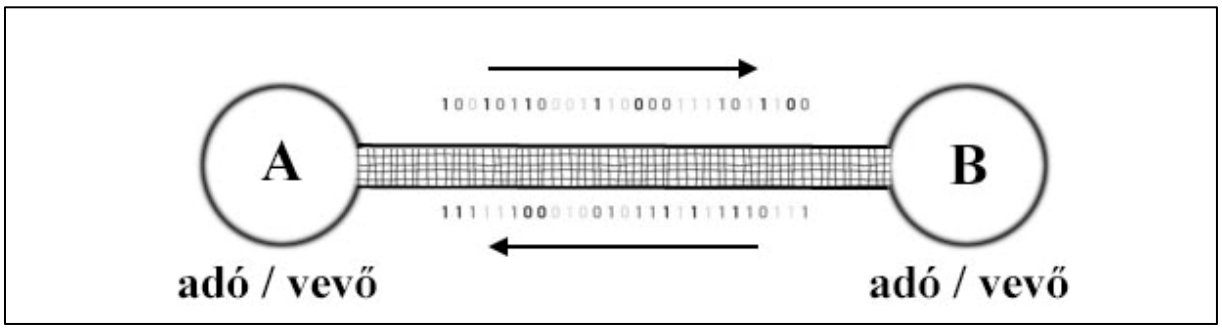
A fentiek alapján, a következő meghatározást teszem:
Kritikus Internetes Szolgáltatás (KRISZ) minden olyan, a világhálón elérhető informatikai szolgáltatás, mely a fenntartó vagy az igénybe vevő működéséhez szükséges információk megszerzését, előállítását, tárolását, elosztását, szállítását és felhasználását teszi lehetővé és **meghibásodása**, **kiesése** vagy **megsemmisítése**, működése **megzavarása közvetlenül** vagy **közvetetten**, **átmenetileg** vagy **hosszútávon** súlyos hatást gyakorolhat a fenntartó, vagy az igénybe vevő működésére, kihathat az állampolgárok gazdasági, szociális jólétére, a közegészségre, a közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére.

A KRISZ álláspontom szerint akkor tartozik bele a KI, vagy KII körébe, ha a szolgáltatás leállása a társadalom jelentős hányadára kihatással van, vagy ha miatta a kormányzat valamely szereplője nem képes feladatait maradéktalanul ellátni.

„Az angol „service” szó magyarra fordítva egyaránt jelent kiszolgálást és szolgáltatást. Egymással rokon értelmű szavak, van is közöttük átfedés, azonban főleg az informatikában mégiscsak markánsan eltér a jelentésük. A kiszolgálás egy állandó, ingyenes rendelkezésre állás, míg a szolgáltatás olyan rendelkezésre állás, melynek teljesítése – általában – valamilyen feltétel függvénye." [13]
„A hálózati szolgáltatás olyan, az informatikai hálózat valamely dedikált pontján működő tevékenység, mely a hálózat aktív elemei között közvetlenül vagy közvetetten adatcserét tesz lehetővé.” [1]
Amennyiben egy interneten megjelenő hálózati szolgáltatás Kritikus Internetes Szolgáltatássá válik, úgy a funkciójában megfogalmazott célt rendeltetésszerűen, állandóan biztosítja, tehát kiszolgál. „A KRISZ tehát olyan szolgáltatás, amely az elvárt állandó rendelkezésre állás következtében egyben kiszolgálás is.” [1]

1.1.2 A KRISZ felépítése

Tekintettel arra, hogy interneten megjelenő szolgáltatásokról van szó – a definícióból adódóan – fontos leszögezni, hogy a szolgáltatás igénybevételekor közvetve, vagy közvetlenül adat-, információcsere történik, melynek egyenes következménye, hogy felek közötti kommunikáció valósul meg.



1. ábra

Kommunikáció; forrás: szerző

Az informatikára vonatkoztatva, a kommunikációban közreműködő felek közül az adót a szerver (kiszolgáló), a vevőt a kliens (ügyfél) valósítja meg, a kommunikációs közeget pedig az informatikai hálózat biztosítja. Figyelembe véve, hogy interneten elérhető szolgáltatásról van szó, a kommunikációs közeg valamely része biztosan érinti a világhálót. A kiszolgálót akkor is internetről elérhetőnek tekintem, ha az DMZ[6]-be rejtett, mert a hozzáférést a szolgáltatónak ekkor is biztosítania kell. A KRISZ igénybevétele szempontjából, a felek és a kommunikációs közeg rendelkezésre állása egyformán fontos és bármelyik hiánya gátolja a szolgáltatást.

„A számítógép-hálózatban csak a dedikált aktív eszközök képesek egymással kommunikálni, amely sikeres kapcsolatfelvétel után valósul meg és a kapcsolat lezárásával végződik. Az eszközök közötti kommunikáció alapfeltételei:

- egymás azonosításának képessége (felismerés);
- kapcsolatteremtő képesség (kérés, válasz);
- közös nyelv ismerete.

[6] „DMZ - (DeMilitarized Zone - demilitarizált övezet)” [14]

Ahhoz, hogy a szolgáltatást nyújtó és az azt igénybe vevő fél egységesen reagáljon a kommunikáció során, viselkedési kultúrára, azaz protokollra van szükség.
Az informatikában a **protokoll** egy egyezmény, vagy szabvány, amely leírja, hogy a hálózat résztvevői miképp tudnak egymással kommunikálni. Ez többnyire a kapcsolat felvételét, kommunikációt, adat továbbítást jelent." [1]
„A protokoll lényegében olyan megállapodás, amely az egymással kommunikáló felek közötti párbeszéd szabályait rögzíti." [14]

A „hivatalos szabványos internet protokollok" listája [15] megtalálható a világhálón, melyek nagyrészt lefedik az általános internetes kommunikáció protokolljait, ugyanakkor természetesen lehetnek egyedileg kifejlesztett kapcsolatteremtési és viselkedési formák.

A hálózati protokollokat ismerő és megvalósító szoftverek a szerver-, és kliens programok. „A szerverprogram hálózati portot nyit a kiszolgáló – informatikai – eszközön, ezáltal biztosítja a hálózati kapcsolódás lehetőségét, melyhez az ügyfél IT eszközére telepített, a szerverprogrammal kommunikálni képes kliens program kapcsolódhat." [1]

Interneten megjelenő szolgáltatáshoz az alábbi összetevők működése szükséges:

1. infrastruktúra
    - támogató információs infrastruktúra;
    - funkcionális információs infrastruktúra.

Támogató információs infrastruktúrák:
„Létrehozzák, és folyamatosan biztosítják a funkcionális információs infrastruktúrák nagy halmazainak zavartalan működéséhez és fejlődéséhez szükséges anyagi és szellemi alapokat valamint támogatási háttereket." [16]

Funkcionális információs infrastruktúrák:
„Fizikailag lehetővé teszik a társadalom valamilyen információs funkciójának zavartalan működését, vagyis infrastrukturális alapon információs alapszolgáltatásokat végeznek." [10]

2. hardver
    - számítógép, IT eszköz;

- hálózati eszközök.

3. szoftver
    - operációs rendszer;
    - szerverprogram;
    - kliens program;
    - háttér-programok.

A hardverre telepített operációs rendszerek, háttér-programok, kliens programok és szerverprogramok – változó összetételben – együttesen biztosítják a szolgáltatás nyújtásának és igénybevételének szoftveres összetevőit. Mind a szerver, mind a kliens programok általában operációs rendszeri környezetben működnek, azonban firmware-be integrálva, annak sajátosságaival előfordulhatnak a nélkül is. A szerver-, és a kliens programok gyakran csak az érintkezési felületet nyújtják, hisz ismerik az alkalmazott protokollt és megvalósítják az adatok áramlását, ugyanakkor az információ előállításához, vagy feldolgozásához további háttér-program(ok) működését veszi(k) igénybe. A háttér-programok önmaguk is lehetnek saját hálózati kapcsolattal rendelkező szerverprogramok, vagy tényleges hálózati port-tal nem-, de „TCP-socket primitívvel” [45] bíró kiegészítő programok, esetleg hálózati kapcsolat nélküli, modulként csatolt, vagy szorosan együttműködő komponens programok. A háttér-programok a kliens alkalmazások használatában is szerepet kaphatnak, hisz gyakran az információk végső feldolgozásához, vagy megjelenítéséhez is kiegészítő modulok alkalmazására van szükség, mely adott esetben a KRISZ igénybevételének elengedhetetlen kelléke.
A KRISZ körébe tartozó szolgáltatások és azok kliens alkalmazásai teljesen változó formában jelennek meg, azonban elmondható, hogy inkább az alkalmazói oldalon törekednek a felhasználó-barát kinézetre és kezelésre. Általánosságban cél az egyszerű kezelhetőség biztosítása, ugyanakkor a számtalan szoftver gyártó miatt jellemző a sokszínűség, de az ebből adódó versenyhelyzet biztosítja a folyamatos fejlődést.

A megfelelő hálózati összeköttetés nélkülözhetetlen feltétele a Kritikus Internetes Szolgáltatásokban résztvevő szerver és kliens közötti adatcserének, tehát a kommunikációs közeg is alap összetevőnek számít. A szerver állandó rendelkezésre állása mellett elengedhetetlen az összeköttetés folyamatos biztosítása is, hogy a klienseknek lehetőségük legyen kapcsolatot kezdeményezni. Figyelembe véve, hogy a KRISZ esetében az internet mindenképpen része az összeköttetésnek, a kapcsolat létrehozásában és fenntartásában

előfordulhat bizonytalanság. Amennyiben a KRISZ-ben résztvevő feleknek egyaránt fontos az összeköttetés megbízhatósága, vagy biztonsága, úgy az összeköttetést meg kell szilárdítani, amely leginkább a rendelkezésre állás fokozásában és a szükséges adatátviteli sebesség biztosításában merül ki. Előfordul, hogy egy KRISZ-ben, az összeköttetés megszilárdítása egy másik erre irányuló szolgáltatás igénybevételével valósul meg, amely így szintén Kritikus Internetes Szolgáltatássá válik. A szerver-kliens közötti összeköttetés csatornán belüli virtuális csatorna létrehozásával alkalmas a hálózat kiterjesztésére és a kommunikáció tulajdonságainak megváltoztatására. A KRISZ virtuális csatornába kényszerítése növelheti a kommunikáció biztonságát, egyben a szolgáltatás igénybevételének feltételéül is szolgálhat.
„A KRISZ működtetése és igénybevétele összetett, infrastruktúrák, hardverek és szoftverek néha bonyolult, összehangolt működésének következménye. Fontos kiemelni, hogy a KRISZ működéséhez szükséges összetevők bármelyikének kiesése a szolgáltatás használhatatlanságához vezet.

1.1.3 A KRISZ aspektusai

A KRISZ megvalósulása szubjektív. A társadalom szereplőinek igényei, szokásai, érdekei, vagy kötelezettségei egyénileg határozzák meg, hogy egy internetes szolgáltatás beletartozik-e a KRISZ körébe, vagy sem. A működés létfontossága a szolgáltató, az igénybe vevő, vagy esetenként mindkettő oldalán egyaránt megjelenhet. A KRISZ számos cél érdekében működhet, amelyben a végeredmény mindig ugyanaz: információcsere biztosítása.” [1]

KRISZ szolgáltatója és felhasználója (szereplője) egyaránt lehet:

- állam, kormányzat;
- jogi személy (vállalkozás);
- természetes személy.

KRISZ lehetséges funkciói:

- a kommunikációban résztvevő felek közötti összeköttetés biztosítása;
- felek közötti adatcsere biztosítása;
- szerver, vagy aktív hálózati eszköz elérése, karbantartása.

Funkcionális rendszerezés szerint, – néhány példa feltüntetésével – KRISZ működhet:

a) kommunikációban résztvevő felek közötti összeköttetés biztosítására:

- új, vagy létező hálózati szegmens rendelkezésre állásának növelésére, a megfelelő adatátviteli sebesség garantált elérésére;
- új hálózati szegmens kialakítására (WLAN[7], PPP[8]);
- létező hálózati szegmens titkosítására (VPN);
- II biztonságos elérésére.

b) adatcsere biztosítása céljából:
- elektronikus levelek küldésére és fogadására (SMTP);
- állományok továbbítására (FTP[9]);
- szövegek, képek, videók, multimédia objektumok megjelenítésére (W3[10] / HTTP[11]).

c) szerver, aktív hálózati eszköz elérése-, karbantartása céljából:
- WinRM[12] alkalmazására;
- SSH[13] használatára;
- Apple Remote Desktop[14] elérésére.

A KRISZ előfordulásának lehetséges esetei szereplők szerinti bontásban:

a) állam, kormányzat
- szolgáltatóként:
  - társadalom információs tájékoztatása;
  - kormányzati kommunikáció biztosítása.
- felhasználóként: elektronikus ügyintézés.

b) jogi személy
- szolgáltatóként: elektronikus kereskedelem;
- felhasználóként: elektronikus bevallás.

c) természetes személy
- „szolgáltatóként": távfelügyelet, virtuális magánhálózat VPN[15];
- felhasználóként: elektronikus banki ügyintézés (e-bank).

---

[7] Wireless LAN - vezeték nélküli hálózat
[8] Point-To-Point Protocol - pont-pont kapcsolati protokoll
[9] File Transfer Protocol - állománytovábbító protokoll
[10] Wolrd Wide Web
[11] HyperText Transfer Protocol
[12] Windows Remote Managment - Windows távoli menedzsment
[13] Secure Shell - biztonságos parancsfuttató környezet
[14] Apple távoli munkaasztal
[15] Virtual Private Network - virtuális magánhálózat

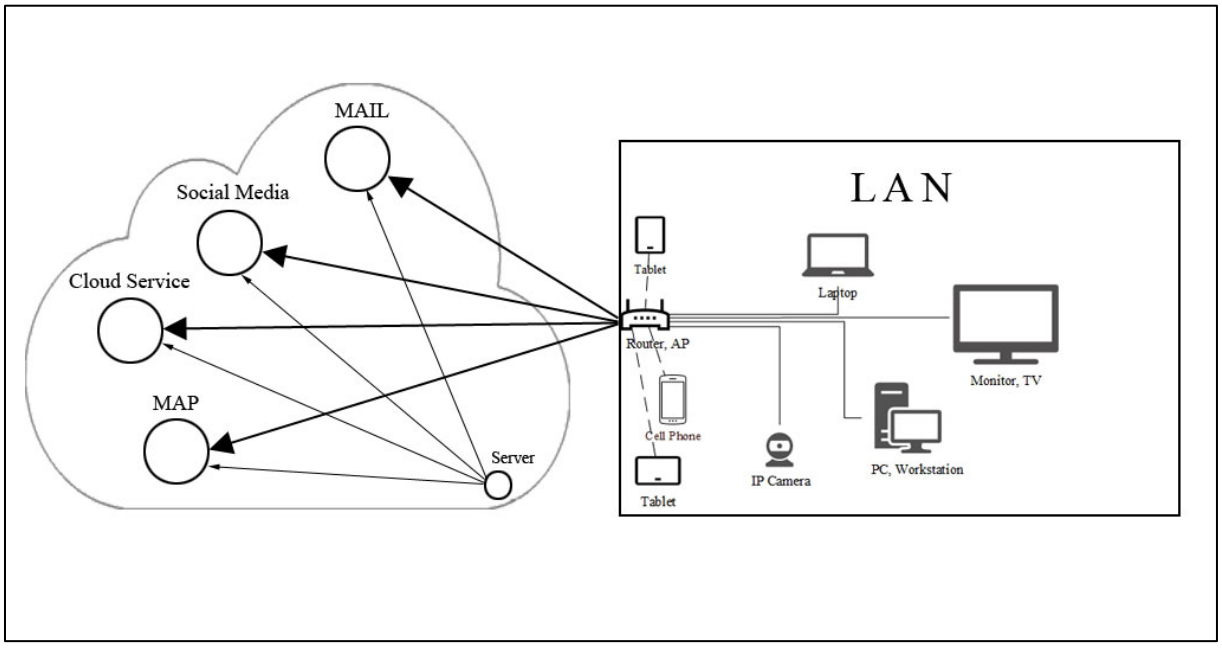
A KRISZ igénybevételének lehetséges módjai:

- felhasználói beavatkozáshoz kötötten, vagy programozottan;
- állandóan, vagy visszatérően;
- a felhasználó tudtával, vagy tudomása nélkül;
- igény szerint, vagy kötelezően;
- közvetlenül, vagy közvetetten;
- ellenszolgáltatásért, vagy ingyenesen.

1.1.4 Kötődés az internetes szolgáltatásokhoz

Az interneten elérhető, rendkívül nagy rendelkezésre állással működő szolgáltatásokhoz gyakran kötődés alakul ki az igénybe vevők részéről, amely értelemszerűen a KRISZ körébe tartozó szolgáltatásokra is vonatkozhat.

A kötődés kialakulásának első lépése mindenképpen az internetes szolgáltatás megjelenése és elérhetősége, amely egyértelműen a szolgáltató döntésének a következménye. A döntés alapja lehet saját elhatározás, továbbá valamilyen jogszabályi, normatív, vagy egyéb előírás. A saját elhatározású döntés gyakran piaci alapú, vagy társadalmi igény következménye.



2. ábra

Kötődések szolgáltatásokhoz; forrás: szerző

Az internetes szolgáltatás megjelenését követően, a kötődés a szolgáltatást igénybe vevők részéről alakul ki, amely így – a felhasználók szempontjából – létfontosságú, Kritikus Internetes Szolgáltatássá minősülhet. A rendelkezésre álló-, és mellette még hasznos szolgáltatások igénybevételekor a felhasználó figyelmen kívül hagyja, hogy a szolgáltatás milyen ok miatt érhető el, egyszerűen természetessé és megszokottá válik a visszatérő használat lehetősége.
A kötődés tehát szabad választás-, vagy kötelezettség miatt alakulhat ki, amelynek mind a felhasználó, mind a szolgáltató lehet érdekeltje, vagy haszonélvezője.

Kötelezettségen alapú kötődés

Az államigazgatásnak, kormányzatnak jól felfogott gazdasági érdeke, hogy az internetet, mint kommunikációs eszközt felhasználja a társadalommal történő, lehetőleg két irányú kapcsolattartásra, amelynek elengedhetetlen feltétele valamilyen internetes szolgáltatás működtetése. A jelenlegi gyakorlatban az államigazgatás saját magát kötelezi bizonyos internetes szolgáltatások működtetésére, a társadalomnak pedig – idő-, és költség megtakarítást ajánlva – lehetőséget ad ezen szolgáltatások igénybevételére, használatára. A kormányzat természetesen az általa működtetett szolgáltatások használatát, igénybevételét – a társadalom szegmenseként, – saját szervezeteinek előírhatja, ezáltal mind a szolgáltató, mind az ügyfél oldalon is megjelenik kötelezettség, az érintett szolgáltatások pedig Kritikus Internetes Szolgáltatásokká minősülnek.
Meggyőző, célzott és megfelelő kommunikációval elérhető, hogy az államigazgatás mellett a lakosságnak is jól felfogott érdeke legyen a szolgáltatások igénybevétele, amelyet tovább erősít, ha azok a szolgáltatások stabilan elérhetők, használhatók és tényleg az emberek kényelmét szolgálják. Számos tényező erősíti a szolgáltatások igénybevételére irányuló hajlandóságot, így például a jogszabályban rögzített határidők adott nap végéig történő kitolásának lehetősége, vagy a postai várakozás elkerülése. Az internet egyetemleges társadalmi rendelkezésre állása esetén akár mindenkire nézve kötelezővé lehetne tenni a kormányzat által biztosított internetes szolgáltatások használatát, ennek bekövetkezéséig azonban marad az erős kormányzati ajánlás.
A kötelezettségen alapuló szolgáltatások rendszeres, visszatérő használata az ügyfél részéről mindenképpen kialakítja a kötődést, ragaszkodást az alkalmazás iránt. A szolgáltató fenntartási kötelezettségébe természetesen az IT biztonság megteremtése is beletartozik.

Szabad választáson alapú kötődés

A piaci alapon működtetett szolgáltatásoknak kifejezett célja a kötődés, vagy esetleg függőség kialakítása a felhasználókkal, hisz ezáltal biztosított a profitjuk, és ebből az önös érdekből táplálódik a szolgáltatás infrastruktúrájára és az IT biztonságra fordítandó forrás. A szolgáltatók az ügyfelek kegyeiért a szolgáltatás minőségével, színvonalával küzdenek meg, a felhasználók részéről pedig szabad választás eredménye az adott szolgáltatás igénybevétele. Napjainkban ügyfelek milliói, százmilliói vesznek igénybe ingyenes internetes szolgáltatásokat, amelyek észrevétlenül, meghatározzák szokásaikat, életvitelüket és válhatnak számukra Kritikus Internetes Szolgáltatásokká. Ezen felhasználók úgy hagyatkoznak „ismeretlen" szolgáltatók internetes szolgáltatásaira, hogy – figyelmen kívül hagyva a szolgáltatás leállásának esetleges következményeit, – garancia nélkül, minimális jogérvényesítési lehetőség mellett is bíznak abban, hogy a korábban rendelkezésre álló szolgáltatások a továbbiakban is működni fognak. A szolgáltatásokba vetett „korlátlan bizalom" a közigazgatás szereplőit is utolérte és egyre nagyobb számban veszik igénybe őket a szervezeti munka során. Ezen használatok oka általában valamely igényhez társítható, „éppen jókor" rendelkezésre álló szolgáltatás elérhetősége, vagy konkrét célzott szolgáltatás alkalmazása, amelyek összességében támogatják, segítik a munkavégzést. A szabadon választható, ugyanakkor munkafolyamatokba integrálódó internetes szolgáltatásokhoz a lakosság és az államigazgatás részéről egyaránt kialakul a kötődés, amelyek így észrevétlenül Kritikus Internetes Szolgáltatásokká válnak.

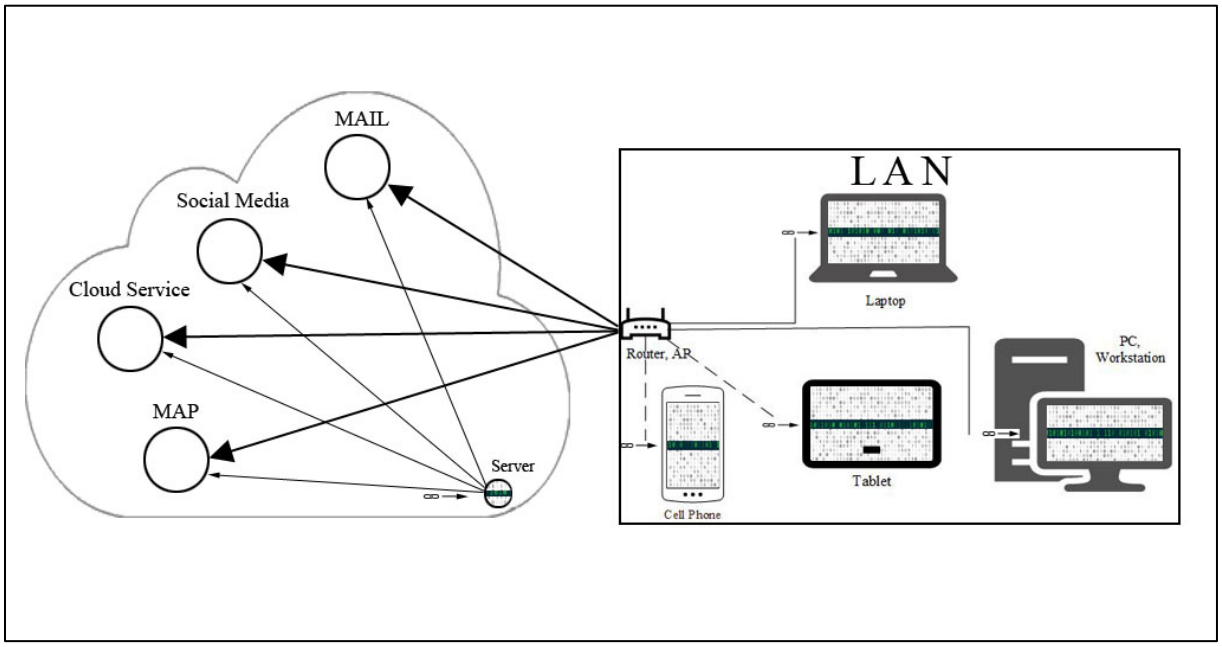
Saját elhatározáson alapuló kötődés

Az internetet használó társadalom tagjai különböző célok miatt, saját döntés alapján, belső használatra, gyakran önmaguknak indítanak internetes szolgáltatásokat. Ezen megoldást a kormányzat, a vállalkozások és a hétköznapi emberek éppúgy alkalmazzák, elsősorban a feladatok hatékonyabb végzése-, az információáramlás megkönnyítése-, és a távolságok áthidalása érdekében. A bevezetett szolgáltatásoknak akkor van értelme, ha azok a felhasználás igénye szerint, az elvárt rendelkezésre állással működnek, amelynek egyenes következménye, hogy a használat folyamatosan visszatérő, továbbá, hogy kialakul a kötődés. A szolgáltatások felhasználói számítanak azok állandó rendelkezésre állására, így rájuk nézve azok Kritikus Internetes Szolgáltatásokká válnak.

Kötődés alapuló működés

Az internetes szolgáltatásokhoz kialakult kötődések sokszor annyira erősek, hogy azokra eszközök, programok, folyamatok, esetleg újabb szolgáltatások is támaszkodnak. Fejlesztők, programokba gyakran úgy integrálják internetes szolgáltatások elérését, mintha magától értetődő lenne, hogy azok állandóan, mindig fognak működni, sőt eszközöket is – a vásárlók tájékoztatásának mellőzésével – adnak el így. Standalone, vagy hálózati szoftverekbe, esetleg internetes honlapok forráskódjaiba, úgy helyeznek el szövevényes kapcsolatokon alapuló külső hivatkozásokat, hogy figyelmen kívül hagyják a hivatkozás megszűnésének következményeit. A hivatkozások mögött találhatók egyrészt harmadik fél által fejlesztett – nyílt, vagy zárt kódolású – eljárások, vagy függvények, továbbá ismeretlenek kezelésében levő adatvagyonokban, külső hivatkozással származtatható adathalmazok.

Ezen szoftverek állandó kötődés mellett működnek és amennyiben állami-, vagy közfeladatba, esetleg a társadalom jelentős hányadát érintően kerülnek bevonásra, úgy a kötődéshez kapcsolódó szolgáltatás biztosan Kritikus Internetes Szolgáltatássá válik. A 3. ábrán a forráskódokban megjelenő kiemeléssel szemléletesen látható, hogy különböző IT eszközökön futó alkalmazásokba miként integrálódnak hivatkozások internetes szolgáltatásokhoz.



3. ábra

Kötődés alapú működés; forrás: szerző

1. Felhasználás további – akár kritikus internetes, – szolgáltatás nyújtására

A fenntartó interneten nyújtott szolgáltatásához igénybe vett másik olyan internetes szolgáltatás, amelynek elérhetősége és használata nélkülözhetetlen a fenntartó internetes szolgáltatásának zavartalan, teljes értékű működtetéséhez. Fontos kiemelni, hogy a távoli hivatkozás egyfajta erőforrásként jelenik meg, amely a szolgáltatás nyújtásához valamilyen formában befektetésre, bevonásra és továbbadásra kerül. Tipikus példa a weblapokba integrált külső programkód, vagy tartalmi elem hivatkozás, amely befolyásolja a fenntartót a szolgáltatása működtetésében.

A hivatkozás kiesése a fenntartó szolgáltatásában zavart kelthet, azt

- részben, vagy egészben meghiúsíthatja, használhatatlanná teheti;
- információhiányhoz juttathatja, vagy pontatlan adatkezelésre kényszerítheti.

Amennyiben a fenntartó internetes szolgáltatása KRISZ, úgy a hivatkozott szolgáltatás is automatikusan Kritikus Internetes Szolgáltatássá válik.

2. Felhasználás önálló feladatok végrehajtására

Végfelhasználói programba, vagy eszközbe integrált olyan internetes szolgáltatás, amelynek rendelkezésre állása nélkülözhetetlen a végfelhasználói program zavartalan, teljes értékű működéséhez. Tipikus példa az interneten elérhető térkép adatbázisokból kinyert adatok felhasználó programokban történő megjelenítése.

1.2 Kritikus Internetes Szolgáltatások a védelmi szférában

A fentiekben leírt, általam elméletben megfogalmazottak bizonyítására a védelmi szférában egy átfogó kérdőíves felmérést-, továbbá szakmai tapasztalatokra alapuló, internetes közegben végrehajtott hálózati vizsgálatokat, elemzéseket végeztem. Mindezek eredményeit tartalmazzák a következők.

1.2.1. Online kérdőíves felmérés

A felmérés körvonalait 2019. márciusában alakítottam ki, végleges változatát októberben készítettem el, a kitöltésre december 31-ig volt lehetőség. A kérdések informatikai végzettséggel nem rendelkező rendvédelmi felhasználók bevonásával kerültek finomításra, amelynél cél volt, hogy

- a megfogalmazás laikusként is érthető-, ugyanakkor pontos legyen;

- a válaszokat lehetőleg kiválasztás módszerével lehessen megadni, amelyek viszont kellően lefedik a lehetséges alternatívákat;
- a feldolgozással egzakt, mérhető eredmény szülessen, amelyből összetett következtetések is levonhatók legyenek;
- választ adjon a hipotézisben megfogalmazott témakörökre.

A mellékletként csatolt, 18 pontból álló kérdőíves kutatás célja a védelmi szférában alkalmazott internetes szolgáltatások – minél szélesebb körű, – hatáselemzéssel bővített felmérése

- szervezetenként;
- felhasználói csoportonként;
- igénybevétel módja szerint.

A kérdőíves felmérés anonim módon-, online kitöltéssel, az információk négyes csoportba rendezésével készült. Cél volt a Kritikus Internetes Szolgáltatások rendvédelemmel kapcsolatos hipotéziseinek igazolása

- a jelenségre (jelenlétre);
- a szervezetekre gyakorolt hatásokra;
- a védekezés szükségességére vonatkozóan.

Fontos kiemelni, hogy a válaszadók jellemzően adminisztratív munkakörben dolgozó, email címmel rendelkező személyek voltak, létszámuk meghaladta a háromszázat, és többnyire elektronikus úton kerültek megkeresésre. A kérdőívek feldolgozása a beérkezett adatok tisztázása, pontosítása és az ellentmondások feloldása után, az IBM SPSS Statistics[16] adatfeldolgozó programmal történt. Az adatok rendszerezéséhez a választható elemeket kódoltam-, a szabadszöveggel kitölthető mezőket pedig mátrixba foglalva összesítettem.

A kitöltőre irányuló információk

Az alábbi kérdések kerültek ebbe a csoportban:

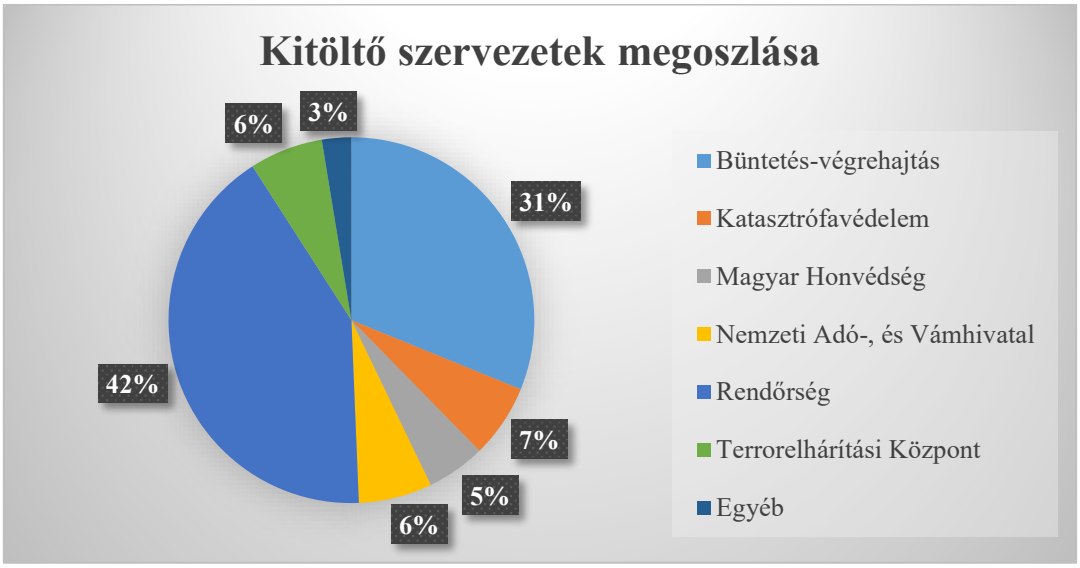
„Ön melyik rendvédelmi szervezetnél dolgozik?”

„Ön miként használja rendvédelmi szerve informatikai rendszerét?”

„Önnek van-e jogosultsága távolról, interneten keresztül belépni rendvédelmi szerve informatikai rendszerébe?”

[16] https://www.ibm.com/analytics/spss-statistics-software

Ezen kérdések kitöltése kötelező volt, a lehetséges válaszok pedig egy kivételével felajánlásra kerültek. A rendvédelmi szervezetre vonatkozó kérdés megteremtette a rendvédelmen belüli rendszerezés, valamint az eredmények összehasonlításának és a különbségek kimutatásának lehetőségét. A rendvédelmi szervezetek közül a Büntetés-végrehajtást, a Katasztrófavédelmet, a Magyar Honvédséget, a Nemzeti Adó-, és Vámhivatalt, a Rendőrséget és a Terrorelhárítási Központot-, továbbá az „Egyéb" mezőt lehetett kiválasztani.



1. diagram

Résztvevő szervezetek százalékos megoszlása; forrás: szerző

A 1. diagramon látható, hogy a kérdőívet legnagyobb arányban a Rendőrség és a Büntetés-végrehajtás dolgozói töltötték ki, a lehetőségként megjelölt szervezetek mindegyike képviseltette magát. Az „Egyéb" kategóriát a kitöltők 2,6%-a jelölte be, amelyek jellemzően a szervezeteket irányító minisztériumok voltak; habár a lehetőség felajánlásra került és biztosított volt, titkosszolgálati szervezettől nem érkezett kitöltött kérdőív.

A Kritikus Internetes Szolgáltatások megítélése szempontjából lényegi különbség, hogy a feltett kérdésekre informatikai végzettséggel rendelkező, vagy nem rendelkező személy ad-e választ, amelyet az informatikai rendszer használatára vonatkozó kérdés volt hivatott eldönteni. Az informatikai rendszerek felhasználói másik két fontos csoportra oszthatók, miszerint többlet jogosultsággal rendelkező – akár felső – vezetők, vagy kevesebb jogosultsággal rendelkező normál felhasználók, amelyet az interneten keresztüli távoli belépési jogosultságra irányuló kérdés alapján lehetett eldönteni. Ezt a kérdést az is indokolja, hogy a távoli belépési jogosultság megteremtéséhez külön szolgáltatást kell fenntartani, amely – tekintettel arra, hogy

utat nyit a rendvédelmi szerv-, vagy szervezet belső informatikai rendszerébe – egyben biztonsági kockázatot is jelent.
A 2. és a 3. kérdés kombinációja további rendezési elvre adott lehetőséget, beazonosíthatóvá tette a kitöltő felhasználó típusát, amely az alábbi lehet:

- felhasználó-vezető;
- vezető;
- informatikus-vezető;
- informatikus.

Ez az információs blokk a kitöltő beazonosítására és a feldolgozás során – a további blokkokkal összekapcsolva – az információk rendszerezésére, osztályozására szolgált.

Igénybe vett szolgáltatások felmérése

Ez a felmérés a védelmi szférában dolgozó felhasználók-, és a rendvédelmi szervezetek igénybe vett internetes szolgáltatásaira tér ki. Feltárja azt a fontos kérdést, hogy az internetes szolgáltatások igénybevétele összességében mennyire meghatározó a védelmi szféra működéséhez, továbbá, hogy annak hiánya mennyire befolyásolja a szervezetek működését.

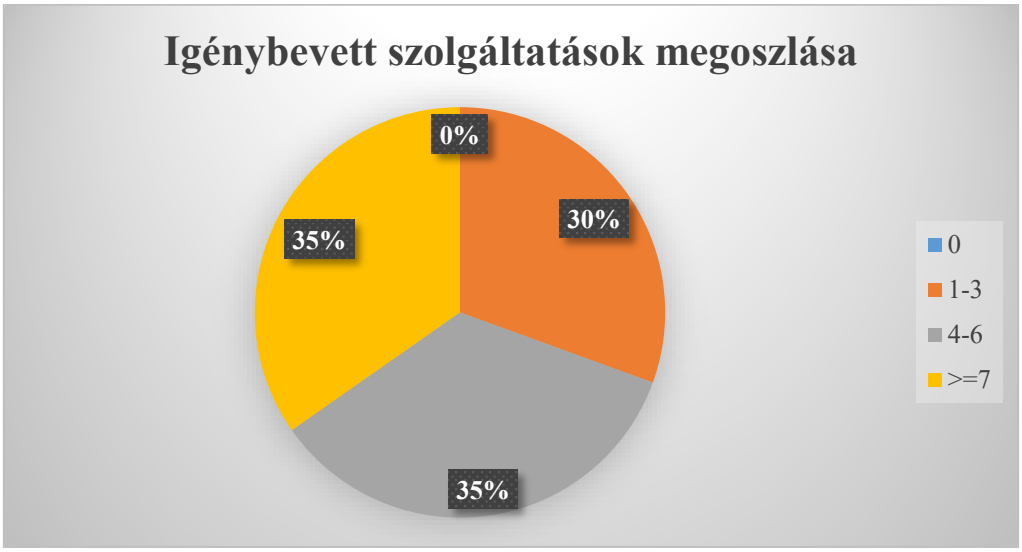
1. A felhasználók által használt internetes szolgáltatások

A feltételezés szerint, a felhasználók munkájuk során – különböző szolgáltatóktól – számos, meghatározó internetes szolgáltatást vesznek igénybe, amelyek kimaradása, vagy kiesése negatív hatással van a munkavégzésükre.

A hipotézis igazolásához az alábbi kérdések kerültek megfogalmazásra:
„Mennyi az Ön munkájához használt, internetes informatikai szolgáltatások (pld. e-mail) száma?”
„Az Ön munkájához használt, internetes informatikai szolgáltatások közül, mennyi az **ingyenes** (pld. gmail) szolgáltatások száma?”
„Az Ön munkájához használt, internetes informatikai szolgáltatások kimaradása, vagy leállása, milyen hatást vált ki az Ön munkájára?”

a) „Mennyi az Ön munkájához használt, internetes informatikai szolgáltatások (pld. e-mail) száma?”

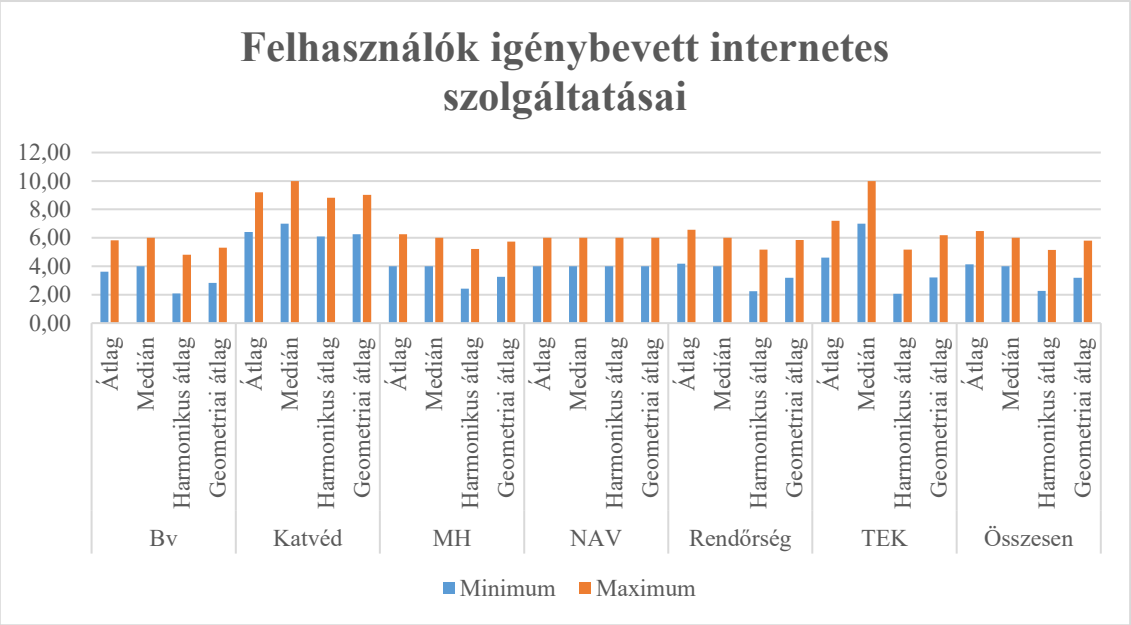
Kötelezően kitöltendő mezőként került definiálásra, a négy lehetséges opció közül csak egyet választhatott a kitöltő, amely a $\underline{0} < \underline{1–3} < \underline{4–6} < \underline{7–\infty}$ képlettel írható le. Ezt a kérdést úgy kellett megfogalmazni, hogy az adott válasszal egyértelműen eldönthető legyen, hogy a védelmi szférában dolgozók a munkájukhoz használnak-e internetes informatikai szolgáltatásokat, továbbá ha igen, akkor azt mekkora nagyságrendben.



2. diagram

Felhasználók igénybe vett internetes szolgáltatásainak megoszlása

Az intervallumok alkalmazása a teljesen egzakt értékek helyett ugyan csak nagyságrendeket mutatnak, viszont alkalmasak az igénybe vett szolgáltatások körülhatárolására, egyben kezelik a kitöltő esetleges pontatlanságát. A felmérés ugyan adott lehetőséget a kitöltőknek, hogy az igénybe vett szolgáltatások számához nulla értéket rendeljenek, azonban ez egyetlen esetben sem fordult elő. Az igénybe vett szolgáltatások módusza, azaz a legtöbbet bejelölt érték a 4-6.



3. diagram

Felhasználók által igénybe vett internetes szolgáltatások átlagai; forrás: szerző

A feldolgozás az intervallumban szereplő alsó és felső érték szétválasztásával, számszerűsítésével, majd a következtetések levonásával történt. A 3. diagramon feltüntetett szervezetenkénti átlagok szerinti kimutatáson látható, hogy változó tendenciával, de minden területen igénybe veszik az internetes szolgáltatásokat, és a tendenciák alapján a szervezetek közül a Katasztrófavédelem dolgozói a legaktívabbak. Az összesített átlagok az 1. táblázatban feltüntetett értékek jellemzik.

	Minimum	Maximum
Átlag	4,13	6,47
Medián	4,00	6,00
Harmonikus átlag	2,26	5,14
Geometriai átlag	3,18	5,80
Szórás	2,438	2,863

1. táblázat

Felhasználók igénybe vett internetes szolgáltatásainak összesített átlagai és szórása; forrás: szerző

A felmérés adatai alapján, a védelmi szféra – elsősorban adminisztratív – dolgozói átlagban 4,13 és 6,47 internetes szolgáltatást vesznek igénybe munkájuk során.

	Minimum	Maximum
Felhasználó, vezető	4,60	7,08
Felhasználó	3,81	6,03
Informatikus, vezető	4,00	6,43
Informatikus	4,00	6,00

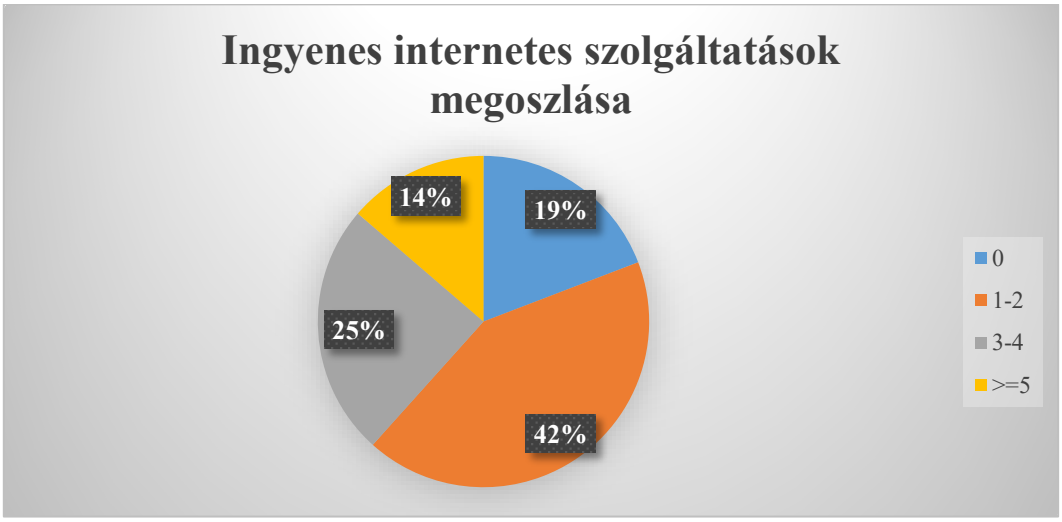
2. táblázat

Szolgáltatások összesített átlagai felhasználó típusonként; forrás: szerző

A 2. táblázatban szereplő, felhasználó-típusonkénti rendszerezésben jól látható, hogy a vezető beosztású, nem informatikus dolgozók veszik igénybe a legtöbb internetes szolgáltatást munkájuk során, a legkevesebbet pedig a nem informatikus felhasználók, akik fejenként így is a 3,81 - 6,03 közötti tartományba esnek.

*b) „Az Ön munkájához használt, internetes informatikai szolgáltatások közül, mennyi az **ingyenes** (pld. gmail) szolgáltatások száma?”*

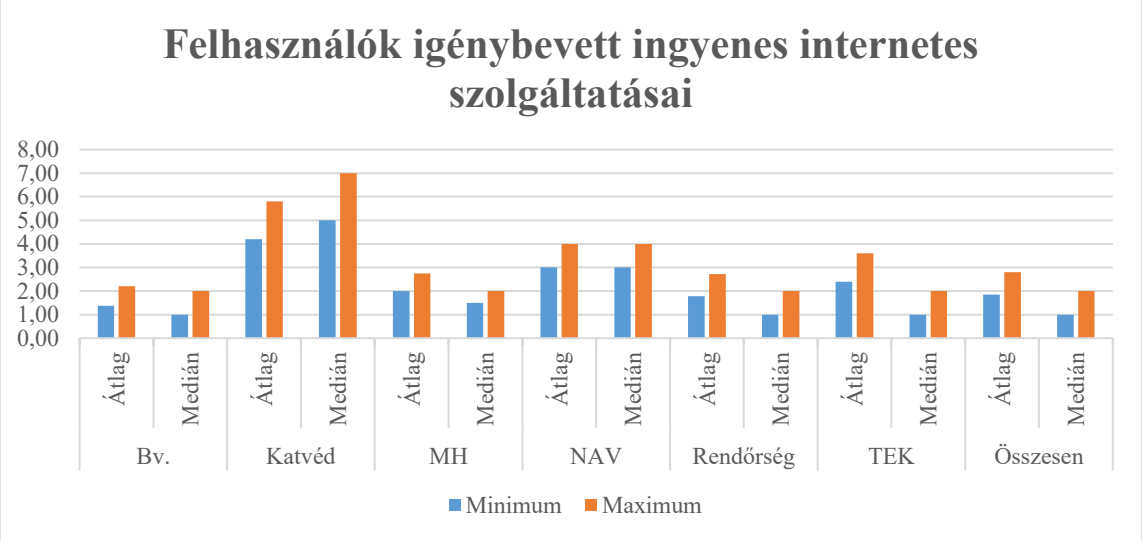
Ez az információ egyrészt rámutat arra a fontos kérdésre, hogy a munkavégzéshez mekkora hányadban vesznek igénybe dolgozók olyan internetes szolgáltatást, amely csupán bizalmi elven működik, másrészt ketté osztja az igénybe vett internetes szolgáltatások halmazát, amelyből további következtetés levonására ad lehetőséget.



4. diagram

Ingyenes felhasználói internetes szolgáltatások megoszlása; forrás: szerző

A válaszadás nem volt kötelező, ennek ellenére minden kitöltő megadta a kérdésre a következő képlet szerinti lehetséges információt: 0 < 1–2 < 3–4 < 5–∞. Ebben az esetben az intervallumok kisebb léptékkel kerültek meghatározásra, amelynek oka, hogy az ingyenes internetes szolgáltatások részhalmazát jelentik az internetes szolgáltatásoknak, így pontosabban meghatározhatók.



5. diagram

Felhasználók által igénybe vett ingyenes internetes szolgáltatások; forrás: szerző

Az 5. diagramon látható, hogy minden szervezetben alkalmaznak a felhasználók ingyenes internetes szolgáltatásokat, annak ellenére, hogy a válaszadók 19%-a nem él ezzel a lehetőséggel.

Átlag	Minimum	Maximum
Internetes szolgáltatás	4,13	6,47
Ingyenes internetes szolgáltatás	1,85	2,79
Ingyenesség aránya	44,79 %	43,12 %

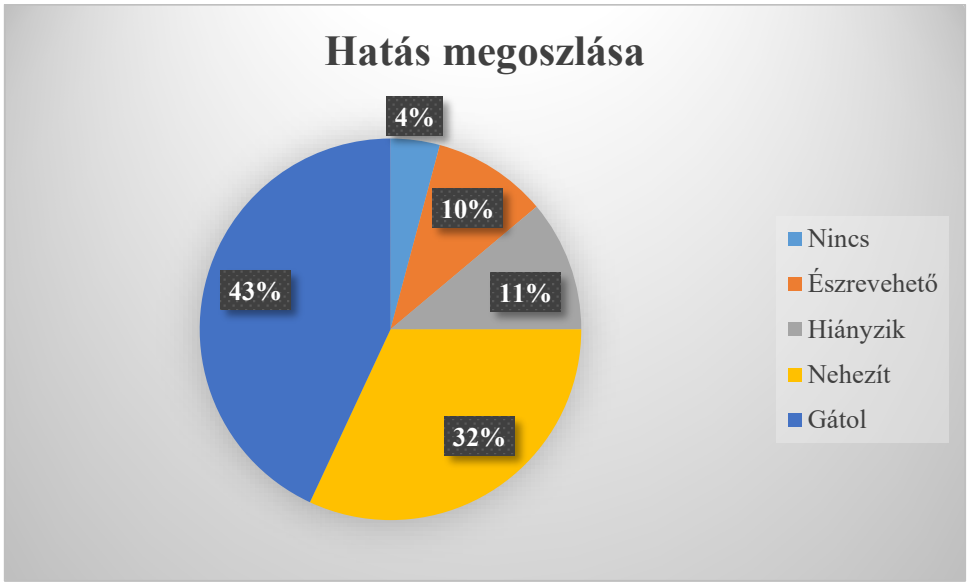
3. táblázat

Ingyenes internetes szolgáltatások aránya; forrás: szerző

A 3. táblázatban feltüntetett összehasonlítás alapján, a felhasználók által igénybe vett ingyenes internetes szolgáltatások aránya az összes átlagosan igénybe vett internetes szolgáltatáshoz képest a minimum értékek vonatkozásában 44,79%, a maximum értékek vonatkozásában 43,12%.

c) „Az Ön munkájához használt, internetes informatikai szolgáltatások kimaradása, vagy leállása, milyen hatást vált ki az Ön munkájára?

