NEMZETI MÉDIA- ÉS HÍRKÖZLÉSI HATÓSÁG

1015 Budapest, Ostrom utca 23–25. • Levélcím: 1525 Budapest, Pf. 75
Telefon: (+36 1) 457 7100 • Fax: (+36 1) 356 5520
E-mail: info@nmhh.hu • Web: www.nmhh.hu

A Nemzeti Média- és Hírközlési Hatóság

ajánlása

az elektronikus hírközlési szolgáltatók részére

az elektronikus adatok hozzáférhetetlenné tételének megfelelő hatékonyságú eljárásairól

(verziószám: 1.2.)

Tartalomjegyzék

1. Bevezetés

1.1. Az NMHH felhatalmazása

Az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) 159/C. § (7) bekezdése alapján a Nemzeti Média- és Hírközlési Hatóság ajánlást adhat ki a hozzáférhetetlenné tételi kötelezettség teljesítésének módjára vonatkozó legjobb gyakorlatokról, illetve felhasználói segítséget nyújt a bíróság, a hozzáférést biztosító elektronikus hírközlési szolgáltatók és a kereső- és gyorsítótár-szolgáltatók számára a KEHTA kezeléséhez.

Ezt az ajánlást a büntetőeljárásról szóló 1998. évi XIX. törvénnyel (Be.), az elektronikus hírközlésről szóló 2003. évi C. törvénnyel (Eht.), a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvénnyel, és az egyszerű adatátvitelt és hozzáférést biztosító elektronikus hírközlési szolgáltatók és a kereső- és gyorsítótár-szolgáltatók központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisához való kapcsolódásának és a Nemzeti Média- és Hírközlési Hatósággal való elektronikus kapcsolattartásának szabályairól szóló a 19/2013. (X. 29.) NMHH rendelettel összhangban szükséges értelmezni.

Az ajánlás célja, hogy elősegítse az elektronikus adatok hozzáférhetetlenné tételét előíró határozatok azonos műszaki szempontok alapján, kellő hatékonysággal történő végrehajtását, ezáltal támogatást nyújtson a szolgáltatóknak ezen kötelezettségük teljesítéséhez.

2. Általános fogalmak

2.1. Elektronikus adat fogalma

Az elektronikus adat hozzáférhetetlenné tétele vonatkozásában elektronikus adat: a hozzáférést biztosító elektronikus hírközlési szolgáltatók által, elektronikus hírközlő hálózat útján közzétett olyan adat, amely IP- és URL-cím, illetve port szám alapján beazonosítható.

2.2. Elektronikus adat azonosítása a hálózatban

2.2.1. URL

„Uniform Resource Locator” [egységes erőforrás-azonosító, „webcím”] Az URL egyetlen címben összefoglalja az elektronikus adat azonosításához szükséges négy alapvető információt:

- a protokollt, ami a célszerverrel történő kommunikációhoz szükséges;
- a célszerver domain nevét vagy IP címét;
- a transzport rétegbeli port számát, amin az igényelt szolgáltatás elérhető a célszerveren;

- az elektronikus adathoz vezető elérési utat a célszerveren belül.

2.2.1. Domain név

Az Internet egy meghatározott részét, tartományát egyedileg leíró megnevezés. A tartománynevek kiosztása és értelmezése a Domain Name System (DNS) szabályai szerint, hierarchikusan történik. A domain nevek célja, hogy az Internethez csatlakozó számítógépek azonosításra szolgáló IP címeit egy könnyen megjegyezhető azonosítóval kapcsolja össze. Amennyiben egy elektronikus adat lekérése a domain név megadásával történik, akkor először a domain nevek és IP címek összerendelését tároló DNS szervereket kérdezi le a felhasználó, és az így visszakapott IP címen kéri le ténylegesen az elektronikus adatot. Egy adott domain névhez több IP cím bejegyzés is tartozhat a DNS szerveren, illetve egy IP cím mögött több domain név kiszolgálását végző szerver is lehet.

