AVG Internet Security 2013

Felhasználói kézikönyv

Dokumentumverzió 2013.11 (13.2.2013.)

Tartalom

1. Bevezetés

Jelen felhasználói kézikönyv átfogó útmutatót nyújt az **AVG Internet Security 2013** programhoz.

Az **AVG Internet Security 2013** többszintű védelmet biztosít online tevékenységeihez, ami azt jelenti, hogy nem kell személyazonosság-lopás, vírusok vagy veszélyes oldalak megnyitása miatt aggódnia. Az AVG Protective Cloud Technology és az AVG Community Protection Network is a termék részét képezik, ami azt jelenti, hogy összegyűjtjük a legutóbbi fenyegetésekkel kapcsolatos adatokat, és megosztjuk a közösséggel a lehető legjobb védelem biztosítása érdekében. Biztonságosan vásárolhat és intézheti banki ügyeit online, élvezheti az életet a közösségi hálózatokon, vagy böngészhet és kereshet a valós idejű védelem által nyújtott magabiztossággal.

2. AVG telepítési követelmények

2.1. Támogatott operációs rendszerek

Az AVG Internet Security 2013 a következő operációs rendszerű munkaállomások védelmére szolgál:

- Windows XP Home SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 és x64, minden kiadás)
- Windows 7 (x 86 és x64, minden kiadás)
- Windows 8 (x32 és x64)

(és esetlegesen újabb szervizcsomagok bizonyos operációs rendszerekhez)

***Megjegyzés**: A Windows XP x64 rendszer nem támogatja a Személyazonosság összetevőt. Erre az operációs rendszerre kizárólag az AVG Internet Security 2013 terméket telepítheti, az IDP összetevő nélkül.*

2.2. Minimum és ajánlott hardverkövetelmények

Minimális hardverkövetelmények az **AVG Internet Security 2013** termékhez:

- Intel Pentium processzor, 1,5 GHz vagy gyorsabb
- 512 MB (Windows XP)/1024 MB (Windows Vista, Windows 7) RAM memória
- 1,3 GB szabad lemezterület *(telepítési célokra)*

Ajánlott hardverkövetelmények az **AVG Internet Security 2013** termékhez:

- Intel Pentium processzor, 1,8 GHz vagy gyorsabb
- 512 MB (Windows XP)/1024 MB (Windows Vista, Windows 7) RAM memória
- 1,6 GB szabad lemezterület *(telepítési célokra)*

3. AVG telepítési folyamat

Az **AVG Internet Security 2013** telepítéséhez szüksége van a legújabb telepítőfájlra. Ha biztosan az **AVG Internet Security 2013** legfrissebb verzióját kívánja letölteni, azt javasoljuk, hogy használja az AVG webhelyét (http://www.avg.com/). A ***Támogatás / Letöltések*** területen az AVG kiadásai szerint elrendezve megtalálja az összes telepítési fájlt.

Ha nem biztos benne, hogy melyik fájlra van szüksége a telepítéshez, használja a webhely alsó részén található ***Termék kiválasztása*** szolgáltatást. Három egyszerű kérdés megválaszolását követően a szolgáltatás meghatározza, hogy pontosan mely fájlokra van szüksége. A ***Tovább*** gombra kattintva az oldal átirányítja egy listához, amely minden olyan fájlt tartalmaz, amire szüksége lehet.

Miután letöltötte és mentette a telepítőfájlt a merevlemezre, indítsa el a telepítési folyamatot. A telepítés egyszerű, könnyen érthető párbeszédablakok sorozata. Minden párbeszédablak röviden leírja a telepítési folyamat adott lépésére vonatkozó tennivalókat. Az alábbiakban az egyes párbeszédablakok részletes leírását találja:

3.1. Üdvözlőképernyő: Nyelvválasztás

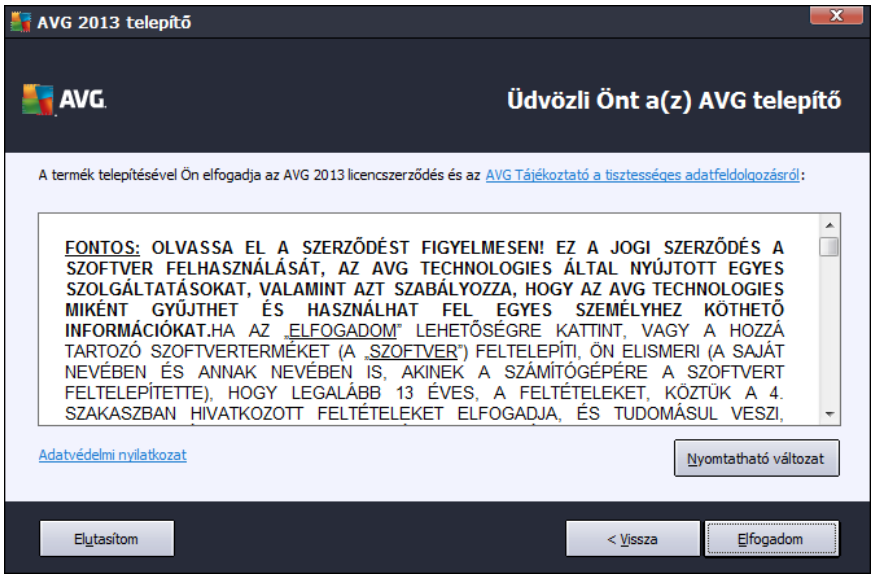
A telepítési folyamat az ***Üdvözli az AVG telepítő*** párbeszédpanellel kezdődik:

Ezen a párbeszédpanelen kiválaszthatja a telepítés nyelvét. Kattintson a kombinált listára a nyelvi menü legördítéséhez. Válassza ki a kívánt nyelvet, és a telepítés folytatódik a kiválasztott nyelven.

Figyelem: Az itt kiválasztott nyelv csak a telepítési folyamatra vonatkozik. Az AVG Internet Security 2013 alkalmazást a kiválasztott nyelven telepíti, az angol nyelvet pedig ezen felül mindig automatikusan telepíti a rendszer. Azonban több nyelvet is lehet telepíthet, és az AVG Internet Security 2013 terméket ezek bármelyikén használhatja. A program a későbbiekben, az Egyéni beállítások párbeszédpanelen lehetővé teszi, hogy megerősítse, mely alternatív nyelveket kívánja használni.

3.2. Üdvözlőképernyő: Licencszerződés

Az ***Üdvözli az AVG telepítő*** párbeszédpanel az AVG licencszerződés teljes szövegét is tartalmazza.



Figyelmesen olvassa el a szöveget. Nyomja meg az ***Elfogadom*** gombot, ha elolvasta, megértette és elfogadta a megállapodást. Ha nem ért egyet a megállapodással, akkor nyomja meg a ***Nem fogadom el*** gombot, ekkor a telepítési folyamat azonnal megszakad.

AVG Adatvédelmi nyilatkozat

A licencszerződés mellett ebből a telepítési párbeszédpanelből jobban megismerheti az ***AVG tisztességes adatfeldolgozási nyilatkozatát***, az ***AVG testreszabását*** és az ***AVG adatvédelmi nyilatkozatát*** *is (az összes említett funkció egy aktív hivatkozás formájában jelenik meg a párbeszédpanelen, amely átirányítja a részletes információkat tartalmazó megfelelő webhelyre).* A megfelelő hivatkozásra kattintva a rendszer átirányítja az AVG webhelyére (http://www.avg.com/), ahol megtalálja a nyilatkozatok teljes szövegét.

Vezérlőgombok

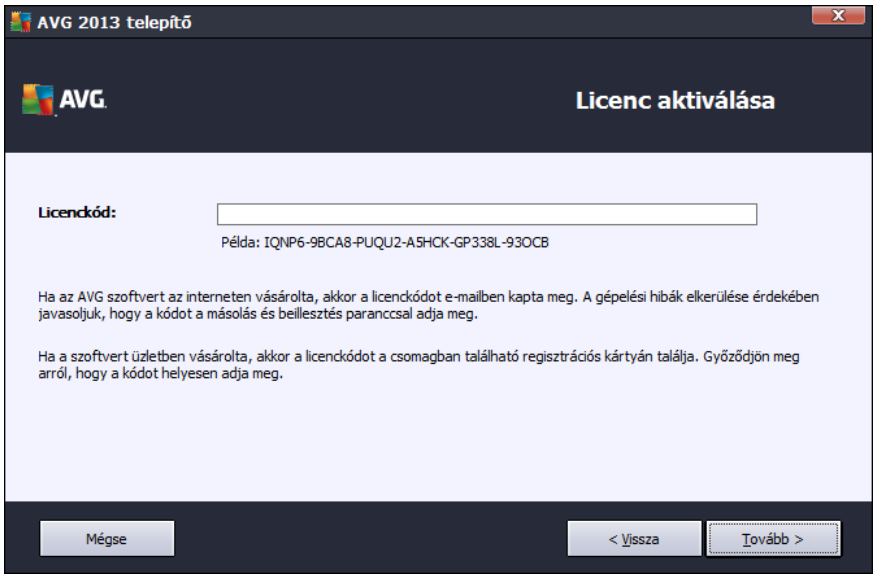
Az első telepítő párbeszédpanelen csak két vezérlőgomb található:

- ***Nyomtatható verzió*** – A gombra kattintva nyomtatóbarát elrendezésű webes felületen jelenítheti meg az AVG licencszerződés teljes szövegét.
- ***Elutasítom*** – Erre kattintva elutasítja a licencszerződést. A telepítési folyamat azonnal megszakad. **AVG Internet Security 2013** az telepítése nem történik meg.
- ***Vissza*** – Kattintson ide, ha az előző telepítési párbeszédpanelre szeretne visszalépni.
- ***Elfogadom*** – Erre kattintva megerősíti, hogy elolvasta, megértette és elfogadta a licenc

feltételeit. A telepítés folytatódik és egy lépéssel tovább, a következő telepítési párbeszédpanelre ugrik.

3.3. Licenc aktiválása

A ***Licenc aktiválása*** panelen írja be a licencszámot a megfelelő szövegmezőbe:



Hol találom a licenckódomat?

Az értékesítési számot saját **AVG Internet Security 2013** példányának dobozában, a CD csomagolásán találja. A licencszám az **AVG Internet Security 2013** megvásárlása után kapott megerősítő e-mailben lesz. A számot pontosan úgy kell megadnia, ahogyan az látható. Ha a licencszám elérhető digitális formában (*pl. e-mailben*), akkor javasoljuk, hogy használja a másolás és beillesztés funkciót a megadáshoz.

A másolás és beillesztés funkció használata

Ha a ***másolás és beillesztés*** funkciót használja az **AVG Internet Security 2013** licenckódjának megadásához, nem kell elgépeléstől tartania. Kövesse az alábbi lépéseket:

- Nyissa meg a licenckódot tartalmazó e-mailt.
- Kattintson a bal gombbal a licenckód elejére, majd a gombot nyomva tartva húzza a mutatót a szám végéig, és engedje fel a gombot. Ezzel kijelölte a számot.
- A ***Ctrl*** billentyűt nyomva tartva nyomja le a ***C*** billentyűt. Ezzel a vágólapra helyezte a számot.
- Kattintson arra a pontra, ahová be kívánja illeszteni a vágólapra helyezett számot.
- A ***Ctrl*** billentyűt nyomva tartva nyomja le a ***V*** billentyűt. Ezzel beilleszti a számot a

kiválasztott helyre.