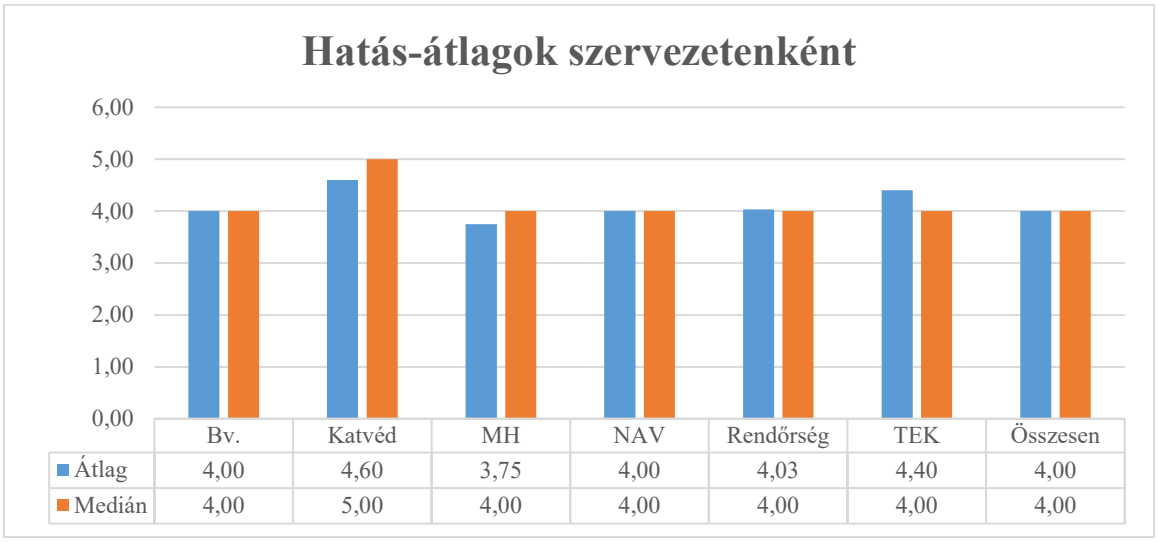
„nincs kihatással 1 2 3 4 5 gátolja a munkavégzést”



6. diagram

Igénybe vett felhasználó internetes szolgáltatások kimaradásának, leállásának hatásai; forrás: szerző

A kérdőív ezen pontja a felhasználók által igénybe vett internetes szolgáltatások kimaradásának, vagy leállásának hatásait méri, amelyből további következtetések eredményeként meghatározható a szolgáltatások kritikussági faktora.



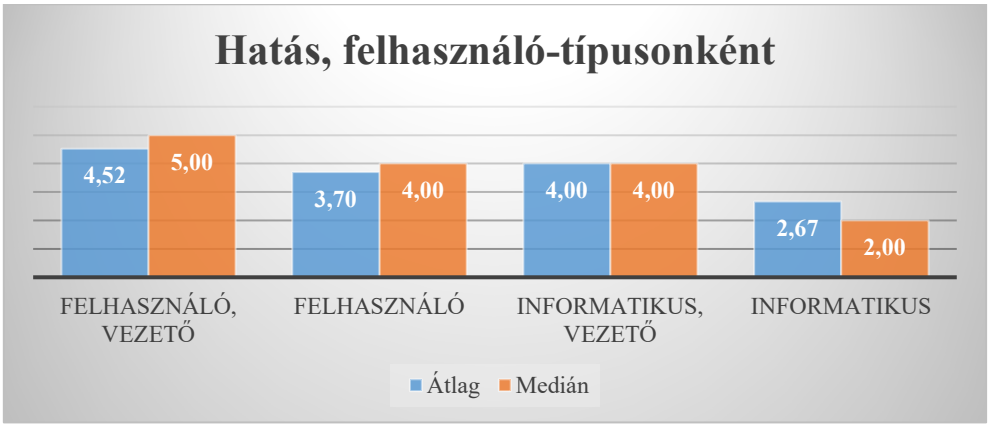
	Bv.	Katvéd	MH	NAV	Rendőrség	TEK	Összesen
Átlag	4,00	4,60	3,75	4,00	4,03	4,40	4,00
Medián	4,00	5,00	4,00	4,00	4,00	4,00	4,00

7. diagram

Felhasználói internetes szolgáltatások kimaradásának, leállásának átlagos hatása szervezetenként; forrás: szerző

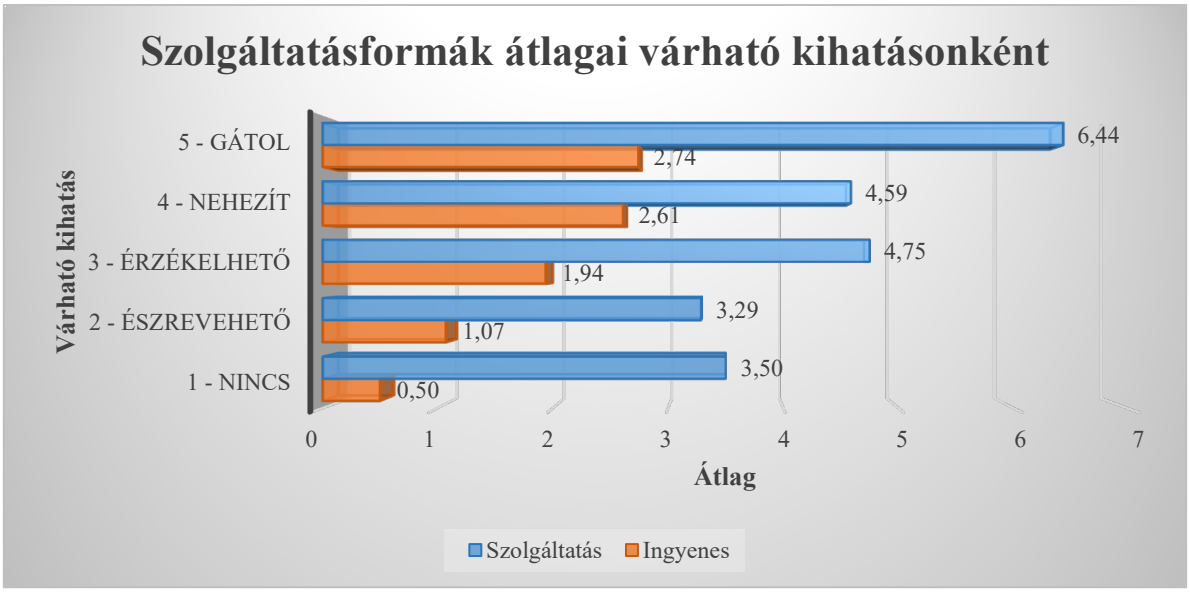
A választ az 1-5-ig terjedő skála valamely értékének kiválasztásával lehetett megadni, amelyből csak az egyik volt kijelölhető. Az értékek növelése a bekövetkező hatás növekedését jelentették. A mező kitöltése nem volt kötelező, ennek ellenére **98,6 %**-ban érkeztek válaszok a kérdésre. Az 6. diagramon látható, hogy a felhasználóknak mindösszesen **4%**-a gondolja úgy, hogy az igénybe vett internetes szolgáltatások kimaradásának, leállásának nincs hatása, ugyanakkor a válaszadók **43%**-a úgy nyilatkozott, hogy gátolná a munkavégzést.

A 7. diagramon feltüntetett szervezetenkénti átlag mutatja, hogy a mindösszesen **4,00** átlagnál csak a Magyar Honvédség válaszadói adtak alacsonyabb, 3,75-os értékeket. A válaszadók véleményének közép-, azaz medián értéke egyetlen esetben sem kevesebb **4,00**-nál, így összességében megállapítható, hogy az internetes szolgáltatások hiánya átlagosan nehezíti a munkavégzést.
A felhasználói csoportokra vonatkoztatott 8. diagram szerinti átlagok azt mutatják, hogy leginkább a vezető beosztású, nem informatikus végzettségű dolgozók érzik úgy, hogy munkájukat gátolná az internetes szolgáltatások kiesése.



8. diagram
Felhasználói internetes szolgáltatások kimaradásának, leállásának átlagos hatása felhasználó típusonként; forrás: szerző

Az internetes szolgáltatások kimaradásának lehetséges hatásaiból következtetni lehet azok kritikussági faktorára, besorolására, hisz a definíció szerint akkor kritikus egy szolgáltatás, ha a meghibásodás, kiesés, vagy megsemmisítés súlyos hatást gyakorolhat a működésre. A nyilatkozatot adó felhasználók hatásra vonatkozó információi a kritikusság szempontjából akkor tekinthetők mérvadónak és objektívnek, ha azt a felmérés többi kérdése érdemben nem befolyásolta.



9. diagram

Igénybe vett felhasználói internetes szolgáltatások átlaga várható hatásonként; forrás: szerző

Az objektivitás leellenőrzése érdekében, a várható hatásokhoz rendelve összesítésre kerültek az igénybe vett szolgáltatások minimumokból és maximumokból származtatott átlagai a 9. diagramon feltüntetett eredmény szerint.

A lehetséges kihatások számszaki 1-5-ig terjedő jelölése szövegszerűen is definiálásra került.

Megállapítható, hogy a lehetséges kihatások minden tartományában 3,29 - 6,44 az igénybe vett internetes szolgáltatások átlaga, amely bizonyítja, hogy a felhasználók internetes szolgáltatás igénybevétele és a kimaradás várható hatása nincs egymással közvetlen összefüggésben.

Érdekesség, hogy két esetben a várható hatás növekedésekor csökken az átlagos szolgáltatás-használat értéke, amely szintét bizonyítja, hogy a szolgáltatásszám és a kiesés hatása nincs közvetlen összefüggésben.

Összegezve a védelmi szféra felhasználóinak igénybe vett internetes szolgáltatásait megállapítható, hogy a felmérés szerint 32%-nak megnehezíti, 43%-nak gátolja a munkavégzését, ha azok nem állnak rendelkezésre, így összesen a dolgozók **75%-a Kritikus Internetes Szolgáltatást használ.**

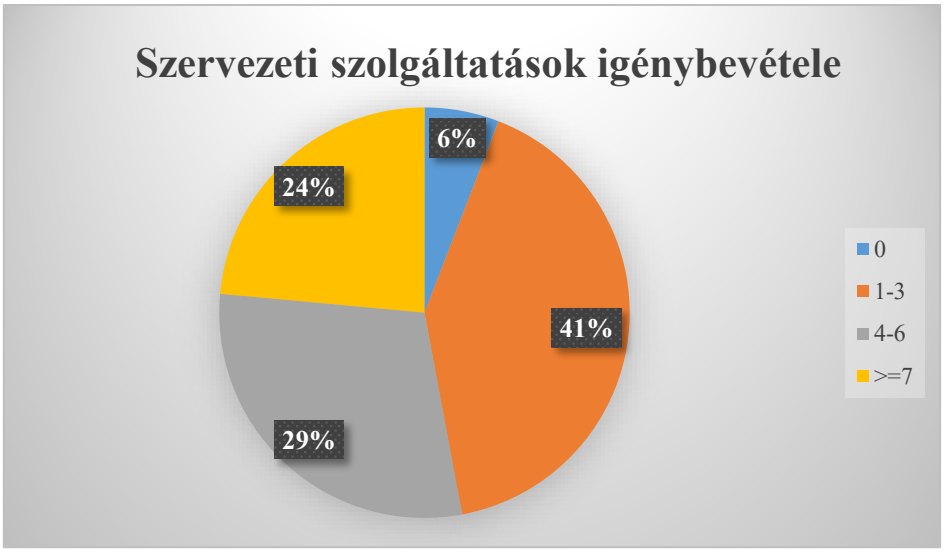
2. A szervezetek által használt internetes szolgáltatások

A feltételezés szerint, a szervezetek informatikai rendszerének hardver és szoftver elemei, működésük során igénybe vesznek olyan internetes szolgáltatásokat, amelyek nélkül nem lennének képesek teljes mértékben hiteles információkkal ellátni a döntéshozókat és a

felhasználók munkáját csak csökkentett mértékben támogatnák. Külön nem került meghatározásra magyarázatként, hogy mit jelent a szervezet által használt internetes szolgáltatás, továbbá, hogy mi a különbség a felhasználói és a szervezeti használat között. Felmerülhet a kérdés, hogy mi az, amit a normál felhasználó nem alkalmaz, de a szervezet igen? Természetesen azok a szervezetek informatikai rendszereibe telepített alkalmazások, amelyek az eseti, vagy folyamatos működésük során programozottan, külön felhasználói beavatkozás nélkül kapcsolódnak valamely internetes szolgáltatáshoz. Ebből a logikából származtatódik majd annak a vizsgálata, hogy a kapcsolatnak a meghiúsulása, vagy rendellenes működése milyen hatással van a szervezet működésére?
Ezekre a kérdésekre tipikusan az informatikai végzettséggel, vagy hozzáértéssel rendelkező felhasználók tudják a pontosabb választ, sőt egyes esetekben csak az informatikai rendszereket mélyebben ismerőknek lehetnek pontos ismereteik. A kiértékelésnél ezt a tényt minden esetben figyelembe kellett venni, ezért tipikusan az informatikusok válaszai számítottak mérvadónak.

A témakör vizsgálatához az alábbi kérdések kerültek megfogalmazásra:
„Mennyi a – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások (pld. google térkép) száma?”
„A – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül, mennyi a **folyamatosan** igénybe vett szolgáltatások száma?”
„A – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül, mennyi az **ingyenes** szolgáltatások száma?”
„Megítélése szerint, a – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások kimaradása, vagy leállása, milyen hatást vált ki szerve működésére?”

a) „Mennyi a – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások (pld. google térkép) száma?”



10. diagram

Az informatikusok véleménye a szervezetek által igénybe vett szolgáltatások megoszlásáról; forrás: szerző

Kötelezően kitöltendő mezőként került definiálásra, a $\underline{0} < \underline{1–3} < \underline{4–6} < \underline{7–\infty}$ képlettel leírható válasz, amelyben a megadott intervallumok szerint, négy lehetséges opció közül csak egyet választhatott a kitöltő. A 10. diagramon látható a témához hozzáértő informatikusok véleménye, amely szerint a 0 érték csak az esetek 6 százalékában fordult elő, a szervezetek által igénybe vett szolgáltatások módusza, azaz a legtöbbet kiválasztott érték pedig 1-3.

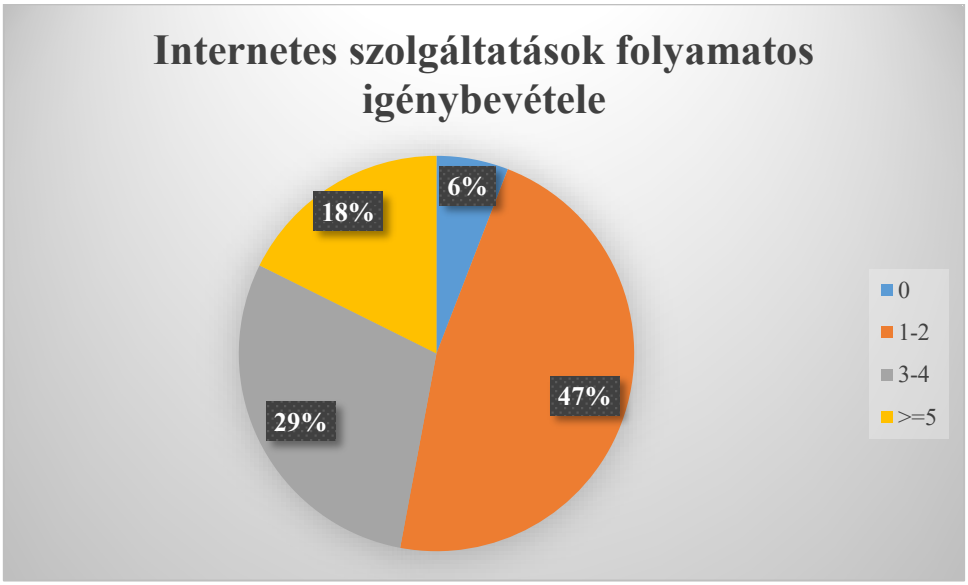
Átlag	Minimum	Maximum
Átlag	3,24	5,35
Medián	4,00	6,00

4. táblázat

Szervezeti internetes szolgáltatások igénybevételének átlagai az informatikusok véleménye szerint; forrás: szerző

A 4. táblázat adatai azt mutatják, hogy a megkérdezett informatikusok véleménye szerint a védelmi szférában a szervezetek által igénybe vett internetes szolgáltatások minimum átlaga 3,24, maximuma 5,35.

*b) „A – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül, mennyi a **folyamatosan** igénybe vett szolgáltatások száma?”*
Lényeges kérdés, mert a folyamatosság jelzéssel bír arra vonatkozóan, hogy a rendvédelmi szervezet-, vagy szerv részéről alakul-e ki kötődés valamely internetes szolgáltatás iránt, amelynek állandó elérhetősége, rendelkezésre állása és igénybevétele meghatározó.



11. diagram
Az informatikusok véleménye alapján, a szervezetek által folyamatosan igénybe vett internetes szolgáltatások megoszlása; forrás: szerző

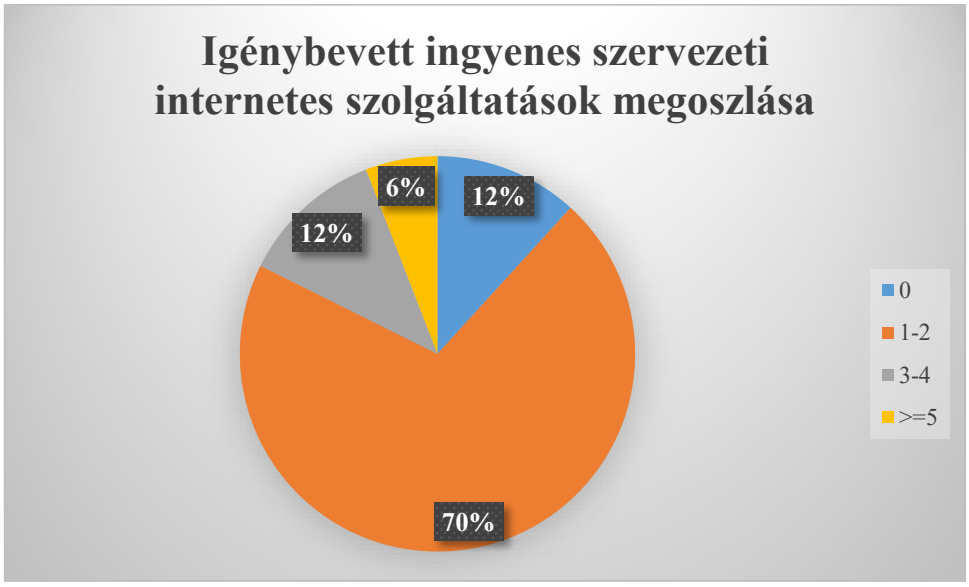
A 11. diagramon látható, hogy a védelmi szférában dolgozó informatikusok **47%**-a szerint adott rendvédelmi szerv **1-2** internetes szolgáltatást folyamatosan igénybe vesz, és csak 6% mondja azt, hogy egyet sem. A kérdésre – annak ellenére, hogy nem volt kötelező a kitöltése, – minden informatikus adott választ. Az 5. táblázat adatai mutatják az informatikusok véleménye szerinti átlag folyamatosan igénybe vett internetesen szolgáltatások minimum és maximum értékeit.

Átlag	Minimum	Maximum
Átlag	2,24	3,35
Medián	1,00	2,00

5. táblázat
Szervezeti internetes szolgáltatások folyamatos igénybevételének átlagai az informatikusok véleménye szerint; forrás: szerző

*c) „A – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül, mennyi az **ingyenes** szolgáltatások száma?”*

Önkéntességen alapuló kérdés volt, ennek ellenére szinte minden kitöltőtől érkezett válasz.



12. diagram

A szervezetek által igénybe vett ingyenes internetes szolgáltatások megoszlása az informatikusok véleménye alapján; forrás: szerző

A 12. diagramon látható, hogy a megkérdezett informatikusoknak 12%-a úgy gondolja, hogy rendvédelmi szerve nem használ-, ugyanakkor **70%**-a azt vallja, hogy használ 1-2 ingyenes internetes szolgáltatást. Ez az adat mindenképpen azt jelzi, hogy a védelmi szféra is komolyan támaszkodik az ingyenes internetes szolgáltatásokra, sőt a válaszadók 6%-a szerint öt, vagy több az igénybevételek száma.

Átlag	Minimum	Maximum
Átlag	1,35	2,29
Medián	1,00	2,00

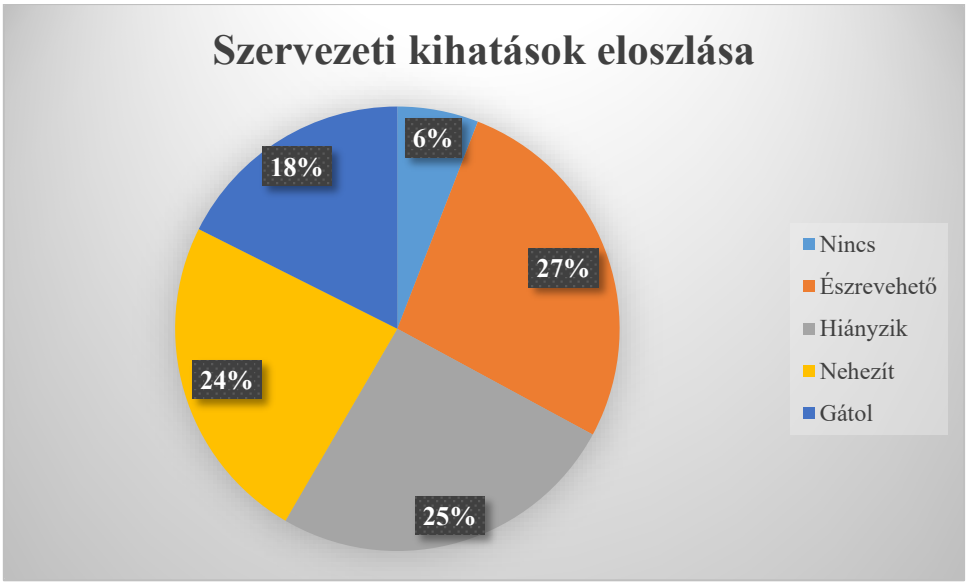
6. táblázat

Ingyenes szervezeti internetes szolgáltatások átlagai az informatikusok véleménye szerint; forrás: szerző

A 6. táblázat adatai mutatják a rendvédelmi szervek által ingyenesen igénybe vett internetes szolgáltatások minimum és maximum átlagait az informatikusok véleménye alapján.

d) „Megítélése szerint, a – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások kimaradása, vagy leállása, milyen hatást vált ki szerve működésére?”

„nincs kihatással 1 2 3 4 5 gátolja a munkavégzést”



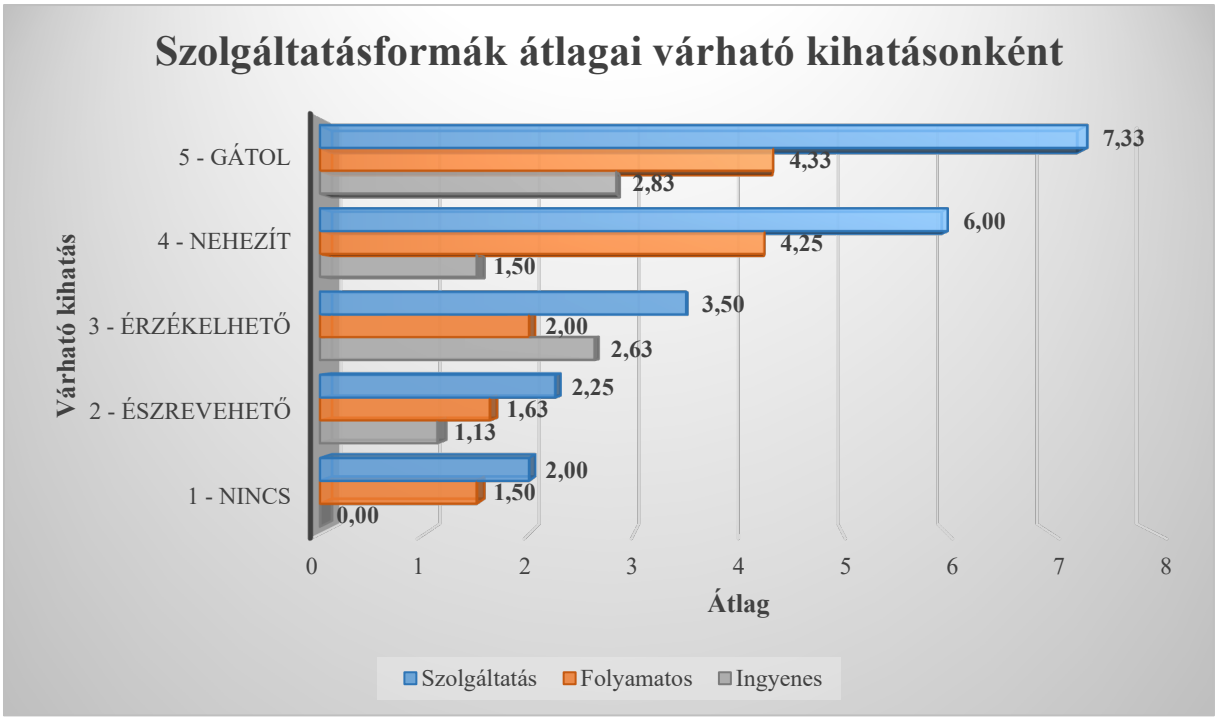
13. diagram

Igénybe vett szervezeti internetes szolgáltatások kimaradásának, leállásának hatásai; forrás: szerző

A rendvédelmi szervek által igénybe vett internetes szolgáltatások kimaradásának, vagy leállásának hatásait méri a kérdőív ezen pontja, amelynek célja, hogy a szolgáltatások kritikussága vizsgálhatóvá váljon.

A választ itt is 1-5-ig terjedő skála valamely értékének kiválasztásával lehetett megadni, amelyből csak az egyik volt kijelölhető. A számok emelkedése a bekövetkező hatás növekedését jelentették.

A 13. diagramon látható, hogy az informatikusoknak mindösszesen **6%**-a gondolja úgy, hogy az igénybe vett internetes szolgáltatások kimaradásának, leállásának nincs hatása, ugyanakkor **18%**-a nyilatkozott, hogy az gátolná a munkavégzést. Az összegzett értékek alapján a várható kihatás **átlaga 3.25**, mediánja 3.00, tehát a vélemények alapján az internetes szolgáltatások kimaradása, leállása átlagosan a „Hiányzik - Nehezíti a munkavégzést” kategóriákba sorolható.



14. diagram

Igénybe vett szervezeti internetes szolgáltatások átlagai várható kihatásonként; forrás: szerző

A 14. diagramon a várható kihatásokhoz hozzárendelve az igénybe vett internetes szolgáltatások-, a folyamatosan igénybe vett szolgáltatások-, valamint az ingyenesen igénybe vett szolgáltatások átlagai kerültek megjelenítésre. Megállapítható, hogy az informatikusok véleménye szerint

- a szolgáltatások számának emelkedésével együtt nő a leállással-, kieséssel együtt járó hatás is;
- minden hatás-kategóriában van igénybe vett internetes szolgáltatás, amelynek legalacsonyabb értéke is kettő;
- az igénybe vett szolgáltatásokhoz képest minden kategóriában kevesebb a folyamatosság és az ingyenesség;
- az ingyenes szolgáltatások átlaga egyetlen esetben haladja meg a folyamatos szolgáltatások átlagát;
- kettő sávban a „Folyamatos” és az „Ingyenes” értékek összege meghaladja, három sávban megközelíti a „Szolgáltatás” értékét, amelyből következtethető, hogy a védelmi szféra a működéséhez folyamatosan használ ingyenes internetes szolgáltatásokat.

Összegezve a rendvédelmi szervek igénybe vett internetes szolgáltatásait – az informatikusok véleménye alapján – megállapítható, hogy

- 24%-ban megnehezíti, 18%-ban gátolja a munkavégzését, ha azok nem állnak rendelkezésre, így azok összesen **42%-ban Kritikus Internetes Szolgáltatásnak minősülnek;**
- a kritikusnak minősülő internetes szolgáltatások **65%-át folyamatosan-**, **32%-át ingyen** veszik igénybe.

A védelmi szféra által nyújtott internetes szolgáltatások

A felmérés ezen része a védelmi szféra által nyújtott szolgáltatásokat vizsgálja, kitérve azokra a fontos részletekre, hogy azoknak kik az igénybe vevői, a szolgáltatás feltételhez kötött-e, a szolgáltatás nyújtás mennyire alapul kötelezettségen, valamint a szolgáltatás leállásának milyen kihatása lehet. A vizsgálat feltételezte, hogy internetes szolgáltatást csak és kizárólag a rendvédelmi szerv-, vagy szervezet nyújthat, figyelmen kívül hagyva azt a rendellenes jelenséget, hogy valamely felhasználó az általa használt munkaállomásra olyan programot telepít, amely adott esetben szolgáltatásként is képes működni. A témakör hitelesebb kiértékeléséhez az informatikus-, vagy vezető beosztású dolgozók válaszai kerültek feldolgozásra, figyelembe véve, hogy a normál felhasználóknak ebben a témában várhatóan nincs kellő ismeretük.

A témában az alábbi kérdések kerültek megfogalmazásra:

„Mennyi a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások (pld. honlap) száma?”

„A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatásoknak kik az igénybe vevői?”

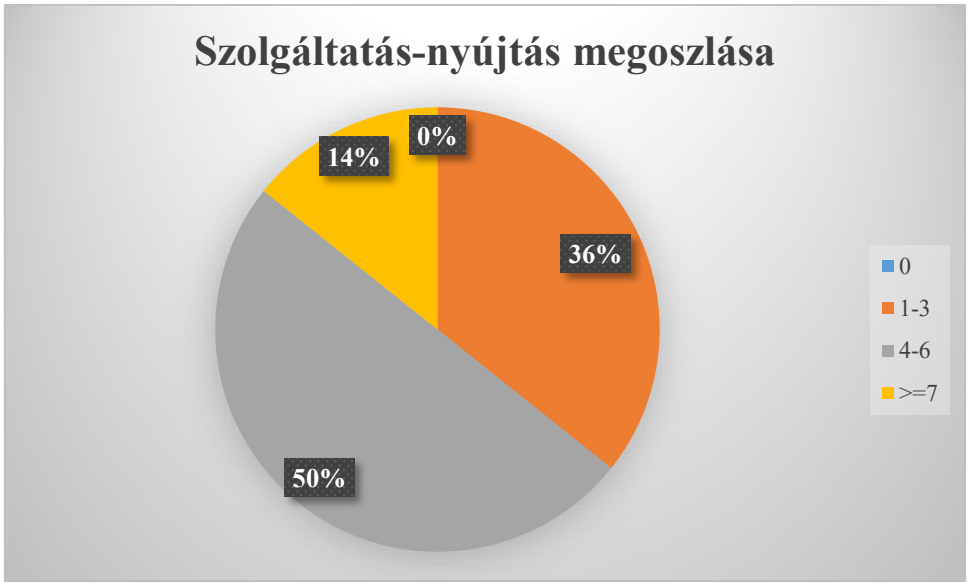
„A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül, mennyi a feltételhez – például bejelentkezéshez – kötött szolgáltatások száma?”

„A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül, mennyi a jogszabályi vagy egyéb kötelezettség miatt fenntartott szolgáltatások száma?”

„Megítélése szerint, a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások kimaradása, vagy leállása milyen hatást vált ki?”

a) „Mennyi a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások (pld. honlap) száma?”

Kötelezően kitöltendő mezőként került definiálásra, a korábban már alkalmazott 0 < 1–3 < 4–6 < 7–∞ képlet szerinti egyik válaszadás lehetőségével.



15. diagram

Az informatikusok és a vezetők véleménye a szervezetek által nyújtott szolgáltatások megoszlásáról; forrás: szerző

Átlag	Minimum	Maximum
Átlag	3,36	5,50
Medián	4,00	6,00

7. táblázat

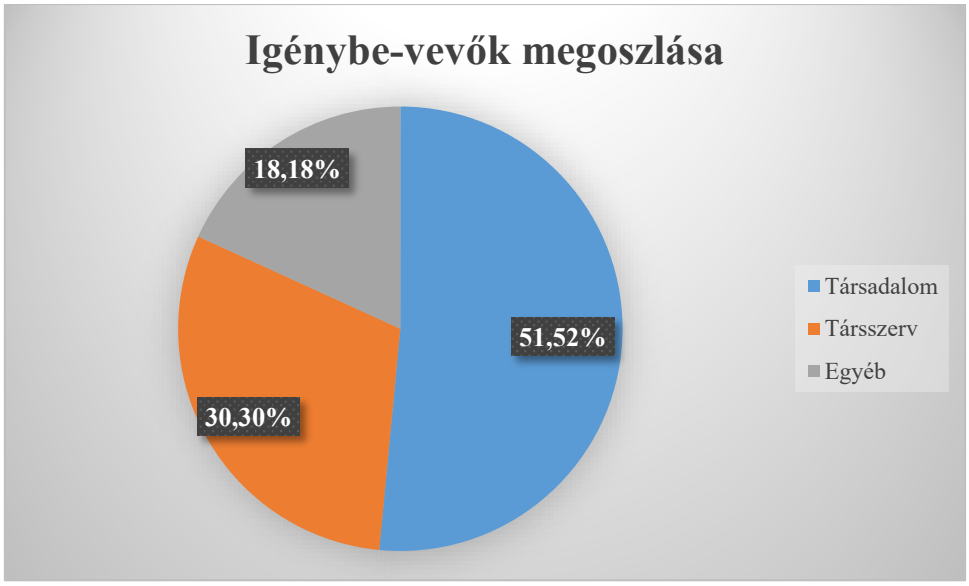
Szervezetek által nyújtott internetes szolgáltatások átlagai; forrás: szerző

A 15. diagramon látható, hogy az informatikusok és a vezető beosztásúak véleménye, miszerint nulla értéket senki sem jelölt be, a legtöbben, azaz a válaszadók fele úgy gondolja, hogy rendvédelmi szerve 4 – 6 internetes szolgáltatást nyújt. A 7. táblázat adatai alapján, az informatikusok és a vezetők véleménye szerint a védelmi szférai szervezetek által nyújtott internetes szolgáltatások minimum átlaga 3,36, maximum átlaga 5,50.

b)„A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatásoknak kik az igénybe vevői?”

Önkéntes kitöltésen alapuló kérdésként került definiálásra, a válaszadó a három lehetséges – „Társadalom”, „Társszerv”, „Egyéb” – mező közül tetszőlegesen, akár többet is választhatott.

A kérdés – amelyre minden releváns kitöltő választ adott, – azt a célt szolgálta, hogy megállapítható legyen, hogy a védelmi szféra által nyújtott internetes szolgáltatásoknak kik a legfőbb igénybe vevői. A 16. diagramon látható, hogy a védelmi szféra elsősorban a társadalmat, majd a társszerveket, végül az egyéb kategóriába tartozó igénybe vevőket szolgálja ki.



16. diagram

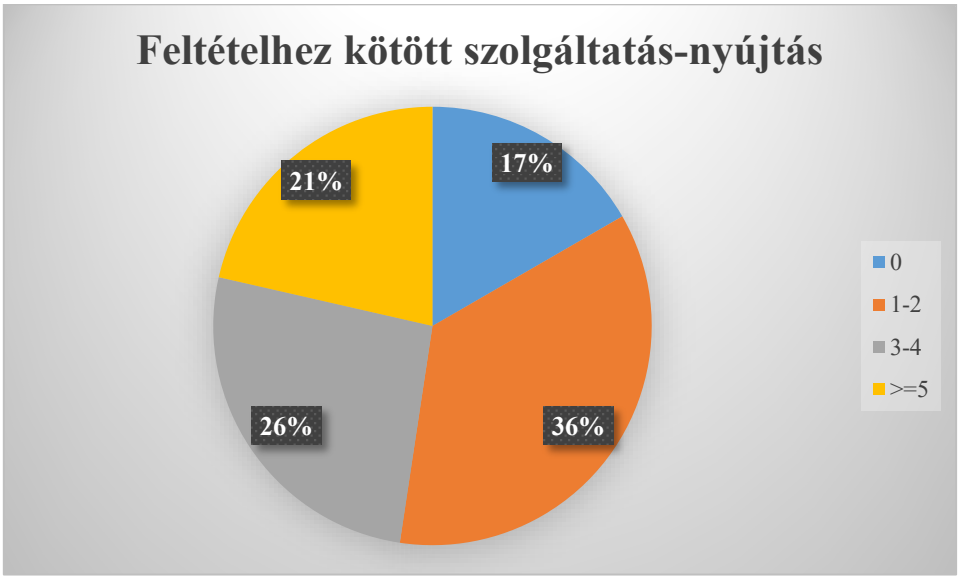
A védelmi szféra által nyújtott internetes szolgáltatások igénybe-vevőinek megoszlása; forrás: szerző

A lehetséges válaszok azért ezen kategóriák szerint kerültek meghatározásra, mert a KRISZ definíciója szerint egy internetes szolgáltatás akkor számít kritikusnak, ha annak kimaradása, vagy leállása kihatással van a társadalomra, vagy a kormányzat működésére. E kérdésre adott válaszok összesítése önmagában csak az igénybe vevők megoszlását mutatja, amelyből azonban már az alábbi következtetések levonhatók:

- amennyiben a társszervek részére nyújtott internetes szolgáltatások a társszervek működését befolyásolják, úgy azok kritikusak;
- amennyiben a társadalom felé nyújtott internetes szolgáltatások kellően nagy kihatással vannak az állampolgárok gazdasági, vagy szociális jólétére, úgy azok kritikusak; e pontban az látszik, hogy a védelmi szféra által nyújtott internetes szolgáltatások legnagyobb felhasználója a társadalom;
- az egyéb kategóriába mindenki más beletartozik, amely esetben kevésbé valószínű a kritikusság, ugyanakkor nem zárható ki.

c) „A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül, mennyi a feltételhez – például bejelentkezéshez – kötött szolgáltatások száma?”

Önkéntes kitöltésen alapuló, egy választásos kérdés volt, ennek ellenére minden releváns válaszadótól érkezett értékelhető válasz a következő képlet alapján: $0 < 1–2 < 3–4 < 5–\infty$. A kérdés feldolgozása arra a lényeges körülményre adott választ, hogy a szolgáltatásnyújtás mekkora részben terjed ki nyilvános-, és mekkora részben zárt adatokra.



17. diagram

A védelmi szféra által nyújtott internetes szolgáltatások feltételhez kötöttségének megoszlása; forrás: szerző

Elkerülhetetlen, hogy kormányzati szinten egymásnak szolgáltassanak – akár érzékeny – adatokat különböző szervezetek, amelynek egyik legkézenfekvőbb módja az internet biztosította kapcsolat, ugyanakkor ezeket az információkat feltételhez kötötten kell átadni. Természetesen a társadalom szereplőinek is nyújthat a védelmi szféra feltételhez kötötten információkat, az érintettnek ebben az esetben is interneten keresztül azonosítania kell magát. A feltételhez kötöttség és a szolgáltatás kritikussága között összefüggés van, figyelembe véve, hogy az igénybe vevőnek az információra szüksége van, amely működését, vagy élethelyzetét befolyásolhatja. A 17. diagramon látható a feltételhez kötöttség eloszlása, amelyen látszik, hogy csak 17%-ban feltétel nélküli a szolgáltatás-nyújtás.

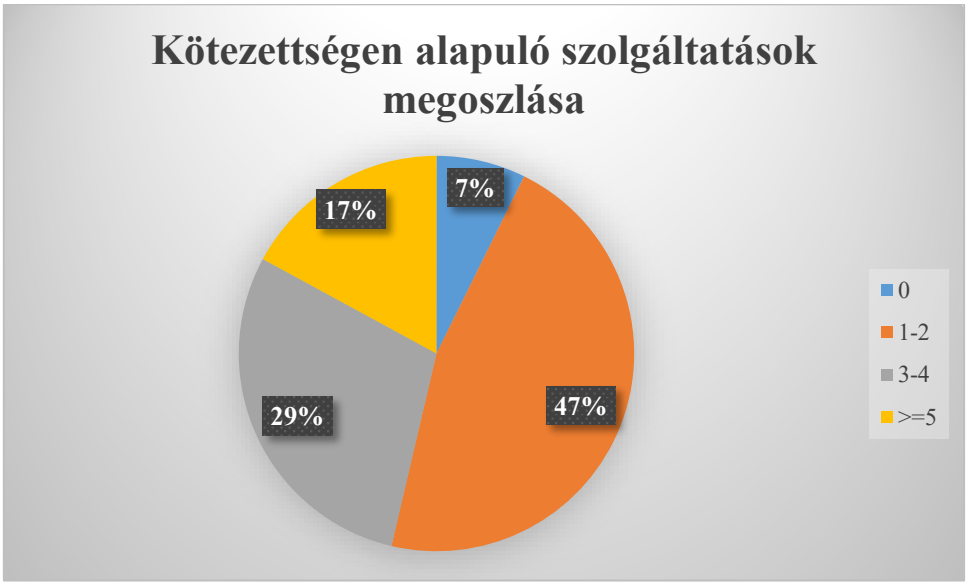
Átlag	Minimum	Maximum
Átlag	2,21	3,26
Medián	1,00	2,00

8. táblázat

Szervezetek által nyújtott feltételhez kötött internetes szolgáltatások átlagai; forrás: szerző

d) „A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül, mennyi a jogszabályi vagy egyéb kötelezettség miatt fenntartott szolgáltatások száma?”

Ennek a kérdésnek a kitöltése is önkéntességen alapult, egy lehetséges válasszal a korábbi 0 < 1–2 < 3–4 < 5–∞ képlet alapján, ennek ellenére néhány kivételtől eltekintve a releváns kitöltőktől érkezett értékelhető válasz.



18. diagram

A védelmi szféra által nyújtott, kötelezettségen alapuló internetes szolgáltatások megoszlása; forrás: szerző

A kérdés választ ad arra a szintén lényeges körülményre, hogy a szolgáltatásnyújtás mekkora részben alapul kötelezettségen, amely nyilvánvalóan kihatással van a szolgáltatást igénybe vevőkre is, akik egyébként szintén lehetnek kötelezettek a felhasználásra, így joggal feltételezik, hogy az a bizonyos szolgáltatás biztosan rendelkezésre áll. A felmérésből nem derül ki, hogy a kötelezettség honnét származik, természetesen az a legmagasabb – törvényi – szinttől egészen az adott szerv határköréig bárhol keletkezhet.

Átlag	Minimum	Maximum
Átlag	2,20	3,29
Medián	1,00	2,00

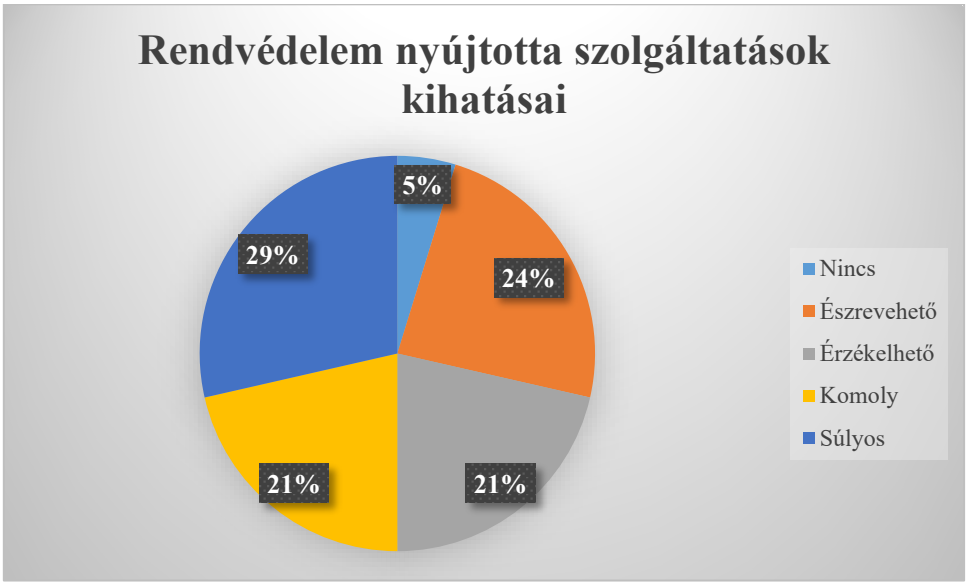
9. táblázat

Szervezetek által nyújtott, kötelezettségen alapuló internetes szolgáltatások átlagai; forrás: szerző

A 18. diagramon látható, hogy az internetes szolgáltatások nyújtása többnyire kötelezettségen alapul, a válaszadók szerint csupán 7%-ban önkéntes azok üzemeltetése.

e) „Megítélése szerint, a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások kimaradása, vagy leállása milyen hatást vált ki?

„nincs kihatással 1 2 3 4 5 súlyos kihatása van”



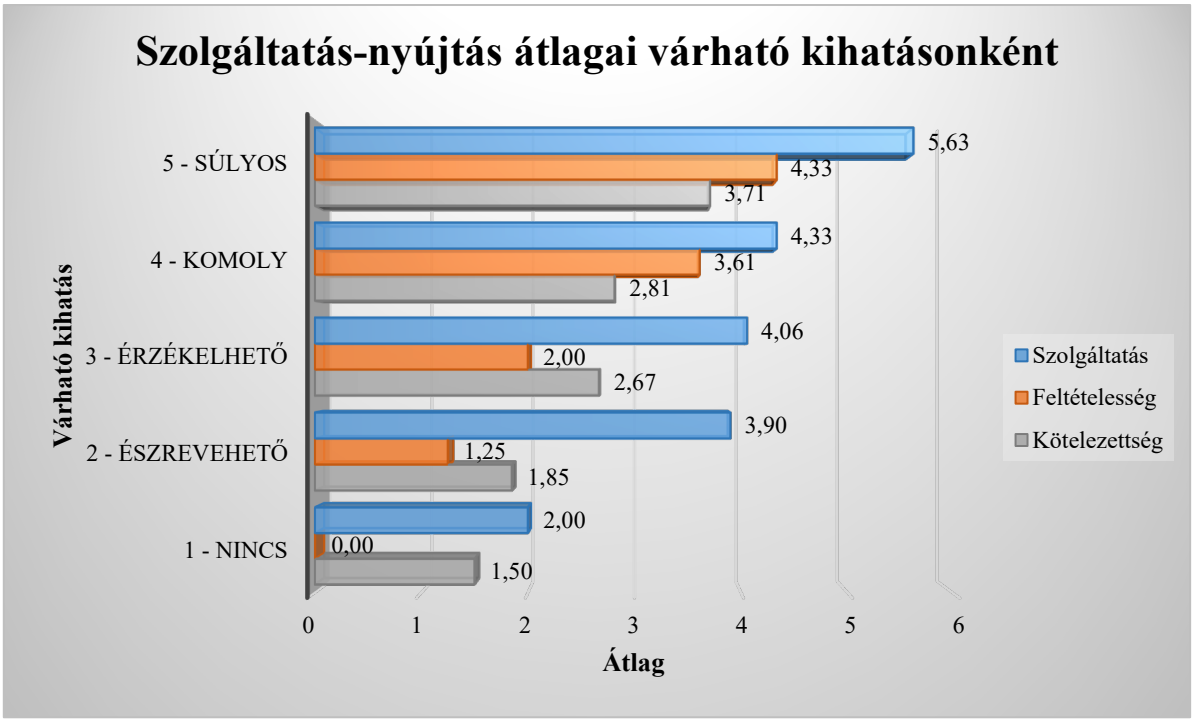
19. diagram

A védelmi szféra által nyújtott internetes szolgáltatások kimaradásának, leállásának hatásai; forrás: szerző

A védelmi szféra nyújtotta internetes szolgáltatások kimaradásának, leállásának hatásait vizsgálja a kérdőív e pontja. A választ 1-5-ig terjedő skálán egyszeri kijelöléssel adhatták meg a kitöltők, akik minden esetben éltek is a felelet lehetőségével.

A 20. diagram adatai alapján látható, hogy a megkérdezettek véleménye szerint

- a kimaradás, leállás várható hatásának növekedésével együtt, párhuzamosan nő a nyújtott internetes szolgáltatások száma, a feltételhez kötöttség száma és a kötelezettségből származó szolgáltatás szám is;
- a várható hatás alsó-, 1-3-ig terjedő tartományaiban, azaz a kevésbé kritikus szolgáltatások között, a kötelezettség száma megelőzi a feltételhez kötöttség számát;
- átlagosan legalább 2,00 a szolgáltatás átlag a várható hatás minden tartományában, továbbá az eloszlás exponenciális, így a kapott eredmény objektívnek tekinthető.



20. diagram

Rendvédelmi internetes szolgáltatás-nyújtás átlagai várható kihatásonként; forrás: szerző

Összegezve a rendvédelmi szervek által nyújtott internetes szolgáltatásokat – a vezetők és az informatikusok véleménye alapján – megállapítható, hogy 29%-ban súlyos, 21%-ban komoly kihatása van, ha nem állnak rendelkezésre a nyújtott internetes szolgáltatások, így azok összesen **50%-ban Kritikus Internetes Szolgáltatásnak minősülnek;**

Alkalmazott internetes szolgáltatások a védelmi szférában

A felmérés 7., 12., és 18. pontjai szabad szöveggel kitölthető mezők voltak, amelyekben az adott fejezet kérdéseivel összhangban írhattak be a válaszadók internetes szolgáltatásokat. A szabad mezők feldolgozása a beírt szövegek értelmezését és esetleges hibajavítását követően táblázatos formában történt, szolgáltatáscsoportok képzésével és a csoportokon belüli szolgáltatás típusok összegzésével, amely így számszakilag értelmezhető formába hozva, lehetőséget adott az eredmények értékelésére.

1. Igénybe vett internetes szolgáltatások szöveges értékelése

„7. Nevezzen meg néhányat, az Ön munkájához használt, internetes informatikai szolgáltatások közül.”

„12. Nevezzen meg néhányat a – rendvédelmi – szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül.”

Mind a felhasználói-, mind a szervezetek vonatkozásában szövegesen is megkérdezésre kerültek az igénybe vett szolgáltatások, ezért a két kérdés összesítve került feldolgozásra. Nem volt kötelező kitölteni ezt a pontot és a „néhány” fogalma sem került előzetesen definiálásra, csupán sugallva volt a felsorolás lehetősége.