2.2.2. IP cím

IP cím/alhálózati maszk – Az IP (Internet Protokoll) cím és az ehhez tartozó alhálózati maszk együttesen meghatározzák, hogy az Interneten milyen hálózati címen érhető el az adott elektronikus adat. Az elektronikus hírközlési szolgáltatók ezen adatpár alapján tudják beállítani a hálózati eszközeikben a hozzáférhetetlenné tételt. Az alhálózati maszk a hálózaton belül csoportosan címezhető IP tartomány méretét határozza meg. Amennyiben 1 db IP címen érhető el az elektronikus adat, úgy értéke „/32”. Amennyiben több IP címről vagy tartományból is elérhető ugyanaz az elektronikus adat (pl. több szerveren van elhelyezve), akkor az alhálózati maszk megadásával határozató meg a kérdéses tartomány (pl. „/24”-es alhálózati maszk esetén egy 253 IP címből álló tartomány határozható meg). Az IP cím és az alhálózati maszk megadása során külön kell feltüntetni a 4-es verziószámú IP címeket (IPv4) és a 6-os verziószámú IP címeket (IPv6). Ez utóbbiak elterjedtsége még alacsony, de különösen a jogsértő tartalmak szolgáltatása esetén fontos lehet.

2.2.3. Cél port cím a transzport rétegben (TCP/UDP cél port szám)

A TCP/IP és az UDP protokollokban az adott célszerveren a logikai csatlakozást meghatározó jelzőszám. A port szám 0-tól 65535 közötti egész érték lehet. A 0-s és 1024-es közötti port számok meghatározott szolgáltatásoknak vannak fenntartva és "jól ismert" (azonosított) portokként kerültek kijelölésre (RFC 1700). A port szám megadása szükséges ahhoz, hogy az elektronikus adat egy adott IP címen üzemelő szerveren vagy szervereken belül azonosítható legyen. Mivel a „jól ismert” portok számozása nem kötelező előírás, ezért egy adott elektronikus adat hozzáférhetetlenné tétele esetén figyelembe kell venni azt a lehetőséget, hogy az nem a megszokott portokon érhető el. (Pl.: http alapú weboldal a 8080-as port számon üzemel a „jól ismert” 80-as port szám helyett.

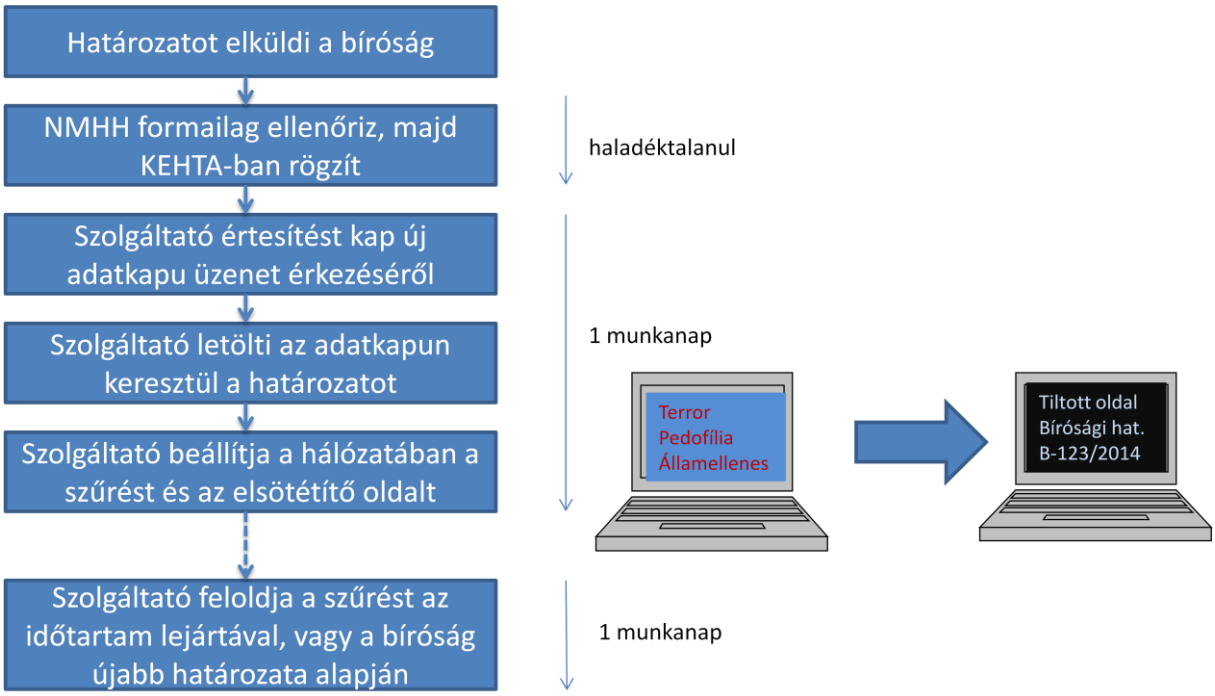
2.2.4. DPI (Deep Packet Inspection) alapú szűrés