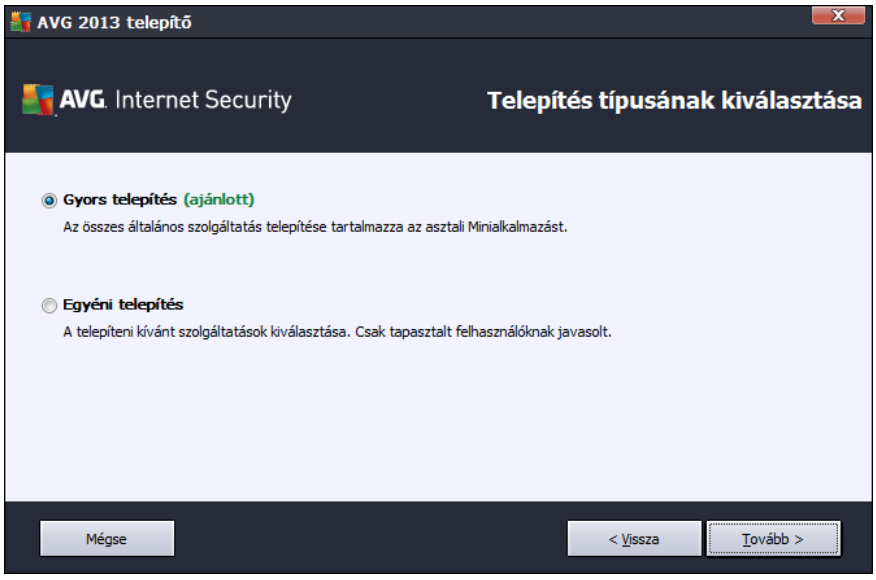
Vezérlőgombok

A legtöbb telepítési párbeszédpanelhez hasonlóan itt is három vezérlőgomb áll rendelkezésre:

- ***Mégse*** – kattintson ide, ha azonnal ki szeretne lépni a telepítési folyamatból; az **AVG Internet Security 2013**-t ebben az esetben nem telepíti.
- ***Vissza*** – kattintson ide, ha az előző telepítési párbeszédpanelre szeretne visszatérni.
- ***Tovább*** – kattintson ide, ha folytatni kívánja a telepítést, és a következő lépésre szeretne ugrani.

3.4. Telepítés típusának kiválasztása

A ***Telepítés módjának kiválasztása*** panel két lehetőséget kínál: ***Gyors telepítés*** és ***Egyéni telepítés***:



Gyors telepítés

A legtöbb felhasználó számára ajánlott a normál ***Gyors*** telepítést elvégezni. Ez teljesen automatikusan telepíti az **AVG Internet Security 2013** programot a gyártó által előre megadott beállításokkal, beleértve az AVG minialkalmazást, az AVG Security Toolbart, valamint az alapértelmezett keresőként konfigurált AVG Secure Search szolgáltatást is. Ez a konfiguráció maximális biztonságot és a rendszererőforrások optimális használatát nyújtja. Ha a későbbiekben meg szeretné változtatni a konfigurációt, akkor ezt közvetlenül megteheti az **AVG Internet Security 2013** alkalmazáson belül.

Nyomja meg a ***Tovább*** gombot a telepítési folyamat következő panelére történő ugráshoz.

Egyéni telepítés

Az ***Egyéni telepítést*** csak azon tapasztalt felhasználóknak ajánljuk, akik mindenképp egyéni beállításokkal szeretnék telepíteni az **AVG Internet Security 2013** programot, például azért, hogy az megfeleljen bizonyos rendszerkövetelményeknek. Ha ezt a lehetőséget választja, egy ***Célmappa*** nevű új terület jelenik meg a párbeszédpanelen. Itt adhatja meg az **AVG Internet Security 2013** kívánt telepítési helyét. Alapértelmezett állapotban az **AVG Internet Security 2013** a C: meghajtón található Program Files mappába települ, mint az a párbeszédpanel szövegmezőjében is látható. Ha módosítani kívánja ezt a helyet, akkor használja a ***Tallózás*** gombot a meghajtó tartalmának megjelenítéséhez, majd válassza ki a kívánt mappát. A gyártó által megadott alapértelmezett cél visszaállításához használja az ***Alapértelmezett*** gombot.

Ezután nyomja meg a ***Tovább*** gombot az Egyéni beállítások panelre történő ugráshoz.

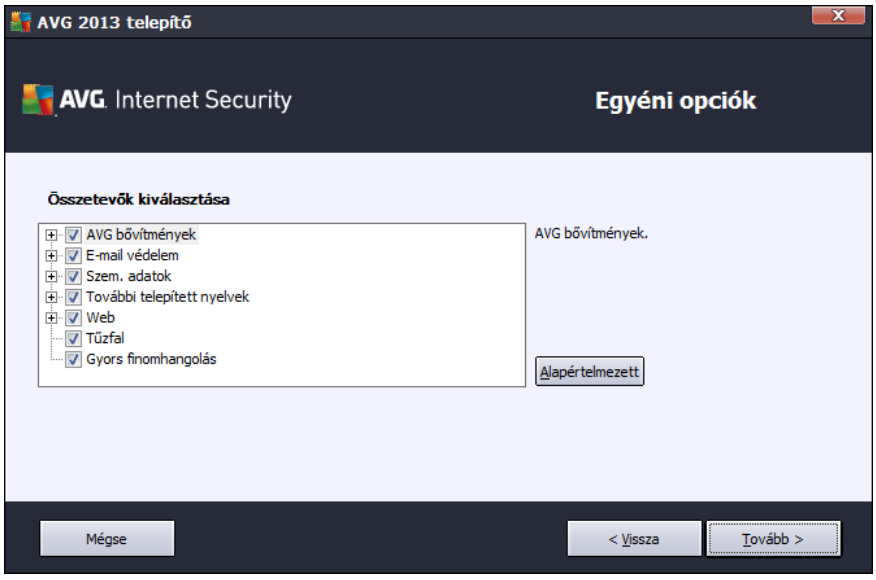
Vezérlőgombok

A legtöbb telepítési párbeszédpanelhez hasonlóan itt is három vezérlőgomb áll rendelkezésre:

- ***Mégse*** – kattintson ide, ha azonnal ki szeretne lépni a telepítési folyamatból; az **AVG Internet Security 2013**-t ebben az esetben nem telepíti.
- ***Vissza*** – kattintson ide, ha az előző telepítési párbeszédpanelre szeretne visszatérni.
- ***Tovább*** – kattintson ide, ha folytatni kívánja a telepítést, és a következő lépésre szeretne ugrani.

3.5. Egyéni opciók

Az ***Egyéni opciók*** párbeszédpanelen beállíthatja a telepítés részletes paramétereit:



Az ***Összetevők kiválasztása*** rész áttekintést nyújt az **AVG Internet Security 2013** összes

telepíthető összetevőjéről. Ha az alapbeállítások nem felelnek meg Önnek, akkor eltávolíthat/hozzáadhat összetevőket. ***Azonban csak olyan összetevőkből választhat, melyek használatára jogosult a megvásárolt AVG termékben!*** Jelöljön ki egy elemet az ***Összetevő kiválasztása*** listán, ekkor az adott összetevő rövid leírása megjelenik a jobb oldalon. Az egyes összetevők részletes adataival kapcsolatban forduljon a dokumentáció Összetevők áttekintése fejezetéhez. A gyártó által megadott alapértékek visszaállításához használja az ***Alapértelmezett*** gombot.

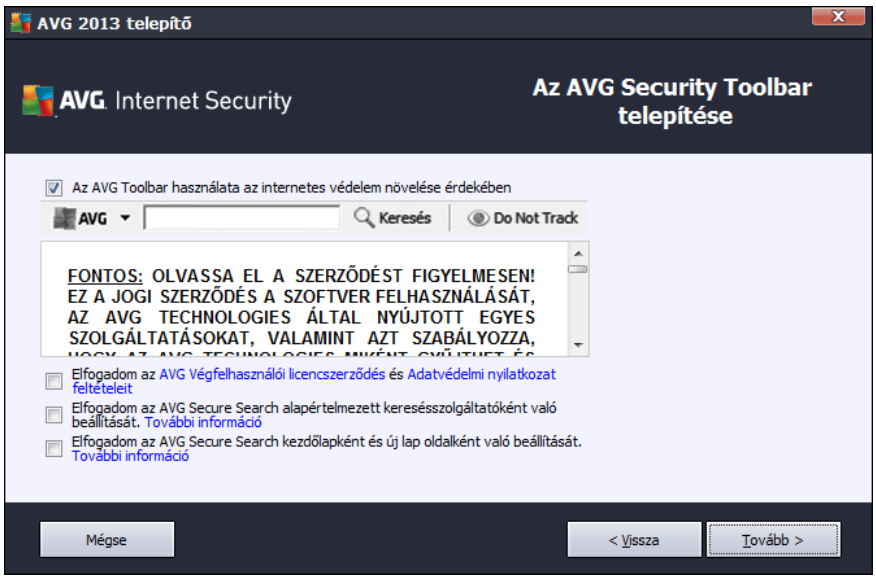
Vezérlőgombok

A legtöbb telepítési párbeszédpanelhez hasonlóan itt is három vezérlőgomb áll rendelkezésre:

- ***Mégse*** – kattintson ide, ha azonnal ki szeretne lépni a telepítési folyamatból; az **AVG Internet Security 2013**-t ebben az esetben nem telepíti.
- ***Vissza*** – kattintson ide, ha az előző telepítési párbeszédpanelre szeretne visszatérni.
- ***Tovább*** – kattintson ide, ha folytatni kívánja a telepítést, és a következő lépésre szeretne ugrani.