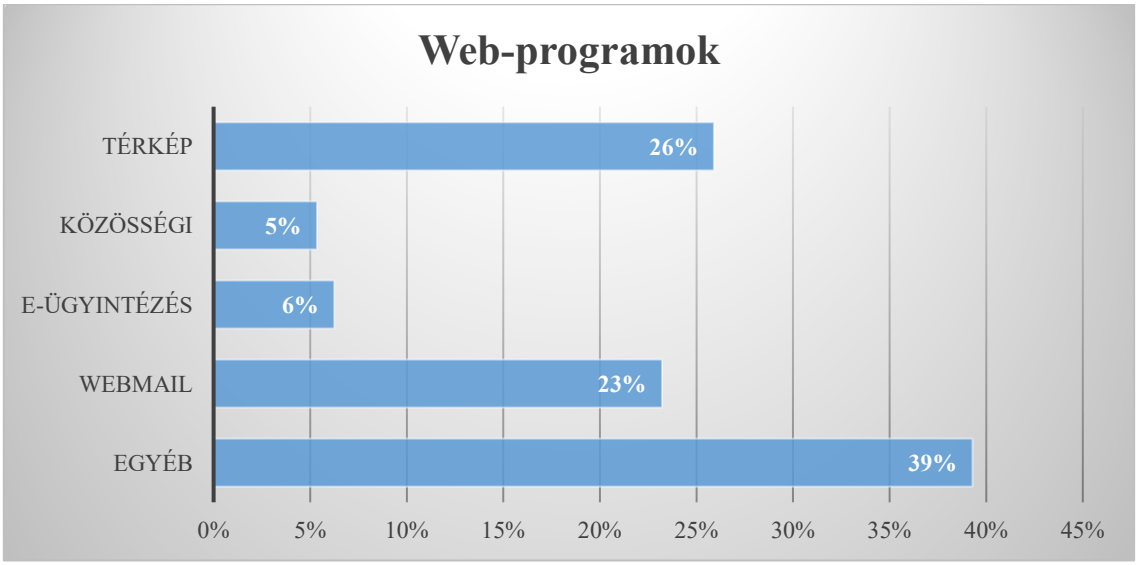
A válaszok alapján az igénybevételek két nagyobb területre oszthatók, egyrészt a böngésző alapú Web-programokra, másrészt az önállóan futtatható Net-programokra.

	Web-programok	Net-programok
Megoszlás	58%	42%

10. táblázat

A szolgáltatásokat igénybe vevő alkalmazások megoszlása; forrás: szerző

Az alkalmazás szerinti megoszlást mutatja a 10. táblázat, miszerint többségben valamelyik internet böngészővel, web-en veszik igénybe az internetes szolgáltatásokat a felhasználók.



21. diagram

Web-es szolgáltatások megoszlása; forrás: szerző

A 21. diagramon látható, hogy a böngészővel igénybe vett szolgáltatások Térkép, Közösségi oldalak, E-ügyintézés és Webmail fő kategóriákra oszthatók, és minden más az Egyéb kategóriába tartozik. Volt, aki – egyébként jogosan – külön megjelölte igénybe vett szolgáltatásként a különböző keresőket is, ugyanakkor figyelembe véve, hogy Web-es keresőt mindenki használ, az eredménybe nem került beszámításra.

Figyelemre méltó, hogy az Egyéb kategórián kívül a Web alapú térkép a leginkább igénybe vett szolgáltatás, továbbá kevésbé váratlanul a Webmail, ami nyilvánvalóan munkavégzéssel függ össze; a közösségi oldalakat mindösszesen biztosan többen veszik igénybe, így a feltüntetett érték valószínűleg a munkával összefüggő közösségi oldal használatot mutatja, az E-ügyintézés pedig az adminisztrációs tevékenységet tükrözi. Az Egyéb kategóriába a teljesség igénye nélkül különböző felhő szolgáltatások, hírportálok, jogszabály nyilvántartások, oktatást elősegítő portálok, vagy éppen aktuális repülőgép helyzetjelentő portál egyaránt bekerült.

2. Internetes szolgáltatás-nyújtás szöveges értékelése

„18. Nevezzen meg néhányat a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül."

Szintén nem volt kötelezően kitöltendő mező. A szervezetek, szervek eltérő számából adódóan értelmetlen lenne összehasonlítani, hogy ki, mennyi szolgáltatást tart fenn, ezért itt általános kategóriák kerülnek felsorolásra:

- Web alapú szolgáltatások
    - Általános információs Weblap, tájékoztatók;
    - Szervezet specifikus;
        - hírfolyam, folyamatos tájékoztatás
        - elektronikus ügyintézés
    - Webmail.
- Nem web alapú szolgáltatás
    - VPN;
    - Mail;
    - Applikáció.

A kitöltések alapján a szervezetek rendelkeznek

- saját tájékoztatási – statikus, vagy ritkán változó adatokat tartalmazó – honlappal, amelyen kapcsolattartási adatok, hasznos-, és kötelező információk kerülnek megjelenítésre;
- szervezeti levelezéshez kapcsolódó webmail elérhetőséggel;
- virtuális magánhálózati kapcsolódási ponttal, amely a szükséges hozzáférések és jogosultságok rendelkezésre állása esetén lehetőséget ad távolról, interneten keresztül a rendvédelmi szerv informatikai rendszerének használatára.

A többi, kategorizált szolgáltatás szervezetfüggő.

1.2.2. Nevesített internetes oldalak a védelmi szférában, a kérdőív alapján

Szervezetekre jellemző internetes oldalak

1. Büntetés-végrehajtás

- Szervezeti weboldal[17];
- Közösségi oldalak[18] [19];
- Internetes felületen keresztül történő csomagküldés fogvatartottak részére[20].

2. Katasztrófavédelem

- Szervezeti weboldal[21];
- Közösségi oldalak[22] [23].

3. Magyar Honvédség

- Szervezeti weboldal[24];
- Közösségi oldalak[25] [26] [27].

4. Nemzeti adó-, és vámhivatal

- Szervezeti weboldal[28];
- Közösségi oldal[29].

5. Rendőrség

- Szervezeti weboldal, Rendőrségi tájékoztató rendszer[30];

---

[17] https://bv.gov.hu/ [17]

[18] https://www.youtube.com/channel/UCfF6gYhUC1JiP9AUS9NMRKA[19]

[19] https://www.instagram.com/hungarianprison/ [18]

[20] https://www.bvcsomag.hu/auth [20]

[21] https://www.katasztrofavedelem.hu/ [21]

[22] https://www.facebook.com/bmokf.hivatalos/ [22]

[23] https://www.instagram.com/katasztrofavedelem_hivatalos/ [23]

[24] https://honvedelem.hu/ [24]

[25] https://www.facebook.com/honvedelem.hu [25]

[26] https://www.instagram.com/magyarhonvedseg/?hl=hu [26]

[27] https://www.youtube.com/channel/UCNVkvmkt_D6_XfE2bQOEkpQ [27]

[28] https://www.nav.gov.hu/ [28]

[29] https://www.facebook.com/NAVprofil [29]

[30] http://police.hu [30]

- RUTIN rendőrségi tájékoztató applikáció[31];
- Elektronikus ügyintézés – inNOVA Portál[32];
- Közösségi oldalak[33] [34] [35].

6. Terrorelhárítási Központ

- Szervezeti weboldal[36];

Általánosan használt internetes szolgáltatások

1. Elektronikus ügyintézés

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvényben foglaltaknak megfelelően. Az alábbi weboldalakon elektronikus JAVA alapú űrlapkitöltőkhöz érhetők el, amelyeket a Központi Azonosítási Ügynök, mint azonosítási portál segítségével lehet eljuttatni az adott szervezethez.

- Büntetés-végrehajtás[37];
- Katasztrófavédelem[38];
- Magyar Honvédség[39];
- NAV[40];
- TEK[41].

2. Elektronikus levelezés

„A centralizált szervezeti levelező szolgáltatás a védelmi szféra – akár teljes – személyi állománya részére internetes, azaz valós, egyénre szóló levelező postafiókot biztosíthat, lehetővé téve az arra jogosultak számára, hogy – biztonsági megoldások használata mellett – a világhálón küldjenek, vagy fogadjanak elektronikus leveleket, csatolmányokat.” [1] Minden

[31] http://www.police.hu/hu/hirek-es-informaciok/utinfo/rutin [31]

[32] https://ugyintezes.police.hu [32]

[33] https://www.facebook.com/legyelteisrendor/ [33]

[34] https://www.youtube.com/user/PoliceHungary [34]

[35] https://twitter.com/police_HU [35]

[36] http://tek.gov.hu/ [36]

[37] https://bv.gov.hu/hu/elektronikus-ugyintezes [37]

[38] https://www.katasztrofavedelem.hu/148/elektronikus-ugyintezes [38]

[39] https://www.ket.hm.gov.hu/SitePages/Kezdolap.aspx [39]

[40] https://www.nav.gov.hu/nav/nav_online [40]

[41] http://tek.gov.hu/eugyintezes.html [41]

szervezet rendelkezik olyan, Web-en elérhető hozzáférési ponttal, amely lehetőséget ad dolgozóinak, hogy távolról interneten keresztül is elérhetővé váljanak az elektronikus küldemények.

3. Rendszer hozzáférés

Szinte megkerülhetetlen, hogy a szervezetek bizonyos felhasználói körnek olyan biztonságos internetes csatlakozási pontot nyújtsanak, amelyre belépbe és a kapcsolatot felépítve, a felhasználó távolról képes legyen a szervezete-, vagy szerve informatikai rendszerébe belépni. A belépést követően az adott személy ugyan interneten keresztül, mégis teljes értékűen képes a szolgálati helye szerinti informatikai rendszerhez kapcsolódni, mintha irodájában, számítógépe előtt ülne.

Adott szervezetekre jellemző, de nem ismert internetes szolgáltatás igénybevételek

Léteznek olyan internetes szolgáltatás igénybevételek, amelyeket a kérdőív sem adott vissza, ugyanakkor egy kis éleslátással megfigyelhetők, vagy kikövetkeztethetők. Egyetlen példaként a Katasztrófavédelem weblapján elérhető Eseménytérkép[42] jól mutatja, hogy a bekövetkezett esemény a Google internetes térképének a segítségével kerül megjelenítésre és behatárolásra, tehát adott rendvédelmi internetes szolgáltatás egy másik nyilvános internetes szolgáltatás igénybevételével történik.

[42] https://www.katasztrofavedelem.hu/modules/vesz/esemenyterkep [42]

Összegzés, következtetések

A Kritikus Internetes Szolgáltatások, a kritikus információs infrastruktúrák egyik – egyre bővülő – szegmensén megjelenő, létfontosságú kiszolgálások köre. Tanulmányomban elsők között tettem kísérletet a kritikus infrastruktúrákhoz, az információs infrastruktúrákhoz és a kritikus információs infrastruktúrákhoz kapcsolódó KRISZ definiálására. Bemutattam, hogy milyen egymásra épülő, további szolgáltatásoknak kell működniük egy internetes kiszolgálás megvalósításához és rávilágítottam, hogy milyen szubjektív szempontok alapján kerülhet egy szolgáltatás a KRISZ körébe. A hálózati kommunikációt alapjaiban meghatározó protokolloktól kiindulva, áttekintettem a jellemző szolgáltatások körét, valamint azok hétköznapi és rendvédelmi alkalmazását. Láthatóvá tettem, hogy **a KI, az II és a KII definícióiból** miként **vezethető le a KRISZ tudományos megközelítésben**, alátámasztva azt az érzést, hogy egyes internetes szolgáltatások megállása esetén szinte „megáll az élet". Érzékelhető, hogy **internetes szolgáltatások** igenis **meghatározzák a mindennapokat és Kritikus Internetes Szolgáltatások a hipotézisnek megfelelően** igenis **léteznek.**

A felmérés során beérkezett adathalmaz – köszönhetően a körültekintő előkészítésnek – megfelelő alapot adott a kiértékeléshez. Az adatelőkészítés a kutatásmódszertani ajánlásoknak megfelelően történt, amellyel a nyers adatok felkészítésre kerültek a számítógépes adatelemzésre. Ennek keretében sor került a kérdőívek egyenkénti átnézésére és ellenőrzésére, az adatok kódtáblaszerű kódolására, az adattisztításra és az esetleges ellentmondások feloldására. A körültekintő előkészítést azt is igazolta, hogy az adattisztítás minimális beavatkozást igényelt, jól feldolgozható adathalmaz állt rendelkezésre. A kérdőív stratégiai felépítése jól működött, hisz a kitöltő személyére vonatkozó információ amellett, hogy anonim volt, lehetőséget adott a feldolgozás szempontjából releváns beazonosításra és a további rendszerezésre. A szolgáltatások igénybevételét és nyújtását mutató információk külön egységekbe kerültek, amely lehetőséget adott az elhatárolt feldolgozásra. E két fő terület kiértékelésénél biztosított volt és meg is történt a kitöltők szerinti mérés és rendszerezés, a kitöltési hajlandóság mérése, a számszaki értékek statisztikai összehasonlítása és a hatáselemzés. Az SPSS program alkalmas volt a statisztikában rejlő összefüggések, valamint a szervezetek közötti különbségek bemutatására is. A programból kinyert statisztikai adatok további formázása és a diagramok készítése az Excel 2016[43] programmal történt, amelyben adatmódosításra már nem került sor. Általánosságban megállapítható, hogy a kitöltők rendkívül

[43] Microsoft ® Excel ® 2016 (16.0.5005.1000)

együttműködők voltak, a kitöltési hajlandóság a választható kérdések esetében is a maximálishoz közelített. Az eltérő véleményeket és érzéseket a statisztikai adatok jól mutatják, ami alátámasztja a véleménykülönbség lehetőségét és megjelenését, továbbá érzékelteti, hogy a kitöltők álláspontjukat szabadon, kényszer nélkül tehették meg.

A kitöltő személyek összetétele teljesen heterogén volt, normál felhasználók, vezetői beosztásban dolgozók, továbbá informatikához értő szakemberek egyaránt előfordultak. A védelmi szféra titkosszolgálati ágán kívül minden területről sikerült kitöltőket találni, amely reprezentatívabbá tette a felmérést, a legtöbben a Rendőrség állományából válaszoltak a kérdésekre. Az eredmények alapján jól látható, hogy az internet használata a rendvédelmi munkahelyeken is annyira fontos, hogy hiányát a dolgozók azonnal észreveszik, nélküle úgy érzik, hogy szinte megáll az élet. **A válaszadó felhasználók 32%-ban úgy érzik, hogy megnehezíti-, 43%-ban pedig gátolja a munkavégzést, ha az internetes szolgáltatások nem állnak rendelkezésre.** Érzékelhető, hogy **bizonyos internetes szolgáltatások „rátelepszenek" a szolgálati feladatokra, hiányukat kritikusnak élik meg a felhasználók**. Érdekes, hogy a szervek-, vagy szervezetek általi rejtett igénybevételek a vártnál kisebb mértékben kerültek felszínre, annak ellenére, hogy jelenlétük informatikai körökben nyilvánvaló. Kijelenthető, hogy egyes internetes szolgáltatások rendelkezésre állása nélkül, a rendvédelmi szervek feladataikat nem képesek maradéktalanul ellátni; **az informatikusok szerint a szervek által igénybe vett szolgáltatások 42%-a kritikusnak tekinthető**.

Látható, hogy a szervezetek a szolgáltatás nyújtással kapcsolatban a jogszabályi feladataiknak igyekeznek megfelelni, és szükség szerint saját hatáskörű vállalásokat is eszközölnek. Látszik ugyanakkor a hajlam a szolgáltatás nyújtásba integrált „helyettesítő szolgáltatás igénybevételre", vállalva a következményét az adatok, információk kiadásának és a számonkérés, felelősségre vonás ellehetetlenülésének. Az internetes szolgáltatásnyújtás elmaradása jellemzően valamilyen jogszabálysértést-, vagy jelentős hátrányt okozna akár a társadalomnak, a társ rendvédelmi szerveknek, vagy önmagának a szolgáltatást nyújtónak. **A** kérdésekre válaszoló **vezető beosztású személyek és az informatikusok véleménye szerint 29%-ban súlyos-, 21%-ban komoly kihatása van annak, ha a nyújtandó internetes szolgáltatások nem állnak rendelkezésre. A felmérés** összességében **igazolta** azt a feltételezést, **hogy** a védelmi szférában is **léteznek** és működnek **Kritikus Internetes Szolgáltatások, és** levonható az a következtetés is, hogy **egyetlen szervezet sem tudná maradéktalanul ellátni feladatait**, vagy tudna megfelelni a rá vonatkozó kötelezettségeknek **a létfontosságú internetes szolgáltatások rendelkezésre állása nélkül**.

2. FEJEZET

A Kritikus Internetes Szolgáltatások alrendszerei

A Kritikus Internetes Szolgáltatások definiálása mellett, az előzőekben meghatározásra került, hogy milyen elengedhetetlen infrastrukturális összetevők szükségesek egy interneten működő szolgáltatás üzemeltetéséhez, továbbá a hardveres és szoftveres összetevők is röviden áttekintésre kerültek. „Tekintettel arra, hogy napjainkban a KRISZ működését befolyásoló tényezők leginkább – a szándékos, vagy véletlen – adat-, program-manipulációkra vezethetők vissza, célszerű a szolgáltatások szoftver oldali, rendszerszintű vizsgálata. Az alrendszerek elemzésével célom az egymásra épülő általános funkciók feltárása, csoportosítása, a leggyakrabban előforduló, ezáltal megkerülhetetlen rendszerelemek taglalása. A rendszer egymásra utalt elemei működésének bemutatásával, a továbbiakban a KRISZ biztonsági kérdéseit szándékozom boncolgatni.

2.1 A KRISZ funkcionális összefüggései

A funkcionális összefüggések vizsgálata a KRISZ mechanizmusainak és működésének feltérképezéséhez, ezáltal az érzékeny, működést befolyásoló pontok megismeréséhez szükséges.

2.1.1 A KRISZ szoftveres környezete

Az előzőknek megfelelően, az alábbi szoftveres összetevők biztosítják a KRISZ működését:

- kiszolgáló operációs rendszere;
- szerverprogram;
- ügyfél operációs rendszere;
- ügyfél program;
- kiszolgáló/ügyfél háttér-programjai.

Érdemes feltenni a kérdést, hogy a felsoroltak közül vajon melyik összetevő sérülékenysége, vagy módosulása akadályozza, akadályozhatja a KRISZ működését? A tapasztalatok azt mutatják, hogy sajnos bármelyik, ezért a szolgáltatások –, mint önmagukban is rendszerként értelmezhető egységek, – alrendszereinek és elemeinek részletes vizsgálata adhat érdemi választ a kérdésre. Egy kritikussá minősített internetes szolgáltatás elindításánál a szélsőségekre is fel kell készülni, hisz alapcél, hogy a szolgáltatás a legnagyobb igénybevétel, illetve egy összehangolt támadás esetén egyaránt működjön. A biztonságos üzemeltetés csakis egy stabil,

ellenálló, a szélsőségekre is felkészített szoftveres környezet alkalmazásával lehetséges. Hierarchikus megközelítésben, mindkét oldal bázisát az operációs rendszerek adják (4. ábra), tehát azok sérülékenysége alapjaiban akadályozhatja meg a KRISZ működését, ugyanakkor a stabil alapprogram, még nem jelenti feltétlenül a szolgáltatás zökkenőmentes működtetését és igénybevételét.

4. ábra

Kliens-szerver elhelyezkedése; forrás: szerző

A továbbiakban feltételezem az operációs rendszerek kifogástalan, biztonságos működését, ugyanakkor le kívánom szögezni, hogy az egymásra utaltság következtében, a szolgáltatások – az alapprogramok adottságainak és környezetének kihasználása mellett, – gyengeségeiken keresztül az operációs rendszerek támadását is lehetővé teszik.

2.1.2 Rendszer-alrendszer viszonyok

A KRISZ sikeres igénybevétele minden esetben a kiszolgáló és az ügyfél együttes, összehangolt működésének eredménye. A végcél elérésében a szolgáltatás rendeltetésétől függően, ugyan eltérő a kiszolgáló és az ügyfél által befektetendő energia és munka mennyisége, azonban leszögezhető, hogy a szolgáltatás sikeres igénybevételéhez mindkét félnek részt kell vállalnia. Ezen okból kifolyólag, amennyiben bármely internetes szolgáltatást egységes rendszernek[44]

[44] A rendszer definíciójára több változat is fellelhető. Többek között BERTALANFFY, HALL - FAGEN, SZADOVSZKIJ különböző megfogalmazásokat tett közzé.
„a rendszer feladatok összességéből, a feladatok és a rájuk jellemző attribútumok kapcsolati hálójából épül fel. Az attribútumok a feladatokat jellemzik és a kapcsolat az, ami egymáshoz kötözi és eggyé teszi azokat [43]
„a rendszert alkotó halmaz elemei között meghatározott viszonyok és összefüggések jóvoltából az elemek együttese olyan összefüggő egésszé válik, amelyben minden egyes elem végső soron valamennyi többi elemmel összefügg, és tulajdonságai ennek az összefüggésnek a figyelembe vétele nélkül nem érthetők meg. A rendszer tulajdonságai viszont nem egyszerűen az alkotóelemek tulajdonságainak összegeként állnak elő, hanem az elemek közötti összefüggések és viszonyok jelenléte és specifikuma által nyernek meghatározást.” [44]

tekintünk, akkor a szerverprogram és a kliens program a rendszer alrendszerei, melyek fő funkciója a szolgáltatás rendeltetésszerű működésének megvalósítása.
A szolgáltatások szereplői viselkedési normák, azaz protokollok alapján alkotnak rendszert, amely lehetővé teszi, hogy a szerver és a kliens oldalon – akár – különböző architektúrákon, eltérő operációs rendszereken, más és más fejlesztők szoftverei együtt tudjanak működni.
Az internet rohamos terjedése, a felhasználók számának drasztikus növekedése, a technikai fejlődés (átvitel), valamint a felhasználói igények bővülése, mindkét oldalon versenyhelyzetet teremtett. Mára számos, egymással – a protokollok és szabványok által – kompatibilis program közül lehet választani, melyek eltérő bonyolultságú, népszerűségű és különböző kiegészítőkkel rendelkező szoftverek.
Visszatekintve az elmúlt évtizedekre, megállapítható, hogy az IP[45] alapú, internetes szolgáltatások programjai is jelentős változáson mentek keresztül, méretükben nőttek, több végrehajtható (bináris) utasítást tartalmaznak, folyamatosan frissebb verziókban jelennek meg. A programsorok számának növekedése a biztonsággal összefüggő javítások mellett, újabb és újabb funkciók megjelenését eredményezte, amelynek katalizátora a versenyhelyzet, azaz az alkalmazóknak történő megfelelés volt. A szolgáltatási rendszerben a protokollokhoz kapcsolódó elvárások teljesítése – mint minimum elvárás – háttérbe, míg az alkalmazókat megnyerni szándékozó extra funkciók előtérbe kerültek. A szoftverek moduláris fejlesztésének eredményeként, a programokon belül egyes részfeladatok végrehajtásáért modulok lettek felelősek, és – első sorban a nyílt forrású alkalmazásoknál, – a különböző fejlesztők által létrehozott célmodulok együttműködése is lehetséges.
A szolgáltatások alrendszereiben az önálló-, vagy célmodulok rendszerelemekké váltak, melyek alkalmazása szintén a fő célt, azaz a szolgáltatások sikeres igénybevételét biztosítja. A modulok alkalmazása mellett, egyes (rész)feladatok végrehajtására, önállóan működő – hálózati port-tal, vagy socket-el rendelkező – kiszolgáló programok rendszeresítésére került sor, melyek rendszerelemként segítik elő az internetes szolgáltatások működését.
Napjainkban egyetlen KRISZ rendszer sem képzelhető el az alrendszerekbe integrált modulok, illetve az alrendszerekhez kapcsolódó kisegítő szolgáltatások alkalmazása nélkül, amelyek azonban minden egyes esetben külön biztonsági kockázatot jelentenek.

[45] Internet Protocol - Internet Protokoll

2.1.3 KRISZ alrendszerek alkalmazása

KRISZ alrendszernek tekintek minden olyan kiszolgáló, vagy ügyfél programot, amelynek funkciója közvetlenül vagy közvetetten adott szolgáltatás működésének biztosítása. Ebben a megközelítésben azokat a programokat is a KRISZ alrendszerei közé sorolom, amelyek szerver-kliens modellben, a háttérből közvetetten biztosítják a zavartalan működést és leállásuk, vagy meghibásodásuk következménye a KRISZ igénybevételének meghiúsulását jelentheti.

KRISZ működését közvetlenül támogató alrendszerek csoportosítása

1. Információkezelés

- Információ előállítást támogató alrendszerek;

  Az internet legnépszerűbb és legnagyobb információ-szolgáltató rendszere a világháló „(amelyet WWW-ként vagy röviden Webként is ismernek)", amely „**weboldalak,** vagy röviden csak **oldalak (pages)** hatalmas, világméretű gyűjteményéből áll".

  „A HTTP (HyperText Transfer Protocol - hipertext átviteli protokoll) a Világháló (Web) általános átviteli protokollja." [45] „A Web kiszolgálói a web szerverek, ügyfél programjai pedig az úgynevezett böngészők. A kezdeti időkben a Weben minden tartalom statikus volt, az információk előre rögzítésre kerültek és változatlan tartalommal továbbítódtak a böngészők, majd a felhasználók elé. A Web fejlődésével és az űrlapok megjelenésével, szinte egyszerre vált szükségessé az adatbáziskezelők és a web szerverek közötti adatkapcsolat biztosítása, valamint a dinamikus weboldalak alkalmazása. Napjainkban az interaktivitást, vagy változó tartalmat megjelenítő weblapok dinamikus, előfeldolgozó programok segítségével kerülnek előállításra, tehát a webszerver mint kiszolgáló oldali alrendszer mögött, egy program állítja elő a böngészők által értelmezhető –, adatbázisból is származtatott – adatokat. A webszerverben általában külön modul felelős a weboldalak előállításáért és külön modul felelős az adatbázis műveletek végrehajtásáért. Egy KRISZ-ként működő dinamikus weboldal használatában elengedhetetlen, ezáltal további kritikus pont a tartalom előállításért felelős program-modul, az adatok kezeléséért felelős adatbázis-ügyfél modul és maga az adatbázis kezelő rendszer.

  A tartalom ügyfél oldali prezentálását a böngészők képességeik és beállításaik szerint végzik. A weboldal tartalmazhat böngésző által

  - megjelenítendő elemeket,

- feldolgozandó és futtatandó programkódot (Javascript[46]),
- alapértelmezetten nem, ugyanakkor beépülő modulok (plugin) segítségével értelmezhető és végeredményben megjeleníthető kódot.

Ebben a megközelítésben a programkód végrehajtó és a beépülő (plugin) modulok, a KRISZ ügyfél oldali alrendszerének további kritikus elemei, melyek képessé teszik a szolgáltatás igénybevételében résztvevő böngészőt a kívánt tartalom megjelenítésére. Az ajánlások ugyan a böngésző felhasználójára bízzák – és biztonsági okok miatt gyakran nem is javasolják – a beépülő modulok, valamint az ügyfél oldali programok használatát, amit azonban a kívánt tartalmak és információk elérése rendszerint felülír.

- Információ továbbítást, célba juttatást közvetlenül támogató alrendszerek (spam, vírus ellenőrzés);

  Az informatikai hálózatok egyik leggyakrabban kihasznált adottsága, hogy lehetőséget biztosít – az információt hordozó – adatok továbbítására. Ezen adottság megvalósítására számos protokoll és szolgáltatás áll rendelkezésre, melyekben közös, hogy az adatcsere a hálózat két dedikált pontja között valósul meg, továbbá, hogy az ügyfél kezdeményezésére a kiszolgáló biztosítja a tranzakciók végrehajtását. A KRISZ-ként működő, adatcserét biztosító rendszerekben a kiszolgálónak állandóan rendelkezésre kell állnia, ugyanakkor az adatok kezelésére különböző szabályok alkalmazása szükséges. Az elektronikus levelezés a legnépszerűbb és legkézenfekvőbb adattovábbító rendszer, melynek kulcs eleme az üzenettovábbító ügynök (Message Transfer Agent - MTA). Az SMTP[47] protokollon alapuló szolgáltatás feladata az üzenetek ellenőrzése és továbbítása az email postafiókokhoz. Az adatcserét biztosító szolgáltatások sarkalatos kérdése, hogy a tranzakciót csak a megfelelő jogosultsággal rendelkező személy indíthassa, illetve, hogy az információ csak és kizárólag az illetékeshez jusson el. A felhasználó-azonosítás származhat a kiszolgáló operációs rendszerén rögzített hozzáférésekből, vagy adatállományban, adatbázisban rögzített forrásból. Előbbi egyrészt biztonsági kockázattal jár, másrészt nagyszámú felhasználó esetén kezelhetetlenné válik, utóbbi pedig az adattovábbító és adatbázis-kezelő rendszer együttműködését feltételezi. Az internet – sajnos – teret adott a kéretlen adatok továbbítására is, amely kiváltképp indokolta az adatcserét biztosító szolgáltatások kontrolálását,

[46] A legnépszerűbb ügyféloldali szkriptnyelv, ideális az interaktív weboldalak létrehozására.
[47] Simple Mail Transfer Protocol

ellenőrzését. Az ismert kártékony programfajták kiszűrésére vírusirtó, a kéretlen adattartalom azonosítására spam szűrő alkalmazható az adatcserét biztosító szolgáltatás szerver és kliens oldalán egyaránt, míg a nagyszámú felhasználó azonosítására a kiszolgálóhoz csatlakoztatott adatbázis-kezelővel van lehetőség. Egy levelező szolgáltatótól napjainkban elvárás a kártékony és kéretlen adattartalmak elleni harc, ellenkező esetben a szolgáltató úgynevezett „fekete" listára kerül és rendeltetését nem láthatja el. A szűrők és az adatbázis modul tehát kritikus alrendszeri elemként jelenik meg az adatcsere szolgáltatásban, nélkülözésük pedig veszélyezteti ezen KRISZ működését.

2. Elhelyezkedés

- KRISZ közbenső alrendszerei;

  A KRISZ rendeltetésszerű működését biztosító kiszolgáló és ügyfél közé egyes esetekben – általában biztonsági célból, – közbenső szolgáltatás kerül telepítésre, melynek használata kikényszerített, megkerülhetetlen. Alkalmazásával többek között biztonságos hálózati csatornán lehet védett adatokhoz hozzáférni, vagy a felhasználók tevékenysége szabályozható, korlátozható. A közbenső szolgáltatás – bevezetése esetén – a KRISZ alrendszereinek kritikus elemévé válik, hisz nélküle az alapszolgáltatás nem vehető igénybe.

- KRISZ külső alrendszerei;

  Az internetes szolgáltatások alrendszereihez gyakran külsőleg kapcsolódnak – kiszolgálónak önállóan nem minősíthető – programok, amelyek a szolgáltatás megvalósulásában nélkülözhetetlen szerepet játszanak. Elsősorban a Web-en léteznek olyan, a KRISZ körébe tartozó kiszolgáló alkalmazások, amelyek kifejezetten – népszerű – futtató programok (Java, Flash) meghívásával érik el a kívánt információk előállítását, megjelenítését. Nagy előnyük, hogy mind a kiszolgáló, mind az ügyfél oldalon egyaránt rendelkezésre állnak, a gyártók a számítógépektől az okos telefonig – platformtól függetlenül – szinte minden eszközre biztosítanak fejlesztő és futtató környezetet, ezért használatuk igen széles körben elterjedt.
  A KRISZ mögött elhelyezkedő külső programok igénybevételével megvalósított szolgáltatásoknál, a meghívásra kerülő alkalmazások az alrendszerek kritikus elemei, nélkülük nem lehet sikeres a szolgáltatás igénybevétele.

3. Függőség

- Kiszolgáló függő KRISZ;

Azok a kritikusnak minősített internetes szolgáltatások sorolhatók ide, amelyek működése további hálózati szolgáltatástól függ. Alapvetően az igénybe vevő felhasználók száma, az információ tartalma, illetve a szolgáltatás igénybevételéhez szükséges hálózati csatorna határozza meg, hogy adott KRISZ függőségben van-e további kiszolgálókkal, azonban leszögezhető, hogy a függőség általában fennáll.

- Független KRISZ;

  Az esetek kis számában – főleg az információ széleskörű terjesztése érdekében – előfordulhat, hogy a KRISZ önmagában, további szolgáltatások igénybevétele nélkül működik.

KRISZ működését közvetetten támogató alrendszerek

A szerver-kliens modell alapján működő, KRISZ működését közvetetten befolyásoló alkalmazások sorolhatók ide. Az operációs rendszerek a KRISZ működését felsőbb szinten biztosítják, egymással oda-vissza kölcsönhatásban vannak, ezért a közvetetten támogató alrendszerek általában operációs rendszer szintű szolgáltatások. Az operációs rendszerek alapvetően a háttérben „észrevétlenül" teszik a dolgukat, ugyanakkor – főleg távoli működtetés esetén – megfelelő mederben kell őket tartani, időközönként korrigálni kell a működésüket, amelyek a KRISZ zökkenőmentes igénybevételére kihatással lehetnek.

- Adminisztráció;

  Minden operációs rendszert karban kell tartani, frissíteni szükséges, a folyamatokba időnként be kell avatkozni, a rendelkezésre álló tárterületet felül kell vizsgálni és még hosszasan lehetne sorolni az elvégzendő feladatokat. Ezen adminisztrációk végrehajtásához távolról, hálózaton keresztül is elérhető kiszolgáló programot kell, vagy lehet alkalmazni, amely operációs rendszer szintű beavatkozásra ad lehetőséget. Tekintettel arra, hogy a KRISZ környezetét mindig operációs rendszer biztosítja, az annak adminisztrálását lehetővé tevő programok használatával, az internetes szolgáltatások közvetetten befolyásolhatók.

- Időzítés;

  A pontos idő fontos lehet a határidők betartásához, betartatásához, vagy többek között az időhöz gazdaságilag kapcsolódó folyamatok kiszolgálásában. Több KRISZ működésében is létfontosságú a pontos idő használata, amelyet a kiszolgáló általában a szerver operációs rendszerének idejéből származtat. Adott esetben szükséges lehet tehát a KRISZ-t biztosító szerver idejét pontosan tartani, ami a pontos időt megadni képes további szerver lekérdezésével lehetséges. Ebben az esetben a KRISZ szervere egy ügyfél programmal kéri

le a pontos időt, majd szükség esetén korrigálja az operációs rendszer idejét, ezáltal biztosítja a rendeltetés szerinti szolgáltatás megfelelő működését.

2.1.4 Megkerülhetetlen alrendszeri elemek

A KRISZ-t közvetlenül támogató alrendszer elemek közül néhány minden kiszolgálóban megtalálható, alkalmazásuk létfontosságú, szinte megkerülhetetlen.

- adatbáziskezelés;

  Az információk dinamikus előállításánál, vagy a nagyszámú felhasználó – virtuális – kezelésénél, kiváló megoldás a KRISZ kiszolgáló oldalához kapcsolt adatbázis-kezelő használata. Napjainkban a legmodernebb adatbázis kezelő rendszerekhez is szállítanak modulos kiegészítőket a fejlesztők, amelyek könnyen integrálhatók a KRISZ kiszolgálóihoz, de adott esetben a „standalone" üzemmódban működő adatbázis szerverek is használhatók.
- authentikáció;

  Az internetes kiszolgálás sarkalatos pontja, hogy az adott szolgáltatást csak és kizárólag a jogosultsággal rendelkező személy vegye igénybe, illetve az információ csak és kizárólag az illetékes személyhez jusson el. Szinte megkerülhetetlen a felhasználó azonosítására való törekvés, amelyre több alternatíva is számításba vehető. Szinte mindegyik KRISZ kiszolgáló rendelkezik saját authentikációs modullal, amely kisebb felhasználó szám esetén kielégítő lehet, ugyanakkor nagyobb létszámhoz adatbázis-kezelő, vagy kifejezetten a felhasználói azonosításra készített kiszolgáló program használható.
- gyorsító tár;

  A cache egy olyan nagyon gyors működésű tároló, amelyben a gyakran használni kívánt adatok átmenetileg tárolásra kerülnek, így azokhoz sokkal gyorsabban hozzá lehet férni, mintha mindig az eredeti, lassabb elérésű forráshoz kellene nyúlni.

  A nagy igénybevételnek kitett KRISZ esetében szinte elkerülhetetlen a gyorsító tár alkalmazása, amely szerver-kliens modellben mind operációs rendszer, mind szoftver szinten elérhető. Használatával elkerülhető a kiszolgálást biztosító szerver kapacitásainak túlzott igénybevétele, túlterhelése, ugyanakkor mellőzése könnyen a KRISZ leállásához, vagy rendeltetéstől eltérő működéséhez vezethet.” [46]

2.2 Az adatbázis-kezelők szerepe a Kritikus Internetes Szolgáltatásokban

Az adatbázis-kezelők a Kritikus Internetes Szolgáltatások nélkülözhetetlen alrendszerei, amelyek egyaránt biztosíthatják az adatfeldolgozás tárgyát, vagy a szolgáltatások működéséhez szükséges kulcs adatokat.

„Már a 60-as évek elején a számítógépek alkalmazásának nagyobbik részét az un. **adatfeldolgozás** tette ki. Korán rájöttek a szakemberek arra, hogy az 'egyszerű' adatfeldolgozás is jobban 'gépesíthető', ha az adatok közötti akár egyszerű kapcsolatokat struktúrának tekintjük, és adatmodellekben, adatsémákban gondolkodunk. Az olyan adathalmazokat, amelyeket modellbe foglalva kezeltek, adatbankoknak, később pedig adatbázisoknak nevezték el." [47]

„Az adatfeldolgozás napjainkban is az informatika kimagasló jelentőségű szakága, amelyben a technikai fejlődés épp úgy fellelhető, mint a többi területen. Az adatokat feldolgozni és értelmezni szándékozó embereknek és az adatbázis-kezelő rendszereknek egészen más kihívásokkal kell szembenézniük, mint 1-2 évtizeddel ezelőtt. Az információs társadalom, a digitalizálás, s az internet elterjedése, szinte felfoghatatlan mennyiségű adat létrehozását eredményezi.” [48] Az úgynevezett „Big Data" jelenségre irányuló kutatások szerint, 2015-ben körülbelül 2,2 millió terra byte adat keletkezett naponta, amely mennyiséget Eric Schmidt, a Google volt elnöke úgy jellemezte, hogy „ennyi adat keletkezett a civilizáció hajnala és 2003 között összesen." [49] „Ezen adatmennyiség tárolására és feldolgozására elsősorban az új generációs, úgynevezett befogadó-, vagy host típusú, – azaz másik programozási nyelvvel együtt használható, – hálózati interfésszel rendelkező, SQL[48] szintaktikát ismerő adatbázis-kezelő rendszerek alkalmasak. A gyakran önálló programozási nyelvvel is rendelkező, de mára elavult, elsősorban egy felhasználós, limitált rekordszámot kezelő, xBase[49] rendszerek egyre kevésbé játszanak szerepet napjaink adatbázisainak kezelésében. A Kritikus Internetes Szolgáltatások működtetésében – szinte – megkerülhetetlen az adatkezelés problematikája, melynek egyenes következménye a KRISZ-hez illesztett, hálózati adatbázis kezelést biztosító rendszerek üzemeltetése, a bizalmasság, a sértetlenség, és az állandó rendelkezésre állás teljesítésével. Kérdésként merül fel, hogy az interneten megjelenő adatok kezelése mennyiben tér el a zárt rendszerben tároltakétól, egyáltalán milyen specialitások jellemzik a hálózati adatbázis kezelést, és milyen jelentőséggel bírnak az internetes szolgáltatások mögött rejlő adatok? Leszögezve azt a tényt, hogy az internetes szolgáltatást támogató adatbázis-kezelőnek állandó elérhetőséggel kell működnie, továbbá hogy a KRISZ felé biztosítani kell az

[48] SQL - Structured Query Language (strukturált lekérdezőnyelv)
[49] Általános kifejezése a dBASE programnyelvből és adatbázis struktúrából származó programozási nyelveknek

adatfeldolgozás alap funkcióit, látszik, hogy a szolgáltatást igénybe vevő (felhasználó) és az adatbázis-kezelő közvetett kapcsolatban állnak egymással. A KRISZ-nek tehát az ügyfél és az adatbázis között egyaránt kell transzparenciát biztosítania az illetékes adatok, információk kinyerésére, ugyanakkor gátat szabnia az adatok korlátlan, illetéktelen felhasználásának. A szolgáltatók az – akár érzékeny – adatok jogosultsághoz kötött rendelkezésre bocsátásával, állandó veszélynek teszik ki magukat az illegális adatszerzést célként kitűző emberekkel szemben, melyet versenyhelyzet, jogszabály, vagy csak az internet adta lehetőségek egyaránt indukálhatnak.

Fontos leszögezni, hogy mindegyik adatbázis-kezelőnek kell rendelkeznie olyan interfésszel, vagy programmal, amely a hozzáférések, a jogosultsági szintek, s az adatbázisban tárolt adatok módosítását lehetővé teszi. A gyakorlat azt mutatja, hogy előbb-utóbb, – az alkalmazói program megkerülésével, – szinte minden adatbázisban valamely adat manuális módosítása-, korrigálása-, továbbá az adatbázis-kezelő, mint bármely más szerverprogram karbantartása, frissítése szükséges. Ezeknek a funkcióknak a biztosítására hozzáférési felületet, vagy más értelmezésben lehetséges támadási pontot kell állandóan, vagy ideiglenesen fenntartani, s egyben a rendszer karbantarthatóságát biztosítani.” [48]

2.2.1 Az adatbázis-kezelők helye a Kritikus Internetes Szolgáltatásokban

„A Kritikus Internetes Szolgáltatások egyik leggyakoribb háttérkiszolgálója az adatbázis-kezelő szerverprogram, amely az alábbi ismertebb internetes szolgáltatásokban rendszerint fellelhető:

- Web;
- E-mail;
- FTP[50].

Használatával a tartalom előállítás, vagy a szolgáltatások authentikációját biztosító felhasználó-kezelés egyaránt lehetséges, praktikus és legfőképpen szükséges. Tekintettel arra, hogy a KRISZ-nek és az adatbázis-kezelőnek állandó on-line kapcsolatban kell állnia egymással, a biztonsági szempontokat is figyelembe véve, eldöntendő, hogy a KRISZ-hez képest milyen elhelyezkedéssel működjön az adatbázis-kezelő? Az elhelyezkedést befolyásolja az adatbázis-kezelő jellege, a hálózati interfész rendelkezésre állása, az adatbázisok száma, illetve az adatbázis kiszolgálást igénybe vevő – egyéb – alkalmazások rendeltetése.

[50] File Transfer Protocol - állomány átviteli protokoll

A KRISZ és az adatbázis-kezelő egymáshoz viszonyított lehetséges elhelyezkedéseiből meghatározhatók a kapcsolódási formák és a megvalósítási módok. Az adatbázis-kezelő KRISZ-en belüli alrendszeri funkciója, a két szerverprogram egymáshoz viszonyított elhelyezkedése, kapcsolódása, valamint a tárolt adatok érzékenységének együttese, meghatározza a rendszer kritikusságát.

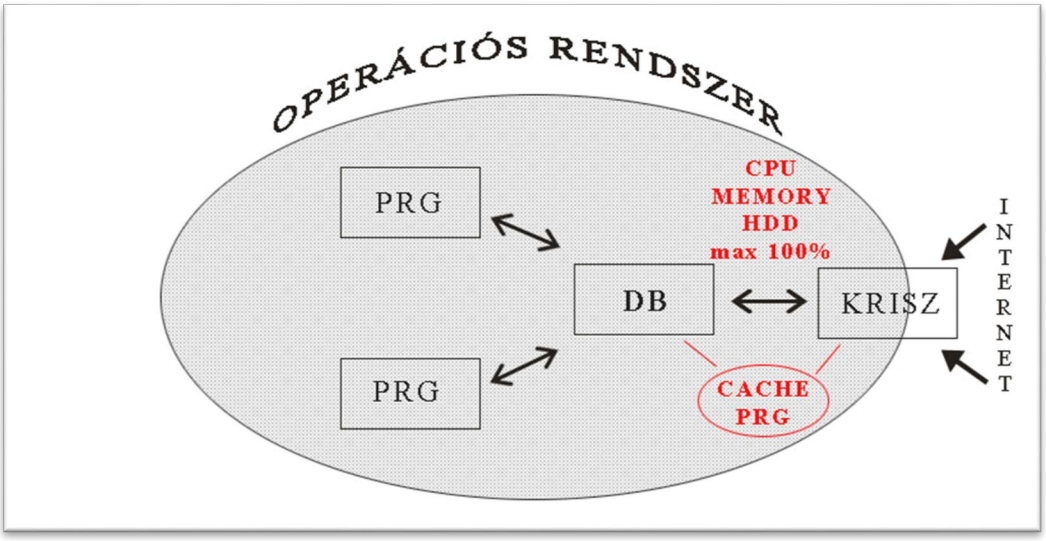
Elhelyezkedés

Tekintettel arra, hogy a KRISZ mindenképpen egy interneten elérhető szolgáltatás, leszögezhető, hogy a rendelkezésre állásnak internet-tartományba tartozó IP címmel[51] rendelkező szerveren, vagy szervereken kell megvalósulnia. A KRISZ jellegéből, illetve a származtatott adatok további felhasználásából adódóan, mérvadó az adatbázis-kezelő KRISZ-hez viszonyított elhelyezkedése.

1. Operációs rendszer szerinti elhelyezkedés

a) Egyazon operációs rendszeren

Napjaink – kiszolgálásra fejlesztett – operációs rendszerei a megfelelő hardver-, és erőforrás kapacitás rendelkezésre állása esetén, könnyedén képesek több szolgáltató program együttes futtatására és kezelésére.



5. ábra

Elhelyezkedés közös operációs rendszeren; forrás: szerző

[51] Internet protokoll cím, egyedi hálózati azonosító

Technikailag tehát viszonylag egyszerűen megvalósítható és nagy rendelkezésre állással – is – üzemeltethető egyazon operációs rendszeren több szolgáltatás (5. ábra), azonban ha van közöttük KRISZ és vele függőségi viszonyban álló adatbázis-kezelő is, akkor természetesen mindkettő szerverprogram kiemelt figyelmet érdemel. Fontos, hogy egyik szolgáltatás sem emésztheti fel úgy a rendelkezésére álló erőforrásokat, hogy a másik működésképtelenné váljon, hisz az közvetlenül, vagy közvetetten a KRISZ üzemképtelenségéhez vezet. Elengedhetetlen ezért a rendszerparaméterek folyamatos monitorozása, a finomhangolások elvégzése, és szükség esetén további erőforrás kímélő szolgáltatások üzembe helyezése. A sikeres erőforrás-gazdálkodás érdekében szinte elkerülhetetlen cache[52] szerver operációs rendszer és/vagy funkcionális program szintű üzemeltetése. A cache használata amellett, hogy nagy leterhelés esetén is képes megfelelő szinten tartani az erőforrásokat, egyben további kockázatot is jelent, hisz a KRISZ alrendszereként, üzemképtelensége egyes esetekben a rendszer túlterheléséhez vezethet. Az egyazon operációs rendszeren működő KRISZ és adatbázis-kezelő bármelyikének szolgáltatás/kapacitás bővítését megfontoltan kell végrehajtani, főleg, ha a rendszer erőforrásainak felhasználása előzetesen, átlagos terhelés esetén is eléri a 25 %-os szintet. Miután bármely szolgáltatás működtetése az operációs rendszer támadhatóságának szempontjából is egyfajta kockázatot jelent, a rendszer – bármely szerverprogramon keresztül történő – sikeres birtokba vétele (Owned[53]), megteremti az összes szolgáltatás, köztük a KRISZ leállításának, használhatatlanná tételének a lehetőségét is.

A KRISZ üzemeltetése – mindamellett, hogy kockázatosabb, – természetesen költséghatékonyabb az adatbázis-kezelővel egyazon operációs rendszeren, hisz a fenntartási költségek mind az energia felhasználás, mind az internet elérés szempontjából jelentősen kisebbek.

b) Különböző operációs rendszeren

A KRISZ-t és az azt kiszolgáló adatbázis-kezelőt – lehetőség szerint – bölcs döntés külön operációs rendszerre telepíteni és úgy üzemeltetni. Fontos megjegyezni, hogy az operációs rendszerek a virtualizációs[54] technológiáknak köszönhetően, akár egyazon hardveren is működhetnek, de az erőforrás felhasználás szempontjából önállók maradnak.

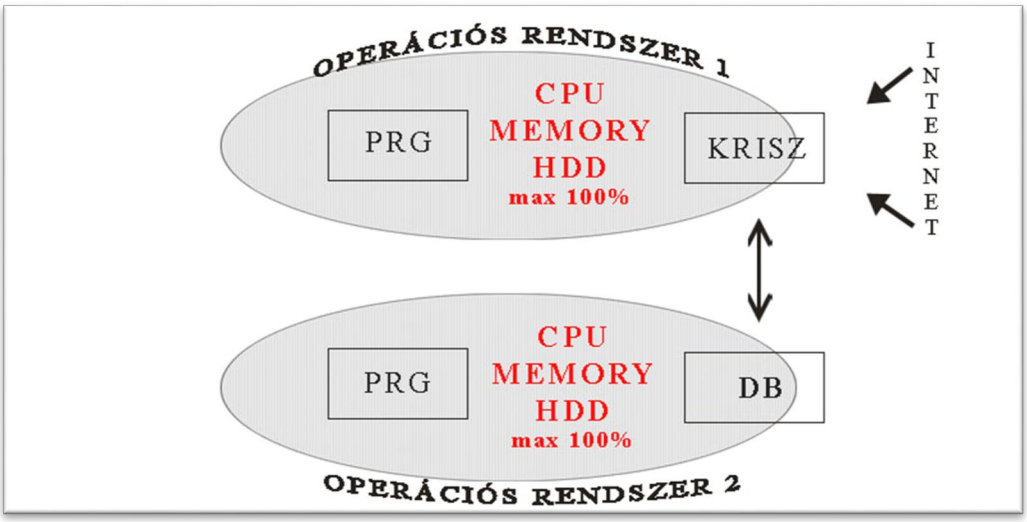
---

[52] gyorsító tár

[53] A hackerek által használt, a rendszer birtokbavételére utaló szleng

[54] „... virtualization is a smorgasbord of technologies that offer organizations many advantages..." [50] - a virtualizáció a technológiák svédasztala, amely számos előnyt nyújt a szevezetek számára

A KRISZ-t vagy az adatbázis-kezelőt célzó támadás az egyenkénti rendelkezésre állás szempontjából közvetlenül nem hat ki a másikra, a KRISZ sikeres működése ugyanakkor feltételezi az adatbázis-kezelő megfelelő rendelkezésre állását.