A DPI technológián alapuló hálózati eszközök a hálózati és transzport protokollok vizsgálatán túlmenően, képesek a teljes adatcsomag tartalmának a vizsgálatára, így alkalmasak csak a magasabb szintű (OSI L5-L7: viszony, megjelenítési, illetve alkalmazási réteg) protokollokban elkülönülő adatfolyamok megkülönböztetésére és specifikus szűrésére.

3. A hozzáférhetetlenné tétel folyamata

Az elektronikus hírközlési szolgáltató által megvalósított, az elektronikus adatok hozzáférhetetlenné tételére irányuló technikai eljárások célja minden esetben az, hogy a bíróság, vagy a külön törvényben meghatározott hatóság (A Nemzeti Adó- és Vámhivatal) tiltó határozatában megadott jellemzők alapján hozzáférhető elektronikus adat helyett a szintén a határozatban megadott, a tiltás tényéről és indokairól tájékoztató szöveg kerüljön megjelenítésre az internet felhasználó számára.

Az alábbi ábrán nyomon követhető az elektronikus adat hozzáférhetetlenné tételének a folyamata.



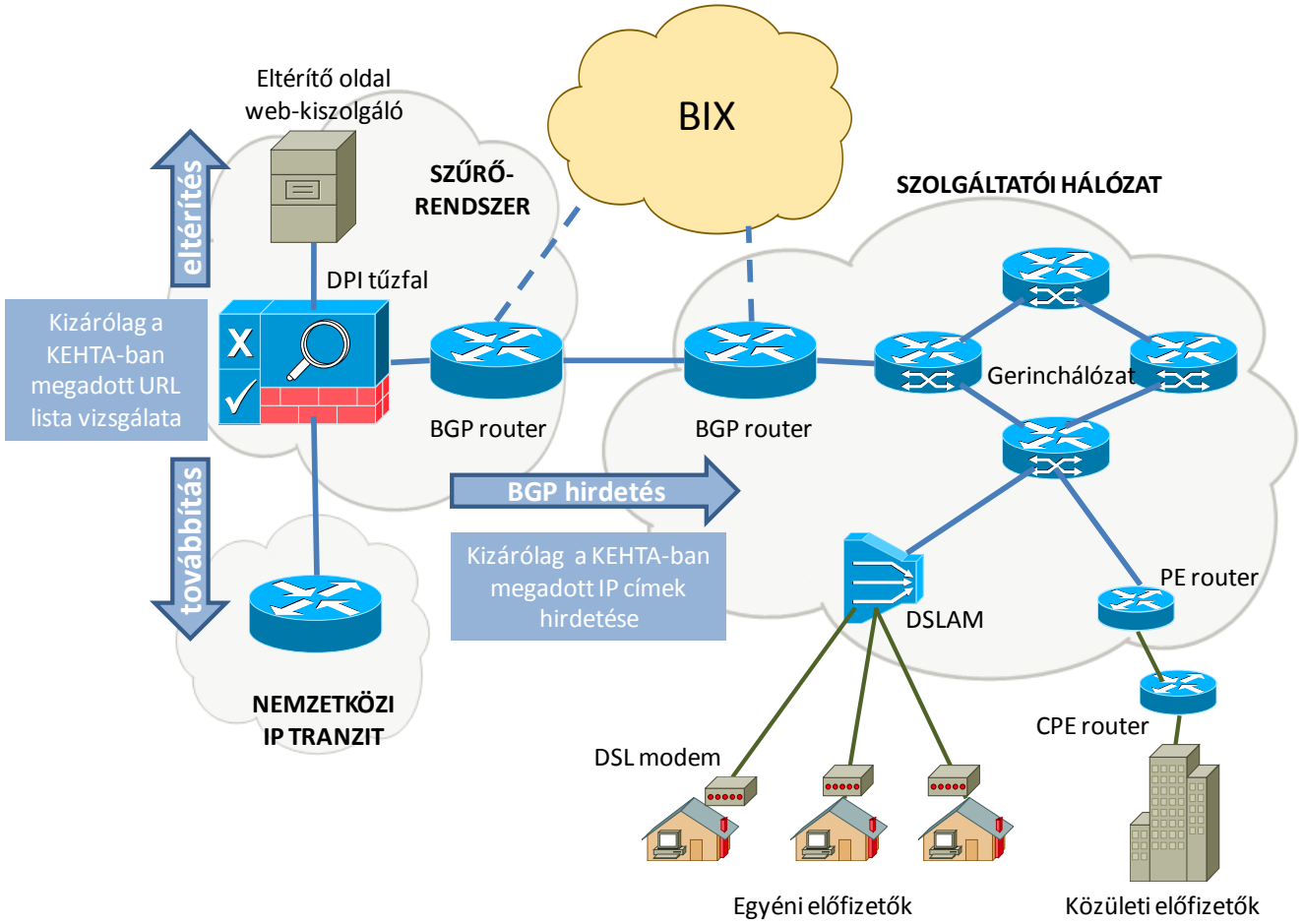
4. Hatékony hozzáférhetetlenné tételi megoldások

4.1. Forgalom elterelés és tartalom vizsgálat alapú hozzáférhetetlenné tétel

Ezt a módszert az EU számos országában alkalmazzák (pl. Egyesült Királyság), különböző műszaki-hálózati megvalósításokkal. A módszer lényege, hogy az elektronikus adat IP címére irányuló forgalom – hálózati protokollok