3.6. Az AVG Security Toolbar telepítése

Az ***AVG Security Toolbar telepítése*** panelen eldöntheti, hogy kívánja-e telepíteni az ***AVG Security Toolbar*** eszköztárat. Ha nem módosítja az alapértelmezett beállításokat, akkor ez az összetevő automatikusan telepítve lesz a böngészőben (*jelenleg a Microsoft Internet Explorer 6.0 vagy újabb verziójának és a Mozilla Firefox 3.0 vagy újabb verziójának használata támogatott*), és átfogó online védelmet nyújt az internet böngészése során. Jelenleg a támogatott internetböngészők a következők: Internet Explorer (*6.0 vagy újabb verziók*) és/vagy Mozilla Firefox (*3.0 vagy újabb verziók*). A többi böngésző nem támogatott *(ha más böngészőt használ, például az Avant böngészőt, akkor a program nem várt módon viselkedhet).*



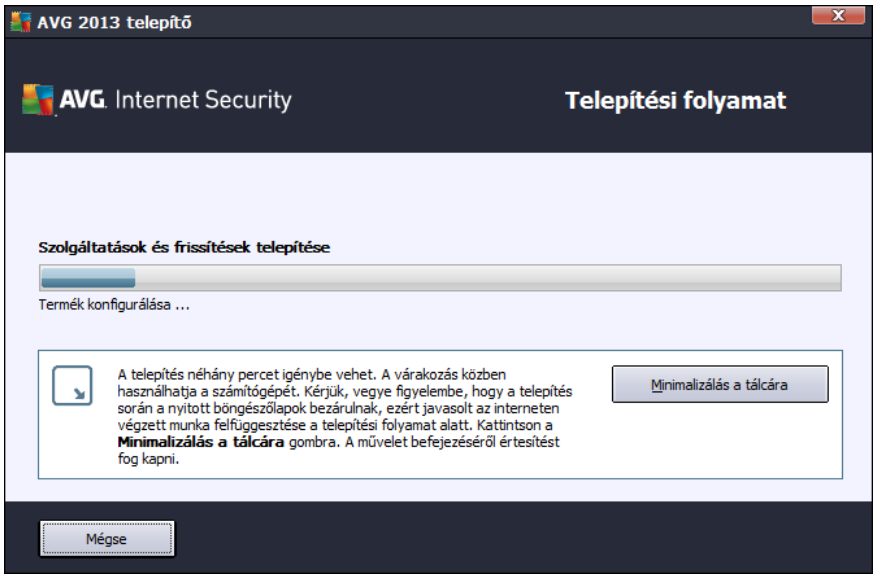
A párbeszédpanelen a következő beállításokról dönthet:

- ***Az AVG Secure Search beállítása és megtartása alapértelmezett keresőként*** – hagyja bejelölve, ha az AVG Secure Search keresőt szeretné használni, amely szorosan együttműködik a LinkScanner böngészésvédelemmel a maximális internetes biztonság érdekében.

- ***Az AVG Security Toolbar telepítése az internetes védelem növelése érdekében*** – hagyja bejelölve az AVG Security Toolbar telepítéséhez, amely maximális biztonságot nyújt az interneten folytatott böngészéskor.

3.7. Telepítési folyamat

A ***Telepítési folyamat*** panel a telepítési folyamat állapotát mutatja, és nem igényel semmilyen beavatkozást:



Miután a telepítési folyamat befejeződött, a program automatikusan továbblép a következő párbeszédpanelre.

Vezérlőgombok

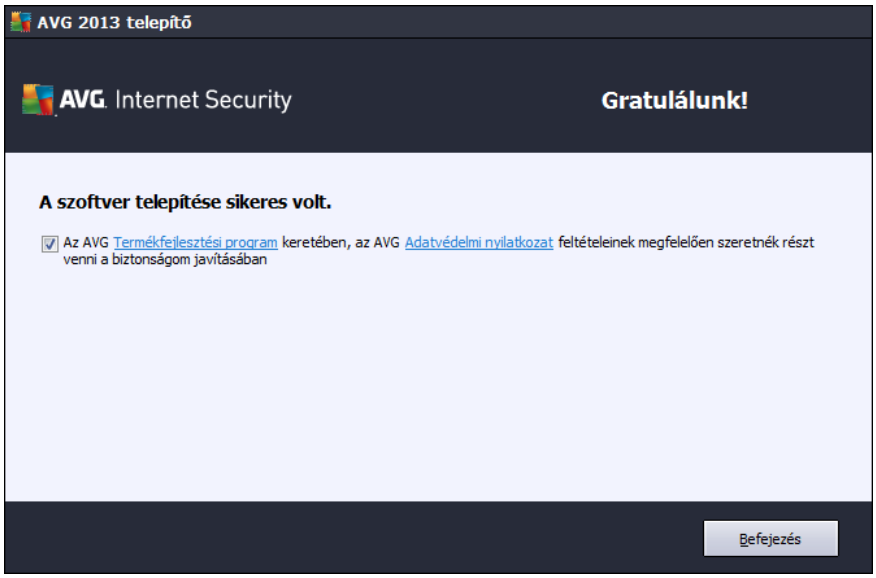
Két vezérlőgomb található az ablakban:

- ***Kis méret*** – A telepítési művelet eltarthat néhány percig. Kattintson a gombra a párbeszédablak a rendszertálcán látható ikonra történő minimalizálásához. A párbeszédpanel újból megjelenik, amikor a telepítés befejeződik.

- ***Mégse*** – Ezt gombot csak akkor használja, ha le kívánja állítani az aktuális telepítési folyamatot. Vegye figyelembe, hogy a folyamat leállítása esetén az **AVG Internet Security 2013** termék telepítése nem történik meg.

3.8. A telepítés sikerült

A telepítés sikerült párbeszédpanel megerősíti, hogy az **AVG Internet Security 2013** terméket a rendszer sikeresen telepítette és konfigurálta:



Termékfejlesztési program és Adatvédelmi nyilatkozat

Itt eldöntheti, hogy részt kíván-e venni az ***Termékfejlesztési programban*** (*erről részleteket a AVG speciális beállítások / Termékfejlesztési program* című fejezetben talál), amely névtelen információkat gyűjt az észlelt fenyegetésekről az online biztonság növelése érdekében. Minden adat kezelése bizalmasan és az AVG Adatvédelmi nyilatkozatával összhangban történik; az ***Adatvédelmi nyilatkozat*** hivatkozásra kattintva a rendszer átirányítja az AVG webhelyére (http://www.avg.com/), ahol megtalálja az AVG adatvédelmi nyilatkozat teljes szövegét. Ha egyetért, hagyja bejelölve a lehetőséget *(a lehetőség alapértelmezés szerint be van jelölve)*.

A telepítési folyamat lezárásához kattintson a ***Befejezés*** gombra.

4. A telepítés utáni teendők

4.1. Termék regisztrálása

Miután befejezte az **AVG Internet Security 2013** telepítését, regisztrálja a terméket az AVG webhelyén (*http://www.avg.com/)*. A regisztráció után teljes hozzáférést kap saját AVG felhasználói fiókjához, az AVG frissítési hírlevélhez és számos egyéb olyan szolgáltatáshoz, amely kizárólag regisztrált felhasználók számára érhető el. Regisztrálni legkönnyebben közvetlenül az **AVG Internet Security 2013** felhasználói felületéről tud. Válassza a felső navigációs sor / Beállítások / Regisztrálás lehetőséget. A rendszer átirányítja az AVG webhely *(http://www.avg.com/)* ***Regisztráció*** oldalára. Kövesse az oldalon megjelenő utasításokat.

4.2. Hozzáférés a felhasználói felülethez

Az AVG fő párbeszédpanel többféle módon is elérhető:

- Kattintson kétszer az AVG ikonjára a tálcán
- Kattintson duplán az AVG ikonra az Asztalon
- A ***Start / Minden program / AVG / AVG 2013 menüpontból***

4.3. A teljes számítógép vizsgálata

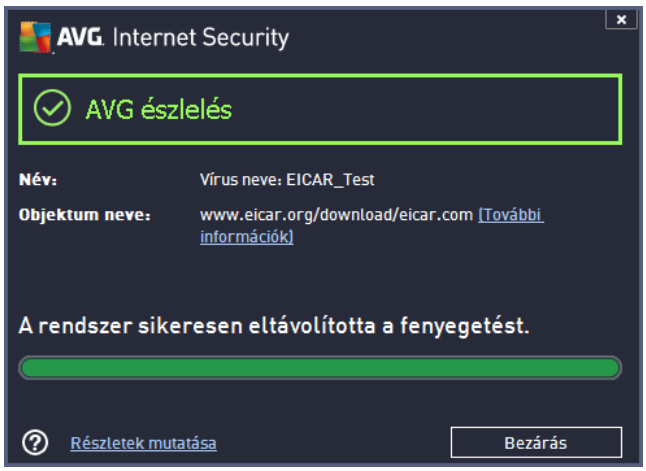
Fennáll a veszély, hogy az **AVG Internet Security 2013** telepítése előtt vírus került a számítógépre. Ezért hajtsa végre a Teljes számítógép vizsgálatát, hogy meggyőződjön a számítógépe vírusmentességéről. Az első vizsgálat hosszú ideig tarthat *(körülbelül egy órán át)*, de ajánlott elindítani annak ellenőrzése végett, hogy a számítógépet nem veszélyeztetik-e fenyegetések. A Teljes számítógép vizsgálata művelet futtatásával kapcsolatban az AVG vizsgálat című fejezetben talál további információt.

4.4. Eicar teszt

Az **AVG Internet Security 2013** sikeres telepítésének ellenőrzéséhez lefuttathatja az EICAR tesztet.

Az EICAR teszt a víruskeresési rendszer ellenőrzésének bevett és biztonságos módja. A teszt biztonságosan terjeszthető, mivel ez nem egy valódi vírus, tehát nem tartalmaz semmilyen veszélyes kódot. Csak a víruskereső működőképességének ellenőrzésére szolgál. A legtöbb vírusirtó vírusként azonosítja a tesztet (*bár a jelentésben valamilyen egyértelmű név szerepel, pl: „EICAR-AV-Test"*). Az EICAR vírust a www.eicar.com címen elérhető honlapról lehet letölteni az EICAR teszthez szükséges információkkal együtt.

Töltse le az *eicar.com* fájlt, és mentse a helyi lemezre. A tesztfájl letöltésének megerősítése után az **AVG Internet Security 2013** azonnal megjelenít egy figyelmeztető üzenetet. A figyelmeztető üzenet tanúskodik arról, hogy az AVG megfelelően lett telepítve a számítógépre.



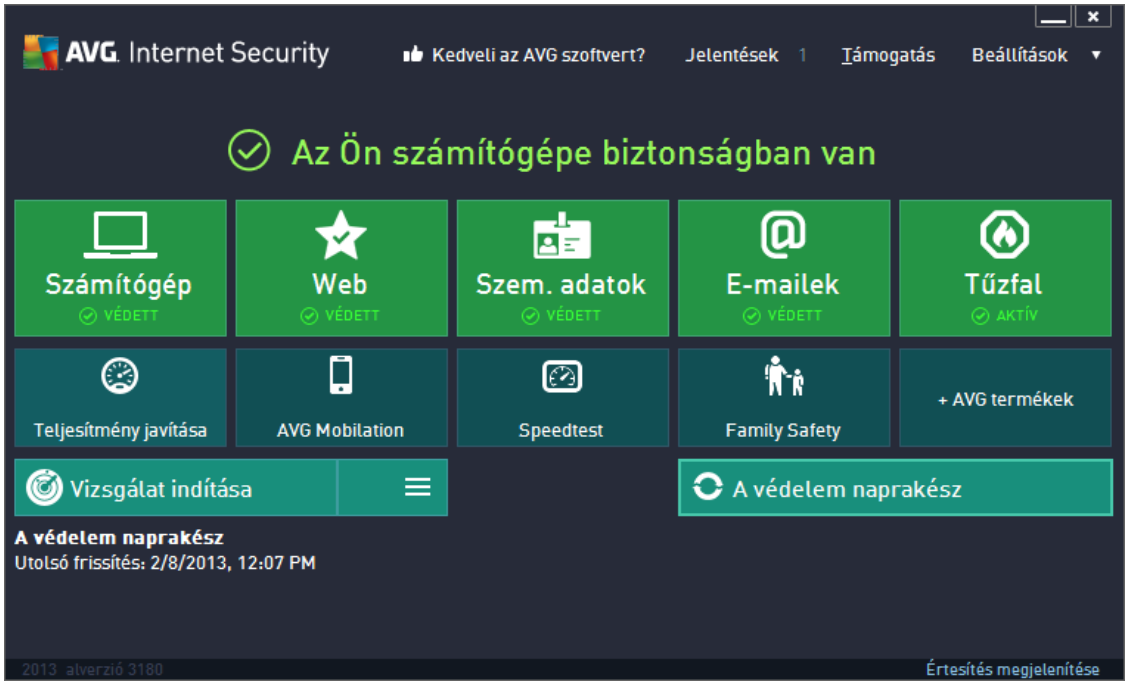
Ha az AVG nem azonosítja vírusként az EICAR tesztfájlt, akkor ismételten ellenőriznie kell a program beállításait.