6. ábra

Elhelyezkedés különböző operációs rendszeren; forrás: szerző

Biztonsági szempontból tehát indokolt a KRISZ és az adatbázis-kezelő külön operációs rendszeren (6. ábra) történő üzemeltetése, azonban a konstrukcióban megoldandó feladat, az operációs rendszerek állandó on-line kapcsolatban tartása és az átvitelre kerülő adatmennyiség függvényében, a szükséges adatátviteli sebesség biztosítása. A megfelelő kapcsolat és sávszélesség megteremtése esetén viszont, a két operációs rendszer- és vele együtt a szolgáltatások közötti távolság, a minimálistól a végletekig növelhető. Az összeköttetési kényszerből adódik, hogy a KRISZ-t és az adatbázis-kezelőt működtető operációs rendszerek IP cím-tartományát hálózati konfigurációval összhangban és szinkronban kell tartani. Függetlenül attól, hogy belső-, vagy külső (internetes) címtartományban valósul meg az egységesítés, leszögezhető, hogy a KRISZ alap rendeltetéséből adódóan, az adatbázis-kezelő pedig a KRISZ kiszolgálása miatt nyitott hálózati porttal rendelkezik, tehát hálózaton elérhető, támadható, ezáltal védendő. A KRISZ és az adatbázis-kezelő operációs rendszer szintű szétválasztása esetén lehetséges, hogy az adatbázis szerver másik funkcionális információs rendszert is kiszolgáljon, sőt a gyakorlatban előfordul, hogy a KRISZ egy már működő IT rendszerre kerül illesztésre és kiterjesztésre.

Mivel tehát ebben a megközelítésben több operációs rendszer üzemeltetése szükséges, a vele járó folyamatos – szolgáltatásra is kiterjedő – karbantartási, frissítési és adminisztrációs

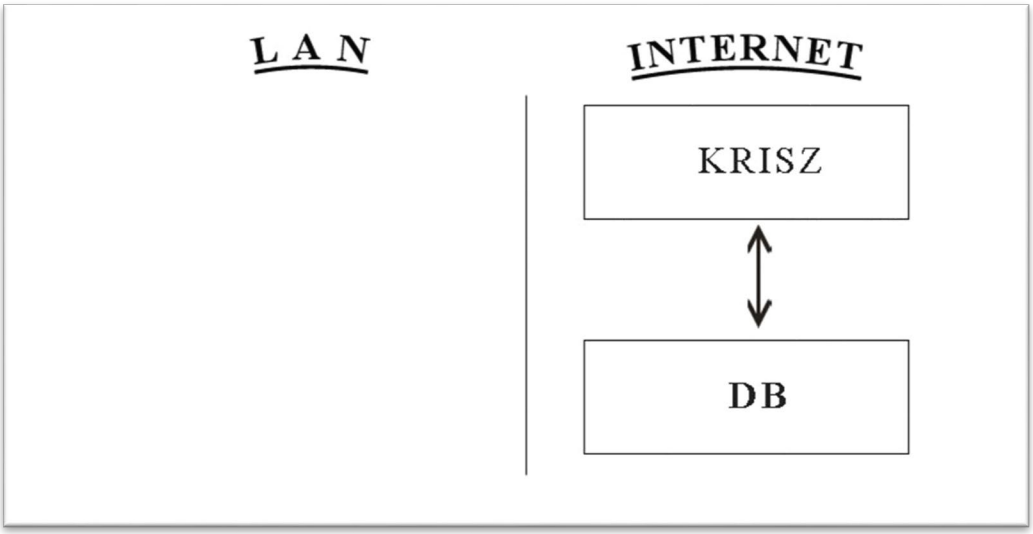
teendőket egyszerre, az operációs rendszer számának megfelelően több helyen is el kell végezni, valamit az összeköttetést biztosító kapcsolat rendelkezésre állását is gyakran ellenőrizni szükséges.

2. Hálózat szerinti elhelyezkedés

Napjaink professzionális adatbázis-kezelői hálózati interfésszel rendelkező szerverprogramok, s a KRISZ támogatása – néhány kivételtől eltekintve – szinte csak ezen adatbázis-kezelőkkel valósul meg. A hálózati adatbázis-kezelők üzemeltethetők internet tartományon belüli-, vagy kívüli IP címen, továbbá „localhost"[55]-on, azaz a visszahurkoló – hálózati – interfészen, amely tényleges, a működtető szerveren kívüli hozzáférést nem tesz lehetővé.

a) Internet tartományon belüli elhelyezkedés

Ebben az esetben, a KRISZ mellett az adatbázis-kezelő szolgáltatás is a világháló tartományába tartozó IP címen üzemel (7. ábra). Elsősorban akkor lehet szükség erre a megvalósításra, ha az adatbázis szerver az internet különböző pontjairól, akár nagy távolságokról érkező kéréseket is ki kell, hogy szolgáljon.



7. ábra

Interneten működő KRISZ és adatbázis-kezelő; forrás: szerző

Az adatbázisokban tárolt adatok érzékenysége alapvetően meghatározza egy internetről elérhető adatbázis-kezelő működtetésének kockázatát, azonban érdemes leszögezni, hogy a

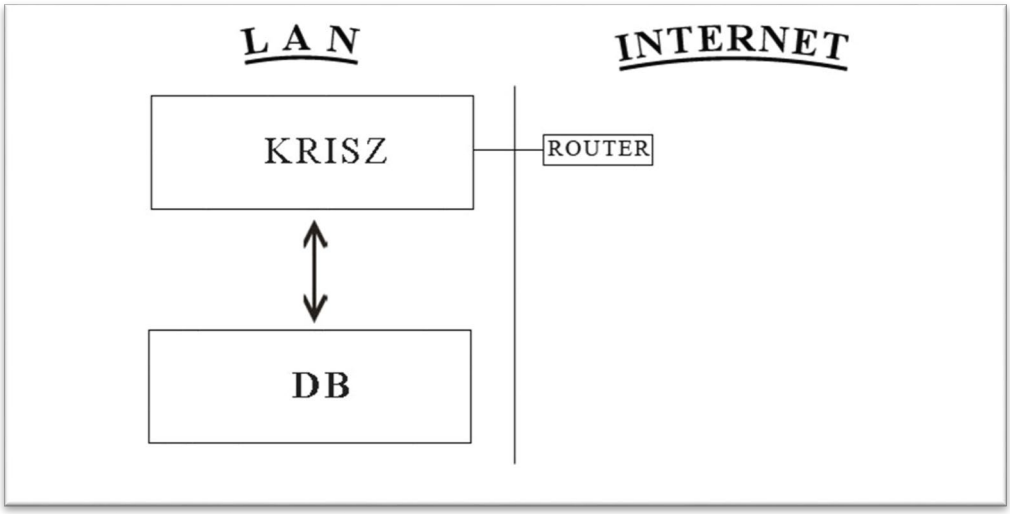
[55] A számítógép hálózatokban az egyes munkaállomások saját magukra mutató neve.

közvetlen internetes elérhetőség, valamint a nyitott adatbázis-kezelő port, a tárolt adatoktól függetlenül csábítja a rossz szándékú kapcsolódni vágyókat. Kiindulva abból, hogy a KRISZ nyílt IP címről kerül kiszolgálásra – akár igen magas kapcsolódási számmal is, – a biztonság fenntartása érdekében szinte alapkövetelmény a titkosítás megvalósításának minden formája (kapcsolódás, adat-továbbítás), továbbá fontos az adatbázis-kezelő authentikációjának és a megfelelő jelszavak használatának a kikényszerítése.

Az adatbázis-kezelő közvetlen internetes elérhetősége komoly kockázattal jár, nyomós érvként csupán a nagy távolságok áthidalásával elérhető költségtakarékosság, valamint egyéb feloldhatatlan kötöttségek, úgymint a szerver hozzáférésből adódó korlátozás hozhatók fel. A gyakorlat sajnos azt mutatja, hogy rossz, vagy figyelmetlen konfiguráció eredményeként is működnek nyitott port-tal adatbázis-kezelők az interneten, gyakran az üzemeltető tudta nélkül is.

b) Internet tartományon kívüli elhelyezkedés

Az internet mögötti, „belső" LAN[56] hálózatban működő szolgáltatások alkalmazásának létjogosultsága pontosan az, hogy a külvilág elől rejtve működjenek, az internetről közvetlen hálózati porton ne legyenek elérhetők (8. ábra).



8. ábra

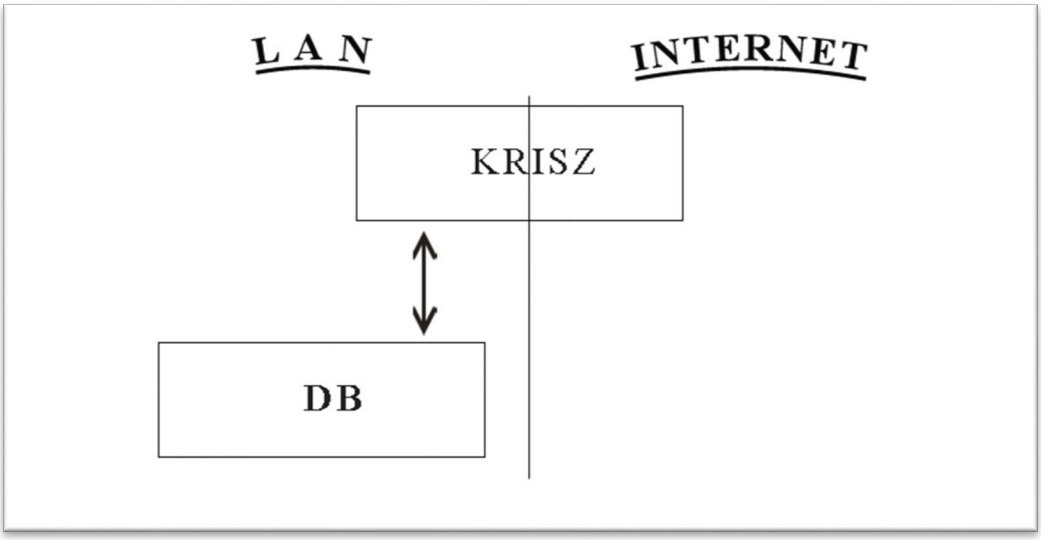
LAN-ba rejtett szolgáltatások; forrás: szerző

Ahhoz azonban, hogy egy internet tartományban üzemelő KRISZ kapcsolatba léphessen egy belső hálózatba rejtett adatbázis-kezelővel, a hálózati szinkronizációt meg kell oldani, azaz a

[56] Local Area Network - helyi hálózat

KRISZ-t működtető operációs rendszernek olyan hálózati interfésszel – is – kell rendelkeznie, amely rálátással bír az adatbázis-kezelőhöz rendelt hálózati pontra.

A megoldásra több lehetőség is kínálkozik, hisz a KRISZ szerverét akár több hálózati interfésszel is lehet konfigurálni, melyek közül egyik az internet, a másik pedig a belső hálózati kapcsolatot biztosíthatja (9. ábra). Megoldást jelenthet a KRISZ és az adatbázis-kezelő együttes LAN-ba „rejtése", amely biztonságosabb környezetben, egyszerűbb hálózati szinkronizációval megvalósítható működést biztosít, ugyanakkor a KRISZ internetes elérhetősége miatt forgalomirányítási kényszert jelent.



9. ábra

LAN-ba rejtett adatbázis-kezelő; forrás: szerző

c) Hálózati cím nélküli működtetés

Tekintettel arra, hogy a kizárólag „localhost"-on figyelő és a hálózati támogatással nem rendelkező adatbázis-kezelők elérhetősége hálózati pontról egyaránt kizárt, őket a hálózati elhelyezkedés szempontjából egy kategóriába sorolom, ugyanakkor megjegyzem, hogy működésük és a KRISZ-hez történő kapcsolódásuk teljesen eltérő. Amíg előző esetben a „localhost"-on hálózati jellegű a kapcsolat, addig utóbbi esetben a kapcsolódás file-rendszer szintű. Az IP cím nélküli adatbázis-kezelő és a KRISZ biztosan egy operációs rendszeren fut és az adatbázis-kezelő hálózati kapcsolat hiányában, közvetlenül csak és kizárólag a lokálisan futó programokat tudja kiszolgálni. Ebben a konstrukcióban, a fentiekben az „azonos operációs rendszer" témakörben már taglalt problémák szintén fennállnak, azzal a kitétellel, hogy az adatbázis-kezelő szolgáltatás csak közvetlenül – a KRISZ-en keresztül – érhető el és esetleg támadható.

Kapcsolódás, megvalósítás

Az adatbázis-kezelőnek és a KRISZ-nek egyaránt kapcsolódási képességgel kell rendelkeznie ahhoz, hogy egymás irányába adatokat tudjanak küldeni és fogadni, amely képesség szükségszerűen az egymáshoz viszonyított – fentiekben taglalt – elhelyezkedéstől függ.

Adatbázis-kezelő ——> „KAPCSOLÓDÁSI KÉPESSÉG" <—— KRISZ

A „KAPCSOLÓDÁSI KÉPESSÉG" lehet mindkét oldal binárisan kódolt-, vagy moduláris fejlesztés eredményeként ki-be kapcsolható funkciója, amelynek aktivizálásával a kapcsolat az alábbiak szerint jöhet létre.

- Hálózati porton keresztül
  Az adatbázis-kezelő hálózati port-on fogadja a kéréseket, amelyhez a KRISZ – a rálátási képesség függvényében, – általában valamelyik modulján keresztül kapcsolódást kezdeményez, majd a megfelelő jogosultság esetén a hálózati kapcsolat létrejöhet. A különböző adatbázis-kezelőkhöz eltérő a kapcsolódás és a kommunikáció protokollja, ezért a gyártók általában biztosítják a megvalósításhoz szükséges fejlesztői környezetet, vagy az előre megírt programokat, könyvtárakat, függvényeket.
- Operációs rendszer közös pontján keresztül (socket[57], memória, file rendszer)
  Az adatbázis-kezelő az operációs rendszer valamely KRISZ által is elérhető pontján keresztül biztosítja a kapcsolódás lehetőségét, amelyhez a KRISZ az adatbázis-kezelő specifikációjának megfelelően modulja segítségével kapcsolódást kezdeményez. Ez a közös pont lehet egyszerűen file, vagy a rendelkezésre álló memória egy bizonyos lefoglalt, fenntartott területe.

A feltételek rendelkezésre állása esetén tehát, a megfelelő konfiguráció alkalmazásával, a KRISZ és az adatbázis-kezelő kapcsolata létrejöhet. Ez a metódus általában még csak a kapcsolódás lehetőségét biztosítja, az adatbázis-kezelőben tárolt adatokhoz történő tényleges hozzáférés rendszerint további eredményes authentikációt követően valósulhat meg. A modern adatbázis-kezelők jogosultsági szintje rétegesen szabályozott

[57] „Egy gyakran alkalmazott szállítási réteg interfész a Berkeley-csatlakozók (sockets) által nyújtott interfész." [45]

- a kapcsolat létrehozására;
- az adatbázishoz történő hozzáférésre;
- az adott adatbázis tábláihoz történő hozzáférésre;
- az adatbázisban tárolt adatok kezelésére (lekérdezés, módosítás, törlés, stb..);
- az adatbázis, a táblák és a mezők struktúrájának, szerkezetének módosítására;
- a rendelkezésre álló jogok továbbadására vonatkozóan.

A jogosultságok beállítására a fentiek rendelkezésre állása esetén viszonylag nagy a mozgástér, amely feladat általában az adatbázis-kezelőt üzemeltető rendszeradminisztrátorra hárul. Fontos megjegyezni, hogy a gyakorlatban az adatbázis-kezelő rendszeradminisztrátora – a felsőbb szintű jogosultságok beállításával – adott adatbázisra vonatkozóan rendszerint tovább delegálja a felhasználók kezelését és egyúttal a felelősséget is a KRISZ üzemeltetőjének. Amennyiben az adatbázisokra, táblákra, oszlopokra vonatkozóan nem történik további hozzáférés szűkítés vagy pontosítás, azaz a KRISZ minden tranzakciót ugyanannak a túlzottan sok jogosultsággal rendelkező felhasználónak a nevében végez(tet), úgy a KRISZ – esetleges – gyenge pontjain keresztül az adatbázisokban tárolt adatok védtelenné válhatnak.

A sikeres kapcsolódást követően, a KRISZ – általában az adatbázis kezelést biztosító modulján keresztül – a rendelkezésre álló jogosultságoknak megfelelő tranzakciókat képes végrehajtani.

Adatbázis-kezelő kritikussága

Az online magyar értelmező szótár definíciója alapján, a kritikusság egyik melléknévi definíciója „Kétséges kimenetelű (helyzet, állapot, időszak, időpont), amely egy fennálló helyzetben, állapotban sorsdöntő fordulatot hozhat, egy folyamat menetét, sorsát döntően alakíthatja, befolyásolhatja, megszabhatja; válságos." [51]; míg a Révai Nagylexikon szerint „döntő, válságos, veszélyes" [52] a szó jelentése.

A „Kritikus Internetes Szolgáltatás" fogalom fentiek szerinti értelmezése egy olyan interneten megjelenő szolgáltatás, amelynek működése kétes kimenetelű is lehet, magában hordozza a veszélyt, megvan az esélye a kedvezőtlen állapotváltozásnak, ami akár válságos helyzet kialakulásához is vezethet.

Kérdésként merül fel, hogy az adatbázis-kezelő és a KRISZ közötti kapcsolat megszakadása, vagy az adatbázisban tárolt adatok kiszivárgása, esetleg az adatok kompromittálódása, mennyire idézi elő a kedvezőtlen – esetleg válságos – állapotot?

Figyelemmel arra, hogy a KRISZ alrendszereként működő adatbázis-kezelőben akár a szolgáltatáshoz szükséges összes információ is eltárolható függetlenül annak végső formájától (kép, hang, állomány stb..), megállapítható, hogy az adatbázis-kezelő olyan mértékben kritikus pontja a rendszernek, amennyire a benne tárolt adatok befolyásolják a szolgáltatás sikerességét.” [48]

2.2.2 A Kritikus Internetes Szolgáltatások adatbázisainak biztonsága

Az adatbázisok biztonsága létfontosságú a bizalmasság, a sértetlenség és a rendelkezésre állás megvalósulásához. „A KRISZ és az adatbázis-kezelő egymáshoz viszonyított, operációs rendszer és hálózati kapcsolat szerinti elhelyezkedése önmagában is komoly kihatással van a tárolt adatok biztonságára, ugyanakkor jelen írás célja, hogy az elhelyezkedési adottságokon túl is vizsgálja a működés biztonsági körülményeit. Jelen esetben az adatbázis-kezelő rendelkezésre állása helyett az adatok rendelkezésre állása a vizsgálat tárgya.

Ki kell emelni, hogy a két szempont szorosan kapcsolódik egymáshoz, hisz adatok nélkül hiába van adatbázis-kezelő, vagy az adatbázis-kezelő nélkül hiába vannak adatok, mindkettő a KRISZ működésképtelenségéhez vezet. Ezért az adatbázis-kezelőt és az általa kezelt adatok együttesét mindenképpen a KRISZ aspektusából, tehát a tranzakciók KRISZ-re gyakorolt hatásának értékelésével kell vizsgálni. Azt tudjuk, hogy az adatbázis-kezelő, mint nélkülözhetetlen alrendszer hiánya mit jelent, de vajon az adatbázisok és az azokon végrehajtott műveletek miként tudnak hatást gyakorolni a KRISZ-re? A választ azzal a továbbiakban fenntartott feltételezéssel keresem, hogy az adatbázis-kezelő rendelkezésre áll, a tranzakciók végrehajtására képes és alkalmas, továbbá általa az adatbázisok elérhetők. A hatás természetesen legfőképpen attól függ, hogy a tárolt adatok mennyire képezik „lelkét" a KRISZ-nek, továbbá, hogy azok a működés szempontjából mennyire hitelesek. A bizalmasság, a sértetlenség és a rendelkezésre állás adatokra vonatkoztatott együttese garantálja a KRISZ rendeltetésszerű működését, ezért a kompromittálódás, mint a legfőbb veszély beállta egyenesen a Kritikus Internetes Szolgáltatás meghiúsulásához vezethet.

Az adatbázis-kezelők leegyszerűsítve olvasási és írási műveleteket hajtanak végre az adatbázisokon, amelyek közül az olvasás a tárolt adatok visszanyerésére, míg az írás az újabb adatok rögzítésére, vagy a már eltárolt adatok módosítására, törlésére szolgál. A KRISZ

aspektusából nézve, az adatbázisokban eredendően a szolgáltatás által nyújtandó –, általában dinamikusan változó – információk tárolódnak, amelyeket először fel kell tölteni, amelynek feltétele az adatbázis-kezelőhöz vezető hozzáférési pont és a szükséges jogosultságok rendelkezésre állása. A KRISZ, a mögötte álló adathalmazból legtöbbször információkat szolgáltat, viszont számos esetben az adatkör bővítését, módosítását, vagy törlését is biztosítania kell, tehát írási műveletet kell végrehajtatnia az adatbázis-kezelővel. A szerepkörök szétválasztásához a KRISZ-nek el kell tudnia dönteni, hogy kik, milyen információhalmazhoz férhetnek hozzá, vagy mely felhasználók, milyen adatrögzítési engedélyekkel rendelkezzenek. Ezen döntését a KRISZ – leggyakrabban, – szintén az adatbázisban tárolt, felhasználói adathalmazból nyeri ki, majd az ellenőrzés pozitív eredménye esetén, az adatok módosíthatók. A metódusból jól látható, hogy – lehetősége esetén – egy rossz szándékú felhasználó, az adatbázis-kezelőnek kiadott olvasási művelettel, akár hozzájuthat az adatok módosítását biztosító hitelesítési információkhoz. Látható tehát, hogy két lépésben akár az adatbázis kompromittálása is végrehajtható, amennyiben a rossz szándékú felhasználó képes hozzáférni a KRISZ mögött működő adatbázis-kezelőhöz és tudja az információk kinyeréséhez vezető módszereket. Következésképpen a tényleges kockázatok feltárásához már a rendeltetésszerű, „normál” működést is célszerű felülvizsgálni, hiszen egy kifogástalannak tűnő rendszer is tartalmazhat támadásra alkalmas pontokat és lehet ártó szándékú a KRISZ-re nézve.

A KRISZ adatbázis-kezelése

Az adatbázis-kezelés sikeressége alapvetően az elérhetőség megteremtésén, az adatbázishoz szükséges elegendő hozzáférés rendelkezésre állásán és – szükség szerint – az írási műveletek abszolválásán múlik, ezáltal három fontos egységre tagolható. A KRISZ-t igénybe vevő felhasználók szándéka egyrészt irányulhat a hétköznapi, rendeltetésszerű használatra, másrészt pedig a kifejezetten rossz szándékú, az adatok kompromittálására irányuló beavatkozásra.

1. Az adatbázisok elérhetősége

Az adatbázis elérhetősége a rendelkezésre álló interfészen keresztüli kapcsolódás képességét jelenti, függetlenül az átviteli közegtől.

A feltételezés szerint az adatbázis-kezelő a KRISZ-nek megkerülhetetlen alrendszere, ezért az adatok átjárhatóságát meg kell teremteni, a szolgáltatásoknak egymással kapcsolatban kell lenniük, együtt kell működniük. A KRISZ-nek tehát az együttműködés érdekében el kell tudnia érni az adatbázis-kezelőt és rajta keresztül a működéshez szükséges adatokat, továbbá a

rendszergazdáknak, vagy adatgazdáknak is valamilyen közvetlen adatbázis-kezelői kapcsolatra van szükségük az adatbázisok karbantartására. A KRISZ definíciójából következően az adatbázis-kezelő folyamatosan rendelkezésre áll, azon keresztül pedig az adatbázisok, s így az adatok elérhetősége is biztosított, tehát az adatbázis-kezelő elérhetősége egyben az adatbázis elérhetőségét is jelenti. Az adatok-, adatbázisok elérése közvetetten, vagy közvetlenül valósulhat meg, amely az igénybe vevő helyzetétől függ; közvetett elérésnek tekintem, amikor az adatbázis-kezelővel egy közbenső, transzparens programon keresztül, csak indirekt módon lehet kapcsolatot létesíteni.

Ha a KRISZ alrendszereként adatbázis-kezelő is működik, akkor a transzparenciát maga a KRISZ biztosítja, hisz összeköttetést jelent a felhasználó és a kezelt adatok között azzal a kiegészítéssel, hogy a KRISZ rendeltetéséből adódóan, a kapcsolatnak állandóan fenn kell állnia. Következésképpen minden, a KRISZ-t igénybe vevő felhasználó közvetetten kapcsolatba lép az adatbázis-kezelővel, vagyis az adatbázisokat eléri.

2. Hozzáférés az adatbázishoz

Az adatbázishoz, illetve az adatbázis-kezelőhöz hozzáférést szerezni nem jelent mást, mint a rendelkezésre álló elérhetőségen kapcsolódni és az adatok jogosultság szerinti kezelésére képesnek lenni.

A KRISZ és az adatbázis-kezelő együttműködését fel kell konfigurálni, amelynek része a kapcsolódás definiálása és az adatbázis műveleteket biztosító jogosultság beállítása is. A KRISZ az adatbázis-kezelőhöz a gyakorlatban egy „adatbázis-account"[58]-al kapcsolódik, amelyhez minden, a KRISZ működésében igényként felmerülő adatkezelési jogosultságot hozzá kell rendelni, amelybe a KRISZ jellegétől függően egyaránt benne foglaltatnak az adatok olvasására és írására vonatkozó műveletek. A KRISZ önmagára nézve elérhetőséggel és a meghatározás szerinti hozzáféréssel rendelkezik az adatbázishoz, azonban az igénybe vevő felhasználónak csak közvetett, korlátozott jogosultságot továbbít, aki a beavatkozási lehetőségeitől függően, a programkód szerint hajtatja végre az adatbázis műveleteket. (10. ábra)

[58] adatbázis hozzáférés

10. ábra

Az adatbázis differenciált kezelése a KRISZ-en keresztül, a felhasználó által; forrás: szerző

A KRISZ programkódjába szándékosan nyilvánvalóan nem kerül olyan rész, amely indokolatlanul adna nagyobb mozgásteret az adatok kinyerésére, ugyanakkor a rossz-szándékú felhasználó rövidtávon az adatbázis védett információit szeretné megszerezni, hosszú távon pedig az adatokat módosítani. Kihasználva azt a lehetőséget, hogy az adatbázis-account a – KRISZ működéséhez szükséges – legszélesebb körű adatbázis műveletekre [47] jogosultságot ad, a KRISZ-t úgy próbálják felhasználni, hogy a hozzáférésüket az adatbázis védett adataira is kiterjesszék.

A hozzáférés kiterjesztéshez a KRISZ-t az alábbiak szerint lehet felhasználni:

- a kiszolgáló helytelen beállításaiból, a hibaüzenetekből, a programhibákból, az alapértelmezésekből és az árulkodó jelekből származó információk kigyűjthetők, amelyek tartalmazhatnak védettnek szánt-, vagy a hozzáférés kiterjesztését lehetővé tevő információkat;
- az ellenőrizetlen, vagy kevésbé ellenőrzött input interfészeken keresztül, SQL[59] utasítások injektálásával [60], a lekérdezések – az eredeti programozói szándékhoz képest – kiterjeszthetők és a KRISZ által nyújtott hozzáférés korlátlan felhasználói hozzáféréssé konvertálható;
- a kiszolgáló programhibáját kihasználva, az operációs-rendszerre belépve, az adatbázis állományi szintű hozzáférése elérhető.

Természetesen a KRISZ típusától függ, hogy interaktív beavatkozásra lehetőséget ad-e, viszont amennyiben igen, úgy figyelembe kell venni az SQL-ben rejlő, nyelvi sajátosságból [60] adódó kihasználhatóságot. Amennyiben a KRISZ üzemeltetője felhasználói táblát tart fenn azon

[59] SQL - Structured Query Language (strukturált lekérdezőnyelv)
[60] SELECT - UNION [47]

ügyfeleinek, akik – sikeres azonosítást követően, – az átlagostól több jogosultsággal használhatják a szolgáltatást, akkor injektált adatkinyeréssel – megszerezve a kiemelt felhasználók adatait, – szintén bővíthető a hozzáférési jogosultság.

3. Írás-műveletek az adatbázisba

Ebbe a témakörbe azok az adatbázis-műveletek tartoznak, amelyek az adatbázis szerkezetében, vagy az tárolt adatokban írási jogosultsághoz kötöttek. A kompromittáló tevékenység végső fázisa és egyben legfőbb célja az adatbázison végrehajtott törlés, módosítás, vagy rögzítés. A KRISZ, típusától függően, vagy csak olvassa az adatokat, vagy – ahogy az jellemzőbb – ír is az adatbázisba. Megjegyzendő, hogy az adatbázist kizárólag olvasásra használó KRISZ esetében is egyszer fel kell tölteni az adatokat, amely az adott pillanatban biztosan írási művelettel jár.

A KRISZ-nek rendelkeznie kell az adatbázis írásához szükséges jogosultsággal, az igénybe vevő felhasználónak pedig csak feltételhez kötötten, programban rögzített metódus szerint szabad ezen adatrögzítési lehetőséget átadni. A rossz-szándékú felhasználó célja az írási jogosultság érvényesítése, amelyet elsősorban az előzőekben részletezett hozzáférés kiterjesztésével szerezhet meg.

A KRISZ adminisztrálása szorosan összefügg (inkább kapcsolódik) az adatbázisok biztonságával, hiszen a karbantartó személy azonosítása rendszerint felhasználó név és jelszó párosítással történik, amelyeket beviteli mezőkbe kell megadni. A rosszindulatú felhasználó az előzőekben tárgyalt injektálással első lépésként megszerezheti a tárolt felhasználói neveket és jelszavakat, majd a rendelkezésre álló információkkal visszaélve, akár mint adminisztrátor léphet be a KRISZ-be és végezhet adatrögzítési műveletet.

A KRISZ védelmi rendszerének függvényében, a támadók használhatják a próbálgatásra alapozott brute-force[61] technikát, illetve az adatfolyam lehallgatásán alapuló adatlopást is. A KRISZ-en keresztül végrehajtott adatbázis kompromittálás befolyása és hatása nagyban függ a programkód adta funkcióktól, de leszögezendő, hogy mindenképpen lehetőséget ad a szolgáltatás teljes, vagy részleges meghiúsítására.

[61] „nyers erő”, más néven a teljes kipróbálás módszere

A KRISZ adatbázisának karbantartása

1. Közvetett eléréssel

A KRISZ szerverére a rendszergazdák, praktikussága miatt telepítenek célzott, az adatbázisok kezelését és karbantartását biztosító, internetről elérhető, közbenső programot. Létjogosultsága azért van, mert az adatbázisok karbantartása elkerülhetetlen, ugyanakkor a módszer alkalmazásával az adatbázis-kezelő maradhat a háttérben, nincs kitéve direkt elérhetőségnek és támadásnak, továbbá interneten keresztül is biztosított az adatbázis adminisztrációja. E közbenső program használatát általában a szerver kevésbé feltűnő IP alapú szolgáltatásához rendelik a rendszergazdák, amely a megfelelő rejtettség mellett kevés kockázattal járó adminisztrációt biztosíthat. Az igazán nagy veszélyt az „alapértelmezett", vagy kiszivárgott hozzáférések alkalmazása jelenti, amelyet tovább gyengít a titkosítás nélküli kapcsolat használata, támadási célpontot adva a rosszindulatú felhasználóknak.

2. Közvetlen eléréssel

Az adatbázis-kezelő közvetlen elérésén értem, ha a felhasználó egy kliens programmal, közvetlenül a rendszeresített interfészen keresztül hajtja végre a kapcsolódást, amely file-rendszeren vagy hálózaton egyaránt megvalósulhat. Közbenső program, így a KRISZ sem vesz részt az adatbázis-kezelő elérésében, így – előre felépített kapcsolat hiányában – adatok injektálással nem nyerhetők ki. A közvetlen eléréssel rendelkező adatbázis-kezelők kockázatot jelentenek, hisz az átviteli közeghez hozzáférő felhasználók – az adatbázis-kezelő authentikációs rendszerének függvényében – lehetőséget kapnak a kapcsolódásra. Az adatbázis hozzáférés a kapcsolódó felhasználó jogosultságai szerint realizálódik, ezért a KRISZ adatbázis accountjának megszerzésével, a rossz-szándékú felhasználó a KRISZ adatbázis-műveleteit képes végrehajtani.

Hálózati kapcsolattal rendelkező, internetről nyitott adatbázis-kezelő esetén veszélyt jelent a túlterheléses támadás (DoS[62], DDoS[63]), amely annak időtartamától függően a KRISZ működését is befolyásolhatja.

File-rendszeren az adatbázisok az általános állományi műveletek hozzáférési jogosultságának függvényében védettek-, vagy védtelenek, szerkezetük, illetve tartalmuk szerint az adatbázis-kezelő valamely kliens programjával olvashatók-, vagy módosíthatók. A file-rendszer szintű

[62] Denial of Service - szoláltatásmegtagadással járó támadás
[63] Distributed Denial of Service - elosztott szoláltatásmegtagadással járó támadás

hozzáférés olvasási jogosultság esetén az adatok kinyerésére, írási jogosultság esetén pedig károkozásra is alkalmas.” [48]

Szerző gyakorlati tapasztalata

A „kalohirek.hu” regionálisan népszerű, nagy látogatottsággal rendelkező, állandóan frissülő, a legaktuálisabb híreket közvetítő internetes on-line médiaportál 2018. novemberében úgy volt a kísérlet alanya, hogy a kísérlet az eredeti rendszer teljes másolataként rendelkezésre álló, saját tesztkörnyezetben zajlott. A megjelenő „khirek.hu” domain a valóságban nem létezik, az a próba idejére, a belső környezetben definiált értékként (hosts) került létrehozásra.

Elsőként az interaktív weboldalak általánosan használt adminisztrációs URL[64]-je, a /admin hivatkozás került teszt alá. Meglepetésre, a 11. ábrán látható hibaüzenet volt látható, amelyből azonnal kiszűrhető volt, hogy egyrészt a szerver nincs felkészítve hibás hivatkozás kezelésre, másrészt kinyerhető volt a weboldal üzemeltetésével kapcsolatos számos fontos információ, úgymint: operációs rendszer; web-szerver; programozási nyelv; tartalmat előállító motor. Az oldal üzemeltetője nagy hibát elkövetve, debug, azaz beszédes módban hagyta a keretrendszer hibaüzenet kezelését, amely – szorgalmasan végrehajtva a kapott utasításokat, – saját magáról adott ki információkat. Átvizsgálva a kapott hibaüzenet forráskódját, a web-portál összes beállítása, köztük az adatbázis hozzáférés felhasználói neve és jelszava is kinyerhető volt. Megszerzésre került tehát a szolgáltatás által használt adatbázis account, s így a következő lépésként már csak közvetlen kapcsolódást kellett találni a keretprogram által használt MySql[65] adatbázis-kezelőhöz.

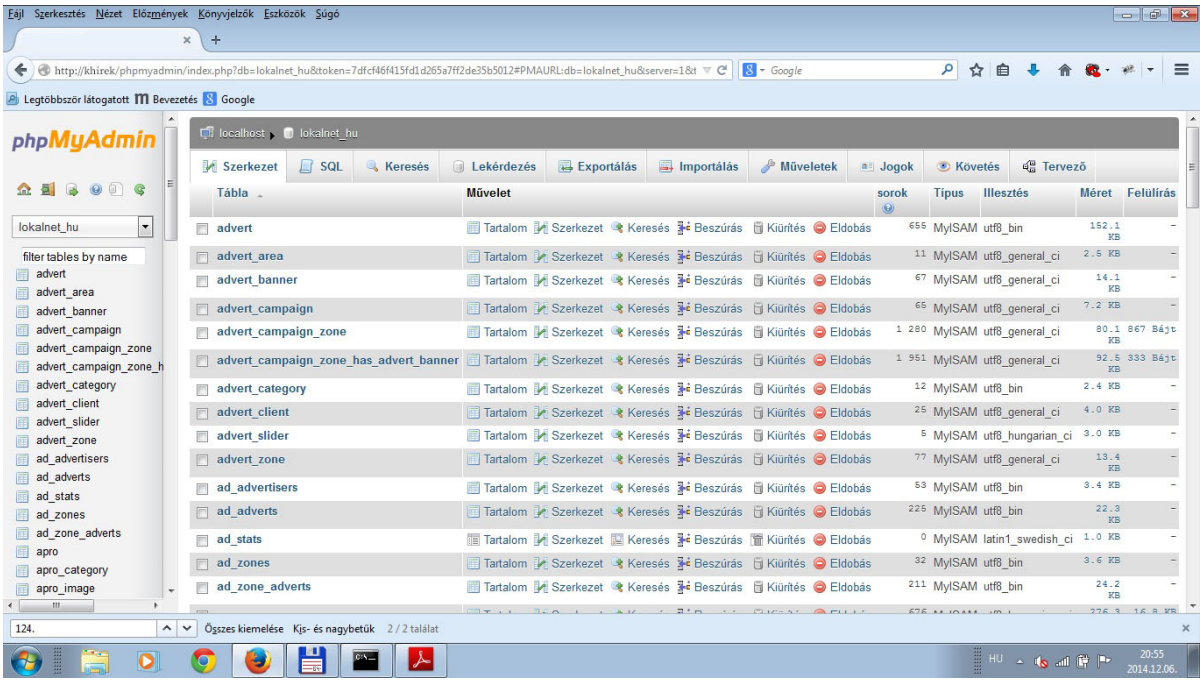
[64] U*niform Resource Locator* - egységes erőforrás-azonosító
[65] https://www.mysql.com

11. ábra

Árulkodó hibaüzenet; forrás: szerző; letöltve: 2018.11.17

Kipróbálásra került, hogy a szerver üzemeltetői alkalmaznak-e direkt adatbázis adminisztrációt. A legnépszerűbb adminisztrációs programból kiindulva (phpMyAdmin[66]), amely Web-szerveren, PHP[67] feldolgozóval használható, annak az esetleges elérése volt a következő célpont. Ismét alapértelmezett elérhetőséget keresve, a /phpmyadmin URL-en az adatbázis-karbantartására irányuló bejelentkezés volt elérhető.

[66] http://www.phpmyadmin.net/home_page/index.php
[67] Hypertext Preprocessor – Hypertext előfeldolgozó



12. ábra

Adatbázis megszerzése (2018.11.17); forrás: szerző

Az előzőekben megszerzett felhasználói név és jelszó a helyi tükörszerveren is aktív hozzáférésként működött, segítségével csatlakozni lehetett az adatbázis-kezelőhöz és a 12. ábrán látható, hogy a végeredmény korlátlan adatbázis jogosultság hozzáférés volt. A web-portál tükör-adatbázisában minden táblához és minden adathoz szabadon hozzá lehetett férni. Az adatbázis-kezelőn keresztül a médiaportál teljes adatvagyona-, valamint ezáltal a médiaportál is „owned” státuszba kerülhetett volna.

Az üzemeltető fatális hibákat követett el, a figyelmetlenségekkel teljesen kitette magát a támadóknak, ugyanakkor a Web-portált nem deface[68]-elték, amely leginkább annak köszönhető, hogy az oldal nem került rosszindulatú felhasználók célkeresztjébe. A kísérlet során komolyabb beavatkozásra nem volt szükség, csupán – az üzemeltető által nyitva hagyott – alapértelmezett beállítások kihasználása történt.

2.2.3 Az adatbázis-kezelők előfordulása a védelmi szféra Kritikus Internetes Szolgáltatásaiban

„Napjainkban a rendvédelmet irányító kormányzatban, annak háttérintézményeiben és magában a védelmi szférában is egyre nagyobb hangsúlyt kapnak azok az interneten elérhető

[68] Honlapcsere (deface)

szolgáltatások, amelyek bevezetését követően a használat kötelező érvényűvé válhat a bevont szervek, vagy akár a társadalom szélesebb körű szereplői részére egyaránt.
Az internetes megjelenés természetesen lehet védett, például virtuális magánhálózatba, vagy szolgáltatók által – garantáltan – szegmentált hálózatba rejtett, vagy bárki által elérhető, teljesen nyilvános. A Kritikus Internetes Szolgáltatások ismérveiben megfogalmazott feltételek teljesülése, azaz a szolgáltatás szükségessé, kritikussá válása esetén, egyrészt teljesülnie kellene az állandó rendelkezésre állás követelményeinek, másrészt az adatbázis-kezelő – mint háttérszolgáltató alrendszer – jelenléte további védelmi intézkedések bevezetését követeli meg.
A teljesség igénye nélkül bemutatásra kerülő alábbi internetes szolgáltatások mindegyike a védelmi szférához tartozik, működésük elvárt, hisz társadalmi és/vagy kormányzati célt szolgál.

Elektronikus levelező rendszerek

A védelmi szférában – és a kormányzatban – használt elektronikus levelező rendszerek többnyire a „gov.hu" domain tartomány részeként, a szervezetre vonatkozó sub-domain alkalmazásával működnek, a kiosztott email címek pedig több esetben a postafiókot használó személyek vezeték-, és keresztneveiből származtatódnak.

A Microsoft platformon biztosított levelezés eredményeként, a végfelhasználók az OWA[69] webmail rendszeren keresztül képesek leveleket küldeni és fogadni, postafiókjaikat kezelni. A rendszer elérhetősége a szervezetek intranet hálózatából és a világhálóról egyaránt lehetséges, ami magában foglalja az állandó rendelkezésre állás-, és az internet irányából bekövetkező támadások elleni védekezés szükségességét.
A levelező felhasználók accountjai Active Directory[70] címtár adatbázisban tárolódnak, ami ugyan nem egy klasszikus adatbázis-kezelő rendszer, de egy speciális adatbázis, amit maga a Microsoft is megerősít: „Active Directory is a special-purpose database — it is not a registry replacement." [53] Azzal, hogy az elektronikus levelezés interneten megjelenő, háttér adatbázissal rendelkező webmail alapú rendszer, azt Kritikus Internetes Szolgáltatásnak tekinthetjük.
A webmail szolgáltatásokat különböző –, azonban hasonló IP tartományban üzemelő – szerverek biztosítják, amelyet az URL[71]-ek névfeloldása bizonyít. A kereséssel megtalálható

[69] Outlook Web Access / Outlook Web App
[70] Active Directory - információkat tárol a hálózaton levő objektumokról, lehetővé téve azok megtalálását, elérését a felhasználók és a rendszergazdák számára. [86]
[71] **U**niform **R**esource **L**ocator - egységes erőforrás meghatározó [45]

szerverek hálózati IP címének scennelése azt mutatja, hogy a Web és az Email szolgáltatások mellett – nagy valószínűséggel – egyéb hálózati kiszolgálás nem üzemel rajtuk, ami azt jelzi, hogy a felhasználói adatbázis a nyilvánosság elöl rejtett, tehát közvetlenül nem érhető el.

Adatbázis alapú egyéb rendszerek

A rendvédelmi portálokon végzett rövid böngészés után, az alábbi adatbázis alapú, kritikusnak tekinthető weboldalak voltak megtalálhatók[72]:

- Jogszabály alapján, tájékoztató az objektív felelősség hatálya alá tartozó szabályszegések elkövetése miatt folytatott közigazgatási eljárás adatairól [54];
- Körözési al-portál [55];
- Építésügyi hatósági engedélyezési eljárásokat támogató elektronikus dokumentációs rendszer, az e-közigazgatás szolgáltatása [56];
- Rendészeti Vezetőképzési, Továbbképzési és Vizsgaportál; Rendészeti feladatokat ellátók képzése és vizsgáztatása[73] [57];
- Pályázatokkal kapcsolatos, kötelező érvényű adatszolgáltatási rendszer [58];
- Honvédelmi Minisztérium - Párbeszéd Portál [59].

A weboldalak mindegyike valamilyen felhasználó-, vagy jogosultság-azonosításhoz kötött, adatbázisból dolgozik, ugyanakkor a fenti webmail rendszerekhez hasonlóan az adatbázis-kezelő rejtett, tehát közvetlenül nem érhető el.” [46]

[72] 2014.11.17-i állapot, amely kisebb domain név eltérésekkel 2020. márciusában is aktuális
[73] 2014.01.30-án 14.621, 2014.11.17-én 22.479 regisztrált felhasználóval

Összegzés, következtetések

A Kritikus Internetes Szolgáltatások rendszerszintű vizsgálatával feltérképezésre kerültek az alrendszerek és rendszerelemek, valamint szolgáltatásokban betöltött szerepük. Láthatóvá vált, hogy a Kritikus Internetes Szolgáltatások támogatása közvetlenül és közvetetten egyformán fontos és miként valósulhat meg. A kiszolgáló és az ügyfél – mint alrendszerek – funkcióinak taglalásával megvizsgáltam, hogy melyek azok a támogató modulok, programok, vagy kiszolgálók, melyek a korszerű szolgáltatások meghatározó, kritikus elemei.

Ebben a fejezetben bemutatásra került, hogy **az adatbázis-kezelő rendszerek nélkülözhetetlen „kellékei" korunk információs társadalmának és vele együtt** annak eredményeként, valamint következményeként, **a Kritikus Internetes Szolgáltatásoknak is**. Bemutattam, hogy milyen relációban alkalmazhatók az adatbázis-kezelők a KRISZ mellett és azoknak milyen előnyei, vagy hátrányai vannak. A felkutatott URL-ek bizonyítják, hogy **számos adatbázis alapú Kritikus Internetes Szolgáltatás működik a védelmi szférában**, amelyek a társadalom és a kormányzat szereplőinek egyaránt rendelkezésre állnak. Látszik, hogy az internet adta lehetőségeket a védelmi szféra is egyre inkább kihasználja, ugyanakkor megállapítható, hogy a rendelkezésre álló szolgáltatások egymástól még mindig elszigeteltek, azonban összefüggés közöttük, hogy a szerverek hasonló IP tartományba tartoznak, amely központosított információbiztonsági háttérre, azaz kormányzati hálózati felügyeletre utal.

A KRISZ mögött elhelyezkedő adatbázisok biztonsága az elérhetőség, a hozzáférés és az adatrögzítés fázisain keresztül került vizsgálat alá. Arra kerestem a választ, hogy a KRISZ alaprendeltetését miként tudja befolyásolni az adatbázis kompromittálása, illetve milyen tevékenységek vezethetnek a szolgáltatás befolyásolásához. Megállapítható, hogy az alapfelvetés, miszerint **a KRISZ** egy állandóan, interneten elérhető szolgáltatás, önmagában is **teret ad a háttérben működő és állandó összeköttetéssel rendelkező adatbázis-kezelő elérhetőségének és az adatbázis részleges hozzáférésnek**. A KRISZ-ben rejlő hibák, figyelmetlenségek, vagy automatizmusok további lehetőséget adhatnak az adatbázis-hozzáférés kiterjesztésére, majd végeredményként az adatbázis kompromittálására. **A KRISZ-en keresztül, mind az operációs rendszerhez, a file-rendszerhez, az adatbázis-kezelőhöz és az adatbázishoz szerzett rosszindulatú hozzáférés a szolgáltatás leállásához vezethet**. A bemutatott személyes tapasztalat is azt támasztja alá, hogy a figyelmetlenül konfigurált internetes szolgáltató rendszerek – a megfelelő adatbázis-biztonság nélkül, – könnyedén támadási célponttá válhatnak és kerülhetnek illetéktelenek fennhatósága alá.

3. FEJEZET

Kritikus, internetes szolgáltatási rendszerek

A Kritikus Internetes Szolgáltatások számtalan formában jelenhetnek meg, ugyanakkor megjelenési formáinak népszerűsége párhuzamba állítható az internet általános „fogyasztási" szokásaival. Teljesen természetes, hogy a legnépszerűbb szolgáltatási formák válnak Kritikus Internetes Szolgáltatássá, hisz az alkalmazók gyakorlati jártassága előnyt jelent az igénybevétel megvalósulásakor. Jelen fejezetben a leggyakoribb igénybe vett-, vagy nyújtott – kritikussá váló – szolgáltatási formák, illetve azok összetevői kerülnek elemzésre, amelyek biztonságos üzemeltetése nélkülözhetetlen a védelmi szféra rendeltetésszerű működése szempontjából.

3.1 A World Wide Web[74] szerepe a Kritikus Internetes Szolgáltatásokban

A Kritikus Internetes Szolgáltatások egyik leggyakoribb előfordulási helye a World Wide Web (a továbbiakban: Web), amely adottságai miatt optimális környezet az információk megjelenítésére, gyűjtésére, tárolására és továbbítására. Az állandó rendelkezésre állás a bizalmasság és a sértetlenség fenntartása mellett, a Weben is komoly kihívást jelent.

„Tim Berners-Lee, brit tudós 1989-ben, a CERN-ben megalkotta a World Wide Web-et. Az első honlapot a CERN-ben – és egyben a világon is – Berners-Lee NeXT számítógépe szolgáltatta és magához a World Wide Web projekthez jegyezték. A honlap a Web alapvető jellemzőit írta le [61]; hogyan lehet hozzáférni más emberek dokumentumaihoz és hogyan kell beállítani egy saját szervert. A CERN a World Wide Web programját 1994. április 30-án nyilvánosan elérhetővé tette, majd a következő kiadást nyílt licensz-el tette elérhetővé, biztosítva a terjesztés maximalizálását. A futtatáshoz szükséges szabadon elérhető webszerverrel, valamint egy alap böngészővel és egy (forrás)kód könyvtárral, a Web virágzása biztosított volt." [62]

„Tim 1990 októberében három alapvető technológiát írt le[75], amelyek a mai Web alapjai is: HTML[76], URL[77], HTTP[78].

A Web fejlődése az első honlap megjelenése óta kétséget kizáróan töretlen, napjainkban a legtöbbet használt kommunikációs eszköze az internetnek és a Kritikus Internetes Szolgáltatásokhoz is számos ponton kapcsolódik. A kezdeti honlapok nyilvánvalóan

[74] World Wide Web – világháló
[75] http://webfoundation.org/about/vision/history-of-the-web/
[76] HyperText Markup Language - hiperszöveges jelölőnyelv
[77] Uniform Resource Locator - egységes erőforrás-azonosító
[78] HyperText Transfer Protocol

összehasonlíthatatlanok a mai modern, összetett, bonyolult, programozott weblapokkal, ezért a fejlődés menetében azokat a pontokat célszerű kiemelni, amelyek megalapozták a Web és a KRISZ közös jövőjét.