segítségével (pl.: BGP) – egy külön hálózati szegmensbe kerül átirányításra, amely szegmensben céleszközök (DPI szerverek) végzik el a forgalom részletes vizsgálatát, és kizárólag a bírósági, vagy hatósági határozatban megnevezett URL-ekre és cél-portokra irányuló lekérések esetén történik meg a tájékoztató oldalra történő átirányítás.

Ezen módszer hatékonysága – a megkerülő technikák elérhetősége mellett is – megfelelő, mivel kellő pontossággal azonosítja a hozzáférhetetlenné tételre rendelt elektronikus adatot, és minimális járulékos hatásokkal rendelkezik.

4.2. Egy lehetséges hatékony műszaki megvalósítás hálózati diagramja DSL szolgáltatói környezetben



4.3. A hozzáférhetetlenné tételi rendszer adat azonosítási komplexitásának a méretezése

A hozzáférhetetlenné tételi műszaki megoldásnak az összes, a bírósági, vagy hatósági határozatban megadott jellemző alapján azonosítania kell tudni az elektronikus adatokat (amennyiben csak domain név kerül megadásra a határozatban, úgy csak az alapján kell azonosítani). A forgalom elterelés alkalmazásával működő műszaki megoldás esetén biztosítani kell, hogy legalább 5.000 db egyedi IPv4 unicast route prefix és 500 db IPv6 unicast route prefix elterelésére legyen alkalmas a rendszer. Az elterelt forgalomban a DPI szervereknek pedig legalább 5.000 db egyedi URL pontos azonosítását kell biztosítaniuk.