4.5. AVG alapértelmezett konfiguráció

Az alapértelmezett konfigurációt (*vagyis a program telepítés utáni viselkedését*) az **AVG Internet Security 2013** szoftvergyártója előre meghatározta az összes funkció és összetevő optimális teljesítményének érdekében. ***Ne változtassa meg az AVG beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást tapasztalt felhasználónak kell végeznie.*** Ha az igényeinek megfelelően módosítani kívánja az AVG konfigurációját, akkor nyissa meg a AVG speciális beállítások párbeszédpanelt, válassza a főmenü *Beállítások/Speciális beállítások* elemét, majd szerkessze az AVG konfigurációját a megnyíló AVG speciális beállítások párbeszédpanelen.

5. AVG felhasználói felület

Az AVG Internet Security 2013 a főablakkal együtt nyílik meg:



A főablak több részből áll:

- ***A Felső navigációs sáv*** négy aktív hivatkozásból áll, amelyek a főablak felső részén találhatók *(Kedveli az AVG szoftvert, Jelentések, Támogatás, Beállítások).* Részletek >>
- ***A Biztonsági állapot információk*** részletekkel szolgál az **AVG Internet Security 2013** program aktuális állapotával kapcsolatban. Részletek >>
- ***A telepített összetevők áttekintése*** a főablak középső részén, egy vízszintes blokksávon található. Az összetevők világoszöld blokkokként jelennek meg a megfelelő összetevőikonnal címkézve, és tartalmazzák az összetevő állapotának információit. Részletek >>
- ***A Saját alkalmazások*** grafikus formában a főablak alsó középső sávján található, és az **AVG Internet Security 2013** kiegészítő alkalmazásainak áttekintéseit biztosítja, amelyek vagy már telepítve vannak a számítógépen, vagy javasolt a telepítésük. Részletek >>
- ***A Vizsgálat / Gyors linkek frissítése*** lehetőségek a főablak alsó blokksorában találhatók. Ezek a gombok azonnali hozzáférést biztosítanak a legfontosabb és leggyakrabban használt AVG funkciókhoz. Részletek >>

Az **AVG Internet Security 2013** főablakán kívül két további vezérlőelemmel érheti el az alkalmazást:

- ***A Tálcaikon*** a képernyő jobb alsó részén található *(a rendszertálcán),* és az **AVG Internet Security 2013** aktuális állapotát jeleníti meg. Részletek >>

- ***Az AVG minialkalmazás*** a Windows oldalsávról érhető el (*csak a Windows Vista/7/8 operációs rendszerben támogatott*) és gyors hozzáférést biztosít a vizsgálathoz és a frissítésekhez az **AVG Internet Security 2013** programon belül. Részletek >>

5.1. Felső navigációs sáv

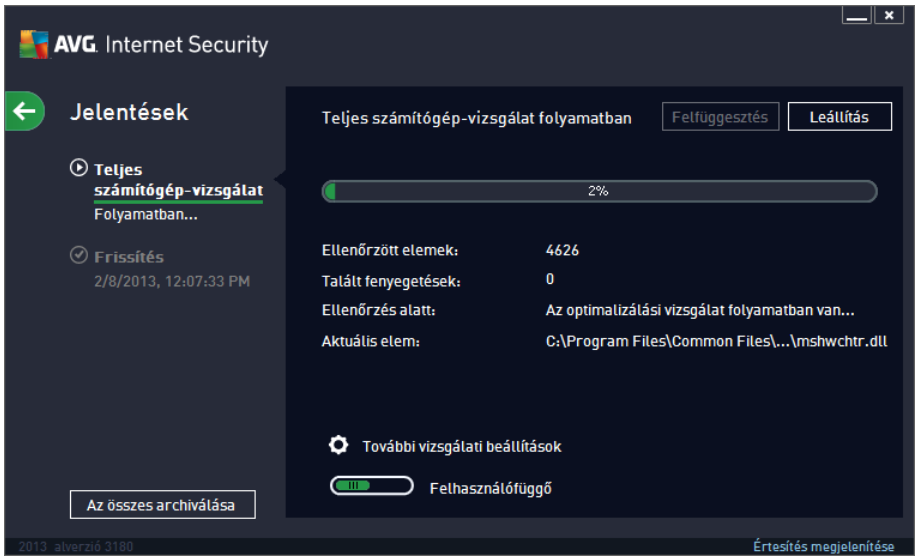
A ***Felső navigációs sáv*** számos aktív hivatkozásból áll, amelyek a főablak felső részén találhatók. A navigációs sáv a következő gombokat tartalmazza:

5.1.1. Kedveli az AVG szoftvert

Kattintson a hivatkozásra egyszer az AVG Facebook közösséghez történő csatlakozáshoz, illetve a legfrissebb AVG információk, hírek, tippek és trükkök megosztásához a maximális internetes biztonság érdekében.

5.1.2. Jelentések

Megnyit egy új ***Jelentések*** párbeszédpanelt, amely tartalmazza a korábban indított vizsgálatok és frissítések minden lényeges jelentését. Ha a vizsgálat vagy a frissítés éppen fut, egy forgó kör jelenik meg a ***Jelentések*** szöveg mellett a fő felhasználói felület felső navigációs sávján. A körre kattintva megnyithatja az éppen futó folyamat állapotát megjelenítő párbeszédpanelt:



5.1.3. Támogatás

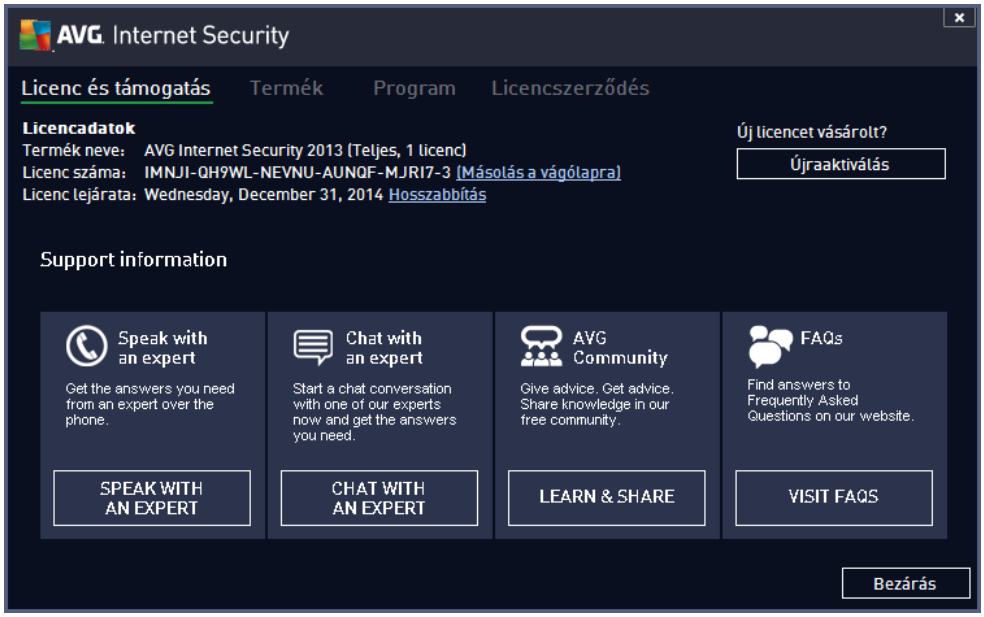
Megnyit egy új, négy lapra osztott párbeszédpanelt, ahol minden fontos információt megtalál az **AVG Internet Security 2013** termékről:

- ***Licenc és Támogatás*** – A lap információt biztosít a termék nevéről, a licencszámról és a lejárati dátumról. A párbeszédpanel alsó szakaszán egy átláthatóan elrendezett összefoglalás található az ügyfélszolgálat valamennyi elérhetőségéről. A lapon a következő aktív hivatkozások és gombok érhetők el:
    - *(Újra)aktiválás* – Kattintson ide az új ***AVG szoftveraktiválás*** párbeszédpanel megnyitásához. Írja be a licencszámát a megfelelő mezőbe, az értékesítési szám

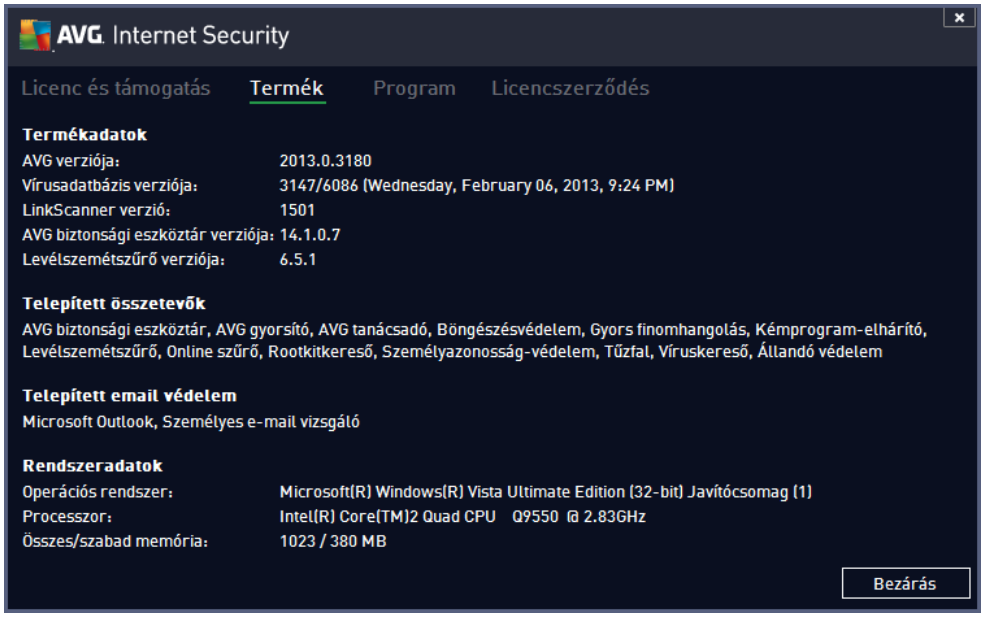
lecseréléséhez *(amit az AVG Internet Security 2013 telepítése során használt),* vagy az aktuális licencszám egy másikra történő módosításához *(például amikor egy bővebb szolgáltatásokat nyújtó AVG termékre frissít)*.

- *Másolás a vágólapra* – Ez a hivatkozás a licencszám másolásához használható, majd beilleszthető oda, ahova szükséges. Ilyen módon biztos lehet abban, hogy a licencszámot helyesen adja meg.