Az innováció követésében, a szerver-kliens modell analógiájára, érdemes különválasztani az információt nyújtó szolgáltatói-, és az azt igénybe vevő felhasználói oldalt azzal a tényszerű kiegészítéssel, hogy a két szegmens egymást a fejlődésben folyamatosan indukálta, erősítette. A Web evolúciójával foglalkozó kutatások, illetve a publikált számszerűsíthető eredmények jobbára a kliens oldalon bekövetkezett változásokat mutatják, ugyanakkor a KRISZ jellegéből adódóan a szerveroldali fejlődést is fontos bemutatni. A „National Center for Supercomputing Applications" (NCSA) „HTTP daemon" nevű programja volt a vezető webszerver 1995. februárjában, azonban a fejlesztő csapatból kilépett programozók 1995. december 1-én kiadták az „Apache" nevű webszerver hivatalos verzióját [64], amely rövid időn belül az elsődleges webkiszolgálóvá vált. A Web szempontjából mérföldkőnek számító, első dinamikus weboldalak kialakulását nehéz meghatározni[79], ugyanakkor az Apache 1.1 béta 3 verziójának 1996. június 14-én megjelent leírásában [65] egyértelműen fellelhetők a CGI[80]-re vonatkozó utalások. A CGI mintegy csatlakozási felületként működik a külső programok és a webszerver között a dinamikus tartalmak előállításához; a leírásban utalást találhatunk[81] a másik nagyon fontos területre, az adatbázis-kezelésre is. Az Apache, az 1.3a1 verziótól – azaz 1997. őszétől – kezdve, a Unix után már Windows NT-n is futtatható vált, lefedve az operációs-rendszer platformok döntő többségét. A 2000-es évektől a webszerverekbe – nélkülözve a CGI-t – közvetlenül integrálhatókká váltak a dinamikus weboldalak előállításához és az adatbázisok kezeléséhez szükséges modulok, kiegészülve számos biztonsági, technológiai és kényelmi szolgáltatással. Az oldalak előállítását biztosító programozási nyelvek dinamikusan fejlődtek és az egyéb szerveroldali szolgáltatások Web-re történő implementálása is folyamatos volt. Napjainkban, köszönhetően a kialakult versenyhelyzetnek, a kiszolgálói oldalon számos – ingyenes – alternatíva közül választhatnak a webszervert üzemeltetők.

A felhasználók kegyeiért folytatott böngésző-verseny azonnal elkezdődött, amint a fejlesztők belátták a Web töretlen népszerűségéből húzható hasznot. A Különböző gyártó-, és fantázianevek folyamatosan bukkantak fel, vagy tűntek el, a legfőbb rendező elv pedig maga a felhasználói tömeg volt, amely saját igényeinek és lehetőségeinek megfelelően választotta ki a

[79] https://en.wikipedia.org/wiki/Dynamic_web_page#History
[80] Common Gateway Interface
[81] „MSQL authentication module improvements,"

böngészőket. A fejlesztések és a felhasználói igények abba az irányba vezettek, hogy napjainkban szoftver óriások szállítják a legkorszerűbb böngésző programokat, amelyek

- felhasználóbarát, kényelmes GUI[82] felülettel rendelkeznek;
- törekednek a szabványokban rögzített feltételek teljesítésére;
- támogatják a szkript-nyelvek és a beépülő programok futtatását;
- képesek az információ minden típusú megjelenítésére (szöveg, kép, hang, stb.);
- több platformon is elérhetők (a szállító üzleti szempontjainak függvényében);
- erős védelmi rendszerrel rendelkeznek, törekednek a biztonságra;
- ingyenesek.

A Web fejlődésébe a kiszolgáló és a felhasználói oldal mellett további, külső tényezők is szerepet játszottak, amelyek együttesen megteremtették a KRISZ, Web-es alkalmazási lehetőségét. Az infrastrukturális fejlődés növelte az internetelérés sávszélességét, nőtt az adattárolási kapacitás-, és biztonság, valamint meredeken emelkedett a mikroprocesszorok számítási teljesítménye.

A kereskedelem gyorsan felmérte a Web-ben rejlő lehetőségeket, hisz az első on-line vásárlás a feljegyzés szerint[83] – 1994-ben – már biztonságos SSL csatornán keresztül zajlott, majd 1995-ben megnyitottak a ma is legnagyobbnak számító webáruházak. A Web rövid időn belül a pénzügyi tranzakcióknak is teret adott, valamint a kereskedelmet mozgató reklámoknak is felületet biztosított. Egyirányúan erősödött és erősödik az a tendencia, hogy az emberek – megtakarítva rengeteg időt és energiát, – ügyeiket kényelmesen az Interneten, azon belül is legfőképpen a Web-en intézzék.

A Web alapjai a fejlődés során mindvégig megmaradtak, viszont létrejött egy komplex IT[84] környezet, amely megfelelő képességgel rendelkezik az információk széles spektrumú, nagy megbízhatóságú továbbítására, hordozására.

3.1.1 Kritikus Internetes Szolgáltatások a Web-en

A Web, adottságaiból adódóan megfelelő környezet a KRISZ üzemeltetéséhez, ezért kedvelt információs platformja a szolgáltatóknak. Megvalósítása kétféle lehet; a KRISZ egyrészt működhet kizárólagosan a Web-en, ekkor a webszerver az egyedüli kiszolgáló, másrészt

[82] grafikus felhasználói felület
[83] https://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html; letöltve: 2020.03.16
[84] Information Technology - információtechnológia

üzemelhet kiegészítő alkalmazásként, mely esetben a webszerver egy másik kiszolgálóhoz kapcsolódva rész-, vagy támogató szolgáltatást nyújt. A Web-re készített KRISZ igénybevétele vagy valamilyen böngészővel, vagy a HTTP(s) protokoll(oka)t ismerő egyéb programokkal történik. A böngésző, vagy az alkalmazás típusa, továbbá alkalmazott operációs rendszere – a bevezetőben felsorolt funkciók rendelkezése állása esetén – nem releváns, tetszőleges.
Ahhoz, hogy a KRISZ Web-re kerüljön, teljesülnie kell a definíciókban megfogalmazott elvárásoknak: a szolgáltatást igénybe vevő felhasználók számától függetlenül, – feltételezve a megfelelő infrastrukturális és hardveres hátteret, – az állandó rendelkezésre állást a bizalmasság és a sértetlenség megvalósulásával kell biztosítani. Ezen elvárások abszolválása összetett, számos biztonsági intézkedés foganatosításával érhető el, amelyeket operációs rendszer-, webszerver-, valamint alkalmazói program szintjén kell-, vagy lehet megvalósítani.
Az alább felsorolt ajánlások, a KRISZ biztonságos üzemeltetésével kapcsolatban megfogalmazott általános irányelvek mellett érvényesek.

3.1.2 Stabilitás, hibatűrő képesség

Ahhoz, hogy a Web-en megjelenő KRISZ stabilitása megfelelő legyen, a közreműködő egységeknek is az elvárt hibatűrő képességgel kell rendelkezniük, hisz a KRISZ a leggyengébb láncszem szerint lesz ellenálló. Az ismert hibák és támadási pontok kiküszöböléséhez minden szinten kötelező a biztonsági frissítések és a szükséges karbantartások elvégzése.
A webszerver, a Web-en alkalmazott KRISZ nélkülözhetetlen komponense, az alkalmazás kiszolgáló-, és végrehajtó motorja, ezért kijelölése felelősségteljes döntés.
Webszervernek egy megbízható, már bizonyított, hatékony erőforrás-gazdálkodással bíró, kellő támogatással rendelkező programot célszerű választani. Figyelembe kell venni, hogy a tesztelés, vagy kipróbálás alatt álló programok még számos hibát tartalmazhatnak, ezért kiszolgálónak stabil kategóriába sorolt verziót ajánlott telepíteni. A HTTP(s), kérés-válasz alapú felépítésére tekintettel, a stabilitást elsősorban a kiszolgáló kérésekre adott reakcióinak szabályozásával lehet elérni, megőrizni.

A kérések feldolgozásában lényegi szerepet játszik a webszerver alá rendelt további kiszolgálók típusa és száma, ugyanis a – KRISZ-re jellemző – dinamikus weboldalak elő-feldolgozó programmal készülnek, tartalmuk pedig gyakran adatbázisból származik. A webszerver tűréshatárát – a rendelkezésre álló infrastruktúra és hardver figyelembevétele mellett, – az egységnyi idő alatt kiszolgálandó ügyfelek számának-, és a kiszolgálásra fordítandó időnek a

szabályozásával szükséges korlátozni. Kiemelt figyelmet érdemel az alrendszeri kiszolgálók pontos és körültekintő, erőforrás orientált konfigurációja, amellyel a túlterhelés megelőzhető és az áthárított feladatvégzés normalizálható.

3.1.3 Kritikus Internetes Szolgáltatásként működő Web biztonsága

A webszerver moduljait a biztonság és a szükségszerűség figyelembevételével kell be-, vagy kikapcsolni, amellyel elérhető, hogy csak a nélkülözhetetlen, vagy a biztonságot támogató programkódok kerülhessenek végrehajtásra, a feleslegesek, vagy kockázatosak pedig inaktívak maradjanak.

Minden webszerver konfigurációjában meg kell határozni a könyvtárstruktúra tetejét kijelölő, úgynevezett „DocumentRoot"[85] könyvtárat, amely egyben az összes URL hivatkozás kiinduló pontja is. A könyvtárstruktúrában a KRISZ, mint alkalmazás is helyet kell, hogy kapjon, s mellette számos olyan állomány és adat is, amelynek illetéktelen kézbe kerülése veszélyt jelent. A webszervert úgy kell konfigurálni, hogy a legkevésbé támogassa a felhasználók által kért mappák, vagy állományok tartalmának megjelenítését, azokat tartsa rejtve.

Az összeköttetés biztonságának megvalósítása céljából, 1995-ben megalkották az SSL[86]-, majd annak továbbfejlesztéseként 1999-ben a TLS[87] nevű biztonsági programcsomagot [45], amellyel megbízható HTTP, azaz a HTTPS protokoll alkalmazására nyílt lehetőség. Napjainkban minden komolyabb webszerver támogatja a használatát, a beállítás és konfigurálás pedig a dokumentációk [66] alapján könnyen kivitelezhető. A KRISZ jelenléte esetén, szinte kötelező a biztonságos átvitel webszerver általi támogatásának beállítása.

Az Interneten található, több milliónyi weboldalt prezentáló szervergépek száma töredéke a fellelhető oldalaknak, amelyből következik, hogy egy-egy számítógép – az úgynevezett „VirtualHost" technológiának köszönhetően – több weboldal egyidejű kiszolgálását biztosítja. Feltételezhető, hogy a KRISZ működéséért felelős webszerver adott esetben további Domain[88] nevekhez tartozó weboldalakat is kiszolgál, amely azonban elővigyázatosságra ad okot. A KRISZ-en kívüli, tetszőleges weboldalról bekövetkező támadás esetén, könnyen a KRISZ is

[85] dokument-gyökér
[86] Secure Sockets Layer
[87] Transport Layer Security
[88] tartomány

áldozattá válhat. Amennyiben az illegális behatoló a webszerver adott könyvtárában írási jogosultsághoz jut és oda saját, szerver által végrehajtható programkódot képes feltölteni, úgy – a webszerver felhasználójának jogosultságával, – a birtokba vett könyvtárból elérhető mappaszerkezetre rálátással bírhat és könnyen módosításokat is végezhet. Fontos kiemelni tehát, hogy a KRISZ programkódját szeparáltan kell elhelyezni a fájlrendszeren, majd kapcsolni a webszerverhez, hogy egyéb weboldalakról érkező támadás esetén is védett legyen.

A Web-en megjelenő KRISZ esszenciáját az a forrásprogram adja, amelyet a webszerver képes értelmezni, szükség esetén feldolgozni és a kliens részére a szabványok szerinti formában továbbítani. Ezen kódok a kezdetek óta nagy változáson mentek keresztül, hiszen amíg a Web-et először statikus oldalak alkották, addig napjainkra bonyolult programrendszerek állítják elő a világhálón megjelenő gigantikus információhalmazt. Temérdek előre megírt forráskód és több tucat ingyenes keretrendszer áll rendelkezésére az érdeklődőknek, akik költséghatékony eszközökkel is képesek –, akár Kritikus Internetes Szolgáltatás nyújtására alkalmas, – saját weboldalt létrehozni. A KRISZ, Web-es rendszerbe állításától kezdődően azonban, elengedhetetlen néhány biztonsági intézkedés foganatosítása.

- Törekedni kell az információszegény URL-ek alkalmazására és a kockázattal járó elérési pontok elrejtésére. Biztonságosabb, ha a böngészés során a felhasználók nem látják, hogy a hivatkozásokban milyen paraméterek, változók és értékek kerülnek átadásra, hisz azok ismeretében számos – adatbázisra és működésre vonatkozó, – logikai következtetés vezethető le;
- Az adminisztráció a dinamikus weboldalak egyik megkerülhetetlen feladata. Fontos megjegyezni, hogy az adminisztrátor az adatokra és gyakran a programkódra vonatkozóan is írási jogosultsággal bír, ezért e lehetőség illetéktelen kézbe kerülése végzetes lehet. Elvárás tehát, hogy az adminisztrációra mutató hivatkozás a normál felhasználók számára ismeretlen, vagy elérhetetlen legyen. Tipikus hiba a „/admin", mint alapértelmezett adminisztrációs belépési pont nyitva hagyása, amely tálcán kínálja a belépés és a támadhatóság lehetőségét;
- A programozás íratlan szabályi szerint, a kód mennyiségével egyenes arányban az elkövetett hibák száma is növekszik. Egy KRISZ esetében, a feltárt hibákat a lehető legrövidebb időn belül javítani-, vagy kiadott biztonsági csomag esetén a programot frissíteni szükséges. A hibaüzenet kezelést éles üzemben ki kell kapcsolni és lehetőség szerint kerülni kell a bonyolult, átláthatatlan, erőforrásokat felemésztő adatbázis műveleteket. A nagyobb keretrendszerekre jellemző, gyártó és verziószámra utaló megjegyzéseket ki kell iktatni,

elkerülve, hogy a rosszindulatú felhasználók annak ismeretében indítsanak támadást, vagy keressenek alapértelmezett, a programra jellemző beállításokat;

- A webszerver titkosított kapcsolat létesítésére vonatkozó alkalmassága esetén, a bizalmas információk továbbítására kötelező a HTTPS protokoll kikényszerítése. Ezek közé sorolandó a weboldal adminisztrálásával-, a pénzügyi tranzakciókkal-, a felhasználók kezelésével-, és a felhasználók megszemélyesítésével kapcsolatos műveleteket. Titkosítás hiányában ezen kommunikációk lehallgathatók és a megszerzett információk könnyedén támadási eszközzé konvertálhatók;
- A nem várt események kezelése és a szolgáltatásban bekövetkező kimaradási idő minimalizálásának érdekében, a webprogramról és az adatvagyonról minél gyakoribb rendszerességgel mentéseket kell végezni és azt a kiszolgálótól eltérő helyen érdemes tárolni. A weboldalra érkező kéréseket lehetőség szerint naplózni kell, amit rendellenesség esetén ki lehet értékelni.

3.1.4 Társszolgáltatások kezelése

Függetlenül attól, hogy a KRISZ működésében résztvevő webszerver fő-, vagy támogató kiszolgáló, elengedhetetlen a funkcionáló szerverprogramok közötti megfelelő összhang. A levelező-, adatbázis-kezelő-, és cache kiszolgálók a Web gyakori –, általában függőségi viszonyban is álló – együttműködői, amelyből következik a precíz konfiguráció szükségessége. A webszerverrel mellé-, vagy alárendeltségben álló szolgáltatások együttesét úgy kell üzemeltetni, hogy a KRISZ rendelkezésre állása ne forogjon kockán, az mindig biztosított legyen.” [63]

3.2 Az elektronikus levelezés szerepe a Kritikus Internetes Szolgáltatásokban

Egy kutatás szerint az e-mail továbbra is az üzleti kommunikáció legelterjedtebb formája, a naponta elküldött és fogadott üzleti és fogyasztói e-mailek száma 2018-ban elérte a 280 milliárdot és az előrejelzések szerint 2022 végére 333 milliárdra növekszik. Az e-mail továbbra is az első számú támadási eszköz.[89]

Az elektronikus levelezés kiemelkedő szerepet játszik a Kritikus Internetes Szolgáltatások családjában, hisz akár önmagában, akár más szolgáltatáshoz kapcsolódva, elvárás és alapvetés az elektronikus levelezés folyamatos, nagy rendelkezésre állással bíró működése. Napjainkban egy természetesnek vehető alapszolgáltatás, amelyet a felhasználók kegyeiért számtalan esetben már ingyenesen bocsátanak rendelkezésre. Az elektronikus levelezés ugyanakkor melegágya az informatikai rendszerek ellen indított sikeres támadásoknak, amelynek számos oka közül egy a működés kicsit rendhagyó mechanizmusa. A KRISZ definícióját figyelembe véve, a mindenkori fő cél a szolgáltató, azaz a levelezőrendszer folyamatos rendelkezésre állásának biztosítása, ugyanakkor a kiberbűnözők egy olyan továbbító eszközként is használják, amellyel számtalan rosszindulatú tevékenységet lehet kezdeményezni.

3.2.1 Az elektronikus levelezés elmélete

„Az e-levél rendszerek két alrendszerből állnak, a felhasználói ügynökből (user agent), amely lehetővé teszi a felhasználók számára az üzenetek olvasását és küldését, valamint az üzenettovábbító ügynökből (message transfer agent), ami a leveleket eljuttatja a feladótól a címzettig.” [68] Az üzenettovábbító ügynökre a továbbiakban ismertebb nevén, levelezőszerverként is fogok hivatkozni.

„A felhasználóiügynök-program grafikus, ritkábban szöveges és parancsalapú csatlakozó felületet nyújt az e-levél rendszerrel való érintkezésre. Ez magában foglalja az üzenetek írásához, megválaszolásához, a beérkező üzenetek megjelenítéséhez valamint az üzenetek iktatással, kereséssel és törléssel való rendszerezéséhez szükséges eszközöket.” [68] A felhasználóiügynök-programot hétköznapi szóhasználattal levelező programnak is nevezik.

[89] „Research by The Radicati Group shows that email remains the most ubiquitous form of business communications, with the total number of business and consumer emails sent and received per day reaching 280 billion in 2018 and projected to grow to over 333 billion by the end of 2022. It should come as no surprise then that email remains the number one vector used by threat actors to launch attacks.” [67]

„A felhasználói ügynökök és az üzenettovábbító ügynökök összekapcsolása adja a postaláda és a szabványos e-levél formátum koncepcióját. A postaládák (mailbox) tárolják a felhasználók által kapott leveleket. Ezeket a levelezőszerverek kezelik.” [68]

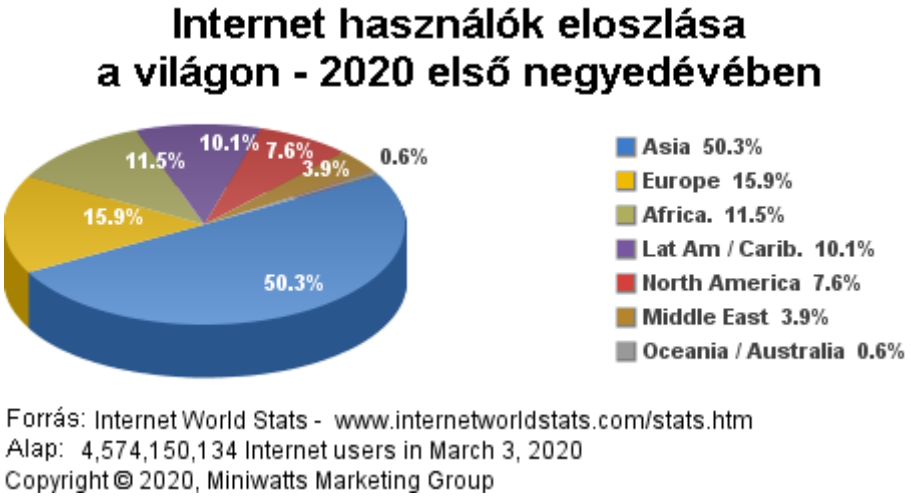
3.2.2 Az elektronikus levélcímek szerepe

Az elektronikus levelezés a történeti leírások szerint valamikor 1965-ben kezdődött, a @ - „at” - jelet 1971-ben RayTomlinson programozó vezette be, aki ezt a karaktert használta a felhasználónevek és a szervercímek szétválasztására. Maga az elektronikus levelezés a kezdetektől nagyon komoly változáson, fejlődésen ment keresztül, de az e-mail cím szerkezete változatlan maradt.

A „www.thegardian.com” e-mail fejlődéséről szóló 2016.03.07-i cikke szerint, 2015-ben 4,4 Mrd e-mail cím volt használatban és naponta 205 Mrd levelet küldtek világszerte. A cikk előrejelzése szerint 2019-re 246 Mrd levélküldésre kerül sor naponta. [69]

A „https://www.emailisnotdead.com” 2019. februári cikke szerint 2018-ban több mint 6,69 Mrd e-mail postafiók volt a világon, amely szám az előrejelzések szerint 2022-re eléri a 7,91 Milliárdot. Naponta 3,83 Mrd ember, összesen 281 Mrd levelet küldött, vagy fogadott. [70]

Az 13. ábra az internet használók földrészek szerinti eloszlását mutatja, és az összegzés alapján 2020. március 03-án 4,57 Mrd internet felhasználó volt a világon. Látható, hogy az internet felhasználói-, és az e-mail címek számában, valamint a levélforgalomban is folyamatos – az előre jelzéseknél gyorsabb – növekedés tapasztalható.

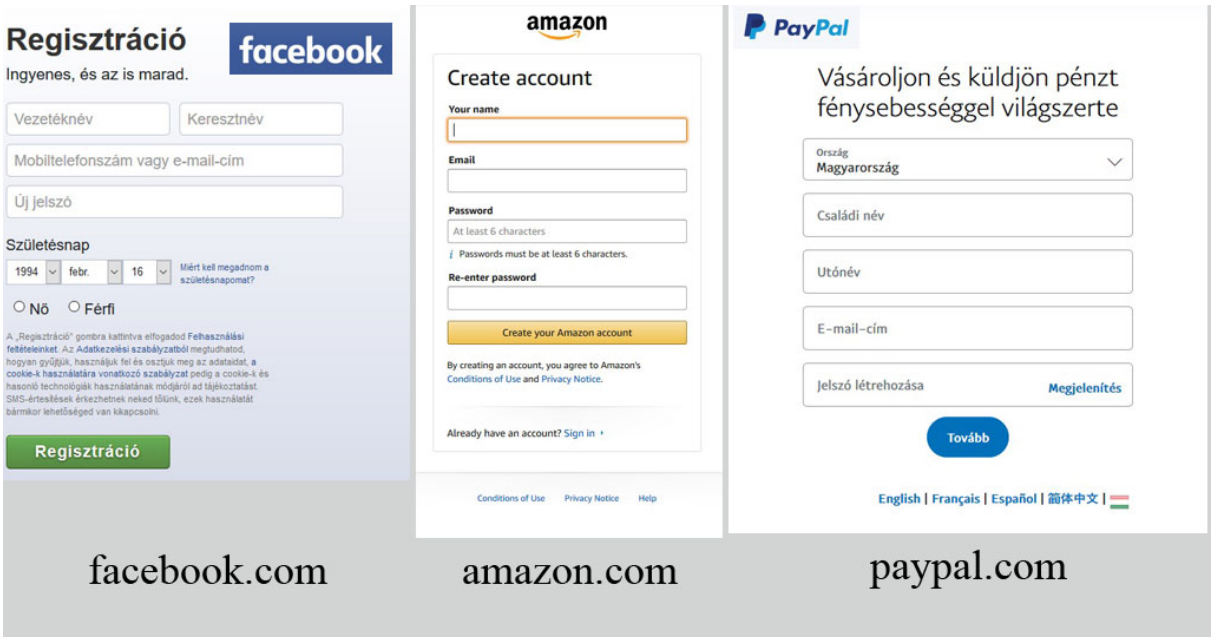


13. ábra; Internet használók a világon 2020-ban

forrás: szerző, https://internetworldstats.com/stats.htm; letöltve: 2020.07.08 [71]

Tényként kijelenthető, hogy az internetet használó embereknek majdnem 2 db e-mail címe van fejenként, amelynek okai az erre irányuló igény és a könnyű hozzájutás. Az e-mail címeket és postafiókokat járulékos szolgáltatásként adják az internet előfizetésekhez, korlátozott tárhellyel ingyen adják az erre szakosodott vállalkozások és az irodákban dolgozók számára legtöbb esetben a munkáltatók is biztosítanak e-mail hozzáférést.

Az elektronikus levelek tartalmának védelme és illetéktelenhez jutásának elkerülése érdekében a postafiók használatát kötelező hozzáférési jogosultsághoz kötni, amelynek leggyakrabban használt módszere a jelszó alkalmazása. A postafiók tulajdonosa az e-mail címmel és a hozzá rendelt jelszó párosával hitelesíti magát, ezáltal a leveleihez hozzáférést-, továbbá a küldéshez és fogadáshoz jogosultságot kap.
Az elektronikus levelezéshez rendelt – kötelező – hitelesítés az e-mail címet a gyakorlatban – mintegy láncfolyamatként – további hitelesítési eljárásokba vonta be. Következményként az internetes, személyhez köthető szolgáltatások regisztrációs folyamatában az e-mail címet a személyes jelenlét nélkülözésére, pótlására használják fel. A regisztrációkor megadott e-mail címre olyan információt küld a szolgáltató, amelynek birtokában a regisztrációs folyamat véglegesíthető, ezáltal az e-mail hitelesítésére támaszkodva, a megkezdett regisztráció az ember személyes jelenléte nélkül, ugyanakkor jóváhagyásával véglegessé válik.



14. ábra; E-mail címek a regisztrációkban

forrás: szerző, a feltüntetett internetes oldalak alapján [72]

A 14. ábra képein látható, hogy a legnagyobb közösségi-, e-kereskedelmi-, és a legnépszerűbb pénzügyi-tranzakciós oldalak regisztrációjához az e-mail cím megadása kötelező, amely később a bejelentkezéshez is szükséges.

A regisztrációs folyamatokból levonható a következtetés, hogy az e-mail címek már nem csupán levelezési postafiókot jelentenek, hanem a köréjük épített egyéb személyes információkkal összekapcsolva, adathalmazban az általuk azonosított személyeket is megtestesítik. A létező e-mail címek birtoklása egyrészt alkalmat ad kapcsolatteremtésre, másrészt az ahhoz társított személyes adatokkal együtt kiváló lehetőséget biztosít célzott marketingre, amely óriási profitszerzéssel kecsegtet. Biztonsági okból előfordul, hogy a bejelentkezési eljárásban az e-mailcím helyett más azonosítót használnak egyes szolgáltatók, a regisztrációban azonban ekkor is rögzítik az elektronikus levelezési címet. Ez az eljárás rejtve tartja a felhasználó e-mail címét, azonban elfeledése bosszúságot is okozhat ritkán használt azonosító esetén.

Figyelembe véve az e-mail címekkel szembeni regisztrációs eljárásokban fennálló többszörös igényt, a felhasználóknak döntést kell hozniuk. Alkalmaznak-e több e-mail címet a különböző internetes szolgáltatások használata során, vagy akár egy e-mail címmel regisztrálnak az összes szolgáltatáshoz. Az előbbinek előnye, hogy az e-mail postafiók feltörése esetén kisebb kár keletkezik, hátránya, hogy a sok e-mailcím miatt több jelszót kell megjegyezni. Az utóbbinál előny, hogy csak egy e-mail postafiók hozzáférését kell megjegyezni, hátrány viszont, hogy minden információ oda fut össze, ezért az ott tárolt adatok felértékelődnek és a postafiók esetleges feltörése jelentős kárt okoz a tulajdonosának.

A meghozott döntéstől függetlenül mindkét esetben visszatérő problémát okoz az e-mail címhez és a szolgáltatáshoz párosított jelszó kezelése. A BitDefender informatikai biztonsági cég 2010. augusztus 09-i tanulmánya szerint 250,000 – interneten online szolgáltatásokból kinyert – e-mail címet vizsgált, amelynek 87%-a valós cím volt és a felhasználók 75%-ban ugyanazt a jelszót használták a közösségi oldalukhoz és az e-mail postafiókjukhoz. [73] Könnyű belátni, hogy mekkora kockázattal jár, ha a szolgáltatási-, köztük a közösségi oldalakon megadott jelszavak megegyeznek az e-mail postafiók használatához alkalmazott jelszavakkal.

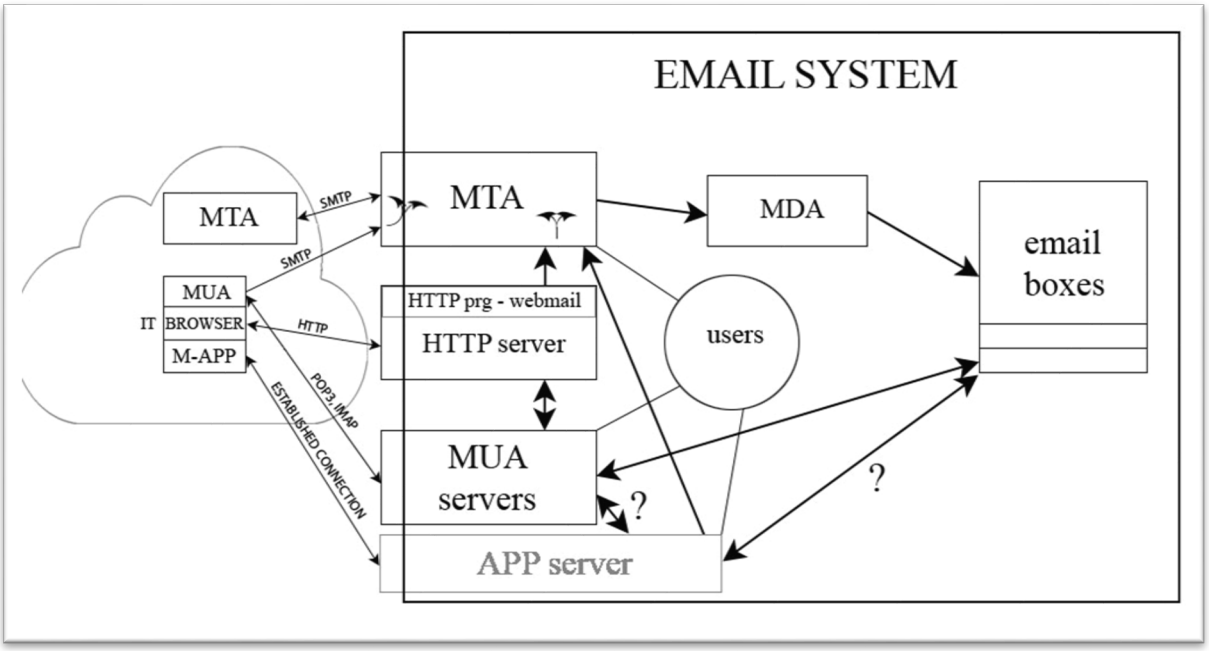
Az e-mailcím korunk elengedhetetlen eszközével, az okostelefonnal is szoros kapcsolatban van, amely működtetése a legnagyobb informatikai szoftveróriások operációs rendszere nélkül szinte lehetetlen. Ahhoz, hogy a kiválasztott operációs rendszer mobiltelefonra írt alkalmazásai és csomagkezelője rendelkezésre álljanak, a szoftveróriás programjait, köztük az előre telepített e-mail alkalmazását is használni kell és postafiók hozzáférést szükséges regisztrálni. Ennek a

kötöttségnek köszönhetően, valamelyik cégóriás levelezési postafiókját is kénytelen lesz használni az okostelefon tulajdonosa. A https://emailmonks.com internetes oldal elektronikus levelezés evolúciójáról szóló cikke szerint, az e-mailcím tulajdonosok leveleiket jelenleg 56%-ban mobil eszközökről, köztük okostelefonról nézik. [74]

A munkahelyen, így a védelmi szférában használt e-mail címeknek is komoly jelentőségük van. A vállalati levelezést azért biztosítja a munkáltató, mert elvárja, hogy a munkával összefüggő – internetes térre kiterjedő – elektronikus kapcsolattartáshoz, levelezéshez azt használja is a dolgozó. Ez magával vonja annak szükségességét, hogy a rendszerbe állított levelezőszerver a céges hálózat mellett internetkapcsolattal is rendelkezzen, továbbá amennyiben érdeke a munkáltatónak, úgy távoli e-mail hozzáférést is biztosítson a dolgozónak, hogy adott esetben otthonából is tudja elektronikus leveleit kezelni. A rendvédelmi szervek internetkapcsolattal rendelkező szerverei, így a levelezőszerverek is a szabályoknak megfelelően kormányzati szintű informatikai biztonsági védelem alatt állnak, azok elkülönített IP címtartományokban, a „gov.hu" felsőbb szintű domain alatt, aldomain-ba rendezve működnek. A kiépített biztonsági rendszerben is nehéz védekezni a felhasználói hanyagságok ellen. Jellemző probléma a rendvédelmi e-mailcímek magáncélú használata, továbbá a fentebb említett jelszóegyezőség. Rendszerszintű gyenge pont továbbá, ha a rendvédelmi e-mailcímben a felhasználói rész egyben bejelentkezési azonosító is a szervezet informatikai rendszeréhez, s ha még az alkalmazott jelszó is megegyezik, akkor a levelezési postafiók feltörésével egyben az informatikai rendszerhez is belépési jogosultság szerezhető. További gyengítő tényező, ha a védelmi szférában használt szervezeti e-mail postafiók levelei – az információ hatékonyabb feldolgozása érdekében, – automatikusan továbbításra kerülnek valamelyik okostelefon-kompatibilis levelező rendszerbe, hogy azt annak tulajdonosa a beérkezést követően azonnal láthassa.

3.2.3 A levelezőrendszer felépítése

Levelezőrendszernek (EMAIL SYSTEM) a levelezőszerver, az ügyfélkiszolgáló, valamint a velük együttműködő azon alkalmazások tekinthetők, amelyek kiesése az elektronikus levelek küldését és kezelését részben, vagy egészében ellehetetlenítik.



15. ábra

Levelező rendszer felépítése; forrás: szerző

Kritikus Internetes Szolgáltatásnak a levelezőrendszer elektronikus levelekkel kapcsolatos küldési és fogadási szolgáltatásai minősülnek.

A levelezőprogram – mint kliensalkalmazás – nem része a levelezőrendszernek, ugyanakkor tény, hogy nélkülözhetetlen összetevője az elektronikus levelezésnek.

Levelezőszerver (MTA[90])

Feladata az elektronikus levelek küldése, fogadása és továbbítása a levelezési postafiókokba. Kiszolgáló típusú alkalmazás, tevékenységet csak levelezőprogrammal, vagy másik levelezőszerverrel együttműködve képes végezni. A levelezőrendszer központi programja, lelke, nélküle nincs elektronikus levelezés. Üzemképtelenné válása esetén az elektronikus levélforgalom megszűnik.

[90] Message / Mail Transfer Agent

Ügyfélkiszolgáló (MUA[91] server)

A levelezőprogramok részére biztosítja a levelezési postafiókokban – levelezőszerver által – elhelyezett elektronikus levelek kiolvasását, karbantartását. Általában POP[92], vagy IMAP[93] protokollok szerint kommunikálnak a levelező programokkal és a levelek olvasása mellett azok rendszerezésére, karbantartására is lehetőséget biztosítanak. Általában a levelezőszervertől függetlenül, önállóan működő kiszolgáló program, kiesésével a postafiókokban tárolt elektronikus levelek elérhetősége hiúsul meg.

Levélkézbesítő (MDA[94])

Egy háttéralkalmazás, amelynek az elektronikus levelek lokális kézbesítése, azaz postafiókba helyezése a feladata. A fejlettebb levelezőszerverekbe általában beépítésre kerül, azonban előfordul, hogy különálló alkalmazásként képezi a levelezőrendszer részét.

Web kiszolgáló (HTTP[95] server)

A levelezőrendszerben a webmail alkalmazás kiszolgálását végzi, amely egyébként bármely Web típusú szolgáltatás nyújtására is alkalmas. A levelezőszerverhez és az ügyfélkiszolgálóhoz kliensként, a hozzá illesztett Webprogramok végrehajtására képes modullal (HTTP prg.) kapcsolódik, így a levelezőrendszerben alrendszeri elemként funkcionál. Sikeres authentikációt követően, a Web kiszolgáló részére a levelezőszervernek biztosítania kell az elektronikus levelek továbbítási lehetőségét.

Kiesésével önmagában az elektronikus levelek Web alapú olvasása és kezelése hiúsul meg, egyébként a levelezőrendszer többi része tőle függetlenül működőképes.

Applikáció kiszolgáló (APP server)

A mobilapplikációk térnyerésével vált igazán a levelezési rendszer részévé, az okos eszközökön futó levelező alkalmazások kiszolgálása a feladata. Ezen szolgáltatást általában az applikáció gyártója a levelezés biztosítása érdekében üzemelteti, így annak pontos működése a nyilvánosság előtt nem ismert. A hálózat analizátorok eredménye alapján az applikáció kiszolgáló egy biztonságos kommunikációs csatornát biztosít az applikációk részére, amelyen

[91] Mail User Agent
[92] Post Office Protocol – posta protokoll
[93] Internet Message Access Protocol - Internetes üzenet-hozzáférési protokoll
[94] Mail Delivery Agent
[95] HyperText Transfer Protocol

a saját protokoll szerinti azonosítást követően, állandó kapcsolat jön létre a kiszolgáló és a levelező alkalmazás között. Az applikáció kiszolgáló kiesése esetén a levelezőrendszer a hagyományos protokollokkal továbbra is működőképes, egyébként ellehetetlenül.

3.2.4 Levelezőprogramok

Olyan programok, amelyek fő funkciói az elküldendő elektromos levelek szerkesztése és közvetlenül, vagy közvetetten

- átadása a levelezőszervernek továbbításra,
- a levelezőrendszer e-mail postafiókjába érkezett levelek olvasása, rendszerezése, karbantartása.

A levelező programok – a levelezőszerverekkel együtt – folyamatosan fejlődnek, az alapfunkciók mellett egyre több kényelmi szolgáltatást nyújtanak. Két fő kategóriába sorolhatók, egyrészt a felhasználók IT[96] eszközein futó önálló alkalmazások, másrészt böngészővel megjeleníthető Webmail programok.

Klienseszközön futó levelezőprogramok

Napjainkban az IT eszközök nagyon sokrétűek, számos, különböző architektúrán, különféle operációs rendszerrel működnek. A teljesség igénye nélkül lehetnek személyi számítógépek, notebook-ok, notepad-ek, okos telefonok és okos eszközök, amelyek közül a hálózati kapcsolattal rendelkező modellekre – szinte kivétel nélkül – létezik levelezőprogram.

A levelezőprogramok piacán is verseny van a felhasználókért, az operációs rendszer gyártók legtöbbször maguk biztosítanak alkalmazást az elektronikus levelek kezelésére és természetesen önálló, akár ingyenes programok is rendelkezésre állnak a kínálatban. A fejlesztők a jobb kinézettel, a kényelmesebb kezelhetőséggel, az extra szolgáltatásokkal és a magasabb biztonsági szint elérésével igyekeznek megnyerni maguknak a felhasználókat.

1. Hagyományos protokollokkal kommunikáló levelező programok

Az elektronikus levelezés hagyományos protokolljai szerint kommunikálnak a levelezőszerverrel és az ügyfélkiszolgálóval; levélküldéshez SMTP[97], levélolvasáshoz POP, vagy IMAP biztosítja az együttműködést. Grafikus és karakteres megjelenésű verziók egyaránt léteznek, igazodva az operációs rendszerek specifikumához, adottságaihoz. Alkalmazásuk

[96] Information Technology – információ technológia
[97] Simple Mail Transfer Protocol

során a kiszolgálókkal csak a küldési - fogadási tranzakciók ideje alatt történik kommunikáció. A különböző változatok között lényegi különbséget jelenthet a titkosított csatornák használatának a képessége, valamint az azonosítási metódushoz használt felhasználónevek és jelszavak tárolásának a módja. E programokra jellemző a kötetlenség, hisz a felhasználók szabadon dönthetnek a levelezőszerver és az ügyfélkiszolgáló-, valamint a hozzájuk történő kapcsolódás beállításairól. Népszerűek és a nagy fejlesztői támogatás miatt viszonylag egyszerű házilag is levelező alkalmazást készíteni.

Jellemzőik:

- a fogadott levelek részben, vagy egészben letöltődnek az eszköz háttértárolójára, ezért a későbbiekben internet kapcsolat nélkül – akár fájlkezelővel – is megtekinthetők;
- általában több postafiók párhuzamos, korlátlan kezelése is biztosított, amelyekhez külön levelezőszerver és ügyfélkiszolgáló is beállítható;
- a küldendő levél szerkesztése és formázása a levelezőprogrammal történik, amely csak a küldéskor hagyja el az eszközt;
- kényelmi szolgáltatásként a postafiókhoz rendelt beállításokat elég egyszer elvégezni, mentés után az azonosító adatokat megjegyzi a program, így a küldés – fogadás automatikussá tehető;
- a kliens eszköz fertőzöttsége esetén a program – és ezáltal a levelezőszerver is – kitetté válik.

2. Saját protokollal működő levelezőprogramok (M-APP)

Elsősorban az okos telefonokra és okos eszközökre készített levelező applikációk tartoznak ebbe a körbe, amelyek internetes szerverhez titkosított csatornán kapcsolódnak és saját – nem nyilvános – protokoll szerint kommunikálnak. Ezen programok használata kötöttségen alapul, amelyet a felhasználók az alkalmazás során elfogadnak. Az okos telefon-, vagy eszköz operációs rendszerének teljes értékű használatához elengedhetetlen a szolgáltató weboldalán regisztrálni, amely adatokkal, az eszközre előtelepített levelező-applikáció képes a kiszolgálóhoz kapcsolódni, valamint e-maileket küldeni és fogadni. Az okos eszközök személyhez kötöttsége vitathatatlan, hisz kis helyen elférnek, használóik általában maguknál tartják, ezért az elektronikus levelek kezeléséhez a legoptimálisabb kényelmi eszköz. Felmérés [75] alapján napjainkban több mint 3 Mrd okostelefon van használatban, amely – a kötöttségek ellenére is – magyarázat a levelező applikációk használatának dinamikus növekedésére. A felhasználók leveleiket közvetlenül, a zsebükben, vagy táskájukban tárolt okos eszközeik

segítségével képesek kezelni és szinte időveszteség nélkül –, perceken belül – láthatják bejövő üzeneteiket.

Jellemzők:

- csak az okos eszköz internetes kacsolódása esetén küldhetők-, és olvashatók elektronikus levelek;
- csak a szolgáltató szerveréhez lehet kapcsolódni az applikációval, amelyen a felhasználó nem tud módosítani;
- a kapcsolódás módját és a kommunikáció titkosítását a fejlesztő egyedileg határozza meg;
- az applikáció állandó és folyamatos kapcsolatban van-, és kommunikál a kiszolgálóval, ezért az érkező levelek azonnal láthatók;
- az alkalmazás fejlesztője és a kiszolgáló üzemeltetője általában azonos;
- kiemelten nagy hangsúlyt fektetnek a kommunikáció-, és a levelezés biztonságára;
- általában képesek a hagyományos protokollok szerint is kommunikálni, amely esetben a felhasználónak kell a beállításokat elvégezni.

Webmail

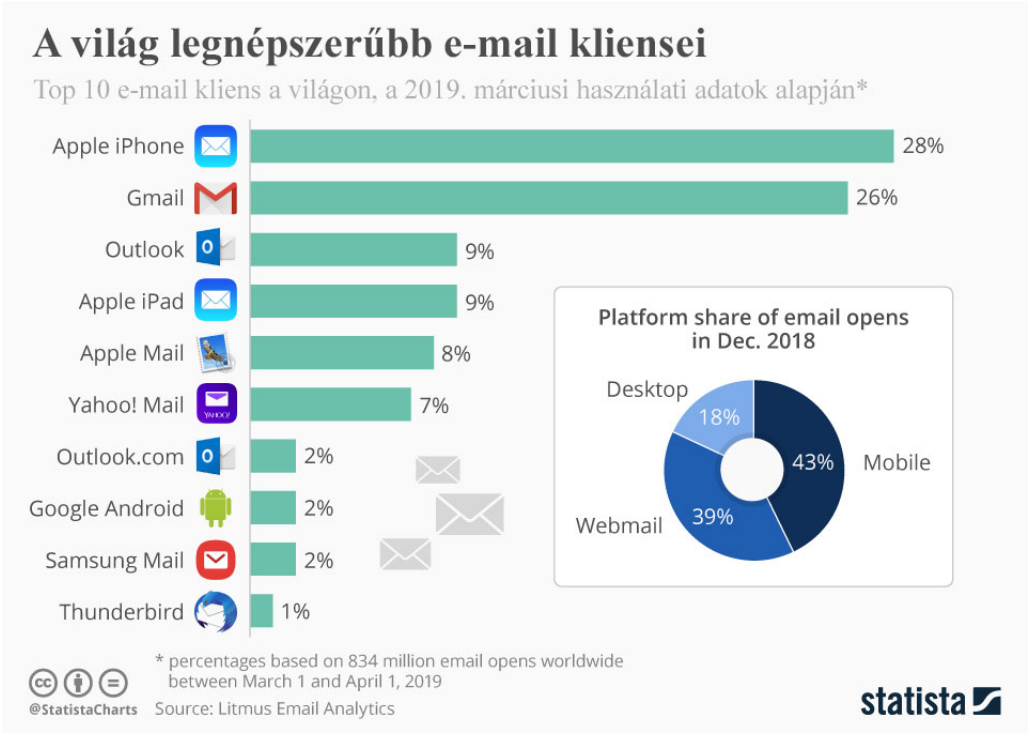
Működése rendhagyó, önmagában is különálló szolgáltatáson alapul, hisz a webmail alkalmazást a böngészés pillanatában egy webszerverbe (HTTP server) integrált program (HTTP prg.) dinamikusan állítja elő, amelyet a felhasználó böngészője (BROWSER), a felhasználó IT eszközén megjelenít.

A felhasználó csak közvetetten van kapcsolatban a levelezőszerverrel és az ügyfélkiszolgálóval, az összeköttetést a webmail alkalmazás biztosítja, amely ebben az összetételben egyben a levelezőrendszer kliens alkalmazása és az ügyfelek webkiszolgálója. Működési elve alapján a felhasználó a böngészője segítségével HTTP protokoll szerint kommunikál a webszerverrel és ad az elektronikus levelek kezelésére utasításokat, amelyeket a webmail alkalmazás a levelezőszerver felé SMTP-, az ügyfélkiszolgáló felé IMAP és POP protokollokkal teljesít. A webszerver és a levelezőrendszer lehet fizikailag közös-, vagy külön hardveren, operációs rendszeren, azonban az összeköttetést mindkét esetben biztosítani kell.

Jellemzők:

- a webszerver kritikus alrendszere a levelezőrendszernek, nélküle a webmail szolgáltatás nem működne;
- a böngésző és a levelezőrendszer közvetett kapcsolata miatt, levélküldéshez és a levelek kezeléséhez felhasználói interaktivitás szükséges, ami növeli a biztonságot;
- a fogadott levelek automatikusan nem töltődnek le a felhasználó IT eszközének háttértárolójára, ezért azok megtekintéséhez internetes elérhetőségre és a webmail alkalmazásra szükség van;
- a kliens eszköz fertőzöttségének a levelezőrendszer kevésbé kitett;
- a webmail alkalmazásnak az – elektronikus levelek védelméhez szükséges – azonosítási metódushoz igazodnia kell;
- több postafiók egyidejű kezelése kötöttségekkel terhelt;
- a webszerver levelezőszerverrel és ügyfélkiszolgálóval történő összekapcsolása és hangolása a szervereket üzemeltető feladata, azon a webmailt használó ügyfél nem képes módosítani, ami azt is jelenti, hogy aki képes a webmailre belépni, levelet is tud küldeni.

Levelezőprogramok megoszlása



16. ábra

E-mail kliens megoszlások [76]; letöltve: 2019.08.25

Az 16. ábrán látható 2019. márciusi –, internetes levelezésre vonatkozó – felmérés szerint, az e-mail kezelés 43%-ban mobil eszközről, 39%-ban Webmail alkalmazásról és 18%-ban munkaállomásról történik, különböző e-mail alkalmazások szerinti bontásban. Természetesen a zárt vállalati-, vagy magán levelezések elérései nem tartoznak a felmérésbe, ugyanakkor a biztonságra is nagy hangsúlyt fektető nyílt levelezőrendszerek elérései irányt mutatnak és követendők. Összességében 82%-ban a levelezőrendszer alrendszereként működő web-, és alkalmazásszerver szolgáltatások biztosítják az elektronikus levelezést az ingyenesen elérhető térben. A levelező alkalmazásokban tapasztalható tolódás is egyértelmű, az okos eszközökön futtatható applikációk nagy előnnyel vezetnek ebben a versenyben.

3.2.5 Az elektronikus levelezés biztonsága

A levelezőszervernek az internet valamely hálózati pontjaként kell működnie, egyébként alkalmatlan lenne a világhálón elektronikus levelek fogadására, vagy küldésére.

Az elektronikus levelezés biztonságát meghatározza a környezet szoftveres stabilitása, az operációs rendszer és a levélkiszolgáló program támadhatósága, továbbá a levelezési szolgáltatás rosszindulatú felhasználásának és kihasználásának lehetősége.

A levelezési környezet szoftveres stabilitása

Az elektronikus levelező rendszer környezetének stabilitása függ

- az alkalmazott operációs rendszer stabilitásától,
- az alkalmazott levélkiszolgáló program és a vele funkcionálisan összekapcsolt alrendszeri elemek robusztusságától, stabilitásától,
- a megfelelő hangolástól.

A levelezőrendszer támadható

- operációs rendszeren keresztül;
- a levelezőrendszer alrendszereként működő szolgáltatásokon, programokon keresztül;
- az egyazon szerveren működő másik szolgáltatásokon keresztül.

A levelezési szolgáltatás rosszindulatú felhasználása és kihasználása

A kibertérben végrehajtott rosszindulatú tevékenységnek kulcsszereplői a „hétköznapi felhasználók”, akik célpontjai, vagy eszközei lehetnek a bűnözőknek. Egyrészt meg lehet őket károsítani, másrészt hasznos információkat lehet tőlük kicsalni a további célpontok eléréséhez,

harmadrészt pedig információs eszközeik erőforrásait fel lehet használni összehangolt kibertámadások végrehajtásához.
Ezen műveletekhez – első lépésként – elengedhetetlen a kapcsolatteremtés az emberekkel, amelynek legkézenfekvőbb eszköze az elektronikus levél, hisz lehetővé teszi a küldő részéről az anonimitást, tartalmába bármi beágyazható, ami a megtévesztéshez, az információ kinyeréséhez, vagy az informatikai eszköz hatalomba vételéhez szükséges.
A levelezési szolgáltatás felhasználásának és kihasználásának mozgatója tehát nem más, mint a célpontként kiszemelt, lehető legnagyobb számú áldozattal történő kapcsolatteremtés. A rosszindulatú tevékenységet folytatók mérhetetlen számú elektronikus levelet igyekeznek kiküldeni a cél elérése érdekében, gondolván, hogy a nagy számok törvénye értelmében lesznek olyan megtéveszthető emberek, akik elhiszik a levél tartalmában foglaltakat, vagy óvatlanul egyes kéréseknek eleget tesznek, így áldozattá válhatnak. Napjainkban a valós elektronikus levelezési címek adatbázisai értéket képviselnek, emberek akár fizetni is hajlandók érte, sőt megszerzésük is kibertámadás tárgyát képezi. Rosszindulatú felhasználás, vagy kihasználás során az egyik legnagyobb érték a minél nagyobb számú valós e-mail cím ismerete.