4.4. A hozzáférhetetlenné tételi rendszer elvárt jellemzői

Jellemző	Elvárt működési mód
IP cím alapú elterelés	A szolgáltató a tiltott elektronikus adathoz tartozó IP címre érkező összes lekérést eltereli egy külön hálózati szegmensbe, ezzel végezve el a szűrés első fázisát. Amennyiben a szolgáltató IPv6 forgalmat is támogat a hálózatában, úgy alkalmasnak kell lennie mind az IPv4, mind pedig az IPv6 címek elterelésére. Ez csak abban az esetben alkalmazható, ha a vonatkozó határozat egy teljes IP-cím hozzáférhetetlenné tételét írta elő.
Tartalomvizsgálat az elterelt forgalomban HTTP protokoll esetén	A szolgáltatónak az elterelt forgalmat további vizsgálatnak kell alávetnie, amely alapján eldönthető, hogy az adott lekérés tiltott URL-re vagy port-számra vonatkozik-e. Amennyiben a megvizsgált IP csomag tartalma alapján megállapítható, hogy tiltott elektronikus adat lekérésére irányul, úgy ezen lekérésre válaszul a tájékoztató oldal címét kell visszaküldeni a kezdeményező számára.
Tartalomvizsgálat az elterelt forgalomban HTTPS protokoll esetén	A HTTP vizsgálathoz képest ebben az esetben csak domain név szintű hozzáférhetetlenné tételre van lehetőség, amelyet a kiszolgáló által titkosítatlan formában átküldött SSL tanúsítványban szereplő domain név alapján lehet megtenni.
Tartalomvizsgálat az elterelt forgalomban egyéb protokollok esetén	Amennyiben a tiltott adathoz történő hozzáférés a fentiektől eltérő protokollon keresztül valósul meg (pl. FTP/SSH stb.), úgy a lekérés vizsgálata esetén elegendő kizárólag az IP cím és a port-szám alapján dönteni a forgalom továbbengedéséről.

4.5. A hozzáférhetetlenné tételi rendszer átviteli teljesítményének a méretezése

Abban az esetben lehet hatékony egy hozzáférhetetlenné tételi műszaki megoldás, amennyiben megfelelő forgalmi kapacitásokkal rendelkezik, és egy esetleges túlterheléses támadás a rendszer ellen sem vezet a hozzáférhetetlenné tétel ellehetetlenüléséhez.

Ennek megfelelően, az internet hozzáférés szolgáltatóknak úgy kell méretezniük a hozzáférhetetlenné tételi műszaki megoldást, hogy az alkalmas legyen legalább az általuk kiszolgált összes nemzetközi irányba indított előfizetői forgalom 5%-át megfelelően kezelni.

4.6. A hozzáférhetetlenné tételi rendszer rendelkezésre állásának a méretezése

A hozzáférhetetlenné tételi rendszer akkor biztosít kellő hatékonyságot, amennyiben az éves átlagos rendelkezésre állása meghaladja a 99,5%-ot, minden teljes naptári évre vonatkozóan.

5. Az NMHH technikai segítségnyújtása

5.1. Szakmai konzultáció és információátadás a szolgáltatók részére

Az NMHH szakmai konzultációt, és igény esetén műszaki/tervezési segítséget nyújt a hírközlési szolgáltatók számára a saját hozzáférhetetlenné tételi rendszereik kifejlesztéséhez.