- *Megújítás most* – Javasoljuk, hogy időben vásárolja meg az **AVG Internet Security 2013** licencmegújítását, legalább egy hónappal az aktuális licence lejárata előtt. Értesítést fog kapni a közeledő lejárati dátumról. Erre a hivatkozásra kattintva a rendszer átirányítja az AVG webhelyére *(http://www.avg.com/)*, ahol részletes információt talál a licence állapotáról, a lejárati dátumról és a megújítási/frissítési ajánlatokról.

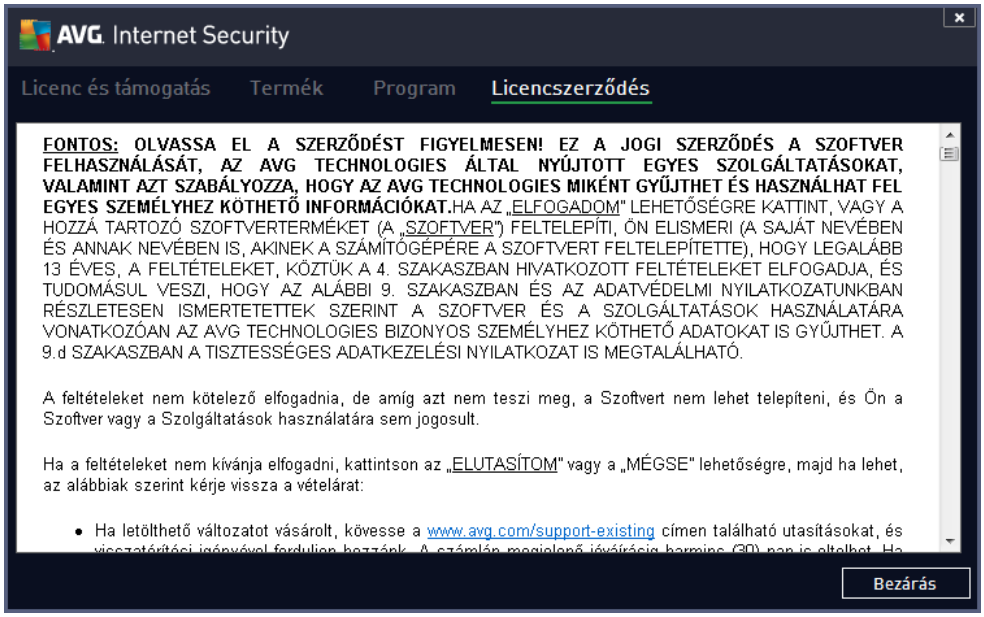


- ***Termék*** – A lap áttekintést biztosít az **AVG Internet Security 2013** termékinformációra, telepített összetevőire, telepített e-mail védelmére, és rendszerinformációra vonatkozó legfontosabb technikai adatokról:



- ***Program*** – Ezen a lapon információt talál a programfájl verziójáról és a termékben használt, harmadik féltől származó kódról:

- ***Licencszerződés*** – A lap tartalmazza az Ön és az AVG Technologies vállalat között létrejött licencszerződés teljes szövegét:



5.1.4. Beállítások

Az **AVG Internet Security 2013 karbantartása** a ***Beállítások*** elemen keresztül érhető el. Kattintson a nyílra a legördülő menü megnyitásához:

- ***A Számítógép vizsgálata*** elindítja a teljes számítógép vizsgálatát.
- ***Kiválasztott mappa vizsgálata...*** – Átvált az AVG vizsgálati felületre, és lehetővé teszi a számítógépen ellenőrizni kívánt fájlok és mappák meghatározását a fastruktúrában.
- ***Fájl vizsgálata...*** – Lehetővé teszi egyetlen meghatározott fájl igény szerinti vizsgálatát. Kattintson erre a pontra a lemez fastruktúráját tartalmazó új ablak megnyitásához. Válassza ki a kívánt fájlt, és erősítse meg a vizsgálat indítását.
- ***Frissítés*** – Automatikusan elindítja az **AVG Internet Security 2013** frissítését.
- ***Frissítés könyvtárból...*** – Elindítja a frissítési folyamatot a helyi lemezen található megadott mappában lévő frissítési fájlokkal. Ez az opció csak vészhelyzet esetén javasolt, pl. olyan helyzetekben, amikor nincs internetkapcsolat (például a számítógép fertőzött, és lecsatlakoztatta az internetről, vagy a számítógépet olyan hálózathoz csatlakoztatta, amely nem fér hozzá az internethez stb.). A megnyíló ablakban válassza ki azt a mappát, mely tartalmazza a telepítőfájlt, és indítsa el a telepítési folyamatot.
- ***Karantén*** – Megnyitja a Karantént, az elkülönített helyet, ahova az AVG program az összes nem javítható fertőzést helyezi. A Karanténban a fertőzött fájlok el vannak különítve, és a számítógép biztonsága garantált. Ugyanakkor a fertőzött fájlok jövőbeli javítás céljából eltárolódnak.
- ***Előzmények*** – További speciális almenü lehetőségeket biztosít:
    - *Vizsgálat eredménye* – Megnyit egy párbeszédpanelt, amely áttekintést biztosít a vizsgálat eredményeiről.

- *Állandó védelem találatai* – Megnyit egy párbeszédpanelt a fenyegetések áttekintésével, amelyeket az Állandó védelem fedezett fel.
- *Személyazonosság-védelem találatai* – Megnyit egy párbeszédpanelt azon fenyegetések áttekintésével, amelyeket a Személyazonosság-védelem fedezett fel.
- *E-mail védelem észlelései* – Megnyit egy párbeszédpanelt azon üzenetmellékletek áttekintésével, amelyeket az E-mail védelem összetevő veszélyesnek talált.
- *Online szűrő találatai* – Megnyit egy párbeszédpanelt az Online szűrő által észlelt fenyegetések áttekintésével.
- *Eseménynapló* – Megnyitja az eseménynaplót az összes naplózott **AVG Internet Security 2013** eseménnyel.
- *Tűzfalnapló* – Megnyit egy párbeszédpanelt a Tűzfal műveletek részletes áttekintésével.

- ***Speciális beállítások…*** – Megnyitja az AVG speciális beállítások párbeszédpanelt, ahol szerkesztheti az **AVG Internet Security 2013** beállításait. Általában nem érdemes módosítani a szoftvergyártó által megadott alapértelmezett beállításokat az alkalmazásban.
- ***Tűzfalbeállítások…*** – Megnyitja a Tűzfal összetevő speciális beállításainak megadására szolgáló külön párbeszédpanelt.
- ***Súgó tartalomjegyzék*** – Megnyitja az AVG súgófájlokat.
- ***Támogatás kérése*** – Megnyitja az AVG webhelyén *(http://www.avg.com/)* az ügyféltámogatási központ oldalát.
- ***AVG online*** – Megnyitja az AVG webhelyét *(http://www.avg.com/).*
- ***A vírusok és fenyegetések ismertetése*** – Megnyitja az online vírusenciklopédiát, ahol részletes információkat találhat az észlelt vírussal kapcsolatban.
- ***(Újra)aktiválás*** – Megnyitja az ***AVG aktiválása*** párbeszédpanelt azokkal az adatokkal, amelyeket megadott a a telepítési folyamat során. Ezen a panelen megadhatja a licencszámot, hogy lecserélje az értékesítési számot (*az a szám, amivel telepítette az AVG terméket*), vagy hogy lecserélje a régi licencszámot (*pl. amikor frissíti az új AVG terméket*).
- ***Regisztrálás/Saját fiók*** – Csatlakozik az AVG webhelyének regisztrációs oldalához (http://www.avg.com/). Töltse ki a regisztrációs adatokat; csak regisztrált ügyfelek jogosultak az ingyenes AVG műszaki terméktámogatásra. Ha az **AVG Internet Security 2013** próbaverzióját használja, akkor az utolsó két lépés a ***Vásárlás most*** és az ***Aktiválás*** lesz, amelyek segítségével megvásárolhatja a program teljes verzióját. Az értékesítési számmal telepített **AVG Internet Security 2013** esetében ezen lépések a következők: ***Regisztrálás most*** és ***Aktiválás***.
- ***AVG névjegye*** – Megnyit egy új párbeszédpanelt négy lappal, amelyek adatokat biztosítanak a megvásárolt licencről és az elérhető támogatásról, a termék- és programinformációkról, valamint a licencszerződés teljes szövegéről.

5.2. Biztonsági állapot információk

A ***Biztonsági állapot információk*** nevű rész az **AVG Internet Security 2013** főablak felső részén helyezkedik el. Itt mindig információkat találhat az **AVG Internet Security 2013** aktuális biztonsági állapotáról. Tekintse át az ebben a részben esetlegesen megjelenő ikonok listáját és jelentésüket:

 – A zöld ikon azt jelzi, hogy az ***AVG Internet Security 2013 teljesen működőképes***. A számítógép teljesen védett, a rendszer naprakész, és a telepített összetevők megfelelően működnek.

 – A sárga ikon figyelmeztet, hogy ***egy vagy több összetevő rosszul van konfigurálva***, ezért ellenőrizni kell ezek tulajdonságait/beállításait. Nincs súlyos hiba az **AVG Internet Security 2013** működésében, és elképzelhető, hogy Ön kapcsolta ki az egyik összetevőt valamilyen okból. A védelme továbbra is garantált. Azonban fordítson figyelmet a problémás összetevő beállításaira! A helytelenül konfigurált összetevő a fő felhasználói felületen egy narancssárga figyelmeztető sávval jelenik meg.

A sárga ikon akkor is megjelenik, ha valamiért úgy dönt, hogy figyelmen kívül hagyja egy összetevő hibás állapotát. A ***Hibaállapot figyelmen kívül hagyása*** lehetőség a Speciális beállítások / Hibaállapot figyelmen kívül hagyása ágban érhető el. Itt jelezheti, hogy tisztában van az összetevő hibás állapotával, de saját elhatározásból ebben az állapotban kívánja tartani az **AVG Internet Security 2013** szoftvert, és nem szeretne figyelmeztetést kapni erről. Elképzelhető, hogy bizonyos helyzetekben használnia kell, de javasoljuk, hogy amint lehetséges, kapcsolja ki a ***Hibaállapot figyelmen kívül hagyása*** lehetőséget!

A sárga ikon akkor is megjelenik, ha az **AVG Internet Security 2013** a számítógép újraindítását igényli (***Újraindítás szükséges***). Figyeljen erre a figyelmeztetésre, és indítsa újra a számítógépet.

 – A narancssárga ikon azt jelzi, hogy az ***AVG Internet Security 2013 kritikus állapotban van***! Egy vagy több összetevő nem működik megfelelően, és az **AVG Internet Security 2013** nem tudja megvédeni a számítógépet. Azonnal javítsa ki a jelentett problémát! Ha nem tudja egyedül kijavítani a hibát, akkor vegye fel a kapcsolatot az AVG műszaki támogatás csapattal.

Ha az AVG Internet Security 2013 szoftver nincs optimális teljesítményre állítva, akkor egy új Kattintson a javításhoz (vagy Kattintson az összes javításához, ha több problémáról van szó) gomb jelenik meg a biztonsági állapottal kapcsolatos információk mellett. Kattintson erre a gombra az automatikus programellenőrzési és konfigurációs folyamat elindításához. Így könnyen optimalizálható az AVG Internet Security 2013 szoftver teljesítménye, és garantálható a lehető legnagyobb biztonság.