A levelezési rendszer rosszindulatú felhasználásának, vagy kihasználásának azt a tevékenységet tekintem, amikor a levelezési szolgáltatás rendeltetésszerű használatával, a rendelkezésre álló, üzemszerű funkciók alkalmazásával, rosszindulatú tevékenységet folytat a szolgáltatást igénybe vevő személy.

Az elektronikus levelezési szolgáltatással szemben minimum elvárás:

- az állandó rendelkezésre állás,
- a levelekhez történő korlátlan hozzáférés,
- az érkező levelek fogadása,
- a küldésre szánt levelek célba juttatása.

Ezeknek a minimum elvárásoknak a teljesítése, megfelelő táptalajt ad a rosszindulatú felhasználás, vagy kihasználás folytatásához, hisz a levelező rendszer, mint eszköz rendelkezésre áll.

A levelezőszerver működésében két fontos terület elkülönül. Az input, mint bemeneti egység, amely az érkező levelek fogadását, az output, mint kimeneti egység pedig a küldendő levelek kibocsátását végzi. A szerver inputján keresztül fogadja az érkező elektronikus leveleket és az

e-mail postafiók rendelkezésre állása esetén elhelyezi azt a tárterületen, egyébként outputján keresztül továbbítja a címzett domain-ja szerinti levelező szervernek.

1. „Nyitott biztonsági rés”

A levelezőszerver egyike azon kiszolgáló programoknak, amelyek segítségével rendeltetésszerűen át lehet mozgatni adatokat egyik IT eszközről a másikra. A „nyitott biztonsági rés” némileg rendhagyó állítást már a definiált működés is részben alátámasztja:

„Feladatuk, hogy a rendszeren keresztül automatikusan eljuttassák az e-leveleket a feladótól a címzettig az SMTP (Simple Mail Transfer Protocol — egyszerű levéltovábbító protokoll) segítségével. Ez az üzenettovábbítási lépés.” [68]

Az automatizmus azt jelenti, hogy a feladótól a címzettig feltétel nélkül eljuthatnak az elektronikus levelek. A kiszolgálás és szolgáltatás közötti különbség éppen a feltételhez kötöttségben mutatkozik meg, amelyből látszik, hogy a levelezőszerver inkább az első kategóriába tartozik.

Az elektronikus levelezési címmel rendelkező felhasználók, azaz a postafiókok tulajdonosai lehetőséget adnak levelek fogadására és elvárják, hogy a részükre küldött e-mail-eket megkapják. Ezen – némileg – jogos elvárás teljesítése érdekében, a levelezőszervernek feltétel nélküli, levélfogadásra alkalmas kiszolgálóként kell működnie. Az üzenet kézbesítésekor a címzett a levelet postafiókjába megkapja, azaz a levelezőszerver tárhelyére az adattartalom fizikailag elhelyezésre kerül. Leegyszerűsítve a levél küldője legálisan, egyszerűen – az SMTP protokolljával – képes adatokat egy adott szerverre eljuttatni, mert a levelezőszerver működtetése alapértelmezésben levelek fogadásának feltétel nélküli biztosítása.

Ezen mechanizmust a rosszindulatú tevékenységet folytatók képesek az ezirányú szándékuk kivitelezésére felhasználni, hisz az elektronikus levélcímek birtokában oda kártékony kódokat, vagy a saját céljaik elérését segítő megtévesztő leveleket tudnak rövid idő alatt is, kis befektetéssel eljuttatni. Az informatikai rendszerekkel szembeni rosszindulatú tevékenységnek egyik sarokpontja az adott célrendszer biztonsági réseinek feltárása, ezért az elektronikus levelezők ezen alapértelmezett „biztonsági rése” kézenfekvő megoldás a támadások előkészítésére.

Természetesen ezt a „biztonsági rést” nem célszerű – teljesen – nyitva hagyni, kontrolljára számos lehetőség mutatkozik, amelyek alkalmazása a levelezőrendszert működtető hatásköre.

Az e-mail címmel rendelkező felhasználók másik jogos elvárása, hogy képesek legyenek elektronikus levelek küldésére. Teljesen helyénvaló ez a folyamat mindaddig, amíg a továbbítás

nem kéretlen, fertőzött levelek küldésére szolgál. Ezen rosszindulatú tevékenységet folytatók célpontjai lehetnek azon hétköznapi felhasználók, akiknek jogosultságait felhasználva, a helyükbe lépve fertőzött levelek tucatját küldik ki, gyakran az érintett felhasználó tudta nélkül. Látható, hogy egy levelező szerver célpontként és eszközként egyaránt szolgálhat, amellyel szemben védekezni szükséges, ellenkező esetben az elektronikus levelezési szolgáltatás rövid időn belül ellehetetlenül, elbukik.

2. Rosszindulatú felhasználás

Az elektronikus levelezés rosszindulatú felhasználása, amikor a levelező szerver bemenetére malware[98], vagy spam[99] érkezik, amelynek célpontja valamely elektronikus postafiók. Önmagában tehát a rosszindulatú tartalommal bíró levél célba juttatását jelenti, amely csatolmányként programtípusú-, vagy megtévesztő, szöveg alapú malware-t tartalmazhat.
Figyelembe véve, hogy a postafiók tulajdonosok leveleiket kliens alkalmazással kezelik, a malware-t küldők célja lehet:

- a kliens gép – rosszindulatú programkód futtatásával történő – teljes, vagy részleges hatalomba vétele;
- megtévesztéssel, vagy programkóddal információ kinyerése.

A levelek szöveges részében megtévesztő tartalommal – általában banki – adatok megadására, fertőzött webhely meglátogatására, vagy egyéb cselekmény végrehajtására próbálják rábírni a levél fogadóját.

A teljesség igénye nélkül e-mailben az alábbi malware-k küldhetők [77]:

- vírusok;
- programférgek;
- ransomware-ek;
- trójai programok;
- backdoor programok;
- dropperek;
- spyware-ek;
- keylogger-ek;

[98] malicious software – rosszindulatú szoftver
[99] kéretlen levél

- adware-ek;
- scareware-ek.

A rosszindulatú felhasználás elsődlegesen akkor eredményes, ha a levél belépve a levelezőszerverre, eljut a címzett postafiókjába, másodlagosan pedig akkor, ha a postafiók tulajdonosát sikerül megtévesztenie, vagy a rosszindulatú kód futtatására rábírnia. Ezen tevékenység folytatásához bármilyen létező és e-mail küldésére alkalmas postafiók használható, a kijuttatás lehet manuális, vagy programozott. Sok esetben önmagában a rosszindulatú felhasználás, további e-mail címek megszerzésére irányul.

3. Levelezési szolgáltatás kihasználása

A levelezési szolgáltatás kihasználásának tekintem, amikor adott levelező szerver kimenetét – leginkább rosszindulatú felhasználás érdekében – veszi igénybe a tevékenységet folytató. A kiszemelt levelezőszerver erőforrásait a fertőzött levelek – elsősorban a világháló irányába történő – kiküldésével használja ki, célja adott időintervallum alatt minél nagyobb számú levél kijuttatása. Általában valamely küldésre jogosult kliens azonosítójának és jelszavának együttes megszerzésével és felhasználásával, az azonosító eredeti tulajdonosának nevében eljárva valósul meg.

„Miután a küldő levéltovábbító ügynök megkapta a levelet a felhasználói ügynöktől, kézbesíti azt a fogadó levéltovábbító ügynöknek az SMTP segítségével.

A megfelelő levelezőszerverrel való kapcsolatfelvétel érdekében meg kell kérdezni a DNS[100]-t.

A válasz egy rendezett lista lesz, amely egy vagy több levelezőszerver nevét és IP[101]-címét tartalmazza.

A küldő levéltovábbító ügynök ezután létrehoz egy TCP[102]-összeköttetést a 25-ös porton lévő levelezőszerver IP-címére, hogy elérje a fogadó levéltovábbító ügynököt, és az SMTP-t használva továbbítja az üzenetet.” [78]

A levelezőszerver tehát a küldendő leveleket az általa kezelt fiókok esetében saját hatáskörön belül kézbesíti, egyébként DNS alapján megkeresi az érintett másik levelezőszervert és az azzal történt kapcsolatfelvételt követően, SMTP protokoll segítségével, kézbesítés céljából továbbítja

[100] Domain Name Server - névszerver
[101] Internet Protocol
[102] Transmission Control Protocol

azokat. A rosszindulatú kihasználás ezt a továbbító funkciót célozza meg és kellemetlen következménye, hogy a kéretlen, vagy fertőzött levelek küldéséért – a küldő személytől függetlenül – a szerver felelős.
A levelezőszerver SMTP alapú megszólítása és levél küldése egyaránt lehetséges programozottan automatikusan, vagy felhasználói beavatkozáshoz kötötten, ugyanakkor az adott idő alatt kiküldött levelek számának maximalizálása és egyben a szerver kihasználására az automatizált levélküldés az optimális. A küldőprogram készülhet bármilyen program-, vagy szkript nyelven amely ismeri az SMTP protokollt és egyaránt lefuthat a levelezőszerveren, vagy az ahhoz kapcsolódó kliens eszközön. Magán a levelezőszerveren, annak tesztelése és karbantartása miatt alapból rendelkezésre állnak azok a programok, amelyekkel levelet lehet – akár programozottan is – küldeni, ezért a levelezőszerver sikeres támadásával és operációs rendszerének hatalomba-, vagy használatba vételével a levelezés kihasználása is megvalósítható.

A kliens eszközről érkező levéltovábbító kérések levelezőszerver általi végrehajtását angolul SMTP Relay-nek nevezik. A levelezőszerveren meg kell határozni, hogy a Relay funkciót milyen feltételek teljesülése esetén hajtsa végre. Beállítható, hogy mely hálózati címekről érkező kérések, milyen felhasználói azonosítás mellett kerüljenek továbbításra, amely azonosítási metódust a levelező programokban is le kell követni. A kliensen meghatározandó a továbbító SMTP szerver címe, és amennyiben van felhasználói azonosítás, úgy azt – ami jellemzően felhasználó név és jelszó – is be kell állítani. Webes levelezőkliens esetén a levelezőszerverhez illesztés a weboldal működtetőjének-, kliens eszközön futó levelező programban az alkalmazás felhasználójának a feladata.

a) Open relay
A levelezőszerver azon beállítását és működését jelenti, amikor a vele SMTP kapcsolatba lépő kliens leveleit felhasználói azonosítás nélkül továbbítja a levél címzettjének. Ez a beállítás általában figyelmetlenség következménye, vagy ritkán szándékos ezirányú konfigurálás. Tekintettel arra, hogy az „open relay” szerverekkel korlátlan lehetőség van – akár fertőzött – levelek anonim küldésére, a rosszindulatú tevékenységet folytatók előszeretettel keresik ezen levélküldő eszközöket az interneten.

b) Auth relay

A levelezőszerver a vele kapcsolatba lépő kliens leveleit feltételhez-, felhasználó név és jelszó párosához kötötten továbbítja. A Relay-hez használt azonosító és jelszó párosa beállítástól függően bármi lehet, de kényelmi okból leggyakrabban magát az e-mail címet és a hozzá beállított jelszót alkalmazzák az üzemeltetők.

A levelezőszerver Auth relay-en keresztül történő kihasználása valamely, továbbításhoz alkalmazott azonosító és jelszó ismeretében lehetséges, amennyiben azt a rosszindulatú tevékenységet folytató megszerzi, majd az eredeti tulajdonosnak álcázva magát fertőzött leveleket küld ki. Az Auth relay-re feljogosító azonosító – jelszó páros megszerezhető a levelezőszerverről, a levelező programot futtató kliensről, illetve az azonosítási folyamat közben a levelezőszerver-, és kliens között a hálózatról. A levelezőszerverről és a levelezőprogramot futtató eszközökről azok támadhatósága esetén nyerhetők ki az információk.

A kliens és a szerver közötti azonosítás folyamata az úgynevezett SMTP AUTH[103], amely az eredeti SMTP protokoll kiterjesztett – Extended SMTP – változatában került jóváhagyásra. A számos azonosítási mechanizmus közül a legismertebbek a PLAIN, LOGIN és MD5 típusok, de általánosságban igaz, hogy a köztük levő különbséget csak a felhasználó azonosító és jelszó kódolása, valamint a kódokból összeállított csomag elküldése jelenti. Természetesen a levelezőszerveren beállított azonosítási mechanizmust a kliens programnak is ismernie kell az együttműködéshez, egyébként az azonosítás nem jöhet létre.

A továbbító funkcióval, vagy a levelezőszerverről direktben egyaránt megvalósítható a kihasználás. Amennyiben a levelezőszerver és a levelezőprogram közötti kommunikáció titkosítatlan, úgy az azonosítási mechanizmustól függetlenül az elküldött adatok a hálózaton lehallgathatók, továbbá a felhasználó név és jelszó párosa kikövetkeztethető, amely birtokában a kihasználás létrejöhet. A kliens eszközön futtatott – akár kártékony – program segítségével, a levelező alkalmazás felhasználói beavatkozás nélküli, programozott e-mail küldésére bírható rá.

A titkosítatlan csatornán használt webmail alkalmazást a hálózaton szintén le lehet hallgatni, megszerezve a postafiókhoz hozzáférést jelentő felhasználó nevet és jelszót. Figyelembe véve, hogy a webmail alkalmazás és a levelezőszerver közötti auth relay előre konfiguráltan

[103] SMTP kliens hitelesítés [14]

biztosított, a hozzáférést megszerzőnek megnyílik a lehetősége a levelezőszerver kihasználására.
A levelezőszerver kihasználása lehet közvetlen kapcsolódással megvalósított online kihasználás, vagy a kliens eszköz megfertőzésével és azon kártékony program futtatásával megvalósítva offline kihasználás.

3.2.6 A levelező védelmi ajánlásai

A felhasználók napjainkban a levelező rendszerrel szemben – további – igényként fogalmazzák meg

- a kéretlen (SPAM) és a fertőzött levelek jelzésének, kezelésének lehetőségét, továbbá,
- a kliens-, és a Webmail alapú hozzáférés együttes megvalósulását,

amelyek egyrészt védelmi-, másrészt kényelmi igények.

A védelmi igények az idők folyamán alakultak ki és tekinthetők egyfajta önvédelmi reakciónak a korábbi negatív felhasználói tapasztalatokra, „élményekre". A védelmi igények kielégítésére szolgáló eszközök egyaránt foganatosíthatók a levelezőszerveren, vagy a kliens eszközön, ugyanakkor a KRISZ definíciója, valamint a kliensek szabadsága és nagy száma miatt a megfogalmazott védelmi ajánlások a levelezőszerverre koncentrálódnak. A levelezőszerver működésének fontosságára és betöltött szerepére tekintettel, a védekezést központilag úgy kell megvalósítani, hogy a kliens eszközök összetételétől és fertőzöttségétől függetlenül a levelezés biztonsága, mint kedvező állapot fennmaradjon. Fontos ugyanakkor megjegyezni, hogy a kliens eszközök biztonságának megteremtése legalább annyira kiemelt feladat, mint a levelezőszerver biztonsága, továbbá, hogy a fertőzött eszközökről küldött, vagy azon fogadott levelek számának növekedése egyenesen arányosan növeli a levelezőszerver – biztonság érdekében végzett – védelmi munkájának mennyiségét és erőforrásainak felhasználását.
A felhasználók védelmi és kényelmi igényei egymásra ellentétes hatást kiváltó folyamatok, hisz visszás úgy kényelmi szolgáltatást nyújtani, hogy a védelem egyidejűleg ne szenvedjen hátrányt. A telepített és alkalmazott védelmi intézkedések egyben befolyásolják a levelezési szolgáltatással szembeni minimum elvárások teljesülését, hisz előfordulhat, hogy bizonyos levelek nem érkeznek meg, vagy nem kerülnek kiküldésre, érzékenyen érintve a felhasználók elvárásait, befolyásolva komfort zónáját.
Alapértelmezésben a levélkiszolgáló feladótól és tartalomtól függetlenül minden érkező levelet fogad és azokat megpróbálja kézbesíteni, valamint a küldendő leveleket küldőtől, gyakoriságtól

és tartalomtól függetlenül megpróbálja továbbítani. Könnyen belátható, hogy az alapbeállítással a levelezőszerver feltétel nélküli kiszolgálóként működik, a leveleket megpróbálja az e-mail postafiókba eljuttatni, akár kéretlen, vagy fertőzött levelek továbbító eszköze, spammer is lehet.

Az elektronikus levelezőrendszer biztonságos működésének feltétele a megfelelő védelmi intézkedések alkalmazása, amely a fenti megfogalmazásnak megfelelően a

1. a szoftveres környezet stabilitásának fenntartásával,
2. az operációs rendszer és a levélkiszolgáló program támadhatóságának megakadályozásával,
3. a levelezési szolgáltatás rosszindulatú felhasználásának és kihasználásának megakadályozásával

érhető el, feltételezve, hogy a szoftverek működtetéséhez szükséges hardver elemek hiánytalanul, elegendő kapacitással rendelkezésre állnak.

A levelezőrendszer szoftveres stabilitásának biztosítása

A stabilitást befolyásolja

- az alkalmazott operációs rendszer stabilitása;
- az alkalmazott levélkiszolgáló program és a vele funkcionálisan összekapcsolt alrendszeri elemek stabilitása, együttműködése;
- a levelezőrendszer hangolása (CPU-hoz viszonyított munkaigény).

1. Alkalmazott operációs rendszer stabilitása

Tekintettel a levelezési szolgáltatás kliens - szerver alapú működésére, elengedhetetlen valamely nagy rendelkezésre állással bíró, hálózati operációs rendszer alkalmazása, amelynek a levelezési szolgáltatást igénybe vevő felhasználók számától függetlenül, biztosítania kell a szoftveres környezetet. A stabilitás alapja a megfelelő erőforrás gazdálkodás és az operációs rendszer folyamatos túlterhelésének megakadályozása.

A levelezőrendszert, mint Kritikus Internetes Szolgáltatást kiemelt prioritással kell az operációs rendszernek kezelnie, az üzemeltetőnek ajánlott az ezen szolgáltatás működtetéséhez nem releváns, egyéb szolgáltatásokat kikapcsolnia.

Elengedhetetlen az elektronikus levelek tárolásához szükséges tárterület biztosítása, melyet célszerű elkülönítetten, csak erre a feladatra biztosítani. Az operációs rendszer és az elektronikus levelek tárolására kijelölt tárterületet mindenképpen hibatűrő, nagyméretű

állományok és hosszú fájlnevek kezelésére is képes fájlrendszerre szükséges formattálni. A rendelkezésre álló tárterületet folyamatosan monitorozni szükséges, helyhiány esetén növelni kell annak méretét. A stabilitás fenntartása érdekében indokolt és szükséges az elektronikus levelek elkülönítésére kijelölt tárterületről másolatot fenntartani, tükrözni, amelyet a hatékonyabb erőforrásgazdálkodás miatt célszerű hardveres támogatással megvalósítani, ugyanakkor a szoftveres tükrözés is képes az elvárt eredmény biztosítására, viszont alkalmazása az operációs rendszer erőforrásait fogyasztja.

2. Levelezőrendszer stabilitása

A levelezőrendszer stabilitását a feladatvégrehajtásban – tökéletesen – együttműködő, alrendszeri elemek összhangja és egységessége biztosítja. A rendszer magját egy stabil, kipróbált, rugalmas, jól konfigurálható –, esetleg programozható – levelezőszervernek kell adnia, amely mellett, amelyhez illesztve, vagy amely részeként elengedhetetlen a

- levelezőkliensek kiszolgálásának,
- felhasználókezelésnek,
- fertőzött levelek kiszűrésének, megtisztításának,
- kéretlen levelek felismerésének, kezelésének rendelkezésre állása.

Ezen részfeladatokat a direkt, kifejezetten e célra kifejlesztett programok – általában – hatékonyabban, gyorsabban képesek ellátni, mint a levelezőszerverbe épített, hasonló feladatra írt kódrészek, ezért is indokolt és gyakori a célprogramok alkalmazása. Az alkalmazott levélkiszolgáló programnak és a vele funkcionálisan összekapcsolt alrendszeri elemeknek egyaránt robusztusnak, hibatűrőnek kell lenniük.

A levelezőrendszer magja egyértelműen a levelezőszerver, ugyanakkor a levelező klienseket kiszolgáló és a levelekhez történő hozzáférést biztosító alkalmazás nélkül önmagában haszontalan. E két szerver alkalmazás általában egymással mellérendelt viszonyban van, azonban csak egymást kiegészítve jelentenek komplex levelezőrendszert, a hozzájuk tartozó alrendszerekkel együtt. A levelezőrendszer stabilitásához a levelezőszervert és az ügyfélkiszolgálást úgy kell egyensúlyban tartani, hogy egyidejűleg mindkettő megfelelően működjön és az erőforrás felhasználás ne menjen a másik rovására.

A felhasználók hozzáférési adatainak tárolását célszerű adatbáziskezelőre bízni, hisz az azonosítási procedúra az elektronikus levélkezelés minden mozzanatában visszatérő, folyamatosan jelenlevő feladat. Nagyszámú felhasználó esetén elengedhetetlen a felhasználói adatok rendezett tárolása, amely ugyanakkor karbantartási kötelezettséget is ró a rendszert

üzemeltető számára, következésképpen, a felhasználók adatainak karbantartását lehetővé tevő adminisztrációs alkalmazás is alrendszere a levelezőrendszernek.
A stabilitás érdekében a levelezőszerver, az ügyfélkiszolgáló, valamint az alrendszerek közötti együttműködéshez a megfelelő kommunikációs átjárhatóságot is szükséges biztosítani, amelyre a hálózati interfész a legkézenfekvőbb megoldás. Alkalmazásával a részfeladatok – terheléstől függően – akár külön hardver eszközökre is csoportosíthatók, egyszerre megvalósítva az együttműködést és a stabilitást. (Kézenfekvő megoldás e két kulcsprogramot különálló hardveren futtatni és ezzel tovább növelni a stabilitást, a felhasználók adatait ekkor is mindkét kiszolgálónak egyszerre biztosítani kell.)

3. Levelezőrendszer hangolása
Ajánlott a rugalmas, jól konfigurálható és paraméterezhető levelezőszerver, klienskiszolgáló és alrendszeri elemek használata, ugyanakkor ezek hibás paraméterezése a stabilitás elvesztéséhez vezethet. A beállításoknál figyelembe kell venni

- a hardver összetételét,
- az egyszerre kiszolgálandó ügyfelek számát,
- a kezelendő levelek méretét, számát,
- az alrendszeri elemek – tervezett kiszolgáláshoz igazított – méretezését.

Az elektronikus levelek fogadásának és küldésének menetét a rendszerbeállítás előtt minden lehetőségre kiterjedően tesztelni kell és éles üzemmódba csak a sikeres próbák után helyezhető. Az esetleges külső programok hívásánál, vagy futtatásánál azok megfelelő működését is ellenőrizni szükséges.

Az operációs rendszer és a levelezőrendszer támadhatóságának megakadályozása
A Kritikus Internetes Szolgáltatások biztonságos üzemeltetése témakörben meghatározottak alkalmazása elengedhetetlen, emellett pedig a levelezőrendszer minden elemének ismert hibáktól mentesnek kell lenniük. A kiadott frissítéseket alkalmazni kell, az Exploitok felhasználásának megakadályozására. A levelezőrendszer legérzékenyebb adatai maguk az elektronikus levelek, valamint a legális hozzáférést biztosító felhasználó nevek és jelszavak párosa, ezért a védelem kialakításakor ezekre kell a legkiemeltebben figyelmet fordítani. Az elektronikus levelek tényleges, fizikai hozzáférését a levelezőszerver tulajdonosára kell korlátozni, amely tulajdonost célszerű az operációs rendszeren virtuálisan, nem létező személyként kezelni, más felhasználóktól különálló csoportban tartani. A levelezőszerver

virtuális tulajdonosától az operációs rendszerszintű belépést célszerű megvonni, ezáltal elérve, hogy a mindenhez hozzáférő rendszeradminisztrátoron kívül más személy az elektronikus leveleket ne legyen képes a fájlrendszeren elérni. A felhasználói adatok rendezett tárolására kijelölt tárhelyet, vagy adatbázist az egyéb adatoktól, adatbázisoktól elkülönítetten, csak a levelezőrendszernek fenntartott hozzáféréssel szabad kialakítani. Adatbáziskezelő alkalmazása esetén elengedhetetlen a Kritikus Internetes Szolgáltatások adatbázisainak biztonsága témakörben leírtak betartása, jelen esetben a levelezőrendszerhez történő hozzáférést biztosító felhasználói adatok vonatkozásában. A felhasználók jelszavait – még az adatbázisban is – csak kódolt formában szabad tárolni, a közvetlen adatbáziskezelés lehetőségét pedig – a rendszeradminisztrátoron kívül – senkinek sem szabad engedélyezni.

A levelezőrendszer tűzfalát célszerű dinamikusan, események bekövetkezéséhez, vagy történésekhez igazítottan szabályozni, amellyel a támadás előkészülete, vagy a támadási próbálkozás nagymértékben csökkenthető, esetleg a támadás teljesen megakadályozható. Ilyen történés lehet az operációs rendszerre irányuló belépési, vagy az adatbáziskezelőre irányuló bejelentkezési próbálkozás, amely bizonyos sikertelen esetszám után tűzfalszabály aktiválásával kizárható.

A rosszindulatú felhasználásának és kihasználásának megakadályozása

A rosszindulatú felhasználás és kihasználás egymással lehetnek átfedésben, amelynek leggyakoribb előfordulása, hogy mindkét műveletet egyszerre próbálja végrehajtani a tevékenységet folytató. Markánsan elkülönül azonban egymástól, hogy a felhasználásnál a KRISZ-ként működő levelezőszerver postafiókja-, a kihasználásnál pedig másik levelezőszerver felé történő továbbítás a fő cél.

1. Rosszindulatú felhasználás megakadályozása

A rosszindulatú felhasználás első lépéseként a fertőzött, vagy kéretlen levél megjelenik a levelezőszerver bemenetén és a küldő reménye szerint a továbbító funkciókon keresztül halad a címzett postafiókja felé. A rosszindulatú felhasználást szűrők közbeiktatásával lehetséges és kell megakadályozni, amelyekkel vizsgálható az érkező levél

- küldőjének egyedi hálózati azonosítója;
- szöveges tartalma;
- csatolmánya, melléklete;
- feladója, címzettje, tárgya, mérete.

Ezen szűrők használata nélkül az érkező levelek kézbesítése automatikusan, feltétel és vizsgálat nélkül végrehajtásra kerülne, használatukkal azonban csak a rostán fennmaradó levelek jutnak el a címzetthez. A szűrők alkalmazásakor eldöntendő az is, hogy fennakadás esetén mi legyen a beérkező levél további sorsa:

- eldobásra kerüljön;
- a címzett figyelmeztetésével egyidejűleg továbbításra kerüljön;
- átmeneti mappába kerüljön.

a) Küldő vizsgálata

Az internet hálózati felépítéséből adódóan a küldő SMTP szerver is egyedi IP címmel rendelkezik. Ezen cím csupán a küldő levelezőszerver internetes azonosítóját takarja, de nem mutatja, hogy a levelet, szerver mögötti kliens küldte-e. A küldő IP címének, e-mail címének, valamint a kettő egyezőségének vizsgálatával megállapítható, többek között hogy

- a küldő e-mail címében szereplő domain név megegyezik-e az IP címből visszafordított domain névvel;
- a küldő IP címe;
    - valamely szolgáltató által dinamikusan kiosztott cím-e;
    - szerepel-e a kéretlen leveleket küldő szerverek nyilvános adatbázisában.

Ezekből az információkból nagy eséllyel már a levelezőszerver bemenetén megjelenő levélről következtethető, hogy kéretlen, esetleg fertőzött lesz-e. Amennyiben a küldő szerver IP címéből visszafordított-, és az e-mail címben szereplő domain név nem egyezik, úgy feltételezhető, hogy a küldő megtévesztő szándékkal ál e-mail címet használt a levél feladásakor. Amennyiben a küldő IP címe valamely szolgáltató által kiosztott dinamikus cím, akkor gyanús, hogy az elektromos levél nem egy kifejezetten levélküldésre rendszerbe állított számítógépről származik. Feltételezhető, hogy egy otthoni háztartás fertőzött eszközéről, egy rosszindulatú program küldi a levelet valószínűleg tovább fertőzési céllal, ugyanakkor az is előfordulhat, hogy valaki marketing célú levelek küldésére – ad-hoc jelleggel – levélküldésre alkalmas programot telepít otthoni gépére és arról küld leveleket. Ha a küldő IP címe valamely nyilvános, naprakész, kéretlen leveleket küldő adatbázisban szerepel, úgy feltételezhető, hogy az érkező levél fertőzött, vagy kéretlen, ezért fogadása nem ajánlott.

A levelezőszervert úgy kell beállítani, hogy a küldő, világháló szerinti IP címe alapján döntést tudjon hozni az érkező levél fogadásáról, vagy elutasításáról.

A Nemzeti Kibervédelmi Intézet is annyira fontosnak tartja a kéretlen levelek elleni küzdelmet, hogy honlapján tájékoztatót adott ki a DNS helyes beállításával kapcsolatban. [78]

b) Szöveges tartalom vizsgálata

Az elektronikus levelek tartalmi vizsgálata lényegében azt dönti el, hogy az érkező levél kéretlennek, azaz SPAM-nek tekinthető-e. Konkrét definíciója nincs a SPAM levélnek, a rövidítés a Monty Python Repülő Cirkusza című tévésorozat egyik jelenetében feltűnt löncshúsra utal, valójában a ráerőltetést szimbolizálja. Általánosságban a „nagy példányszámban elküldött, azonos tartalmú kéretlen elektronikus üzenet" [79] leírással határolják körül a fogalmat, azonban az egyes leveleket már eltérően sorolják kéretlennek, vagy nem kéretlennek az elektronikus levelet vizsgáló programok.

A kéretlen levelek elterjedésük óta rengeteg formában jelentek meg. A Kaspersky – ismert – kiberbiztonsági vállalat enciklopédiája [80] szerint az összes e-mail forgalom 70-80%-a SPAM, amely elleni védelem nélkül az aktív levelezés lehetetlen, továbbá tapasztalataik szerint a kéretlen levelek 50%-ban az alábbi fő kategóriákba sorolható:

- felnőtt tartalom;
- egészség;
- információtechnológia (IT);
- személyes pénzügyek;
- tanulás és tréning.

A SPAM tartalmakban új irányok is megjelennek, úgymint a politikai típusú, vagy a spam elleni védelmet ajánló levelek.

A HTML alapú megjelenést kihasználva a megtévesztő szövegbe linket helyeznek el, amely látszólag kapocs a tartalommal összefüggő ügyintézéshez, de legtöbb esetben kattintásra aktivizálódó, valamilyen beavatkozást végrehajtó programkód.

A SPAM-ek elleni védelemhez elkerülhetetlen és kötelezően alkalmazandó valamilyen levelezőszerverhez illeszthető, szűrésre alkalmas program. A kéretlen levelek szűrésének összetettsége miatt, mindenképpen a levelezőszerverrel együttműködő, erre specializálódott, folyamatosan frissülő külső program használata ajánlott, hisz a kéretlen levelek tartalma dinamikusan változik, amihez igazodnia kell a szűrési feltételeknek is. Az egyik legnépszerűbb, nyílt forráskódú SPAM szűrő alkalmazás leírása alapján [81] a program egy nagy szabályrendszert alkalmaz, amely optimalizált keresést tesz lehetővé, minimalizálva a tévesztés

lehetőségét. A programban szereplő szabályok manuálisan is bővíthetők, amely lehetővé teszi a személyre szabott, speciális beállítások alkalmazását.
A SPAM szűrő programok az elektronikus levél tartalma és az aktuális szabályrendszer alapján a levélhez egy pontértéket rendelnek, amelyből következtetni lehet a kéretlen levél valószínűségére, majd a levelezőszerver dönt a levél további sorsáról.
A SPAM-ek szűrésének legnagyobb problematikája az emberi leleményesség és a gépiesített, algoritmusszerű vizsgálat közötti ellentmondás. A kreativitás nyilvánvalóan azt a célt szolgálja, hogy az elektronikus levél a szűrőkön átjusson, ugyanakkor a hatalmas mennyiségű levél átnézésére emberi kapacitás nem áll rendelkezésre, azt csak programok, algoritmusok képesek vizsgálni. A jól és hatékonyan működő SPAM szűrő a felhasználói igényeknek megfelelően a kéretlen leveleket megfogja, a többit viszont hiánytalanul átengedi, ami csak

- a megfelelő szűrőalkalmazás használatával,
- a levelezőszerver és a szűrőalkalmazás precíz finomhangolásával,
- a SPAM-re adandó megfelelő válaszreakció beállításával

valósítható meg.
Tekintettel arra, hogy a SPAM-ek elleni védelem erősségi szintjét a levelezőszervert üzemeltető saját belátása szerin határozza meg, a megfelelő védelemre egzakt küszöbérték, vagy számszaki meghatározás nem adható.
Eldöntendő kérdés a SPAM kategóriába sorolt levelek további sorsa. Az üzemeltetők hozzáállása különböző, hisz van, aki a felhasználó mappájában egy elkülönített almappába helyezi a kéretlennek minősített leveleket, de van, aki egyszerűen eldobja a SPAM-eket és annak tényét nem is hozza a felhasználó tudomására. Ajánlásom szerint a kéretlen levelek kezelését nem szabad a felhasználókra bízni és a levelezőszerver felhasználását a szerveren kell megakadályozni.

c) Csatolmány, melléklet vizsgálata

Elsősorban az elektronikus levél mellékletébe rejtett rosszindulatú kódok elleni védelmet jelenti, amelyet leghatékonyabban külső, erre a feladatra specializálódott, frissülő adatbázissal rendelkező program képes ellátni. A megfelelően rugalmas levelezőszerverekhez illeszthetők a rosszindulatú programokat feltárni képes keresőprogramok. A gyakorlatban az elektronikus levél – kézbesítés előtt – átadásra kerül a vizsgáló alkalmazásnak, amely a mellékletek átnézését követően egy jelzéssel visszaadja azt a levelezőszervernek és a levelezőszerver dönt a levél további sorsáról. Erősen ajánlott a malware-t tartalmazó elektronikus leveleket a

levelezőszerveren kézbesítés előtt megsemmisíteni és mellőzni a postafiók tulajdonosokhoz történő eljuttatást.
A rosszindulatú kód vizsgálata előtt szofisztikált megoldást jelent még a csatolmány típusának, kiterjesztésének beazonosítása és kezelése. A legnagyobb – ingyenes – levelezőszerverek is használják ezt a módszert, amelynek lényege, hogy a végrehajtható kódot tartalmazó elektronikus leveleket egyszerűen blokkolják, vagy csak csatolmány nélkül továbbítják a címzettnek, amelyről általában értesítést is küldenek.
A csatolmányok természetesen lehetnek tömörített állományok is, amely esetben a vizsgálatot a kitömörítési eljárással szükséges kombinálni, ugyanakkor figyelembe kell venni, hogy a csatolmányokon végrehajtott műveletek nagyon erőforrásigényesek.
A csatolmányok vizsgálata a levelezőszerver rosszindulatú felhasználásának elkerülése érdekében kötelező, a vizsgálat mélységét pedig az erőforrások rendelkezésre állásának függvényében célszerű beállítani.

d) Az elektronikus levél paramétereinek vizsgálata
Az elektronikus levél feladójának, címzettjének, másolati-, vagy titkos másolati címzettjének, tárgyának és méretének vizsgálatával is érdemes foglalkozni. Megítélésem szerint a mezők kitöltöttsége esetén azok tartalmi vizsgálata mindenképpen indokolt, egyes mezők – például a feladó – ki nem töltöttsége pedig egyenesen felveti a kéretlen levél gyanúját. A levél mérete is beszédes, hisz egy minimális méret alatt erősen ajánlott SPAM vizsgálat alá vetni, egy bizonyos méret felett pedig az erőforrások védelme érdekében célszerű korlátokat alkalmazni.

2. Rosszindulatú kihasználás megakadályozása
Alapvetően a levelezőszerver általi tömeges levélküldés megakadályozását jelenti, amely magában foglalja a levélküldéshez szükséges jogosultságok illetéktelenhez jutásának megakadályozását is. A kihasználás leggyakrabban valamely rosszindulatú programmal fertőzött – levelezőszerverhez kapcsolódott – kliens eszközről, SMTP protokollon keresztül következik be, amely ellen a levelezőrendszer alábbi területein érdemes védelmet kiépíteni:

- relay funkció;
- hozzáférések;
- levélforgalom;
- kimenő levelek tartalma.

a) Relay funkció védelme

A levelezőszerver Relay funkciójának működtetése ugyan elengedhetetlen a világháló irányába történő levélküldéshez, azonban lehetséges és mindenképpen ajánlott is meghatározni, hogy azt milyen hálózati tartományból, vagy IP címekről érkező kliens eszközöknek biztosítsa a levelezőszerver. Ajánlott alkalmazni az alapértelmezésben „senkinek, kivéve akinek" továbbítási alapelvet, amellyel jelentősen szűkíthető a levelezőszervert potenciálisan kihasználni képes eszközök száma. Ezzel a lehetőséggel biztosítható, hogy csak „megbízható" kliensek tudjanak leveleket küldeni kifelé, egyébként a levelezőszerver csak a levelek fogadását biztosítsa. A küldési jogosultsággal nem rendelkező klienseknek pedig alternatívát jelenthet a Webmail alkalmazás telepítése, amely eltérő specifikumából adódóan minimálisra csökkenti a kihasználás megvalósítását, ugyanakkor lehetőséget teremt a levelek világháló irányába történő továbbítására. A legnagyobb interneten elérhető ingyenes levelezőrendszerek biztonsági okból alapértelmezésben szintén Webmail hozzáférést biztosítanak és kerülik a kliens eszközökről, hagyományos levelező programmal és protokollal folytatott levelezést.

Amennyiben nélkülözhetetlen a Relay biztosítása, úgy azt mindenképpen authentikációhoz, kötötten szabad csak biztosítani. Érdemes megvizsgálni annak a lehetőségét, hogy a Relayhez alkalmazni kívánt authentikációs adatok lehetnek-e különbözők a levelezési postafiók hozzáférési adataitól, s amennyiben igen, úgy ezt a lehetőséget ajánlott alkalmazni. Szintén elvárt beállítás továbbá a Relayhez alkalmazott hálózati csatorna biztonságossá tétele, amely kódolttá teszi a kommunikációt és nagyban megnehezíti a hálózaton lehallgatott authentikációs adatok visszafejtését.

b) Hozzáférések védelme

Ha a levelezőszerveren tárolt felhasználói adatok a fentebb említetteknek megfelelően védve vannak, akkor is van lehetőség némelyik megszerzésére, amelyet erősít az általános gyakorlat. Amennyiben az ügyfélkiszolgáló szerveralkalmazás elérhető a világhálón, úgy ahhoz bárkinek lehetősége van csatlakozást kezdeményezni és a megfelelő felhasználó név – jelszó páros ismeretében a postafiók leveleit kiolvasni. A levelezőprogramokban létezik olyan beállítási lehetősége, hogy a levelek küldéséhez ugyanaz az authentikáció tartozzon, mint a levelek olvasásához, amely gyakorlatilag sugallja a felhasználók és az üzemeltetők felé, hogy érdemes ezzel a lehetőséggel élni. A rossz beidegződés miatt a levélküldéshez és a levelek olvasásához gyakran ugyanaz az authentikáció tartozik, ezért aki próbálozással kitalálja, hogy adott e-mail postafiók milyen jelszóval olvasható, úgy annak nagy eséllyel arra is lesz lehetősége, hogy

leveleket küldjön ki a levelezőszerverrel, majd azt véletlenül, vagy szándékosan kihasználja. Figyelembe véve, hogy a felhasználói azonosító – egyediségéből adódóan – legtöbbször maga az e-mailcím, a próbálkozónak még arra sem kell nagy befektetést fordítania, elég csak az ismert e-mailcímekhez jelszavakat találnia.
A próbálkozásokkal szemben hatékony védelmi lehetőség a dinamikus tűzfal használata, amely a napló állományok figyelésével, meghatározott sikertelen belépési kísérletet követően, a kliens eszköz csatlakozását – hálózati azonosítója alapján, – bizonyos időre megtagadja, ezáltal kizárja a további próbálkozásból. Ez a beállítás egyaránt alkalmazható a levelezésben érintett SMTP, POP3, IMAP protokollokat használó programokhoz. A jól beállított helytelen próbálkozási szám és kitiltási idő garantálja, hogy ne sikerüljön kitalálni a postafiókhoz tartozó jelszót, megakadályozva a levelezőszerver kihasználását. Három helytelen próbálkozás után, legalább öt perces kitiltást ajánlott alkalmazni.

c) Levélforgalom kontrollja

Figyelembe véve, hogy a levelezőszerver kihasználása a levelek tömeges kiküldésével valósul meg, mindképpen ajánlott ennek a védelmét is megoldani. A jól kiválasztott levelezőszerver rendelkezik azzal a beállítással, amelyben megadható, hogy adott időintervallum alatt, mekkora számú levelet, hány címzettnek küldhet csak ki. Ennek a paraméternek a helyes megválasztásával garantálható, hogy a felhasználó a leveleit kényelmesen, még sietség esetén is kiküldhesse, ugyanakkor a tömeges levéláradatot megakadályozza. Megítélésem szerint, egy perc alatt maximum 10 levelet, maximum 20 címzettnek elégséges engedélyezni.

d) Kimenő levelek vizsgálata

A levelezőrendszer rosszindulatú falhasználása témakörben kifejtett tartalmi és melléklet vizsgálat – kimenő levelekre vonatkoztatott – végrehajtásával tovább növelhető a levelezőszerver kihasználásának megakadályozása, azonban figyelembe kell venni, hogy alkalmazása jelentősen terheli a szerver erőforrásait.

3. Felhasználók védelme

A rosszindulatú felhasználás és kihasználás áldozatai a felhasználók, amelyhez egyfajta „segédeszköz” a levelezőrendszer. Az üzemeltetők a védelmet a levelezőrendszerre tudják felépíteni, ugyanakkor figyelembe véve, hogy mindig a felhasználó a leggyengébb láncszem, tehetnek és ajánlott is tenni lépéseket a felhasználók védelme érdekében. Érdemes a

felhasználókat, vagy ügyfeleket meggyőzni a biztonságról, hogy ők maguk is igényként fogalmazzák meg a lehetséges védelmi szolgáltatások működtetését. A rosszindulatú, vagy kéretlen levelek felhasználói fiókba eljutása önmagában csak annyit jelent, hogy a levél a levelezőrendszer szűrőin átjutott és a felhasználón múlik annak további sorsa.

a) Felhasználók oktatása

A felhasználók rosszindulatú programokkal és azok terjedésével kapcsolatos hétköznapi, érthető formában történő tájékoztatása nagyban elősegíti a rosszindulatú felhasználás megakadályozását. Amennyiben tisztában vannak a gyanús jelekkel és a felhasználói interaktivitás lehetséges következményeivel, akkor kisebb eséllyel aktiválják a rosszindulatú programkódokat, vagy tesznek eleget ismeretlenek kéréseinek. Amennyiben a levelezőrendszer postafiókjainak felhasználóival az üzemeltetőnek – például munkahely esetén – közvetlen kapcsolata van, úgy mindenképpen személyesen ajánlott visszatérő rendszerességgel oktatást tartani, eltérő esetben elektronikus tájékoztató levelek, vagy kisfilmek is sokat segíthetnek a megelőző tevékenységben. Érdemes e-mail használati protokollt készíteni, amely többek között kitér a többes címzés, a másolat és a titkos másolat közötti különbségre és azok biztonságos alkalmazását mutatja be, továbbá leírja, hogy miként lehet az e-mail-ek forrásából meggyőződni a levél eredetéről.

b) Felhasználók munkakörnyezetének alakítása

A felhasználók munkakörnyezetét munkahely esetén a vezető befolyásolhatja, egyébként pedig ajánlás tehető annak kialakítására.

Napjainkban számtalan – akár ingyenes – program áll rendelkezésre, amely képes a levelezőprogramba integráltan védelmet nyújtani a kéretlen, vagy fertőzött levelekkel szemben, megakadályozva azok aktivizálódását. Ezen programok telepítése erősen ajánlott.

A levelezőprogram és a levelezőszerver közötti kapcsolat felépítésére legtöbbször olyan segítő alkalmazás – „súgó” – áll rendelkezésre, amely laikusként is végig vezeti a felhasználót az elektronikus levelek sikeres kezeléséhez, azonban az alternatív beállítások elvégzésében csak ritkán segít. Ha a felhasználó választhat a biztonságos, vagy a nyílt hálózati csatorna-, illetve a kódolt vagy a kódolatlan kommunikáció között, akkor előfordulhat, hogy a helytelen döntést hozza meg, mit sem sejtve annak negatív következményeiről. Ebben a témakörben is ajánlott az iránymutatás, vagy a helyes beállítás kikényszerítése.

4. Üzemeltetés

A levelezőrendszer összetettségéből adódóan elkerülhetetlen üzemeltető személy alkalmazása, mert az elektronikus levelezés biztonsága dinamikusan változik, amely kihívásokra időben, megfelelő válaszokat kell adni. A levelezőrendszer a biztonságra tett erőfeszítések nélkül is képes átmenetileg ellátni feladatát, azonban a postafiókok felhasználói ez esetben kitetté válnak, a levélkézbesítés fázisai rendelkezésre állásként, automatikusan végrehajtódnak és a rendszer valóban „nyitott biztonsági résként" fog üzemelni. A rendszer biztonságának kialakításában létezik radikálisabb, vagy humánusabb hozzáállás, a helyes utat azonban a KRISZ definíciójában megfogalmazott cél elérése adja, a felhasználói elvárásoknak történő megfelelés figyelembe vételével. Fontos kiemelni, hogy a felhasználók levelező rendszerrel szemben támasztott igényei közül, a – hagyományos protokollokkal működő – levelezőprogramok használata növeli a levelezőrendszer kihasználásának lehetőségét, míg a kéretlen és fertőzött levelek elleni védelem növeli a biztonságot, s vele együtt a szerver leterheltségét is.

Üzemeltető feladatai:

- a felhasználók biztonságkerülő hozzáállása mellett is a rendelkezésre állás megteremtése;
- legalább napi mentés, archiválás kialakítása;
- a támadások elhárítása;
- a rendszerben található hiányosságok folyamatos feltárása, kijavítása;
- ügyfelek igényeinek lehetőség szerinti teljesítése.

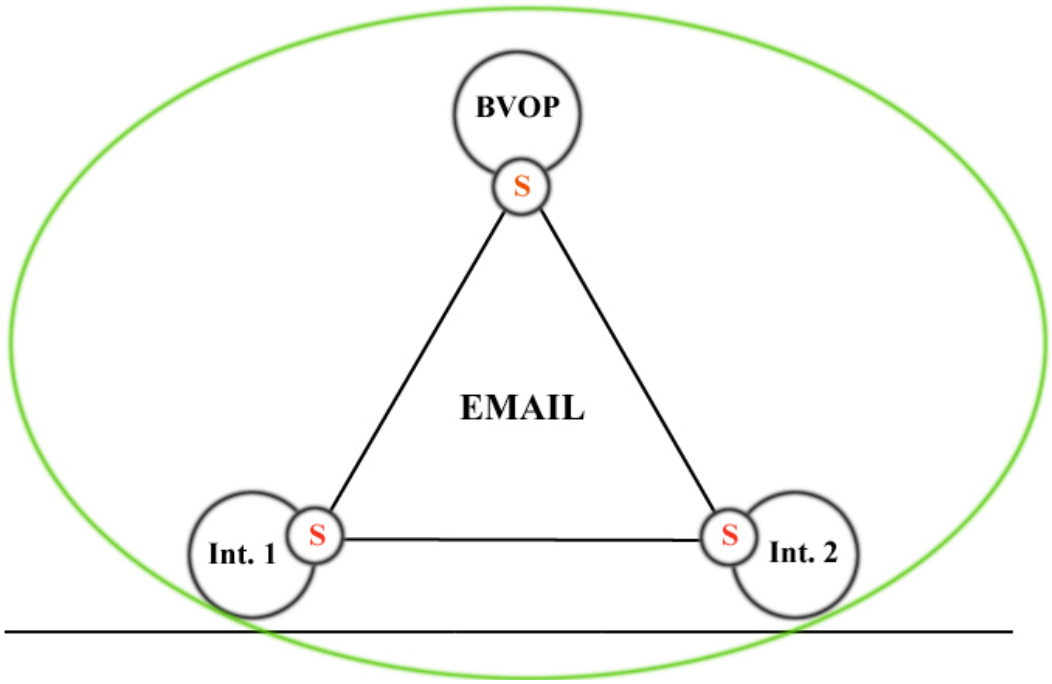
3.2.7 Elektronikus levelezés a védelmi szférában

Az elektronikus levelezés megteremtésével, a védelmi szférában is bevezetésre került ez a szolgáltatás, és a benne rejlő lehetőségek felismerésével terjedt egyre nagyobb körben.

Kezdetek

A megelőző időszakot lekövetve, először a hagyományos papír alapú levélmozgás szerint zajlott az elektronikus levelek küldése és fogadása, a szervezet kommunikációs csatornáinak rendelkezésre állásától függően, elsősorban zárt-, ritkábban internetes hálózatban.

A büntetés-végrehajtás 1996-os elektronikus levelezési modelljét mutatja a 17. számú ábra, amelyen látható, hogy szervezeti egységenként egy postafiókkal, zárt hálózatban folyt az elektronikus levelezés.