5.2. Az NMHH Technikai Segítségnyújtó Rendszere

Az Ajánlás 1. számú mellékletében meghatározott jogi keretrendszer alapján az elektronikus hírközlési szolgáltató térítésmentesen csatlakozhat az NMHH által közérdekből működtetett a Technikai Segítségnyújtó Rendszerhez (TSR), ami a hírközlési szolgáltató által előszűrt forgalmi adatfolyam pontosabb szűrését segítheti.

1. sz. melléklet

A TSR rendszerhez történő csatlakozás jogi feltételei

1. A Hatóság a büntetőeljárásról szóló 1998. évi XIX. törvény 2014. január 1-től hatályos 158/D. és 596/A. §-ai, a szerencsejáték szervezéséről szóló 1991. évi XXXIV. törvény 2014. január 2-től hatályos 36/G.-J. §-ai és az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban: Eht.) 2014. január 1-től hatályos 92/A. § és 159/B.-159/C. §-ai alapján 2014. január 1-től szervezi és ellenőrzi a büntetőügyben a bíróság által elrendelt elektronikus adat ideiglenes és végleges hozzáférhetetlenné tételének végrehajtását, továbbá a külön törvényben meghatározott hatóság (A Nemzeti Adó- és Vámhivatal) által elrendelt elektronikus adat ideiglenes hozzáférhetetlenné tételének végrehajtását. A Hatóság ennek érdekében működteti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát (a továbbiakban: KEHTA), és a működtetés céljából feldolgozza az oda bevitt adatokat.

2. A Hatóság az Eht. 159/C. § (4)-(5) bekezdése értelmében hozzáférést biztosító elektronikus hírközlési szolgáltató vagy a kereső- és gyorsítótár-szolgáltató kérésére közreműködik az elektronikus adat hozzáférhetetlenné tételét elrendelő határozatok végrehajtásához szükséges technikai környezet biztosításában. Ha a Hatóság az elektronikus adat ideiglenes és végleges hozzáférhetetlenné tételében közreműködik, az érintett hozzáférést biztosító elektronikus hírközlési szolgáltatóval, illetve az érintett kereső- és gyorsítótár-szolgáltatóval közigazgatási szerződést köt. A közreműködés keretében a Hatóság a közigazgatási szerződésben meghatározott módon és feltételekkel hozzáférést biztosít az érintett hozzáférést biztosító elektronikus hírközlési szolgáltató vagy a kereső- és gyorsítótár-szolgáltató részére olyan technikai segítségnyújtó rendszerhez, amely műszaki jellemzőinél fogva alkalmas a hozzáférhetetlenné tétel megvalósítására.

3. A technikai segítségnyújtó rendszer célja, hogy a szolgáltatók erre vonatkozó igénye esetén a hozzáférés megakadályozásával kapcsolatos technikai terheket a hatóság részben levegye a szolgáltatók válláról.

Kérjük, amennyiben közigazgatási szerződést kötésére jogosult és ilyen szerződést kíván kötni, azt jelezze a tsr-info@nmhh.hu elektronikus levélcímen. Ebben az esetben a szerződés mintapéldányát elpostázzuk és azt aláírva az alábbi címre kérjük visszaküldeni:

Nemzeti Média- és Hírközlési Hatóság
1015 Budapest, Ostrom u. 23-25.

A szerződés hatóság által is aláírt példányát ezután visszapostázzuk a szolgáltató címére.

A hatóság konzultációs lehetőséget biztosít a szolgáltatók számára a technikai segítségnyújtó rendszerrel kapcsolatban az alábbi helyszínen és időpontokban:

Nemzeti Média- és Hírközlési Hatóság

1015 Budapest, Ostrom u. 23-25., II-III.-as tárgyaló

1. időpont: 2013. november 20. (szerda), 14.00 óra
2. időpont: 2013. november 28. (csütörtök), 14.00 óra

A konzultációs időpontokra a tsr-info@nmhh.hu elektronikus levélcímen lehet jelentkezni az elérhetőségi adatok megadásával.