Különösen javasolt, hogy figyelmet fordítson a ***Biztonsági állapot információk*** részre, és probléma esetén azonnal javítsa a hibát. Különben biztonsági kockázatnak teszi ki számítógépét!

Megjegyzés: *Az AVG Internet Security 2013 állapota bármikor ellenőrizhető a tálcaikon segítségével.*

5.3. Összetevők áttekintése

A telepített összetevők áttekintése a főablak középső részén, egy vízszintes blokksávon található. Az összetevők világoszöld blokkokként jelennek meg a megfelelő összetevőikonnal címkézve. Minden blokk a védelem aktuális állapotáról szolgáltat információkat. Ha az összetevő megfelelően van beállítva és teljesen működőképes, akkor az információ zöld betűkkel jelenik meg. Ha az összetevőt leállították, a működése korlátozott vagy az összetevő hibaállapotban van, egy narancssárga szövegmezőben megjelenő figyelmeztető szöveg fogja értesíteni. ***Feltétlenül ajánlott figyelmet fordítani az egyes összetevők beállításaira.***

Helyezze az egeret az összetevőre egy rövid szöveg megjelenítéséhez a főablak alján. A szöveg az összetevő működésének alapvető bemutatását tartalmazza. Emellett az összetevő aktuális állapotáról is tájékoztat, és meghatározza, hogy az összetevő mely szolgáltatásai nincsenek megfelelően konfigurálva.

Telepített összetevők listája

Az **AVG Internet Security 2013 termékben** az ***Összetevők áttekintése*** rész a következő összetevőkről nyújt információkat:

- ***Számítógép*** – Ez az összetevő két szolgáltatást tartalmaz: a ***Víruskereső védelem*** vírusokat, kémprogramokat, férgeket, trójaiakat, kéretlen végrehajtható fájlokat, valamint kódtárakat keres a rendszeren, és a kártékony reklámprogramoktól is véd; a ***Rootkitkereső*** pedig alkalmazásokban, illesztőprogramokban vagy kódtárakban elrejtett veszélyes rootkiteket keres. Részletek >>
- ***Webes böngészés*** – A webes alapú fenyegetések ellen nyújt védelmet internetes keresés és böngészés közben. Részletek >>
- ***Személyazonosság*** – Az összetevő futtatja a ***Személyazonosság-őrző*** szolgáltatást, amely folyamatosan védelmezi digitális adatait az új és ismeretlen internetes fenyegetésektől,. Részletek >>
- ***E-mailek*** – Levélszemetet keres a bejövő emailekben, és blokkolja a vírusokat, az adathalász támadásokat és az egyéb fenyegetéseket. Részletek >>
- ***A Tűzfal*** irányítja a kommunikációt az egyes hálózati portokon, véd a rosszindulatú támadásoktól, valamint blokkolja a behatolási kísérleteket. Részletek >>

Elérhető műveletek

- ***Helyezze az egérmutatót bármely összetevő ikonjára*** az összetevők áttekintésében történő kiemeléshez. Ezzel egy időben az összetevő alapvető működésének leírása megjelenik a felhasználói felület alsó részén.
- ***Ha egyszer kattint egy összetevő ikonjára***, akkor megnyílik az összetevő saját felülete az összetevő aktuális állapotára vonatkozó információkkal, illetve megtekintheti a konfigurációját és statisztikai adatait.

5.4. Saját alkalmazások

A ***Saját alkalmazások*** területen *(a zöld blokkok sora az összetevőkészlet alatt)* az olyan további AVG alkalmazások áttekintését láthatja, amelyek már telepítve vannak a számítógépén, illetve ajánlott a telepítésük. A blokkok feltételesen jelennek meg, és a következő alkalmazások bármelyikét jelölhetik:

- ***A Mobilvédelem*** egy alkalmazás, amely megvédi a mobiltelefonját a vírusoktól és kártevőktől. Lehetővé teszi az elveszett okostelefonok távoli követését is.

- ***A LiveKive*** összetevő online adatmentésre szolgál. Az adatokat biztonságos kiszolgálókon tárolja a rendszer. A LiveKive automatikusan biztonsági másolatot készít az összes fájlról, képről és zenéről egyetlen biztonságos helyre, és lehetővé teszi a családtagokkal és ismerősökkel való megosztásukat, valamint az elérésüket bármilyen internetezésre alkalmas eszközzel, például iPhone vagy Android rendszerű készülékkel.

- ***A Family Safety*** segít megvédeni gyermekeit a nem megfelelő webhelyektől, médiatartalmaktól és online keresésektől, illetve jelentésekkel szolgál az online tevékenységükről. Az AVG Family Safety a billentyűleütés-követő technológia segítségével felügyeli gyermeke tevékenységét a csevegőszobákban és a közösségi oldalakon. Amennyiben a gyermekek online becsapásával kapcsolatos szavakat, kifejezéseket vagy nyelvezetet talál, a program azonnal értesítést küld SMS-üzeneten vagy e-mailen keresztül. Az alkalmazás használatával minden egyes felhasználó esetében megadhatja a kívánt védelmi szintet, és külön-külön figyelheti a felhasználók tevékenységét az egyedi bejelentkezéseken keresztül.

- ***A PC Tuneup*** alkalmazás részletes rendszerelemzésre szolgáló eszköz, amely meghatározza, hogy miként javítható a számítógép sebessége és teljesítménye.

- ***A MulitMi*** az összes e-mail és közösségi fiókját egy biztonságos helyen egyesíti, egyszerűbbé téve a családtagokkal és az ismerősökkel való kapcsolattartást, az internetböngészést és a fényképek, videók és fájlok megosztását. A MultiMi LinkScanner szolgáltatása a weboldalakon megjelenő számos hivatkozás mögött található weboldalak elemzésével és ellenőrzésével megvédi Önt az interneten egyre nagyobb számban terjedő fenyegetésektől.

- ***Az AVG Toolbar*** közvetlenül elérhető a webböngészőből, és maximális biztonságot garantál az internetes

A ***Saját alkalmazások*** részletes információiért kattintson a megfelelő blokkra. A rendszer átirányítja a termékhez tartozó AVG weboldalra, ahol azonnal le is töltheti ezt az összetevőt.

5.5. Vizsgálat/Gyorshivatkozások frissítése

A ***Gyorshivatkozások*** az **AVG Internet Security 2013** felhasználói felületén, a gombok alsó sorában találhatók. Ezek a gyorshivatkozások lehetővé teszik, hogy azonnal hozzáférjen az alkalmazás legfontosabb és leggyakrabban használt funkcióihoz, amilyenek például a vizsgálat és a frissítés. Ezek a gyorshivatkozások bármikor elérhetők a felhasználói felület összes párbeszédpaneléről:

- ***Vizsgálat indítása*** - Ez a gomb grafikusan két részre van osztva. Kövesse a ***Vizsgálat indítása*** hivatkozást a Teljes számítógép-vizsgálat azonnali indításához. Az állapot és az

eredmények az automatikusan megnyíló Jelentések ablakban tekinthetők meg. A ***Beállítások*** gomb megnyitja a ***Vizsgálati beállítások*** párbeszédpanelt, ahol az ütemezett vizsgálatokat kezelheti és a Teljes számítógép-vizsgálat / Kiválasztott fájlok és mappák vizsgálata funkció paramétereit szerkesztheti. *(A részletekért tekintse meg az AVG vizsgálat című fejezetet)*

- ***Frissítés indítása*** – A gomb megnyomásával azonnal elindul a termékfrissítés. Az AVG tálcaikon feletti párbeszédpanelen látja a frissítés eredményeit. *(A részletekért tekintse meg az AVG frissítések című fejezetet)*

5.6. Tálcaikon

Az ***AVG tálcaikon*** *(a Windows tálcán a képernyő jobb alsó sarkában található)* jelzi az **AVG Internet Security 2013** alkalmazás aktuális állapotát. Ez mindig látható a tálcán, attól függetlenül, hogy az **AVG Internet Security 2013** felhasználói felülete meg van-e nyitva:

AVG tálcaikon megjelenése

- Ha színes, és semmilyen egyéb elem nem látható rajta, az azt jelzi, hogy az **AVG Internet Security 2013** összetevők aktívak és tökéletesen működőképesek. Az ikon akkor is így jelenhet meg, ha egy összetevő nem működik tökéletesen, de a felhasználó úgy döntött, hogy figyelmen kívül hagyja az adott összetevő állapotát. *(Dönthet úgy, hogy figyelmen kívül hagyja az összetevő állapotát. Ezzel jelzi, hogy tisztában van az összetevő hibaállapotával, de saját elhatározásból ebben az állapotban kívánja tartani, és nem szeretné, hogy a program figyelmeztesse erre.)*

- A felkiáltójellel kiegészített ikon azt jelzi, hogy egy *(vagy akár több)* összetevő hibaállapotban van. Mindig ügyeljen az ilyen figyelmeztetésekre, és próbálja meg elhárítani a nem megfelelően beállított összetevők konfigurációs problémáit. Az alkalmazás felhasználói felületének megnyitásához és az összetevő beállításainak módosításához kattintson duplán a tálcaikonra. Részletes információkért azzal kapcsolatban, hogy melyik összetevő van hibaállapotban, tekintse meg a biztonsági állapot információk nevű szakaszt.

- A tálcaikon ezenfelül megjelenhet színesen, egy villogó vagy forgó fénynyalábbal is. Az így kinéző ikon azt jelzi, hogy éppen frissítési folyamat zajlik.

- A színes ikonon megjelenhet egy nyíl is, ami azt jelenti, hogy az **AVG Internet Security 2013** éppen vizsgálatot futtat.

AVG tálcaikon információk

Az ***AVG tálcaikon*** tájékoztatja az **AVG Internet Security 2013** aktuális műveleteiről és esetleges állapotváltozásokról (*például egy ütemezett vizsgálat vagy frissítés automatikus indítása, Tűzfalprofil-váltás, összetevő állapotváltozása, hibaállapot felmerülése, ...*) egy felbukkanó ablak formájában a tálcaikonnál.