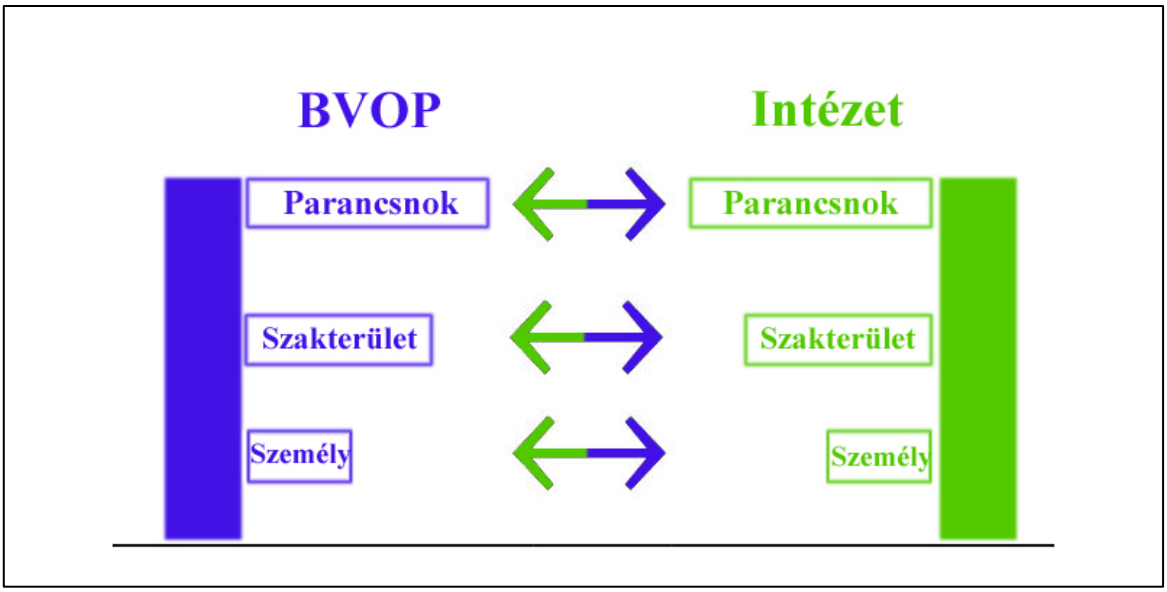
17. ábra

A Bv. elektronikus levelezése 1996-ban [82]; forrás: szerző

Az akkori rendszer jellemzői voltak: „

- a Bv. Országos Parancsnokságát (továbbiakban: BVOP) is beleértve minden intézet részéről csak egyetlen privilegizált felhasználó – a parancsnok nevében – küldhetett és fogadhatott levelet („S”);
- a küldemények minden esetben iktatásra kerültek és a rendszer biztosította az automatikus – válasz – nyugtalevél alkalmazását;
- a Bv. egy –, az Internettől független – zárt hálózatot alkotott, egyéb szervezet nem kapcsolódhatott be a levelezésbe;
- a rendelkezésre álló egyszerű szövegszerkesztő semmilyen hitelesítést nem biztosított, aláírás helyett az „sk.”, mint saját kezűleg felirat alkalmazása került bevezetésre.” [82]

Az 1996-os büntetés-végrehajtási modell 2012-re a 18. számú ábra szerint változott.



18. ábra

A Bv. elektronikus levelezése 2012-ben [82]; forrás: szerző

„A centralizált levelező szolgáltatás a Bv. – akár teljes – személyi állománya részére internetes, azaz valós, egyénre szóló levelező postafiókot biztosít, lehetővé téve az arra jogosultak számára, hogy – biztonsági megoldások használata mellett – a világhálón küldjenek, vagy fogadjanak elektronikus leveleket, csatolmányokat. Az Intézet központi és vezetői e-mail címeire a külső kapcsolatoktól rendszeresen érkeznek – a már említett aláírási módokkal hitelesített, – feladat meghatározásokat tartalmazó levelek, csatolmányok. Az elektronikus levelezés elsősorban a vertikális, azaz a kormányzati struktúrában érvényesül a levelezési címek tartományi kialakítása miatt (gipsz.jakab@bv.gov.hu). Az e-mail alkalmazásával rendkívül dinamikussá vált az irányító rendszer, a feladatok, utasítások rövid időn belül a legmagasabb szintekről is képesek eljutni a végrehajtókhoz. Az utasítások csatolmányban elhelyezett elektronikus dokumentumba, kézzel aláírt és újradigitalizált állományba, vagy az e-mail tartalmi részébe kerülnek elhelyezésre.

A gyors és kényelmes e-mail használata az alábbi változásokat hozta:

- a határidős feladatok (adatszolgáltatások) száma növekedett;
- a feladatok végrehajtására rendelkezésre álló idő csökkent;
- az adatszolgáltatásokban a redundáns adatok száma növekedett;
- a kommunikációs csatornák száma növekedett;
- a szakmai irányítás nagyobb hangsúlyt kapott.” [82]

A változás a védelmi szféra teljes spektrumában hasonlóan történt, amelyet egyértelműen a szervezeti egységek internetes végpontjai közötti sávszélesség bővítése, valamint az informatikai eszközpark fejlesztése tett lehetővé.

Napjaink rendvédelmi – elektronikus – levelezése

A 2012-es állapothoz képest hatványozódott az elektronikus levelezés iránti igény és egyben fejlődött a szolgáltatás minősége. A belső hálózatból és az internet irányából érkező levelek fogadását a rendvédelmi szerv levelezőszervere biztosítja és továbbítja azokat a felhasználók postafiókjába.

A vizsgálatok alapján, a védelmi szférában dolgozókra nézve általánosságban igaz, hogy

- az informatikai rendszerhez hozzáféréssel rendelkező felhasználóknak az internetre kiterjesztett elektronikus levelezés is biztosítható;
- a rendelkezésre álló postafiók mérete – általában – korlátozott;
- a rendszerhez és az e-mail fiókhoz – a központi azonosításnak köszönhetően – egyazon bejelentkezés tartozik;
- a felhasználók – szervezeti – e-mail címei kereshetők;
- a belső rendszerből levelezőprogrammal, továbbá az interneten keresztül is – pld. webmail alkalmazással – biztosított a levelezés;
- a levelezőprogram integrált – naptár, feladatkezelő – alkalmazásokkal is rendelkezik.

1. Hálózaton belüli levelezés

A rendvédelmi szerv informatikai rendszerébe belépve, az e-mail postafiókkal rendelkező felhasználó az előre telepített levelező alkalmazás használatával képes az elektronikus levelek kezelésére, valamint e-mailek – akár világháló irányába történő – küldésére. A rendszerbe történő belépést követően, a levelező alkalmazás általában további azonosítást nem követel meg.

2. Interneten keresztül használható rendvédelmi levelezés

A felhasználók meghatározott – elsősorban vezetői beosztásban dolgozó – részének elengedhetetlen

- az e-mail fiókok állandó elérése;
- az érkező levelek haladéktalan megtekintése.

A szolgálati helytől távol, értelemszerűen az internet biztosítja a rendvédelmi postafiók és a felhasználó közötti hálózati kapcsolatot és teszi lehetővé az e-mailek távoli elérését. Az általános trendnek megfelelően az elektronikus levelek állandó figyelése legkézenfekvőbben okos eszközzel, valamelyik levelező applikáció alkalmazásával valósítható meg, amely képes azonnal mutatni az érkező leveleket.

a) Levelezés applikációval

Saját applikáció-kiszolgáló alkalmazása

Amennyiben a rendvédelmi szerv levelezőrendszere tartalmaz saját applikáció kiszolgálót, úgy ahhoz kapcsolódva folyamatosan figyelemmel kísérhető a hitelesítés szerinti postafiók, az érkező levelek azonnal megjelennek és a küldés is biztosított.

A szolgáltatás előnye, hogy a felhasználó az adott postafiókra nézve tetszőleges műveleteket hajthat végre, viszont hátránya, hogy a használt okos eszköz – az egyszeri hitelesítést követően – a levelezőrendszer állandó kapcsolódási pontjává válik, így az eszköz idegen kézbe kerülése esetén a postafiók kitetté válik.

Idegen applikáció-kiszolgáló alkalmazása

A levelezőrendszerek támogatják, így a felhasználóknak lehetőségük van az érkező levelek automatikus továbbítására egy külső levelező szolgáltatóhoz, amely rendelkezik applikáció kiszolgálóval. Ebben az esetben az okos eszköz levelező-applikációja a védelmi szféra levelezőrendszere helyett egy másik szolgáltató levelezőrendszeréhez kapcsolódik, amelybe a rendvédelmi e-mailek a beállított továbbítási feltételeknek megfelelően megérkeznek. Ennek a megoldásnak előnye, hogy a rendvédelmi postafiók érintetlensége végig megmarad, ugyanakkor hátránya, hogy a levelekben tárolt információk külső levelezőrendszerbe kerülnek, továbbá, hogy válaszlevelet csak az idegen levelezőrendszerbe regisztrált postafiók nevében lehet küldeni.

b) Webmail

A rendvédelmi e-mail-ek kezelésére rendelkezésre áll a webmail lehetősége is, amellyel minden esetben csak bejelentkezést követően tekinthető meg a postafiók tartalma. Ehhez a rendvédelmi szervnek interneten elérhető webszervert is kell üzemeltetnie.

c) Levelezés interneten keresztül belső hálózatból

A védelmi szférában is alkalmazott VPN[104] szolgáltatás lehetőséget ad interneten keresztül a rendvédelmi hálózatba történő biztonságos belépésre. Használatával egy biztonságos hálózati csatorna jön létre a dolgozó IT eszköze és a rendvédelmi informatikai rendszer között, így a felhasználó távolról is képessé válik a belső rendszer informatikai szolgáltatásaihoz, többek között az elektronikus levelezéshez is hozzáférni. A megoldás előnye, hogy biztonságos és szükségtelenné teszi a többi internetes – rendvédelmi – levelező szolgáltatást, hátránya, hogy a VPN jogosultsággal rendelkező dolgozók száma alacsony, továbbá a belső hálózatba lépéshez minden esetben külön kapcsolódni kell.

A büntetés-végrehajtás levelezése napjainkban

2019. szeptember végi adatok szerint a büntetés-végrehajtás központi levelező rendszere

- 6262 db email postafiókot tartalmaz;
- 6168 db elektronikus levelet fogad és 4045 db-ot küld ki naponta;
- 1405 db fertőzött, vagy kéretlen levelet szűr ki naponta, amely a beérkező levelek 22,4%-a;
- a felhasználói fiókok korlátozása mellett, 1,35 TB méretben tartalmaz leveleket.

A levelező rendszer szűk keresztmetszete az állandóan bővítésre szoruló hardver, továbbá problémát okoznak a szűrőn átjutó kéretlen levelek.

A védelmi szféra levelező rendszereinek biztonsága

Természetes, hogy internetről elérhető levelezőrendszert informatikai biztosági kockázat nélkül nem lehet működtetni, ugyanakkor – tekintettel arra, hogy a rendvédelmi szervek számára nélkülözhetetlen a szolgáltatás fenntartása – a kockázatvállalás szintjét minimalizálni szükséges. Amennyiben a levelezőrendszer összeköttetésben van a belső informatikai rendszerrel, úgy el kell fogadni, hogy az kiskaput jelent a kibertámadások végrehajtásához.

A rendvédelmi szervek[105] mindegyike saját – elsősorban tájékoztatási – honlapot tart fenn, amelyeken kivétel nélkül előtalálható legalább egy élő szervezeti e-mail cím, amellyel kapcsolatteremtési lehetőséget kínálnak a külvilágnak. Az elérhetőség arra is utal, hogy a

[104] Virtual Private Network – virtuális magánhálózat

[105] Vizsgált szervek: Alkotmányvédelmi Hivatal, Büntetés-végrehajtás, Katasztrófavédelem, Magyar Honvédség, Nemzeti Adó és Vámhivatal, Nemzetbiztonsági Szakszolgálat, Rendőrség, Terrorelhárítási Központ, Terrorelhárítási Információs és Bűnügyi Elemzők Központ

szervezetek rendelkeznek saját, interneten elérhető – folyamatos fenntartású – levelező rendszerrel.

A megadott e-mail címekre irányuló, interneten is elérhető lekérdezések és kutatások számtalan információt adnak az érintett rendvédelmi szervek levelezőrendszereiről. Megtudhatók a levelezőszerverek domain nevei és IP címei, s a lefolytatott internetes – kockázati szempontú – kapcsolatfelvétel az alábbiak szerint összegezhető:

- Egyik sem nyitott továbbító szerver, azonosítási feltétellel azonban egy szerver engedélyezi a továbbítást;
- Kettő kivételével a többi szerver kódolatlan, azaz lehallgatható SMTP csatornán küldi a leveleket;
- Kettő szerver a megszólításkor elárulja magáról, hogy melyik gyártó, milyen programja adja a levelező szolgáltatást, amely információ lehetőséget ad a támadóknak a gyenge pontok feltérképezésére;
- Egy kivételével mindegyik levelezőszervernél kikövetkeztethető volt a webmail URL[106]-je, amely kapcsolódási pontot ad a levelezőrendszerbe történő belépéshez. Egy esetben további feltételhez kötött volt a bejelentkezés.

A kódolatlan SMTP csatorna magában hordozza az információ illetéktelen általi kinyerésének a kockázatát. A levelezőszerverek közötti hálózati kapcsolat lehallgatásával az elektronikus levélként továbbítandó információ kinyerhető.

A webmail hozzáférések ismerete több kockázatot is hordoz magában. A belépési oldalon feltüntetett felhasználó név és a jelszó együttes ismeretével a rendvédelmi szerv levelezőrendszere elérhető, amelyből az adott postafiókon keresztül az összes e-mail cím kinyerhető és kereshető. Figyelembe véve, hogy a felhasználónév maga az e-mail cím, jelszópróbálgatással elérhető valamelyik rendvédelmi postafiók. Az internetes keresőkkel is számtalan élő szervezeti e-mail cím – azaz felhasználónév – megtudható, amelyhez a megfelelő jelszót kell megtalálni.

Nem hanyagolható el azon kutatási tény sem, hogy a közösségi oldalakhoz használt jelszavak nagy arányban megegyeznek az e-mail címekhez használt jelszavakkal. Tehát amennyiben a rendvédelmi e-mail címek azonosítóként szolgálnak valamely közösségi oldal hozzáféréséhez, úgy a közösségi oldal adatbázisa nagy eséllyel rendvédelmi webmail hozzáférést is tartalmaz.

[106] Uniform Resource Locator - webcím

Az elmúlt időszakban is nagy hírértéke volt, hogy több millió közösségi hozzáférés szivárgott ki, amely között akár rendvédelmi e-mail hozzáférések is lehettek.
További biztonsági kockázat, hogy az e-mail postafiókhoz használt hozzáférés legtöbbször megegyezik a védelmi szféra informatikai rendszerébe használt hozzáféréssel, így aki a webmail szolgáltatáson keresztül – akár illegálisan – bejelentkezik egy postafiókba, annak hozzáférése lesz az adott rendvédelmi informatikai rendszerhez is.
A rendvédelmi levelezőrendszerek biztonságosabbá tételéhez a fent összegzett kockázati tényezőket mindenképpen el kell hárítani, továbbá a webmail szolgáltatáshoz kétfaktoros azonosítást célszerű alkalmazni. A védelmi szféra e-mailcímek közkincsé tételét célszerű minimalizálni, a felhasználók figyelmét pedig fel kell hívni azok magánjellegű használatának tilalmára. A tájékoztató weboldalakról az e-mail elérhetőségeket célszerű levenni és helyettük kapcsolati űrlapot kialakítani, amelyben az oldal látogatójának e-mail szolgáltatás nélkül is van lehetősége közleményének átadására.

A MI[107] alkalmazásának lehetősége a védelmi szféra levelező szolgáltatásával összefüggésben

Az elektronikus levelezésnek számtalan olyan kapcsolódási pontja van, amelyre a levelezőrendszert üzemeltetőnek nincs-, vagy csak csekély ráhatása van. Követhetetlen, hogy – a tiltás ellenére – a rendvédelmi e-mailcímek hova kerülnek felhasználásra, megadásra, illetve milyen más, a felhasználó birtokában levő címlistában szerepelnek, amelynek kiszivárgása, vagy illetéktelenhez kerülése esetén a rendvédelmi postafiók támadási célponttá válik. Nehéz követni továbbá, hogy távoli bejelentkezés esetén a postafiók milyen IT – védelemmel rendelkező – eszközről kerül elérésre, az esetleges kéretlen, vagy fertőzött leveleknek mi a további sorsa és következménye. A vizsgálatokhoz rendelkezésre álló humán erőforráskapacitás mindig szűk keresztmetszet, továbbá a változó környezethez igazodás legkönnyebben öntanuló, mesterséges intelligenciával érhető el.

1. Kéretlen levelek tartalmának értelmezése

A kéretlen levelek tartalmát, annak készítői folyamatosan megújítják, megpróbálva kikerülni a szűrőkön történő fennakadást. Az e-mail-ek mennyiségéből adódóan a vizsgálatot végrehajtani és elbírálni csak programok képesek, a folyamatos megújulást viszont leghatékonyabban MI alkalmazásával érhető el. Segítségével a védelmi szférába érkező kéretlen levél áradat

[107] mesterséges intelligencia

folyamatosan szűrhető, ezáltal a levelezőrendszer felhasználása és későbbi kihasználása a változó körülményekhez dinamikusan igazodva akadályozható meg.

2. Rendvédelmi e-mailcímek használatának monitorozása

A rendvédelmi e-mailcímeket azok használói – sajnos – nem csak elektronikus levelek fogadására, hanem azonosítóként is használják az internet nyújtotta szolgáltatások igénybevétele során, amely a szolgáltatásokból küldött visszaigazoló levelek érkezésekor válik nyilvánvalóvá. Ezen szolgáltatások egy része összefüggésben lehet a rendvédelmi feladatok ellátásával úgy, mint például munkáltatói intézkedések, vagy beiskolázással kapcsolatos értesítések elektronikus átvétele, azonban számtalan esetben magáncélú használatról van szó. Az e-mailcímek a kibertérben értéket képviselnek, széleskörű megjelenésük veszélyforrást jelent, ezért felkutatásuk érdekében célszerű lépéseket tenni. A MI-vel felruházott alkalmazás képes lehet az interneten terjedő rendvédelmi e-mailcímek feltérképezésére, figyelésére és a használat jogszerűségének eldöntésére. A közösségi szolgáltatásokban használt e-mailcímek visszaszorításával csökkenthető az informatikai rendszerek kitettsége és célponttá válása.

3.3 A Kritikus Internetes Szolgáltatások biztonságos üzemeltetése

„A Kritikus Internetes Szolgáltatásokkal szemben alapkövetelmény az állandó rendelkezésre állás biztosítása, a bizalmasság és a sértetlenség fenntartása mellett. Jelen írás azt foglalja össze, hogy a napi üzemeltetési gyakorlatban milyen általános és speciális védelmi intézkedéseket kell, vagy lehet tenni, a Kritikus Internetes Szolgáltatások biztonságos üzemeltetéséhez.

A Kritikus Internetes Szolgáltatások definíciójából és legmarkánsabb tulajdonságából egyenesen következik az a tény, hogy a szóban forgó interneten elérhető kiszolgáló programoknak állandó rendelkezésre állással, ugyanakkor az illetéktelen behatolás(ok) megakadályozásával kell működniük. Ezen feladatok együttes érvényre juttatásához összehangolt, tervezett és szakszerű megoldások foganatosítására van szükség.

A KRISZ folyamatos rendelkezésre állásához nélkülözhetetlen egy hálózati interfésszel és internetkapcsolattal rendelkező hardver, egy stabil, megfelelő erőforrás gazdálkodásra képes operációs rendszer, továbbá a szolgáltatást végző szerverprogram az összes szükséges alrendszerével együtt. A téma feldolgozásánál feltételezem, hogy a hardveres és az infrastrukturális adottságok, valamint szükségletek 100%-ban, azaz teljes mértékben biztosítják a rendszer működését, megjegyezve, hogy ezen feltételezés megvalósítása természetesen csak komoly ráfordítással érhető el és önmagában is kutatásra érdemes. A szoftveres elemekre

szűkítve tehát a KRISZ működését, kiemelkedő fontosságú az operációs rendszer-, valamint az általa vezérelt – hálózatról elérhető, illetve zárt – szolgáltatások kiegyensúlyozott, összehangolt működése.

3.3.1 Operációs rendszer üzemeltetése

Az operációs rendszer [84], mint a számítógép hardverével közvetlen kapcsolatban álló alapprogram, teret biztosít a végrehajtandó, vagy végrehajtás alatt álló szolgáltatások számára. Az összes felhasználói program felett áll, képes azok indítására, megszakítására, leállítására, tehát egyszerűen képes a beavatkozásra. Napjaink szolgáltatás orientált operációs rendszerei jogosultsági szintekkel rendelkeznek, melyben a hierarchia csúcsán álló kiemelt felhasználó a rendszer működésével kapcsolatos minden folyamatra ráhatással lehet.
A Kritikus Internetes Szolgáltatás is, mint bármely más folyamat teljesen alárendelt és kiszolgáltatott az operációs rendszernek, ezért úgy kell megszervezni az operációs rendszer üzemeltetését, hogy az lehetőleg ne kerülhessen illetéktelen „kezébe".

Behatolás megelőzése

Tekintettel arra, hogy a KRISZ biztosan egy internetről elérhető szolgáltatás, egyértelmű, hogy annak operációs rendszere közvetett kapcsolatban áll a világhálóval. Ahhoz, hogy az operációs rendszer ne kerülhessen illetéktelen irányítása alá, meg kell előzni a behatolást. Az internetről az operációs rendszerhez a szolgáltatások csatornáin keresztül vezet az út, ezért a nyitva hagyott hálózati portok számát a minimálisra kell csökkenteni. Egy frissen telepített operációs rendszer indításakor alapértelmezésben is számos hálózati szolgáltatás aktivizálódik, amelyek adott esetben feleslegesen kínálnak hálózati csatornákat a rossz szándékú felhasználóknak. Mivel minden hálózati szolgáltatás üzemeltetése biztonsági kockázat, a feleslegeseket ki kell kapcsolni, ezáltal erőforrás takarítható meg és csökkenthető a támadási felület.

A biztonságos üzemeltetés, így a hálózati szolgáltatások védelme érdekében erősen ajánlott tűzfal alkalmazása, amely többféle szempont szerint képes szűrni a hálózati adatforgalmat. Alkalmazástól függően többféle lehetőség kínálkozik a védelem megteremtésére, mégis célszerű reagáló képesség szerint rendszerezni a tűzfalak viselkedését.

1. Statikus tűzfal alkalmazása

A tűzfalak mechanizmusa egyrészt a csomagszűrésen (packet filter), másrészt az alkalmazási átjárón (application gateway) alapszik. Míg az előző az áthaladó csomagokat a forrás és a cél IP cím, illetve hálózati port szerint vizsgálja és dönt azok további sorsáról, addig az utóbbi a csomagok összeállását követően, az üzenet mérete vagy tartalma szerint engedélyezi, vagy tiltja a hálózati forgalmat. [14]

A tűzfal működését alapvetően az előre rögzített tűzfal-szabályok befolyásolják, amelyek a tartalom „értelmezése" szempontjából részben tekinthetők dinamikusnak is, azonban a szabályok bővítése, vagy változtatása aspektusából teljesen statikusak, váratlan eseményre nem képesek reagálni.

2. Dinamikus tűzfal alkalmazása

„A tűzfal alapötlete az, hogy megakadályozza a támadók be-, valamint a titkos adatok kijutását. Sajnos vannak azonban olyan emberek is, akiknek nincs jobb dolguk, mint hogy megpróbáljanak egyes helyeket térdre kényszeríteni. Ezt úgy érik el, hogy olyan nagy számban zúdítják az egyébként legális csomagjaikat a céljukra, hogy az összeomlik a terhelés alatt." [14]

Számos olyan szituáció létezik, amikor az előre megírt, egyébként a céljuknak teljesen megfelelő tűzfal szabályok nem képesek reagálni olyan eseményre, amely a KRISZ működését – könnyen – negatívan befolyásolhatja, vagy gátolhatja.

A próbálgatás (brute force[108]) alapú, vagy a szolgáltatás megbénítására irányuló (DoS[109], DDoS[110]) támadásokra megoldást jelenthet a napló állományok elemzése alapján, dinamikusan módosuló tűzfal szabályok alkalmazása. A reagáló képesség lényege, hogy az operációs rendszer állandó háttérfolyamataként egy program [85] vizsgálja és analizálja a megjelölt napló állományokat, majd annak tartalma szerint, előre rögzített eseményekre (pld. meghatározott időn belül túl gyakori kapcsolat létrehozás kérése) az előző pont szerinti statikus tűzfal szabályt aktivál, illetve a biztonság helyreállása esetén in-aktivál.

Rendszergazdai feladatok ellátása

Az operációs rendszereket időnként karban kell tartani, felhasználói hozzáféréseket kell kezelni, állományműveleteket kell végezni. A gyártók folyamatosan biztosítják a frissítő-,

[108] nyers erő
[109] Denial of Service - szoláltatásmegtagadással járó támadás
[110] Distributed Denial of Service - elosztott szoláltatásmegtagadással járó támadás

karbantartó csomagokat, amelyek – általában – a felfedezett programhibák és biztonsági rések javítását szolgálják és telepítésük erősen ajánlott. Kérdés, hogy az operációs rendszert üzemeltető rendszergazda milyen eljárással kívánja az adminisztrációs feladatokat végezni? Egyik lehetőség, hogy a szerverrel megteremti a fizikai kontaktust, amely – tekintettel arra, hogy az operációs rendszer kapcsolatban áll az internettel – valószínűleg több-kevesebb utazással jár, vagy kialakítja a távoli adminisztráció lehetőségét. Az utóbbi kézenfekvő megoldás, viszont egy plusz szolgáltatás fenntartásával és egy újabb kockázat viselésével jár, hisz behatolásra ad lehetőséget.

1. Távoli shell alkalmazása

Távoli shell-ként a továbbiakban azt a hálózaton keresztül elérhető parancsértelmezőt értem, amely az adott operációs rendszer típusától függetlenül, lehetőséget ad az operációs rendszerbe történő belépésre, majd ott – jogosultság és parancsértelmező függvényében – utasítások végrehajttatására.

A távoli elérés biztosításának és a megfelelő védelem kiépítésének problematikája sajnos megkerülhetetlen, mert a szolgáltatás fenntartása és a biztonságos üzemeltetés egymással ellentmondásban vannak, hisz

- az operációs rendszer és a telepített programok normális működése esetén a távoli shell egy „szükségtelen alkalmazás", mert biztonsági kockázatot jelent és fogyasztja az erőforrásokat;
- bármilyen operációs rendszer-, vagy szoftver-szintű probléma esetén a távoli shell az elsődleges megoldás a beavatkozásra, hiányában utazni kell a szerverhez.

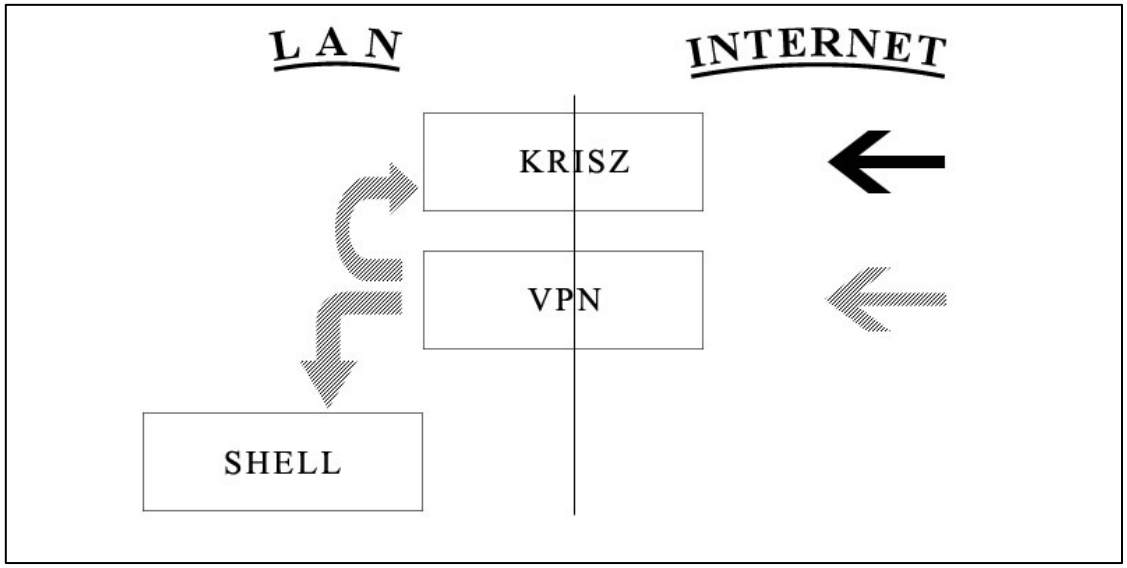
Alapvetően a távoli shell kiszolgálója egy biztonságos, titkosított csatornán ad lehetőséget a hozzáférésre, ugyanakkor próbálgatással, akár brute-force módszerrel előbb-utóbb – főleg gyenge jelszavak esetén – mégiscsak be lehet jelentkezni az operációs rendszerre, továbbá a próbálgatások kiszolgálása erőforrás vesztéssel és felesleges energia felhasználással jár.

Az ellentmondás feloldására megoldást jelenthet a távoli shell – szükség szerinti, – interneten keresztül történő ki-be kapcsolásának a lehetősége. A KRISZ feltételezhetően rendelkezésre fog állni, hisz az erőfeszítések alapvetően annak működése érdekében történnek, így lehetőséget adhat arra, hogy egy előre programozott eljárással és a szükséges jogosultságok

érvényesítésével a távoli shell ki-be kapcsolása megtörténhessen. Alkalmazásával a rendszeradminisztrátori feladatok biztonságosan végezhetők.

2. Virtuális magánhálózat (VPN) használata

„... a VPN-ek (Virtual Private Networks - virtuális magánhálózatok) a nyilvános hálózatok tetejébe épülnek, mégis rendelkeznek a magánhálózatok legtöbb tulajdonságával." [14] A VPN adta lehetőségeket kiválóan ki lehet használni a KRISZ-el kapcsolatos üzemeltetési feladatok biztonságának növelése érdekében. Az alap koncepció szerint, a KRISZ szerverét el kell látni plusz egy belső, internet előtt rejtett IP címmel, továbbá egy biztonságos VPN csatornát kell kiépíteni az internethez kapcsolódó interfészen keresztül. A virtuális magánhálózat csatornáján, a belső rejtett IP címhez kapcsolódva el lehet végezni azokat az üzemeltetési feladatokat, amelyek közvetlen internetes felületen keresztül kiemelten nagy kockázattal járnának (19. ábra).



19. ábra

VPN működtetése interfészek szerint; forrás: szerző

A VPN-en keresztül biztonságosan elérhető az előző pontban ismertetett távoli shell is, továbbá a KRISZ alrendszereként működő adatbázis-kezelőhöz is e titkosított csatornán keresztül ajánlott a közvetlen csatlakozás.

Helyreállítás biztosítása

A KRISZ működését biztosító operációs rendszeren elengedhetetlen ütemezetten mentéseket végezni, melynek magában kell foglalnia az operációs rendszer, valamint a KRISZ teljes értékű

helyreállításához szükséges adatokat. Nem várt esemény bekövetkezése esetén, a mentésből – minimális veszteséggel – visszaállíthatók azok az adatok, amelyek a rendszer újraindításához, ismételt működéséhez szükségesek. Az automatizált, rotációs rendszerű archiválások a legcélszerűbbek, amelyek lehetnek növekményes alapon-, vagy mindenre kiterjedően szervezettek. Az archívumokat célszerű úgy tárolni, hogy azok bármikor rendelkezésre álljanak, ugyanakkor védettek legyenek a külső környezeti hatásoktól.

3.3.2 KRISZ üzemeltetése

A KRISZ, mint kiemelt szolgáltatás üzemeltetésénél, a hangsúlyok részben eltérnek az operációs rendszernél megfogalmazottaktól, amelynek legfőbb oka a közvetlen internetes elérés. A biztonságos üzemeltetéshez legfőképpen az árulkodó információk elrejtésére és a felesleges támadási pontok megszüntetésére van szükség.

Érzékeny információk elrejtése

Függetlenül attól, hogy a KRISZ Web[111], Mail[112], FTP[113], vagy egyéb kiszolgálásra irányul, kerülni kell, hogy a szerverprogram önmagáról, vagy alrendszereiről felesleges – kompromittáló – információkat adjon ki. A fejlesztők gyakran alapértelmezésként úgy konfigurálják ezen programokat, hogy azok a kapcsolódásnál önmagukról és néha még az operációs rendszerről is minden, típussal és verziószámmal kapcsolatos információt kiadjanak. Természetes, hogy a támadó a szolgáltatás „térdre" kényszerítéséhez elsősorban pontosan azokat az információkat szeretné beszerezni, amelyek a támadás előkészítéséhez szükségesek. A programok hibáiról, gyengeségeiről, támadhatóságáról – az interneten is – fellelhető tudásbázisok rendezési elve, pontosan a programok típusára és verziószámára irányul, ezért a „tálcán kínált", – ismert – biztonsági réssel működő szolgáltatások kitettséget jelentenek a rossz szándékú internet használók felé. Ezért azon – alapértelmezett – beállításokat ki kell iktatni, amelyek a kiszolgáló programról, vagy az operációs rendszerről árulkodó információkat közölnek.

A Web alapú KRISZ gyakran olyan összetett szolgáltatás, amelyből a felhasználó felé közvetített információ, HTTP[114](s) protokollra ültetve, programozott módon, adatbázisból származtatva, interaktívan kerül előállításra. A Web népszerűségéből adódóan, az előre

[111] World Wide Web - világháló
[112] e-mail - elektronikus levelezés
[113] File Transfer Protocol - állomány átviteli protokoll
[114] HyperText Transfer Protocol

elkészített – tartalomkezelő – programok nagy számban jelentek meg, amelyek web-kiszolgálóra telepített használata közkedvelt, olcsó és KRISZ-ként is használható. Számos esetben ezek a Web-es rendszerek programozási hibákat, így támadható pontokat is tartalmaznak, ezért kiemelt fontosságú, hogy ne adjanak önmagukról a gyártóra, a verzióra, a mögöttes adatbázis-kezelőre, vagy az operációs rendszerre vonatkozóan információkat. Az árulkodó információk elrejtése az üzemeltető feladata, amely a legtöbb esetben kellő programozási gyakorlatot feltételez.

KRISZ karbantartása

Mint bármely szolgáltatást, időközönként a KRISZ-t is karban kell tartani, amelynek az operációs rendszer-, a kiszolgáló-, vagy a mögöttes információhalmaz változása egyaránt oka lehet, ezért meg kell teremteni a lehető legegyszerűbb, ugyanakkor kellően biztonságos adminisztrációs feltételeket. A KRISZ karbantartására az adminisztráció jellegétől függően, általában három ponton nyílik lehetőség.

1. Operációs rendszeren keresztül

A lehető legmagasabb jogosultsági szintű beavatkozást biztosítja, amely a KRISZ bármely pontjának megváltoztatására alkalmas. Használata általában a legmélyebb – akár operációs rendszer közeli – összetevők módosítása esetén (pld. programfrissítés) ajánlott, amelyhez a korábban részletezett hozzáférések biztosítása elengedhetetlen. Amellett, hogy ez a módszer a lehető legnagyobb mozgásteret biztosítja a szolgáltatás karbantartására, fontos kiemelni, hogy illetéktelen „kézre kerülése" esetén a KRISZ-re korlátlan csapás mérhető, tehát ezen karbantartási felület fenntartása veszélyes.

2. Adatbázis-kezelőn keresztül

Az adatbázis-kezelők szerepe kiemelt fontosságú a KRISZ működésében, hisz az adatbázisban tárolt adatok gyakran a szolgáltatás működésének alapját jelentik. Példaként említve a fájl-cserélő, mint KRISZ azon esetét, amikor a felhasználók, valamint a konfiguráció minden paramétere adatbázisban kerül tárolásra, a szolgáltatás karbantartása az adatbázis-kezelő adminisztrálásával – is – megoldható. Ez esetben az internet adta lehetőséggel élve, az adatbázis-kezelőhöz – a lehető legkisebb biztonsági kockázattal – adminisztrációs felületet szükséges biztosítani. Kifejezetten veszélyes az adatbázis-szerver közvetlen internetes elérhetőségének biztosítása, inkább javasolt valamely közvetett – például Web-es, vagy VPN-

es – hozzáférés megvalósítása. Illetéktelen hozzáférése esetén a KRISZ fájl-cserélő alapfunkciója kevésbé sérülhet, viszont – a felhasználói adatok kiszolgáltatottsága miatt, – a szolgáltatás alaprendeltetése meghiúsulhat, ezért célszerű és indokolt az adminisztrációs felülethez tartozó hozzáférési pontot rejtve tartása.

3. KRISZ adminisztrációs felületén

A KRISZ saját kiszolgálóján keresztül gyakran adminisztrálható is, amely meglehetősen kényelmes és kézenfekvő megoldás. Alapkövetelmény, hogy az adminisztrációs felület használatához csak valamilyen további jogosultság rendelkezésre állása esetén legyen lehetőség, illetve, hogy a sikeres bejelentkezéskor minden szükséges karbantartási eszköz elérhetővé váljon. A hozzáférési pont ismerete és a bejelentkezés sikeressége egyben az adminisztráció végrehajtásának a kulcsa.

Web-es szolgáltatás esetén gyakori beállítás, hogy az elérhetőség URL-jéhez egyszerűen hozzáillesztésre kerül az alapértelmezett „/admin" hivatkozás, amely ismeretében a felhasználó belépési lehetőséget kap az adminisztrációs felületre (pld. „http://www.kriszem.org/admin"). Nagy felelőtlenség és egyben komoly kockázatot hordoz magában az adminisztrációs bejelentkezési felület nyílt felajánlása, hisz a rossz szándékú felhasználó próbálgatással, vagy SQL Injection[115] típusú támadással adminisztrációs felülethez-, és jogokhoz juthat, amellyel a KRISZ működésében beláthatatlan károkat okozhat.

Kiemelten fontos tehát, hogy az adminisztrációs felület hozzáférése rejtett maradjon, ezért olyan, lehetőleg egyedi elérhetőséget kell beállítani – a „/admin" URL helyett –, amelynek kitalálása nagy energiát és sok időt követel meg a rossz szándékú felhasználótól. Fontos továbbá, hogy az adminisztrációs felülethez – akár kikényszerítetten – csak titkosított csatornán keresztül lehessen eljutni (pld. HTTPS protokoll), továbbá, hogy a bejelentkezési pont az Injection típusú támadásra ellenálljon.” [83]

[115] kód injektáló technika

Összegzés, következtetések

Összefoglalásra került, hogy a Kritikus Internetes Szolgáltatások Web-es megjelenésekor milyen intézkedéseket kell, vagy lehet tenni a biztonság fenntartásához. Megállapítható, hogy **az elmúlt több mint két évtized dinamikus IT fejlődésének köszönhetően, a Web, az Internet meghatározó információs platformjává vált**. A virtuális tér, mint lehetséges megjelenési pont, napjainkban társadalmi normaként, elvárásként van jelen és kihasználása standarddá vált. A hatalmas népszerűség tömegeket vonz a Web-kompatibilis eszközök (számítógép, okostelefon, különböző IT eszközök) elé és oltja az állandóan fellobbanó információs éhséget. **Az áldozatul esett, feltört, módosított weboldalak** azonban jól **mutatják, hogy egy hozzáértőbb kört kifejezetten szórakoztat a hibák, vagy figyelmetlenségek kihasználása és a károkat elszenvedők bosszantása**.

Az internetet-, és az okos eszközöket **használók folyamatos létszámemelkedése egyértelműen kihatással van az elektronikus levelezést igénybe vevők számára is, amely** egyenesen arányosan **előtérben tartja az e-mail címeket, mint lehetséges támadási célpontokat**. A nagyszámok törvénye miatt **a kiberbűnözők az elektronikus levelezést, mint eszközt, folyamatosan igénybe veszik**, az elektronikus levelezőrendszereket üzemeltetőknek pedig a biztonságot fenn kell tartaniuk.

Az elektronikus levelezés iránti igény a védelmi szférában – a belső kommunikációs csatornák rendelkezésre állása ellenére – **is folyamatosan nő**, ezért vele együtt **a biztonságra fordítandó kapacitást is bővíteni szükséges**. Figyelembe véve, hogy **az elektronikus levelezés még mindig az első számú, mindamellett „legális" támadási eszköz az interneten**, kiemelt figyelmet fordítottam a biztonsági kérdéseke. **A** levelezési rendszer **rosszindulatú felhasználás**ának **és kihasználás**ának **bemutatásával tártam fel** és alapoztam meg **a „nyitott biztonsági rés"-re vonatkozó véleményemet**. A központi biztonság azonban önmagában kevés, ha a felhasználók nincsenek megtanítva és felruházva a saját védelmük érdekében teendőkre. Az internetes hozzáféréssel rendelkező felhasználók a munkahelyüktől távol a kor vívmányainak segítségével keresik a leggyorsabb és legkényelmesebb levelező alkalmazásokat, gyakran figyelmen kívül hagyva a biztonsági szempontokat. A munkáltatóknak és az IT vezetőknek szem előtt kell tartaniuk a felhasználók laikusságát és kitettségét, ezért a szükséges intézkedéseket meg kell hozniuk. Természetesen – a humán erőforrás véges rendelkezésre állása miatt – figyelembe kell venni a MI adta lehetőségeket is és lehetőség szerint használatba kell venni azokat.

A Kritikus Internetes Szolgáltatásokkal kapcsolatos elvárásokat figyelembe véve, személyes tapasztalataimból is merítve foglaltam össze a biztonsággal kapcsolatos általános intézkedéseket. A KRISZ biztonságos üzemeltetése során ezért a hétköznapi gyakorlatból kiindulva vizsgáltam, hogy mi vezethet a KRISZ üzemképtelenségéhez. **A megkerülhetetlen üzemeltetési feladatokon keresztül bemutatásra került, hogy miként lehet a távoli elérés mellett a szükséges biztonságot fenntartani.** Természetesen a leírtakon túl további megoldások is segíthetnek, ugyanakkor egy alap lefektetésre került, amelyek betartásával a kockázatokat elviselhető szintre lehet csökkenteni. Le kell szögezni, hogy néha a legtökéletesebb üzemeltetési praktikák sem nyújtanak segítséget, mert nem védenek a szerverhez fizikailag hozzájutó támadóval-, a szolgáltatás megbénítására irányuló zombie hálózattal-, valamint a KRISZ-ben, vagy annak alrendszereiben rejlő programhibákkal, hátsó ajtókkal szemben.

4. FEJEZET

A KRISZ védelmi ajánlásai

A korábbiakból látható, hogy Kritikus Internetes Szolgáltatás megjelenhet egyrészt szolgáltatói-, másrészt igénybe vevői oldalon, a velük kapcsolatos védelmi intézkedések pedig részben átfedésben vannak, ugyanakkor néha markánsan eltérnek egymástól. Ebben a fejezetben ajánlásszerűen áttekintésre és felsorolásra kerülnek azok az általános-, vagy specifikus védelmi lehetőségek, amelyek segítik a KRISZ állandó rendelkezésre állásának biztosítását.

4.1 Összeköttetés védelme

Célja a KRISZ nyújtásához és igénybevételéhez szükséges kapcsolat és sávszélesség rendelkezésre állásának megteremtése, valamint a hálózati csatorna titkosított használatának elérése, ezért javasolt

- a saját hatáskörbe tartozó – szolgáltató – szerver részére elegendő és nagy rendelkezésre állással bíró sávszélesség biztosítása. A szervert célszerű olyan, nagy sávszélességű, lehetőleg – internet – gerinchálózatba kapcsolni, amely garantálja a szolgáltatást igénybe vevők részére a zavartalan információáramlást.
- az internetes szolgáltatásokat igénybe vevő kliensek részre elegendő sávszélesség biztosítása. Az igénybe vevők számát és lehetséges tartózkodási helyét figyelembe véve, elegendő és elérhető internet sávszélességet szükséges biztosítani.
- az internet elérést lehetőség szerint szabályozott formában, kontrolláltan rendelkezésre bocsátani. Érdemes élni weboldalak, vagy internet címek elérésének tiltásával, vagy engedélyezésével a megfelelő sorrendiség kialakításával.
- a titkosított csatornák alkalmazása. Indokolt a saját hatáskörbe tartozó szervereken a kommunikációt titkosított csatornába terelni, amely használatával megakadályozható, vagy megnehezíthető a lehallgatással, szaglászással történő információszerzés. Kiváló – akár ingyenes – titkosító eljárások állnak rendelkezésre, amelyek alkalmazása nagyban növeli a biztonságot.
- a hálózati eszközök biztonságban tartása. A KRISZ igénybevételének – helyszíntől függetlenül, – helyt adó rendszerben, a hálózati elemek fizikai hozzáférésének megakadályozásával, az illetéktelen személyek távol tarthatók.

- információbiztonsági eszközök alkalmazása és azok informatikai biztonsági szabályoknak megfelelő konfigurálása, amely megakadályozhatja az illetéktelen behatolásokat és védhet a célzott támadásoktól.

- a hálózati információk elrejtése. Minden hálózatban léteznek olyan – a működést meghatározó – beállítások, adatok, melyeket eltitkolni ugyan nem lehet, de kerülendő velük hivalkodni. Célszerű az IP címeket névfeloldással helyettesíteni, és feltűnés nélkül használni a tűzfal-, átjáró-, proxy-, adatbázis-szerverek címeit.

4.2 Szolgáltatások védelme

A szolgáltatás védelmének egyrészt a saját hatáskörű szolgáltatások nyújtására, másrészt az igénybe vett, létfontosságú szolgáltatások megőrzésére kell kiterjednie.

4.2.1 Nyújtott szolgáltatások védelme

A szolgáltatásnyújtás mindenképpen saját hatáskörű, függetlenül attól, hogy ahhoz esetleg külső erőforrás felhasználása is történik; a saját összetevőknek tökéletesen kell működniük, a külső forrásoknak pedig maradéktalanul rendelkezésre kell állniuk. A folyamatos, megszakítás nélküli szolgáltatásnyújtáshoz ajánlott

- stabil, ellenálló, szélsőségekre is felkészített szoftveres környezetet alkalmazni. Célszerű a már mások által is kipróbált, többször bizonyított programokat telepíteni és kerülni a különböző teszt verziók éles üzemű kipróbálását.
- megteremteni az adatbázis hozzáférések korlátozását. Az adatbázis-kezelőt indokolt biztonságosan, lehetőleg internetes tartományon kívül elrejteni, ha viszont megkerülhetetlen az internetes jelenlét, akkor erős azonosítással, titkosított csatornán keresztül kell az elérhetőséget biztosítani.
- a KRISZ és az adatbázis-kezelő közötti kapcsolatteremtéshez a mindenkori minimális jogosultsági szinteket alkalmazni és kerülni az elégségestől több jogosultság kiadását.
- az alkalmazott adatbázis-kezelési műveleteket a lehető legnagyobb precizitással megtervezni és az injektálás lehetőségét kizárni.
- az adatbázis karbantartására célzott, egyedi megoldásokat alkalmazni, a standard beállításokat kerülni, továbbá az erőforrásokat felemésztő adatbázis műveleteket nélkülözni.

- a webszerver többes kiszolgálása esetén (VirtualHost), a weboldalakat hermetikusan elkülöníteni egymástól. A KRISZ mellett lehetőleg másik weboldal ne üzemeljen, ha viszont az elkerülhetetlen, akkor meg kell akadályozni, hogy valamelyik oldal támadása esetén az operációs rendszert, vagy a KRISZ-t is támadás érje.
- információszegény hivatkozásokat (URL-t) alkalmazni, a forráskódok árulkodó jeleit kiiktatni, megszüntetni.
- a web-hez kapcsolódó összes adminisztrációs felületet és a nyilvánosságra nem tartozó elérhetőségeket elrejteni, a web hibakereső funkcióját éles üzemmódban nélkülözni, kikapcsolni.
- az elektronikus levelezési szolgáltatás rosszindulatú felhasználását-, és kihasználását megakadályozni, a kéretlen leveleket, és a hozzájuk csatolt kártékony kódokat hatékonyan kezelni, kiiktatni.
- az operációs rendszer KRISZ-en keresztüli elérhetőségét megakadályozni, a „hátsó ajtók”-at kiiktatni.
- bármilyen KRISZ-t befolyásoló karbantartás biztonságos végrehajtásának a kialakítása.
- szolgáltatások körültekintő, biztonságos beállítása. Némely szolgáltatás konfigurációs lehetőségei annyira sokrétűek, hogy jelentős időt és energiát jelent az aprólékos hangolás. Vállalni kell az időigényes, legapróbb részletekre is kiterjedő konfigurálást és ezáltal is törekedni kell a biztonságos üzemeltetésre.
- a rendszerállományok jogosultságait rendszeresen ellenőrizni. A kielégítő állapot ellenőrzésére szkriptek, programok állnak rendelkezésre, melyek futtatásával meg lehet győződni az operációs rendszer sértetlenségéről.
- a jelszavak biztonságos tárolása. Több lehetőség is rendelkezésre áll, napjaink szolgáltatásait gyakran virtuális felhasználók veszik igénybe. A hozzáféréseket mindenképpen kódoltan, megfelelően védett állományokban, vagy adatbázisban célszerű tárolni.
- a tűzfalak használata. Alkalmazása nélkül mind a hálózatok, mind a szerverek veszélynek vannak kitéve, ráadásul – lelkes fejlesztőknek köszönhetően – alacsony költségvetéssel is kiváló tűzfalak építhetők. Ajánlott a szolgáltatások túlterheléses támadása (DOS, DDOS) elleni védelemhez, továbbá a KRISZ szempontjából nem releváns igénybe vevők (például más országok felhasználóinak) kiiktatásához.

- a mentések ütemezett, visszatérő végrehajtása, amelyek segítségével a nem várt események bekövetkezése esetén visszaállíthatók az elveszett adatok. Az archívumokat célszerű a fizikailag elkülönítetten, megbízható, villámvédelmi helyen tárolni.
- szolgáltatások indítása és leállítása feletti közbenső felügyelet megvalósítása. A szerver távoli adminisztrációs felületét veszélyes fenntartani, ezért indokolt annak elérhetőségét olyan szolgáltatáson keresztül (például KRISZ) egyedi megoldással ki-, bekapcsolni, amely folyamatosan elérhető.

4.2.2 Igénybe vett szolgáltatások védelme

Furcsa kijelentés az igénybe vett szolgáltatás védelme, hisz valójában a szolgáltatás meghiúsulásának a védelmét jelenti, mert jelen esetben ez jelenti a negatív hatást.

Idegen hatáskörű szolgáltatások felhasználásának védelme

A nevében is benne van az idegen szó, amely érzékelteti, hogy az internetes szolgáltatás az igénybe vevő hatáskörén kívülről érkezik, amely egyébként természetes, hisz túlnyomó részt ez a konstrukció a jellemző. Attól, hogy egy internetes szolgáltatás saját hatáskörön kívülről érkezik, még lehet megbízható, ugyanakkor érdemes fenntartással kezelni és figyelni, hogy az azt nyújtó félnek van-e bármilyen elköteleződése a szolgáltatás fenntartására.

1. Elköteleződés alapú idegen szolgáltatások felhasználása

Ebben az esetben a szolgáltatónak – valamilyen ok miatt – kötelezettsége van a szolgáltatás fenntartására, amely az igénybe vevőnek egyfajta biztosítékot jelent. A kötelezettség lehet közvetlen, például szerződéses jogviszony alapján, vagy közvetetten jogszabályi kötelezettség miatt, amely a felek érdekeit összekapcsolja. Elköteleződés esetén a szolgáltatás rendelkezésre állása elvileg biztosított, ugyanakkor ajánlott

- a rendelkezésre állás tényszerűségét és körülményeit – az esetleges változások miatt – rendszeresen ellenőrizni és szükség esetén a problémát a szolgáltató felé jelezni.
- a lejáró szerződések, vagy a jogszabályi változások esetén a folytatásról időben és megnyugtatóan rendelkezni.
- az igénybevételhez tartozó jogosultságokat nyilvántartani és személyre szólóan kiosztani.