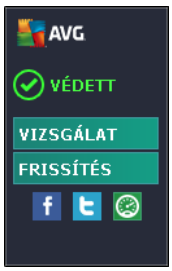
Az AVG tálcaikonról elérhető műveletek

Az ***AVG tálcaikon*** gyorshivatkozásként is szolgál az **AVG Internet Security 2013** felhasználói felületének azonnali eléréséhez. A felület megnyitásához csak kattintson duplán az ikonra. Kattintson a jobb gombbal az ikonra a helyi menü megnyitásához, amely a következő lehetőségeket tartalmazza:

- ***AVG felhasználói felület megnyitása*** – kattintson ide az **AVG Internet Security 2013** felhasználói felületének megnyitásához.
- ***AVG védelem ideiglenes letiltása*** – ez a beállítás lehetővé teszi az **AVG Internet Security 2013** által nyújtott teljes védelem azonnali kikapcsolását. Ezt a beállítást csak akkor használja, ha feltétlenül szükséges. A legtöbb esetben nem szükséges letiltani az **AVG Internet Security 2013** védelmet új szoftver vagy illesztőprogram telepítése előtt, még akkor sem, ha a telepítő vagy a varázsló javasolja a futó programok és alkalmazások bezárását a telepítési folyamat zavartalansága érdekében. Ha ideiglenesen ki kell kapcsolnia az **AVG Internet Security 2013** védelmet, akkor mielőbb kapcsolja azt vissza. Ha kikapcsolt víruskereső szoftverrel csatlakozik az internethez vagy egy hálózathoz, akkor a számítógépe védtelen a támadásokkal szemben.
- ***Vizsgálat*** – kattintson ide az előre meghatározott vizsgálatok (*Teljes számítógép-vizsgálat* és *Kiválasztott fájlok és mappák vizsgálata*) helyi menüjének megnyitásához, majd válassza ki a kívánt vizsgálatot, amely azonnal elindul.
- ***Futó vizsgálatok...*** – ez az elem csak akkor jelenik meg, ha egy vizsgálat éppen fut a számítógépen. A vizsgálatnál beállíthatja annak prioritását, illetve leállíthatja vagy felfüggesztheti azt. A következő műveletek szintén elérhetők: *Összes vizsgálat prioritásának beállítása, Összes vizsgálat felfüggesztése,* illetve *Összes vizsgálat leállítása*.
- ***Számítógép-elemző*** futtatása - kattintson ide a Számítógép-elemző összetevő indításához.
- ***Saját fiók*** – Megnyitja a Saját fiók oldalt, ahol kezelheti az előfizetett termékeit, további védelmet vásárolhat, telepítési fájlokat tölthet le, ellenőrizheti korábbi megrendeléseit és számláit, valamint kezelheti személyes adatait.
- ***Frissítés most*** – elindítja az azonnali frissítést.
- ***Súgó*** – megnyitja a súgó fájlt a kezdőlapon.

5.7. AVG minialkalmazás

Az ***AVG minialkalmazás***a Windows asztalon jelenik meg (*Windows oldalsáv*). Ez az alkalmazás csak a Windows Vista és a Windows 7/8 rendszereken támogatott. Az ***AVG minialkalmazás*** azonnali hozzáférést biztosít az **AVG Internet Security 2013** legfontosabb szolgáltatásokhoz, például a vizsgálathoz és a frissítéshez:

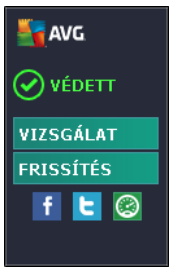


Az AVG minialkalmazás vezérlői

Az AVG minialkalmazás szükség esetén lehetővé teszi a vizsgálatok és frissítések azonnali indítását, továbbá tartalmaz egy gyorshivatkozást a főbb közösségi hálózatok eléréséhez és gyors keresést biztosít.

- ***Vizsgálat indítása*** – Kattintson a ***Vizsgálat indítása*** hivatkozásra a Teljes számítógép-vizsgálat funkció közvetlen elindításához. A vizsgálat állapotát a minialkalmazás alternatív felhasználói felületén követheti nyomon. A rövid statisztikai áttekintés információkat nyújt a vizsgált objektumok, az észlelt fenyegetések és a javított fenyegetések számával kapcsolatban. A vizsgálat során bármikor felfüggesztheti vagy leállíthatja a folyamatot. A vizsgálati eredményekhez tartozó részletes adatokért tekintse meg A vizsgálat eredményének áttekintése párbeszédpanelt, amely közvetlenül a minialkalmazásból nyitható meg a ***Részletek mutatása*** gombra kattintva *(az eredmények az Oldalsáv minialkalmazások vizsgálata területen láthatók)*.

- ***Azonnali frissítés*** – Kattintson az ***Azonnali frissítés*** hivatkozásra az **AVG Internet Security 2013** közvetlen frissítéséhez a minialkalmazásból:



- ***Twitter-hivatkozás*** – megnyitja az ***AVG minialkalmazás*** egy új felületét, amelyen áttekintheti az AVG legújabb bejegyzéseit a Twitter webhelyen. ***Az AVG összes Twitter-hírcsatornájának megtekintése*** hivatkozásra kattintva megnyílik egy új böngészőablak, amely közvetlenül a Twitter webhelyre irányítja át, ahol megtekintheti az AVG vállalathoz kapcsolódó hírek oldalát:

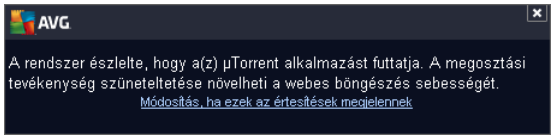
- ***Facebook-hivatkozás*** – megnyitja az internetböngészőt, és megjeleníti az ***AVG közösségi*** oldalát a Facebook webhelyen.

- ***Keresődoboz*** – Írjon be egy kulcsszót, és a találatok azonnal megjelennek az alapértelmezett böngésző egy újonnan megnyíló ablakában.

5.8. AVG Tanácsadó

Az AVG Tanácsadó olyan problémák észlelésében segít, amelyek lelassítják a számítógépét, vagy kockázatnak teszik ki, és ilyenkor egy intézkedést javasol a helyzet megoldásához. Ha a számítógép hirtelen lelassulását észleli *(internetböngészés, általános teljesítmény terén)*, általában nem egyértelmű, hogy mi is pontosan ennek az oka, és ebből következően, hogy mi a probléma megoldása. Itt lép a képbe az ***AVG Tanácsadó***: Megjelenít egy értesítést a tálcán, amely a probléma lehetséges okáról tájékoztatja, és javaslatot tesz annak kijavítására. Az ***AVG Tanácsadó*** a számítógép minden futó folyamatát figyelemmel követi a lehetséges hibák felderítésére, és tippeket ajánl fel a problémák elkerülésére.

Az ***AVG Tanácsadó*** egy beúszó felugró menü formájában jelenik meg a tálcán:



Az ***AVG Tanácsadó*** kiemelten figyeli a következőket:

- ***Bármely futó webböngésző állapota***. A webböngészők túlterhelhetik a memóriát, különösen, ha több lap vagy ablak van nyitva hosszabb ideig, és túl sok erőforrást foglalnak le, azaz lelassítják a számítógépet. Ebben a helyzetben általában segít, ha újraindítja a webböngészőjét.

- ***Fájlcserélőkapcsolatok futtatása***. Ha P2P protokollt használt fájlok megosztásához, a kapcsolat néha aktív maradhat, ami a sávszélesség egy részét elfoglalja. Ennek eredményeképpen a webböngészés lelassulását észlelheti.

- ***Ismeretlen hálózat ismerős névvel***. Ez általában csak azokra a felhasználókra

vonatkozik, akik különböző hálózatokra csatlakoznak, jellemzően a hordozható számítógépükről: Ha egy új, ismeretlen hálózatnak megegyezik a neve egy jól ismert, gyakran használt hálózatéval *(például Otthon vagy SajátWifi)*, összetéveszthetik azokat, és véletlenül csatlakozhat egy teljesen ismeretlen és potenciálisan veszélyes hálózathoz. Az ***AVG Tanácsadó*** megelőzheti ezt, ha értesíti, hogy az ismert név valójában egy új hálózatot takar. Természetesen, ha úgy dönt, hogy az ismeretlen hálózat biztonságos, elmentheti azt az ***AVG Tanácsadó*** ismert hálózatok listájába, hogy azt ne jelentse többet a jövőben a program.

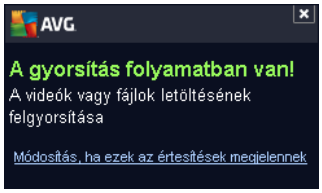
Ezekben az esetekben az ***AVG Tanácsadó*** figyelmezteti a lehetséges problémára, és megjeleníti a problémát okozó folyamat vagy alkalmazás nevét és ikonját. Az ***AVG Tanácsadó*** emellett lépéseket is javasol a lehetséges zavar elkerülésére.

Támogatott webböngészők

A szolgáltatás az alábbi webböngészők esetén működik: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.9. AVG gyorsító

Az AVG gyorsító folyamatosabb online videolejátszást tesz lehetővé, és megkönnyíti a további letöltéseket. Amikor videogyorsítás van folyamatban, a tálcán megjelenik egy felugró ablak.



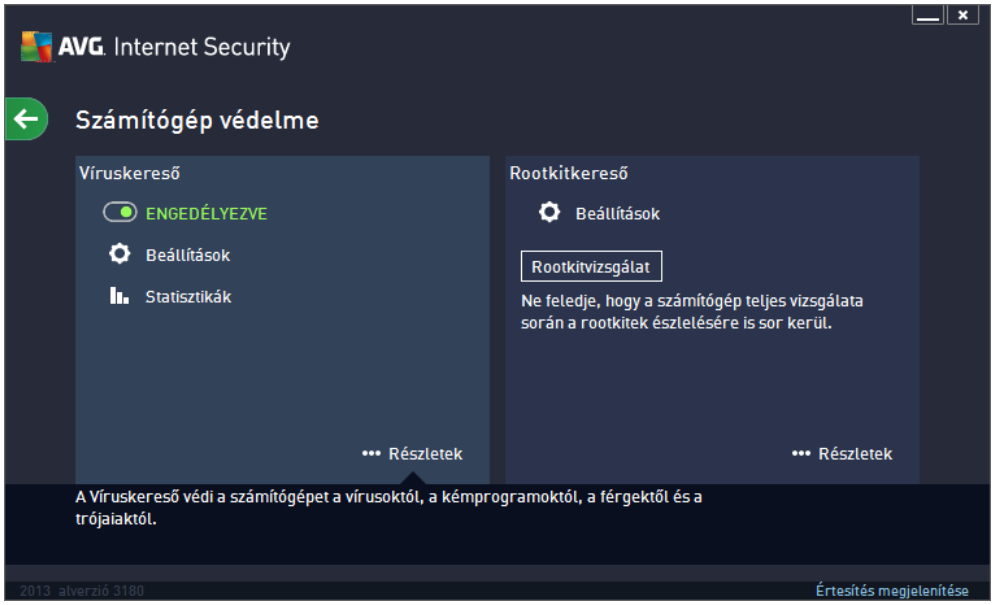
6. AVG összetevők

6.1. Számítógép

A ***Számítógép*** összetevő két fő biztonsági szolgáltatást takar: a ***Víruskereső*** és a ***Rootkitkereső*** szolgáltatásokat:

- ***A Víruskereső*** egy olyan vizsgálómotorból áll, amely védi az összes fájlt, a számítógép rendszerterületeit és a cserélhető adathordozókat *(flash meghajtó stb.)* és ismert vírusokat keres. A felismert vírusokat a program elzárja minden fájlművelettől, ezután pedig megsemmisíti vagy karanténba helyezi azokat. A felhasználó észre sem veszi a folyamatot, hiszen az úgynevezett állandó védelem „a háttérben" fut. A Víruskereső heurisztikus vizsgálatra is képes, amelynek során a program vírusra utaló tulajdonságokat keres az egyes fájlokban. Ez azt jelenti, hogy a Víruskereső felismerhet teljesen új, idáig ismeretlen vírusokat is, ha az tartalmaz bizonyos – már létező vírusokra jellemző – tulajdonságokat. Az **AVG Internet Security 2013** képes a rendszer nemkívánatos végrehajtható alkalmazásainak és DLL könyvtárainak elemzésére és azonosítására is *(különféle kémprogramok, reklámprogramok stb.)*. Ezenkívül a Víruskereső megvizsgálja a beállításjegyzéket is, ahol gyanús bejegyzéseket és ideiglenes internetes fájlokat keres, és lehetőséget nyújt a potenciálisan kártékony elemek fertőzésként történő kezelésére.