*2. Elköteleződés **nélküli** idegen szolgáltatások felhasználása*

Ezekre a szolgáltatásokra úgy kell tekinteni, hogy semmilyen garancia nincs azok további rendelkezésre állására, továbbá jogkövetkezménye sincs a megszűnésnek. Tehát amennyiben egy szolgáltatás igénybevétele olyannyira fontossá válik, hogy az nélkülözhetetlen másik folyamatok biztosításához, úgy potenciális veszélyként kell rá tekinteni. A szolgáltatást, amíg rendelkezésre áll fel kell használni, de úgy, hogy megszűnése ne okozzon nagyobb kárt. Cél a kiegyensúlyozott igénybevétel megteremtése, figyelembe véve, hogy a szolgáltatás csupán bizalmi elven működik, ezért ajánlott

- az igénybevétellel járó kockázatok minimalizálása. Érdemes kockázatértékelést végezni, beleértve a kieső szolgáltatás várható következményét és a lehetséges reakciókat is; a túlzott kockázattal járó igénybevételek helyett ajánlott alternatív megoldást keresni.
- nyilvántartást vezetni az elköteleződés nélkül igénybe vett idegen szolgáltatásokról és azok céljáról, valamint azok használatára helyi szabályokat létrehozni.
- a külső informatikai beszállítókat nyilatkoztatni e témakörben és a válasz függvényében felvezetni az általuk megadott szolgáltatást is a nyilvántartásba, továbbá indokolt esetben szerződésben kikötni az elvárásokat.
- törekedni az elköteleződés alapú szolgáltatás megteremtésére.

Saját hatáskörű szolgáltatások védelme

A szolgáltatók elleni internetes támadások gyakran az igénybe vevő kliens eszközökön keresztül történnek, ezért leegyszerűsítve: a saját hatáskörű szolgáltatást úgy kell igénybe venni, hogy az igénybevétel ne váljon támadás eszközévé, a szolgáltatás pedig támadás célpontjává. Saját hatáskörű szolgáltatást védeni igénybe vevőként tehát úgy lehet, hogy a kliens ne okozzon kárt a szervernek. Ez egyrészt jelenti azt, hogy kerülni kell a kártékony kód szerverre jutását, másrészt meg kell akadályozni a szerver illetéktelen kézbe kerülését. A saját hatáskörű szolgáltatások védelme érdekében nélkülözhetetlen a biztonságos igénybevétel megteremtése, amelyhez ajánlott

- biztonságos összeköttetés alkalmazása.
- a kapcsolat során cserélendő adatok érzékenységének megfelelő biztonságos –, akár steril – kliens környezet kialakítása.
- az alkalmazandó jelszavak és biztonsági kulcsok átmeneti, kliens oldali tárolásának kiiktatása.

- az elérhető szolgáltatás érzékenységéhez igazított biztonsági szintű – lehetőleg két lépcsős – azonosítás alkalmazása.
- a szolgáltatás által biztosított beavatkozás mértékéhez igazított, személyre szabott jogosultságok kiosztása.

Szolgáltatás igénybevétel általános védelme

Mind az idegen-, mind a saját hatáskörű szolgáltatások igénybevételénél ajánlott

- a használaton kívüli végpontok inaktiválása. A támadók szeretnének csatlakozni a hálózatokhoz, ezért keresik az elhagyatott aktív hálózati végpontokat. A nyilvántartásokat folyamatosan aktualizálni kell, s a magára hagyott végpontokat célszerű inaktiválni.
- a felhasználói fluktuáció lekövetése. A munkáltatóknál bekövetkező fluktuációt indokolt az információ-technológia szintjén is követni, mellyel szavatolható, hogy – mindig – csak és kizárólag az aktív dolgozóknak legyen hozzáférésük a rendszerekhez. A távozott egykori munkatársak aktívan hagyott belépési kódjai szándékos, vagy véletlen kellemetlenséget okozhatnak.
- a felhasználók visszatérő oktatása. A felmérések szerint 90 %-ban a felhasználók jelentik a biztonsági kockázatot, ezért nélkülözhetetlen őket rendszeres oktatásban részesíteni. Tudniuk kell, hogy a hozzáféréseket miért kell bizalmasan kezelni, mit jelent a social engineering és mit jelent a hálózatok védelme.
- a többletfunkciók tiltása. A munkaállomások támadása gyakran többletfunkciókat biztosító beépülő modulokkal valósul meg, melyek alkalmazása opcionális. A megfelelő arányú tiltások és engedélyezések beállításával, elviselhető mértékűre csökkenthető a kockázat.
- a hátrahagyott munkaállomások inaktiválása. Tipikus felhasználói magatartás a használatban levő munkaállomás felügyelet nélkül hagyása, amely komoly kockázatot jelent. Indokolt bizonyos üresjárati idő eltelte után kezdeményezni a kapcsolat megszakítását, vagy jelszavas képernyő-védelem indítását.
- munkaállomásokon a korlátozott jogok alkalmazása. Egyrészt megakadályozható, hogy a felhasználó programokat telepítsen, töröljön, vagy módosítson a munkaállomáson, másrészt szavatolható, hogy az alkalmazott hálózati, biztonsági és egyéb beállítások ne változzanak meg.

4.2.3 Általános védelmi intézkedések

Az általánosságban alkalmazandó védelmi intézkedések a KRISZ igénybevételének és nyújtásának területére egyaránt érvényesek, ezért összesítve kerülnek feltüntetésre. Betartásuk az alacsony befektetés ellenére is jelentősen csökkenti a szolgáltatások támadásának kockázatát, ezért ajánlott

- az operációs rendszerek, alkalmazások folyamatos frissítése. A programok gyártóinak konkurencia harca gyakran hibás, vagy biztonsági réseket tartalmazó kódok fejlesztéséhez vezet. A nyilvánosságra kerülő hibák kihasználhatók, gyenge láncszemek, ezért a gyártók által kiadott javításokat szükségszerű alkalmazni. A programok készítői – általában – internetes frissítő oldalak üzemeltetésével biztosítják a legfrissebb javítócsomagok letöltését.
- kártékony programok elleni védelmi rendszer használata és az adatbázisok folyamatos frissítése. A rosszindulatú kódokat távoltartó alkalmazások elengedhetetlenek, és azok adatbázisait is naprakészen kell tartani, hogy felismerjék a legújabb kártékony programokat.
- mindenhol jogosultságok alkalmazása és a biztonságos jelszavak kikényszerítése. A megfelelő bonyolultságú jelszavak kikényszerítése, illetve az alapértelmezett jelszavak megváltoztatása nagyban megnehezíti a támadási lehetőségeket. A jogosultsági szintek beállításával meghatározható a rendszerben tárolt állományok, adatbázisok illetékessége.
- a használaton kívüli szolgáltatások kikapcsolása. Egy operációs rendszer telepítése után, szerver és munkaállomás tekintetében egyaránt rengeteg használaton kívüli szolgáltatás működhet. Minden hálózati szolgáltatás üzemeltetése biztonsági kockázat, ezért a feleslegeseket ki kell kapcsolni, ezáltal erőforrás takarítható meg és csökkenthető a támadási felület.

Összegzés, következtetések

Ahogy a létfontosságú-, vagy Kritikus Internetes Szolgáltatások témakörével sem, úgy értelemszerűen azok védelmével sem foglalkozott bővebben a tudomány ezidáig. Internetes szolgáltatások védelmi ajánlásai természetesen régóta léteznek, azonban az általam készített ajánlás egyrészt a kritikus kategóriába sorolt internetes szolgáltatásokkal foglalkozik, másrészt, egyaránt koncentrál annak szolgáltatói és felhasználói oldalára. **Az ajánlással igyekszem rendszerezve, és nem csak informatikus szemmel segíteni a Kritikus Internetes Szolgáltatásokat igénybe vevők, vagy nyújtók munkáját.**

Az összeköttetés védelmére tett javaslatok a kommunikációban résztvevő felek közötti információs csatorna állandó rendelkezésre állását, az adatmennyiséghez igazodó adatátviteli kapacitást, valamint a kommunikáció biztonságát hivatottak szavatolni.

A szolgáltatás nyújtásra vonatkozó ajánlások a szolgáltató rendszer részeinek, alrendszereinek és elemeinek taglalásával, egységekre bontva ad kézzel fogható megoldást mind a biztonság, mind a stabilitás témakörében. A spektrum a szoftveres alapkörnyezettől, a karbantartási tevékenységen át az adatok védelméig lefedi a tevékenységet.

A szolgáltatás igénybevételének védelme egy absztrakt megközelítés, ugyanakkor szintén létfontosságú, ezért is hiánypótló az ebben a témában tett ajánlások összegzése. Alapvető különbség van a saját-, és az idegen hatáskörű internetes szolgáltatások igénybevételében, így két különálló részben foglaltam össze az adott területre alkalmazható megoldásokat, továbbá egységbe foglaltam az általánosan alkalmazható lehetőségeket.

Az **általános védelmi intézkedések** részben, a két nagy terület specialitásain kívül, összevontan teszek ajánlást az alkalmazandó, támadást megakadályozó lépésekre.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Dolgozatomban megfogalmaztam, hogy az internetes szolgáltatások működése infrastruktúra specifikus, ezért a – rendelkezésre állás szükségessége miatt – kritikussá minősített típusok megközelítésére a kritikus infrastruktúrák-, az információs infrastruktúrák-, és a kritikus információs infrastruktúrák tudományos magyarázata a leghelyénvalóbb. **Megállapítottam, hogy önmagában a KI, a KII és a KRISZ is önálló halmazt alkotnak, viszont közös metszetük esetén a KRISZ leállása a társadalom jelentős hányadára is kihatással van, vagy miatta a kormányzat valamely szereplője nem képes feladatait maradéktalanul ellátni.** Az internetes szolgáltatások főbb infrastrukturális szükségletei az építmény, az áramellátás, a hűtés, az internetes átviteli közeg, valamint a számítástechnikai hardver elemek, ugyanakkor ezek összessége még mindig nem elegendő azok működtetéséhez. Egy internetes szolgáltatás létfontosságúvá válása mindenkire nézve szubjektív, ezért **a KRISZ definícióját az infrastrukturális kötöttségek rendelkezésre állását feltételezve, a szolgáltatási tevékenységet és a szolgáltatás leállásának következményeit alapul véve fogalmaztam meg.** Az infrastrukturális háttéren túl, dolgozatomban részleteztem azokat a további nélkülözhetetlen elemeket, amelyek egy internetes szolgáltatást „felépítenek”. A szolgáltatások vizsgálata során –, a kommunikáció működését alapul véve – egyértelművé vált, hogy milyen összetevők szükségesek azok sikeres igénybevételéhez, továbbá a KRISZ aspektusai is számbavételre kerültek. Áttekintettem, hogy miként alakul ki kötődés internetes szolgáltatásokhoz, az milyen következményekkel jár, és miként változnak kritikussá azok az igénybe vevők számára.

Az internetes szolgáltatások létfontossága, kritikussága leginkább akkor válna egyértelművé, ha azok elérhetősége megszűnne, ezért ezt a feltételezést volt hivatott alátámasztani az a védelmi szféra dolgozói által kitöltött kérdőív, amely racionálisan, mérhetővé konvertálta a felhasználók véleményét, érzését. **A gyakorlatban, kérdőíves felméréssel bizonyítottam, hogy egyes internetes szolgáltatások rendelkezésre állása nélkül, a rendvédelmi szervek feladataikat nem képesek maradéktalanul ellátni.** A kérdőív több hónapos előkészítő munka után, felhasználók bevonásával nyerte el végső formáját, a kitöltésére pedig három hónap állt rendelkezésre. A rendvédelmi szervek mindegyike – felsőbb vezetőkön, vagy ismeretség alapján, – e-mail formájában megszólításra került, és kitöltésében a titkosszolgálatok kivételével mindenki részt is vett. A kitöltési hajlandóság kimagasló volt, a nem kötelezően kitöltendő mezőkre nagy többségben érkezett válasz, és szándékos rontásra, vagy ellentmondásos kitöltésre nem volt példa.

Az elméleti megközelítést alátámasztotta a felmérés, amely a védelmi szférában előforduló internetes szolgáltatások igénybevételére és nyújtására egyaránt kitért.

Bebizonyosodott, hogy az internetes szolgáltatások meghatározzák a mindennapokat, azok elérhetetlenné válása a működésre súlyos kihatással van, így Kritikus Internetes Szolgáltatások a hipotézisnek megfelelően igenis léteznek. Az internetes szolgáltatások hiánya a védelmi szférában is azonnal észrevehető, azok gyakorlatilag a munkavégzés szoros kellékévé váltak, amit alátámaszt azt a tény is, hogy **a rendvédelmi szerveknek kötelezettségük van internetes szolgáltatások működtetésére**, következésképpen azok igénybevételére is. A nevesített internetes szolgáltatások elemzésekor bizonyosságot nyert, hogy minden rendvédelmi szerv

- működtet információs, tájékoztató honlapot, hírfolyamot és elektronikus ügyintézést;
- biztosít e-mail, webmail hozzáférést a dolgozóinak;
- titkosított internetes csatornán keresztül, rendelkezésre állít bizonyos felhasználói körnek hozzáférést az informatikai rendszeréhez.

Az internetes szolgáltatások rendszerszintű vizsgálata során **megállapítottam, hogy azok alrendszerekre és rendszer-elemekre bonthatók, amelyek a rendszerben betöltött szerepüknek megfelelően befolyásolják az internetes szolgáltatások működését.** Megvizsgáltam a KRISZ működését közvetlenül és közvetetten támogató alrendszereket, valamint azok funkcióit. **Megállapítottan, hogy az internetes szolgáltatásoknak léteznek megkerülhetetlen alrendszerei, amelyek közül kiemelkedők az adatbáziskezelők, amelyek korunk információs társadalmának és vele együtt az informatikai szolgáltatásoknak is nélkülözhetetlen elemei.** Bemutattam, hogy az adatbázis kezelők milyen formációban és kapcsolódási pontokkal működhetnek az internetes szolgáltatások mellett, előnyeikkel és hátrányaikkal együtt. Az adatbázisokban tárolt adatok általánosságban „aranyat érnek”, amely álláspontom szerint érvényes az internetes szolgáltatások mögött meghúzódó adatokra is. Az elvégzett vizsgálataimból azt a következtetést vontam le, hogy az adatbázisokban tárolt adatok egyrészt befolyásolják az internetes szolgáltatások működőképességét, másrészt a rosszindulatú tevékenységet folytatók célpontja, **ezért az adatbáziskezelők internetes szolgáltatások melletti működése kiemelt fontosságú.** Megállapítottam, hogy az internetes szolgáltatás és az adatbázis kezelő folyamatos kapcsolata miatt a támadóknak állandó felület áll rendelkezésükre az adatok megszerzéséhez, vagy kompromittáláshoz, és a védelmet legtöbb esetben magának az internetes szolgáltatás felhasználói felületének kell biztosítania. Az adatbázisokban rejlő

adatok karbantartása időközönként elkerülhetetlen, amely felület internetes elérhetősége mindenképpen kockázattal jár. Ezt támasztják alá gyakorlati tudományos kutatási tapasztalataim, amelyek során megállapítottam, hogy egy internetes szolgáltatás mögött megtalálható, elérhető és manipulálható adatbázis káros következményekkel járhat az internetes szolgáltatás működésére.

Az internetes szolgáltatásokat „fogyasztó" társadalom szokásaival párhuzamosan, a Kritikus Internetes Szolgáltatások megjelenési formái is hasonló képet mutatnak. Léteznek markáns, jellemző, népszerű szolgáltatási platformok, amelyeket, mint internetes szolgáltatási rendszereket mutattam be, leginkább szem előtt tartva az állandó rendelkezésre állás és a biztonságos üzemeltetés követelményét. A Web pillanatnyilag is a legnépszerűbb internetes tájékoztatási forma, minden rendvédelmi szerv tart fenn saját honlapot, azokon pedig kötelező és választható tartalmakat egyaránt megjelentet. Fejlődésének köszönhetően számtalan alrendszeri elemmel rendelkezhet, biztosított benne az interaktivitás lehetősége, számtalan fejlesztési-, és keretrendszer áll rendelkezésre, amelyek persze hibázásra is adnak lehetőséget. Áttekintettem, hogy milyen szempontokat kell figyelembe venni egy stabil, hibatűrő webszerver működtetéséhez, továbbá milyen biztonsági intézkedéseket kell megtenni a Web támadásainak elhárításához.
Az elektronikus levelezés népszerűsége vetekszik a Web népszerűségével, továbbá rendelkezésre állása is több évtizedre tekint vissza, ugyanakkor a Kritikus Internetes Szolgáltatások szempontjából teljesen eltérő funkcióval rendelkezik. Megkerülhetetlen kommunikációs eszköze az internetnek, amely egy internetes szolgáltatás által ember – ember, felhasználó – felhasználó közötti kapcsolattartást eredményez, amelyben minden informatikai adat, fájl, szöveg továbbítható. Az elektronikus levelező rendszer kettős szerepet is betölt, hisz egyrészt lehet támadási célpont, másrészt lehet támadási eszköz. Az elektronikus levelezés a teljes védelmi szférában rendelkezésre áll, minden rendvédelmi szervnek van saját interneten elérhető webmail rendszere, és szinte minden dolgozónak lehet saját munkahelyi e-mail címe. Ez a tény azt is alátámasztja, hogy az elektronikus levelezés a védelmi szférában még mindig a legfőbb kommunikációs eszköz, így a szolgáltatás leállása rövid időn belül információhiányt idézne elő. A hozzáférés a rendvédelemmel szemben is adott, minden kitudódott e-mail cím lehet támadási pont, azaz kártékony kódok elhelyezésére alkalmas célhely. Dolgozatomban rámutattam, hogy a világon minden internetet használó személynek átlagban kettő darab e-mail címe van, továbbá az e-mail címet a személy megtestesítésére, beazonosítására használják,

illetve a személyek beazonosításához az e-mail a legfőbb hitelesítő eszköz. **Rámutattam arra a tényre is, hogy az elektronikus levelezés az interneten még mindig a legfőbb támadási eszköz, illetve bemutattam, hogy mit jelent a levelezőrendszer felhasználása és kihasználása.** Az elektronikus levelezésben egyfajta szélmalomharc folyik a kártékony kódok és a kéretlen levelek tömege ellen, amely környezetben a megfelelő védelmi intézkedések alkalmazása nélkül, ezen internetes szolgáltatás mások számára szolgál eszközként kibertámadás végrehajtásához.
Egy internetes szolgáltatás üzemeltetése során visszatérően jelentkeznek olyan üzemeltetési feladatok, amelyek megkerülhetetlenek. Összefoglaltam azokat a megoldásokat és betartandó biztonsági intézkedéseket, amelyek hosszú távon segíthetnek megőrizni az internetes szolgáltatások rendelkezésre állását.

Az általam, a dolgozatban javasolt védelmi ajánlások rendszerezve, a KRISZ felépítéséhez igazodva tudnak segítséget adni azok felhasználóinak, és üzemeltetőinek. Látható, hogy a védelem kialakításában mindenkinek része van, a felhasználóktól a vezetőkig széles spektrumban képződnek feladatok. Természetesen a felsorolást lehet-, és szükséges is bővíteni, amelyet majd a gyakorlat és a KRISZ további terjedése alakít, azonban a mostani leírás mindenképpen egy olyan mankó, amely jó kiinduló pontot jelent a folytatáshoz. Természetesen a védelmi felfogások és szemléletek is eltérőek, a mostani egy hosszú évek rendszergazdai gyakorlatával rendelkező-, ugyanakkor döntési helyzetben is résztvevő felhasználó szemszögéből születtek.

TUDOMÁNYOS EREDMÉNYEK

Az elvégzett vizsgálataimat, valamint a tudományos kutatómunkámat a következő tudományos eredményekben foglalom össze:

1. **Megfogalmaztam a Kritikus Internetes Szolgáltatások létezését, megalkottam definícióját és tartalmi elemeit.**

Az internetes szolgáltatások kritikussága sokkal inkább szubjektív, mint a hátteret biztosító eszközöké, szolgáltatásoké, ezért létezésükhöz a fennálló függőségeket és az esetleges megszűnés következményeit kellett vizsgálnom. Feltártam, hogy az internetes szolgáltatások kritikussága függ a szolgáltatások mögött húzódó infrastruktúráktól, továbbá az adott internetes szolgáltatás leállásának, kimaradásának hatásaitól, következményeitől. Figyelembe véve, hogy a háttérszolgáltatások leállásának egyenes következménye az internetes szolgáltatások megszűnése, evidens, hogy a Kritikus Internetes Szolgáltatás levezetése a függőségi viszonyból eredően onnét származtatható. **A definícióhoz a kritikus infrastruktúrák és a kritikus információs infrastruktúrák megfogalmazásaiból kellett kiindulnom**, figyelembe véve, hogy a Kritikus Internetes Szolgáltatás minden esetben részhalmaza a felette álló infrastruktúráknak.

2. **Levezettem a Kritikus Internetes Szolgáltatások lehetséges kialakulását, kialakítását.**

Rámutattam, hogy egyes internetes szolgáltatásokhoz az igénybe vevők részéről fennálló kötelezettség, vagy saját elhatározás miatt kötődés-, sőt néha függőség alakul ki, amely így kritikussá transzformálja az internetes szolgáltatásokat, így azok a „fogyasztók” lételemévé válnak. A kötődés kialakulása szolgáltatói érdek azzal a céllal, hogy a felhasználók adott internetes szolgáltatáshoz forduljanak, és ahhoz rendszeresen vissza is térjenek. Rávilágítottam, hogy a védelmi szféra hétköznapi működésében megjelenő, internetes szolgáltatásokra irányuló kötődés miként alakíthatja azokat rövid időn belül létfontosságúvá, kritikussá, továbbá mit jelent a kötődésből átalakult függőség és annak milyen következményei lehetnek.

3. **Bizonyítottam, hogy Kritikus Internetes Szolgáltatások mind a védelmi szférában, mind a hétköznapokban léteznek.**

Tényként kezelve, hogy a védelmi szféra az internet alkalmazása szempontjából egy szegmensét képviseli a társadalomnak, megállapítható, hogy amennyiben a védelmi szférában léteznek Kritikus Internetes Szolgáltatások, úgy a társadalomban is, sőt ott sokkal nagyobb nagyságrendben vannak jelen. Egy internetes szolgáltatás hiányát mérhetővé és tudományosan

beazonosíthatóvá tenni az érintettek, azaz a felhasználók objektív megkérdezésével lehet leginkább. A védelmi szférában készült felmérés kitért az internet „fogyasztói”, és szolgáltatói oldalára egyaránt, továbbá vizsgálta az esetleges megszűnés, vagy leállás következményeit is. **A**z aktuális **jogszabályokban található**, internetes megjelenéssel kapcsolatos **kötelezettségek**, továbbá **az (információs) infrastruktúrák**, mint háttérszolgáltatások **kritikusságára irányuló kutatások**, **valamint a védelmi szférában készített felmérés együttesen bizonyítja, hogy** internetes szolgáltatások is lehetnek kritikusak, ezáltal **a Kritikus Internetes Szolgáltatások léteznek**. A felmérésben szereplő, nevesített internetes szolgáltatások összegzése és csoportosítása, valamint a témában folytatott ezirányú **kutatómunkám feltárt számos, kritikusnak számító internetes szolgáltatást** mind általánosságban, mind rendvédelmi alkalmazásban.

4. **A Kritikus Internetes Szolgáltatások biztonságának vizsgálatával rámutattam azok lehetséges támadására, továbbá bizonyítottam a védekezés szükségességét és a védelemben alkalmazható legjobb gyakorlatokat.**
A KRISZ alrendszereinek és rendszerelemeinek feltérképezése és **vizsgálata bizonyította, hogy** az internetes szolgáltatás **annyira ellenálló, mint az őt alkotó egységek leggyengébb eleme, továbbá** egyértelművé vált, hogy **az adatbáziskezelő** mint alrendszeri elem, **elengedhetetlen napjaink Kritikus Internetes Szolgáltatásaiban.** Az adatbáziskezelő, valamint az adatbázisok vizsgálatával **bemutattam, hogy önmagában a tárolt adatok biztonságának hiánya is elegendő a KRISZ rendeltetésszerű működésének meghiúsulásához**. A leggyakrabban előforduló internetes szolgáltatásokon keresztül, amelyek egyben a legtöbbször előforduló Kritikus Internetes Szolgáltatások is, **bemutattam a Kritikus Internetes Szolgáltatási rendszereket, foglalkoztam azok biztonságos üzemeltetésével, illetve biztonsági kérdéseivel**. Az elektronikus levelezés működésének részletezésével rámutattam annak kettős szerepére, hisz egyrészt állandó támadási célpontot jelent, másrészt támadási eszközként is funkcionál.

5. **Védelmi ajánlást fogalmaztam meg a Kritikus Internetes Szolgáltatások biztonságos és eredményes üzemeltetéséhez, fenntartásához.**
Az ajánlás átfogó, gyakorló informatikai és vezetői eszköz lehet a Kritikus Internetes Szolgáltatások fenntartására, a hosszútávú igénybevétel biztosítására.

Ajánlások

Az értekezésben megfogalmazottak további hasznosíthatóságát az alábbiakban látom:

1. Felhasználható a Nemzeti Közszolgálati Egyetem oktatási tevékenysége során, kiemelten a Hadtudományi és Honvédtisztképző Kar nemzetbiztonsági alap és mesterképzésén, valamint a Nemzetbiztonsági Intézet által oktatott tárgyak esetében, akár önálló oktatási anyagrészenként, akár forrásmunkaként, akár ajánlott irodalomként.

2. Az egyes fejezetek következtetései részben a leírtaknak megfelelően, további tudományos vizsgálatok, kutatások alapját képezheti, így például a Kritikus Internetes Szolgáltatások szélesebb körű vizsgálata, felmérése is megvalósítható.

3. A dolgozatomban feltártakat ajánlom felhasználásra a védelmi szférában dolgozó vezetőknek és informatikusoknak egyaránt, az informatikai szabályozások megalkotása-, az informatikai tárgyú beszállítókkal kötött szerződések előkészítése-, valamint az internetes szolgáltatások üzemeltetése során.

4. Az internetes szolgáltatások biztonsági kérdéseivel foglalkozó részeket mindenképpen ajánlom az internetet közvetlenül-, vagy közvetetten jövedelemszerzésre használó vállalkozások tulajdonosainak, illetve azon magánszemélyeknek, akik bármilyen formában tartósan működtetnek internet végpontot.

5. Az elektronikus levelezésről szóló fejezetet minden e-mail címmel rendelkező internet használónak ajánlom saját-, és mások internetes biztonságának fenntartása érdekében

Fogalomtár-, és rövidítések jegyzéke

Bv.		büntetés-végrehajtás
BVOP		Büntetés-végrehajtás Országos Parancsnoksága
CGI	Common Gateway Interface	közös átjáró interfész
CPU	Central Processing Unit	központi vezérlő egység, mikroprocesszor
DB	database	adatbázis
DDoS	Distributed Denial of Service	elosztott szoláltatásmegtagadás
DNS	Domain Name Server	névszerver
DoS	Denial of Service	szoláltatásmegtagadás
FTP	File Transfer Protocol	állomány átviteli protokoll
GUI	graphical user interface	grafikus felhasználói felület
HDD	hard disk drive	merevlemez
HTML	HyperText Markup Language	hiperszöveges jelölőnyelv
HTTP	HyperText Transfer Protocol	hipertext átviteli protokoll
HTTP daemon		webszerver
HTTPS	HyperText Transfer Protocol Secure	biztonságos hipertext átviteli protokoll
II		információs rendeltetésű infrastruktúra
IMAP	Internet Message Access Protocol	Internetes üzenet-hozzáférési protokoll
IP	internet protocol	internet protokoll
IT	Information Technology	információ technológia
KI		kritikus infrastruktúra
KII		kritikus információs infrastruktúra
KRISZ		Kritikus Internetes Szolgáltatás
LAN	Local Area Network	helyi hálózat
MDA	Mail Delivery Agent	levél kézbesítő ügynök
MEMORY		memória
MTA	Message Transfer Agent	levéltovábbító ügynök
MUA	Mail User Agent	ügyfélkiszolgáló
NAV		Nemzeti Adó- és Vámhivatal
NCSA	National Center for Supercomputing Applications	
OWA	Outlook Web Access	
PHP	Hypertext Preprocessor	Hypertext előfeldolgozó

POP	Post Office Protocol	posta protokoll
PPP	Point to Point Protocol	pont-pont protokoll
PRG		program
SMTP	Simple Mail Transfer Protocol	egyszerű levéltovábbító protokoll
SMTP AUTH	SMTP Authentication	SMTP azonosítás
SQL	Structured Query Language	strukturált lekérdezőnyelv
SSH	Secure Shell	biztonságos parancsfuttató környezet
SSL	Secure Sockets Layer	biztonságos tartó réteg
TCP	Transmission Control Protocol	átvitelvezérlő protokoll
TEK		Terrorelhárítási Központ
TLS	Transport Layer Security	biztonságos átviteli réteg
URL	Uniform Resource Locator	egységes erőforrás-azonosító
VPN	Virtual Private Network	virtuális magánhálózat
W3		lásd:WWW
Web	World Wide Web	világháló
WinRM	Windows Remote Management	Windows távoli menedzselése
WLAN	Wireless LAN	vezeték nélküli hálózat
WWW	World Wide Web	világháló
	account	felhasználói hozzáférés
	adware	reklámprogram
	APP server	applikáció kiszolgáló
	application gateway	alkalmazási átjáró
	Auth relay	jogosultsághoz kötött levéltovábbító
	backdoor	hátsóajtó
	Browser	böngésző
	brute force	nyers erő, próbálgatási módszer
	brute-force	nyers erő
	cache	gyorsítótár
	debug	nyomkövetés, hibakövetés
	deface	honlapcsere
	domain	tartomány
	dropper	rosszindulatú kódot előállító trójai program
	EMAIL SYSTEM	levelezőrendszer
	Exploit	kihasználás
	HTTP prg.	webprogram
	keylogger	billentyűnaplózó program

	LOGIN	LOGIN SMTP azonosítás
	malware , malicious software	rosszindulatú szoftver
	M-APP	Saját protokollal működő levelezőprogramok
	MD5	MD5 SMTP azonosítás
	MI	mesterséges intelligencia
	Open relay	nyílt levéltovábbító
	owned	megszerzett, tulajdonlott
	packet filter	csomagszűrés
	PLAIN	PLAIN SMTP azonosítás
	plugin	program komponens, beépülő modul
	proxy	közvetítő
	ransomware	zsarolóvírus
	Relay	továbbító
	scareware	megtévesztő program
	shell	héj
	social engineering	pszichológiai manipuláció
	socket	csatlakozó
	spam	kéretlen levél
	spyware	kémprogram
	SQL Injection	kód injektálás
	standalone	egyedülálló
	VirtualHost	több domain-t kezelő webszerver
	xBase	dBase kompatibilis adatbáziskezelő

Ábrák jegyzéke

Táblázatok jegyzéke

Diagramok jegyzéke

A témakörben megjelent publikációim

Lektorált folyóiratban megjelent cikkek:

1. Jéri Tamás: The Security Of Databases In Critical Internet Services, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919; Online: http://hadmernok.hu/153_18_jerit.pdf;
2. Jéri Tamás – Pándi Erik – Jobbágy Szabolcs: A hálózatok világa, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 168-177. oldal, 2010.; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
3. Jéri Tamás – Pándi Erik – Jobbágy Szabolcs: A hálózatok védelmi aspektusai, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 210-220. oldal, 2010; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
4. Jéri Tamás – Pándi Erik – Tóth András: A kommunikációs infrastruktúrákkal szembeni rosszakaratú tevékenységek:,
   Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 276-288. oldal, 2010.; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
5. Jéri Tamás: A kommunikációs eszközök fejlődésének kihatásai a büntetés-végrehajtás rendszerére, Hadmérnök VII. Évfolyam 2. szám - 2012. június ISSN 1788-1919; Online: http://www.hadmernok.hu/2012_2_jeri.pdf;
6. Jéri Tamás: Kritikus internetes szolgáltatások, Hadmérnök VIII. Évfolyam 1. szám - 2013. március ISSN 1788-1919; Online: http://www.hadmernok.hu/2013_1_jerit.pdf;
7. Jéri Tamás: A kritikus internetes szolgáltatások biztonságos üzemeltetése, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_20_jerit_2.pdf
8. Jéri Tamás: Az adatbázis-kezelők szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_19_jerit_1.pdf
9. Jéri Tamás: A Web szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919; Online: http://www.hadmernok.hu/153_17_jerit.pdf

Konferencia kiadványban megjelent cikk:

10. Jéri Tamás: A Kritikus Internetes Szolgáltatások alrendszerei, A Haza Szolgálatában konferenciakötet; Társadalom és Honvédelem XVII. évf. 3-4. szám ISSN 1417-7293 2013. 205-214. oldal;

Felhasznált irodalom

[1] Jéri Tamás: Kritikus internetes szolgáltatások, Hadmérnök VIII. Évfolyam 1. szám - 2013. március ISSN 1788-1919;
Online: http://www.hadmernok.hu/2013_1_jerit.pdf;

[2] Országos Rendőr-főkapitányság, Közigazgatási Hatósági Szolgálat;
https://kozigbirsag.police.hu/; letöltve: 2020.04.21.

[3] Révész Béla: Egyszerű és hatékony, 2017.03.27; https://honvedelem.hu/cikk/egyszeru-es-hatekony/; letöltve: 2020.03.16.

[4] Magyar Közlöny Lap- és Könyvkiadó Kft., Nemzeti jogszabálytár;
http://njt.hu/cgi_bin/njt_doc.cgi?docid=140039.379553; letöltve 2020.03.16

[5] Dr. Várhegyi István, Dr. Makkay Imre: Információs korszak, információs háború, biztonságkultúra. OMIKK, Budapest, 2000. ISBN 963-593-238-3

[6] Magyar Közlöny Lap- és Könyvkiadó Kft., Nemzeti jogszabálytár;
http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.369611; letöltve: 2020.03.16.

[7] Magyar Közlöny Lap- és Könyvkiadó Kft., Nemzeti jogszabálytár;
http://njt.hu/cgi_bin/njt_doc.cgi?docid=193173.377340; letöltve: 2020.03.16.

[8] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról; Hatályos: 2008.12.17 - 2014.03.05

[9] BM Országos Katasztrófavédelmi Főigazgatóság, Kritikus infrastruktúrák védelmével összefüggő hatósági feladatok, jogszabályok;
https://www.katasztrofavedelem.hu/109/kritikus-infrastruktrk-vdelmvel-sszefgg-hatsgi-feladatok-jogszablyok; letöltve: 2020.03.16.

[10] Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005. ISBN: 963-327-391-9

[11] Európai Bizottság, *Zöld Könyv egy Kritikus Infrastruktúra Védelmi Európai Programról*, COM(2005) 576, 2005. november 17. (Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, Brussels, 17.11.2005 COM(2005) 576 final)

[12] Dr. Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft., 2009; http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; letöltve: 2012.11.05

https://nki.gov.hu/wp-content/uploads/2009/10/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf; letöltve: 2020.07.01

[13] Jéri Tamás, Pándi Erik, Jobbágy Szabolcs: A hálózatok világa
Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499
http://193.224.76.4/download/hirado/kiadvanyok/hirvill_1evf_1sz.pdf; letöltve: 2012.11.05

[14] Andrew S. Tanenbaum, David j. Wetherall: Számítógép-hálózatok
Panem Könyvek, Budapest 2013., ISBN 978-963-545-529-4

[15] Official Internet Protocol Standards
http://www.rfc-editor.org/rfcxx00.html; letöltve: 2012.11.05
http://www.rfc-editor.org/standards; letöltve: 2020.03.16

[16] Munk Sándor: Információs színtér, információs környezet, információs infrastruktúra
Nemzetvédelmi Egyetemi Közlemények 2002. 2. sz. ZMNE
http://193.224.76.4/download/konyvtar/digitgy/nek/2002_2/12_munk.pdf; letöltve: 2012.11.05
http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1083/nek_2002_2_munk.pdf?sequence=1&isAllowed=y; letöltve: 2020.03.16

[17] Büntetés-végrehajtás Országos Parancsnoksága, BÜNTETÉS-VÉGREHAJTÁS - Az igazság védelmében https://bv.gov.hu/; letöltve 2020.03.16

[18] Instagram, „hungarianprison”; https://www.instagram.com/hungarianprison/; letöltve 2020.03.16

[19] YouTube, „Prison Hungary”;
https://www.youtube.com/channel/UCfF6gYhUC1JiP9AUS9NMRKA; letöltve 2020.03.16

[20] Bv. Holding Kft., Bv. csomag webáruház; https://www.bvcsomag.hu/auth; letöltve 2020.03.16

[21] BM Országos Katasztrófavédelmi Főigazgatóság;
https://www.katasztrofavedelem.hu/; letöltve 2020.03.16

[22] Facebook, „BM Országos Katasztrófavédelmi Főigazgatóság”;
https://www.facebook.com/bmokf.hivatalos/; letöltve 2020.03.16

[23] Instagram, „katasztrofavedelem_hivatalos”;
https://www.instagram.com/katasztrofavedelem_hivatalos/; letöltve 2020.03.16

[24] Honvédelmi Minisztérium, Magyar Honvédség Online; https://honvedelem.hu/; letöltve 2020.03.16

[25] Facebook, „honvedelem.hu”; https://www.facebook.com/honvedelem.hu; letöltve 2020.03.16

[26] Instagram, „magyarhonvedseg”; https://www.instagram.com/magyarhonvedseg/?hl=hu; letöltve 2020.03.16

[27] Youtube, „amagyarhonvedseg”; https://www.youtube.com/channel/UCNVkvmkt_D6_XfE2bQOEkpQ; letöltve 2020.03.16

[28] Nemzeti Adó- és Vámhivatal; https://www.nav.gov.hu/; letöltve 2020.03.16

[29] Facebook, „Nemzeti Adó- és Vámhivatal”; https://www.facebook.com/NAVprofil; letöltve 2020.03.16

[30] Országos Rendőr-főkapitányság, RENDŐRSÉG - Szolgálunk és Védünk; police.hu; letöltve 2020.03.16

[31] Országos Rendőr-főkapitányság, RUTIN; http://www.police.hu/hu/hirek-es-informaciok/utinfo/rutin; letöltve 2020.03.16

[32] Országos Rendőr-főkapitányság, ELEKTRONIKUS ÜGYINTÉZÉS; https://ugyintezes.police.hu; letöltve 2020.03.16

[33] Facebook, „Legyél Te is rendőr”; https://www.facebook.com/legyelteisrendor/; letöltve 2020.03.16

[34] Youtube, „PoliceHungary”; https://www.youtube.com/user/PoliceHungary; letöltve 2020.03.16

[35] Twitter, „Magyar Rendőrség”; https://twitter.com/police_HU; letöltve 2020.03.16

[36] Terrorelhárítási Központ; http://tek.gov.hu/; letöltve 2020.03.16

[37] Büntetés-végrehajtás, ELEKTRONIKUS ÜGYINTÉZÉS https://bv.gov.hu/hu/elektronikus-ugyintezes; letöltve 2020.03.16

[38] BM Országos Katasztrófavédelmi Főigazgatóság, Elektronikus ügyintézés; https://www.katasztrofavedelem.hu/148/elektronikus-ugyintezes; letöltve 2020.03.16

[39] Honvédelmi Minisztérium, Elektronikus Ügyintézési Portál; https://www.ket.hm.gov.hu/SitePages/Kezdolap.aspx; letöltve 2020.03.16

[40] Nemzeti Adó- és Vámhivatal, NAV Online; https://www.nav.gov.hu/nav/nav_online; letöltve 2020.03.16

[41] Terrorelhárítási Központ, Szabályzatok; http://tek.gov.hu/eugyintezes.html; letöltve 2020.03.16

[42] BM Országos Katasztrófavédelmi Főigazgatóság, Eseménytérkép; https://www.katasztrofavedelem.hu/modules/vesz/esemenyterkep; letöltve 2020.03.16

[43] Hall A.D., Fagen R.E. (1968): Definition of system. In W. Buckley (szerk.), Modern systems research for the behavioral scientist. Chicago, Aldine Kiadó. 80.-81. p.

[44] V. N. Szadovszkij: Az általános rendszerelmélet alapjai, ISBN 963-340-063-5 Statisztikai Kiadó Vállalat, Budapest 1976.

[45] Andrew S. Tanenbaum: Számítógép-hálózatok, ISBN 963 545 384 1 Panem Könyvkiadó Kft., Budapest 2004.

[46] Jéri Tamás: A Kritikus Internetes Szolgáltatások alrendszerei, A Haza Szolgálatában konferenciakötet; Társadalom és Honvédelem XVII. évf. 3-4. szám ISSN 1417-7293 2013. 205-214. oldal;

[47] Szelezsán János: Adatbázisok, ISBN 963 577 189 4; LSI Oktatóközpont

[48] Jéri Tamás: The Security Of Databases In Critical Internet Services, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919; Online: http://hadmernok.hu/153_18_jerit.pdf;

[49] Portfolio, „Elképesztő, mennyi adat létezik - Mire lehet felhasználni?” http://www.portfolio.hu/vallalatok/it/elkepeszto_mennyi_adat_letezik_mire_lehet_felhasznalni.186053.html - letöltve 2013.11.23

[50] Dan Kusnetzky: Virtualization: A Manager's Guide, ISBN 978-1-449-30645-8 O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472 United States of America, 2011.

[51] WikiSzótár.hu magyar értelmező szótár, Kritikus szó jelentése; http://wikiszotar.hu/wiki/magyar_ertelmezo_szotar/Kritikus - letöltve 2014.01.25

[52] Révai nagy lexikona - pdf változat http://mek.oszk.hu/06700/06758/pdf/revai12.pdf - letöltve 2014.01.25

[53] Microsoft, Tutorial Overview: ADSI with Visual Basic; http://msdn.microsoft.com/en-us/library/windows/desktop/aa746492%28v=vs.85%29.aspx - letöltve 2014.01.29

[54] Országos Rendőr-főkapitányság, Közigazgatási Hatósági Szolgálat; https://kozigbirsag.police.hu/; letöltve: 2014.11.17

[55] Országos Rendőr-főkapitányság, Körözési alportál; http://kirportal.police.hu/koral-1.0/page/szemelydetails.xhtml; letöltve: 2014.11.17

[56] Miniszterelnökség, Lechner Nonprofit Kft.: E-építés portál; https://www.e-epites.hu/etdr; letöltve: 2014.11.17

[57] Belügyminisztérium, Rendészeti vezetőképzési és vizsgaportál; http://rvv-rvki.hu; letöltve: 2014.11.17

[58] Belügyminisztérium, Monitoringadatszolgáltatás; https://monitoringadatszolgaltatas.bm.hu/default.aspx; letöltve: 2014.11.17

[59] Honvédelmi Minisztérium, Párbeszéd lap – Magyar Honvédség Tájékoztató Portál https://www.parbeszed.hm.gov.hu/; letöltve: 2014.11.17 http://m.mkle.net/products/a-parbeszed-lap-a-magyar-honvedseg-tajekoztato-portalja-/; letöltve: 2020.07.01

[60] Fleiner Rita: SQL injekcióra épülő támadások és védekezési lehetőségek Hadmérnök, 2008 (III.)/4. (117-128.o.), ISSN 1788- 1919 http://hadmernok.hu/archivum/2008/4/2008_4_fleiner.pdf - letöltve 2015.05.04

[61] CERN, World Wide Web; http://info.cern.ch/hypertext/WWW/TheProject.html; letöltve: 2015.07.06

[62] CERN, The birth of the web; http://home.web.cern.ch/topics/birth-web; letöltve 2015.07.06

[63] Jéri Tamás: A Web szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919; Online: http://www.hadmernok.hu/153_17_jerit.pdf

[64] The Apache Software Foundation, APACHE http server project; http://httpd.apache.org/ABOUT_APACHE.html; letöltve 2015.07.06

[65] Redhat, apacheweek; http://www.apacheweek.com/issues/96-06-14; letöltve 2015.07.06

[66] The Apache Software Foundation, Apache HTTP Server Version 2.4; http://httpd.apache.org/docs/2.4/ssl/; letöltve 2015.07.06

[67] Ashley Arbuckle on March 21, 2019: How Three of 2018's Critical Threats Used Email to Execute Attacks; https://www.securityweek.com/how-three-2018s-critical-threats-used-email-execute-attacks; letöltve: 2019.03.16

[68] Andrew S. Tanenbaum: Számítógép-hálózatok, ISBN 978-963-545-529-4 Panem Könyvkiadó Kft., Budapest 2013. 648. oldal

[69] Samuel Gibbs Mon 7 Mar 2016 15.07 GMT: How did email grow from messages between academics to a global epidemic?;

https://www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history; letöltve: 2019.02.12

[70] Jordie van Rijn, Email is not dead.; https://www.emailisnotdead.com; letöltve: 2019.02.17

[71] Miniwatts Marketing Group, Internet World Stats – Usage and Population Statistics; https://internetworldstats.com/stats.htm; letöltve: 2019.02.17

[72] Facebook; https://facebook.com; letöltve: 2019.02.16
Amazon; https://amazon.com; letöltve: 2019.02.16
PayPal; https://paypal.com; letöltve: 2019.02.16

[73] Bitdefender 09 August 2010: BitDefender Finds Exposed Social Media Credentials Often Provide Access to Email Accounts;
https://www.bitdefender.com/news/bitdefender-finds-exposed-social-media-credentials-often-provide-access-to-email-accounts-1682.html; letöltve: 2019.02.16

[74] EmailMonks, THEORY OF EMAIL EVOLUTION;
https://emailmonks.com/infographics/evolution-of-emails; letöltve: 2019.02.16

[75] Statista, Number of smartphone users worldwide from 2016 to 2019;
https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide; letöltve: 2019.02.16

[76] Felix Richter, Apr 2, 2019: The World's Most Popular Email Clients https://www.statista.com/chart/17570/most-popular-email-clients; letöltve: 2019.04.16

[77] Dr. Kovács László: A kibertér védelme; Dialóg Campus Kiadó, 2018;
ISBN 978-615-5889-64-6

[78] Nemzeti Kibervédelmi Intézet, SPF rekord; https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/spf; letöltve: 2019.09.25

[79] 2F 2000 Kft.; http://www.virushirado.hu/oldal.php?hid=21; letöltve: 2019.02.17

[80] AO Kaspersky Lab, encyclopedia by Kaspersky - Types of spam; https://encyclopedia.kaspersky.com/knowledge/types-of-spam; letöltve: 2019.08.18

[81] Apache Software Foundation, SpamAssassinRules;
https://wiki.apache.org/spamassassin/SpamAssassinRules; letöltve: 2019.06.10

[82] Jéri Tamás: A kommunikációs eszközök fejlődésének kihatásai a büntetés-végrehajtás rendszerére
Hadmérnök, VII. Évfolyam 2. szám 2012. június, NKE Budapest, ISSN 1788- 1919
http://hadmernok.hu/2012_2_jeri.pdf; letöltve: 2019.01.25

[83] Jéri Tamás: A kritikus internetes szolgáltatások biztonságos üzemeltetése, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_20_jerit_2.pdf

[84] Andrew S. Tanenbaum, Albert S. Woodhull: Operációs rendszerek 2. kiadás, ISBN 978-9-635454-76-1
Panem Könyvkiadó Kft., Budapest 2007.

[85] Free Software Foundation, Fail2ban;
http://www.fail2ban.org/wiki/index.php/Main_Page - letöltve 2014.01.25

[86] AD DS Getting Started;
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/ad-ds-getting-started – letöltve 2020.09.24

1. számú melléklet - kérdőív

Tisztelt Olvasó!

Jéri Tamás bv. alezredes vagyok, a Nemzeti Közszolgálati Egyetem doktorandusza, értekezésemet a kritikus internetes szolgáltatások rendvédelmi alkalmazásának témaköréből írom. Tisztelettel megköszönöm, ha szán néhány percet az általam készített felmérés kitöltésére és hozzájárul kutatásom eredményeihez!

Jéri Tamás bv. alez. sk.

Jelmagyarázat:

* kötelezően kitöltendő

O egy választható mező

□ több választható mező

1. Ön melyik rendvédelmi szervezetnél dolgozik? *

O Büntetés-végrehajtás

O Katasztrófavédelem

O Magyar Honvédség

O Nemzeti Adó és Vámhivatal

O Rendőrség

O Terrorelhárítási Központ

O Egyéb: …….

2. Ön miként használja rendvédelmi szerve informatikai rendszerét? *

□ felhasználója

□ működtetésében, vagy fejlesztésében vesz részt

3. Önnek van-e jogosultsága távolról, interneten keresztül belépni rendvédelmi szerve informatikai rendszerébe? *

O van

O nincs

4. Mennyi az Ön munkájához használt, internetes informatikai szolgáltatások (pld. e-mail) száma? *

O 0

O 1 - 3

O 4 - 6

O 7, vagy több

5. Az Ön munkájához használt, internetes informatikai szolgáltatások közül, mennyi az **ingyenes** (pld. gmail) szolgáltatások száma?

O 0

O 1 – 2

O 3 – 4

O 5, vagy több

6. Az Ön munkájához használt, internetes informatikai szolgáltatások kimaradása, vagy leállása, milyen hatást vált ki az Ön munkájára?

nincs kihatással 1 2 3 4 5 gátolja a munkavégzést

7. Nevezzen meg néhányat, az Ön munkájához használt, internetes informatikai szolgáltatások közül.

.....

8. Mennyi a - rendvédelmi - szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások (pld. google térkép) száma? *

O 0

O 1 – 3

O 4 – 6

O 7, vagy több

9. A - rendvédelmi - szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül, mennyi a **folyamatosan** igénybe vett szolgáltatások száma?

O 0

O 1 – 2

O 3 – 4

O 5, vagy több

10. A - rendvédelmi - szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül, mennyi az **ingyenes** szolgáltatások száma?

O 0

O 1 – 2

O 3 – 4

O 5, vagy több

11. Megítélése szerint, a - rendvédelmi - szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások kimaradása, vagy leállása, milyen hatást vált ki szerve működésére?

nincs kihatással 1 2 3 4 5 gátolja a munkavégzést

12. Nevezzen meg néhányat a - rendvédelmi - szerve feladatainak ellátásához és működéséhez hozzájáruló internetes informatikai szolgáltatások közül.

.....

13. Mennyi a rendvédelmi szerve által **nyújtott** internetes informatikai szolgáltatások (pld. honlap) száma? *

O 0

O 1 – 3

O 4 – 6

O 7, vagy több

14. A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatásoknak kik az igénybe vevői?

- □ társadalom
- □ valamelyik társszerv
- □ egyéb

15. A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül, mennyi a feltételhez – például bejelentkezéshez – kötött szolgáltatások száma?

- O 0
- O 1 – 2
- O 3 – 4
- O 5, vagy több

16. A rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül, mennyi a jogszabályi vagy egyéb kötelezettség miatt fenntartott szolgáltatások száma?

- O 0
- O 1 – 2
- O 3 – 4
- O 5, vagy több

17. Megítélése szerint, a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások kimaradása, vagy leállása milyen hatást vált ki?

nincs kihatása 1 2 3 4 5 súlyos kihatása van

18. Nevezzen meg néhányat a rendvédelmi szerve által nyújtott internetes informatikai szolgáltatások közül.

.....