- ***A Rootkitkereső*** egy speciális eszköz, amely felismeri és hatékonyan eltávolítja a veszélyes rootkiteket, azaz az olyan programokat és technológiákat, amelyek rosszindulatú szoftverek jelenlétét leplezhetik a számítógépen. A rootkiteket arra tervezték, hogy átvegyék az irányítást a számítógép felett annak tulajdonosának vagy jogos használójának hozzájárulása nélkül. A Rootkitkereső előre meghatározott szabályok alapján képes észlelni a rootkiteket. Ha a Rootkitkereső rootkiteket talál, az nem feltétlenül jelenti, hogy az adott rootkit fertőzött. Bizonyos esetekben a rootkitek illesztőprogramok vagy legitim alkalmazások részei.



A párbeszédpanel vezérlői

A párbeszédpanel részei közötti váltáshoz csak kattintson a kívánt szolgáltatáspanel bármelyik részére. A panel ezután világoskék színnel kiemelve jelenik meg. A panel mindkét részén a következő vezérlők találhatók. A működésük ugyanaz mindkét biztonsági szolgáltatás *(Víruskereső vagy Rootkitkereső)*esetén:

 ***Engedélyezve / Letiltva*** – A gomb megjelenése és funkciója is egy közlekedési lámpára hasonlít. Egy kattintással válthat a két pozíció között. A zöld szín az ***Engedélyezve*** értéket jelenti, vagyis hogy a Víruskereső biztonsági szolgáltatás aktív, és minden funkciója működik. A vörös szín a ***Letiltva*** állapotot jelzi, vagyis hogy a szolgáltatás ki van kapcsolva. Nyomatékosan javasoljuk, hogy ne módosítsa az alapértelmezett biztonsági beállításokat, hacsak nincs jó oka a szolgáltatás kikapcsolására. Az alapértelmezett beállítások garantálják az alkalmazás optimális teljesítményét és a maximális biztonságot. Ha valamiért ki szeretné kapcsolni a szolgáltatást, a rendszer egy vörös ***Figyelmeztetés*** jellel azonnal figyelmezteti a lehetséges kockázatokra, és tájékoztatja, hogy nem teljes körű a védelme. ***Ne feledje a lehető leghamarabb ismét aktiválni a szolgáltatást!***

 ***Beállítások*** – A gombra kattintva a speciális beállítások felületre ugorhat. Megnyílik a megfelelő panel, és beállíthatja a kiválasztott szolgáltatást, vagyis a Víruskeresőt vagy a Rootkitkeresőt. A speciális beállítások felületen szerkesztheti az **AVG Internet Security 2013** programban valamennyi biztonsági szolgáltatásának összes konfigurációját, de a konfigurálás csak tapasztalt felhasználók számára ajánlott!

 ***Statisztika*** – A gombra kattintva a rendszer átirányítja az AVG webhelyének (http://www.avg.com/) megfelelő oldalára. Ezen az oldalon részletes statisztikai áttekintést talál az **AVG Internet Security 2013** a számítógépen egy adott időtartamon belül, valamint összességében végzett tevékenységeiről.

 ***Részletek*** – A gombra kattintva a párbeszédpanel alján megjelenik a kiemelt szolgáltatás rövid leírása.

 – A párbeszédpanel bal felső részén lévő zöld nyíllal térhet vissza az összetevők áttekintését tartalmazó fő felhasználói felületre.

A Rootkitkeresőben található egy külön ***Rootkitek vizsgálata*** gomb, amellyel közvetlenül indíthatja el az önálló rootkitvizsgálatot *(a rookitvizsgálat azonban része A teljes számítógép vizsgálata funkciónak)*.

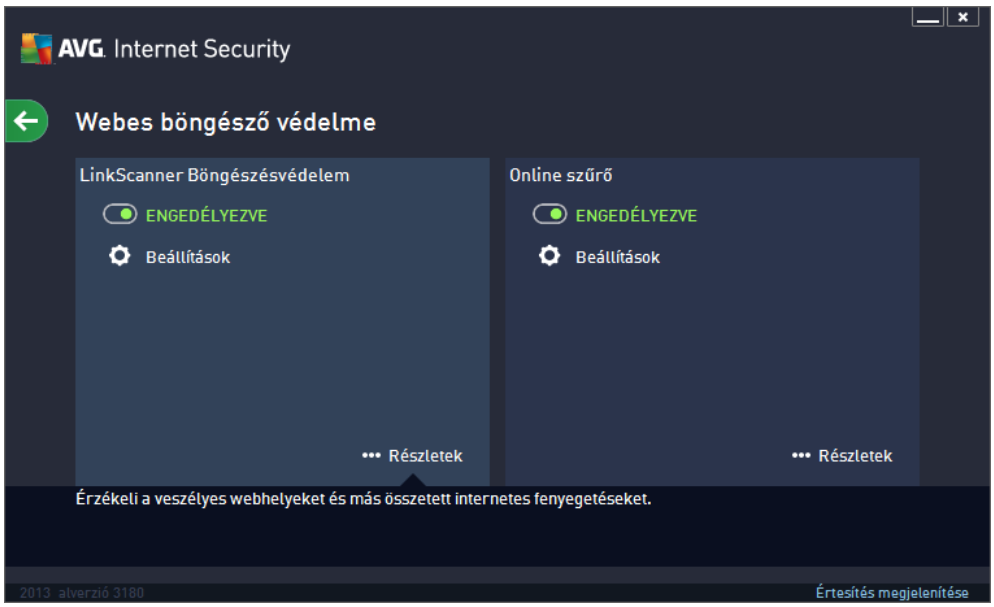
6.2. Webes böngészés

A ***Webes böngésző védelme*** két szolgáltatásból áll: ***a LinkScanner böngészésvédelemből*** és az ***Online szűrőből***:

- ***A LinkScanner böngészésvédelem*** védi Önt napjaink gyorsan felbukkanó és eltűnő online fenyegetéseitől. Ezen fenyegetések rejtve lehetnek bármilyen szervezet weboldalán (a kormányzatoktól kezdve, a nagy és jól ismert márkákon át, egészen a kisvállalkozásokig), és ritkán maradnak ugyanazon a weboldalon 24 óránál tovább. A LinkScanner elemzi a linkek mögött lévő, megtekintendő weboldalak tartalmát, és biztosítja, hogy Ön már akkor biztonságban legyen, mielőtt még rákattintana az adott linkre. ***A LinkScanner***

böngészésvédelem nem a kiszolgálóplatformok védelmére szolgál!

- ***Az Online szűrő*** valós idejű állandó védelmet nyújt. Ellenőrzi a meglátogatandó weboldalakat (és az esetlegesen beágyazott dokumentumokat), mielőtt azok megjelennének a webböngészőben vagy letöltődnének a számítógépre. Az Online szűrő felismeri, ha a meglátogatandó oldal veszélyes java szkriptet tartalmaz, és megakadályozza annak betöltődését. Természetesen azonosítja a beágyazott rosszindulatú kódokat is, és megakadályozza azok letöltődését is a számítógépre. Ez a hatékony védelem blokkolni fogja bármilyen megnyitni kívánt káros weboldal tartalmát, és megelőzi, hogy azok letöltődjenek a számítógépre. Ha egy veszélyes weboldalra mutató hivatkozásra kattint vagy annak címét írja be, akkor a program automatikusan letiltja az oldal megnyitását, és ezáltal megvédi Önt a véletlen megfertőződéstől. Fontos, hogy ne felejtse el, hogy a káros weboldalak már azzal megfertőzhetik a számítógépet, ha egyszerűen csak felkeresi azokat. ***Az Online szűrő nem kiszolgálóplatformok védelmére szolgál!***



A párbeszédpanel vezérlői

A párbeszédpanel részei közötti váltáshoz csak kattintson a kívánt szolgáltatáspanel bármelyik részére. A panel ezután világoskék színnel kiemelve jelenik meg. A panel mindkét részén a következő vezérlők találhatók. A működésük mindkét biztonsági szolgáltatás *(LinkScanner böngészésvédelem vagy Online szűrő)* esetén azonos:

 ***Engedélyezve / Letiltva*** – A gomb megjelenése és funkciója is egy közlekedési lámpára hasonlít. Egy kattintással válthat a két pozíció között. A zöld szín az ***Engedélyezve*** értéket jelenti, vagyis hogy a LinkScanner böngészésvédelem / Online szűrő biztonsági szolgáltatás aktív és minden funkciója működik. A vörös szín a ***Letiltva*** állapotot jelzi, vagyis hogy a szolgáltatás ki van kapcsolva. Nyomatékosan javasoljuk, hogy ne módosítsa az alapértelmezett biztonsági beállításokat, hacsak nincs jó oka a szolgáltatás kikapcsolására. Az alapértelmezett beállítások garantálják az alkalmazás optimális teljesítményét és a maximális biztonságot. Ha valamiért ki szeretné kapcsolni a szolgáltatást, a rendszer egy vörös ***Figyelmeztetés*** jellel azonnal figyelmezteti a lehetséges kockázatokra, és tájékoztatja,

hogy nem teljes körű a védelme. ***Ne feledje a lehető leghamarabb ismét aktiválni a szolgáltatást!***

 ***Beállítások*** – A gombra kattintva a speciális beállítások felületre ugorhat. Megnyílik a megfelelő panel, és beállíthatja a kiválasztott szolgáltatást, vagyis a LinkScanner Böngészésvédelmet vagy az Online szűrőt. A speciális beállítások felületen szerkesztheti az **AVG Internet Security 2013** programban valamennyi biztonsági szolgáltatásának összes konfigurációját, de a konfigurálás csak tapasztalt felhasználók számára ajánlott!

 ***Statisztika*** – A gombra kattintva a rendszer átirányítja az AVG webhelyének (http://www.avg.com/) megfelelő oldalára. Ezen az oldalon részletes statisztikai áttekintést talál az **AVG Internet Security 2013** a számítógépen egy adott időtartamon belül, valamint összességében végzett tevékenységeiről.

 ***Részletek*** – A gombra kattintva a párbeszédpanel alján megjelenik a kiemelt szolgáltatás rövid leírása.

 – A párbeszédpanel bal felső részén lévő zöld nyíllal térhet vissza az összetevők áttekintését tartalmazó fő felhasználói felületre.

6.3. Személyazonosság

A ***Személyazonosság-védelem*** összetevő futtatja a ***Személyazonosság-őrző*** szolgáltatást, amely folyamatosan védelmezi digitális adatait az új és ismeretlen internetes fenyegetésektől,:

- ***A Személyazonosság-védelem*** olyan, kártevőktől védő összetevő, amely mindenféle kártevő (*kémprogramok, robotprogramok, személyes adatokat eltulajdonító programok stb.*) ellen véd, viselkedésalapú technológiát használ, és azonnali védelmet biztosít a legújabb vírusok ellen. A Személyazonosság-védelem megakadályozza, hogy tolvajok jelszavakat, banki adatokat, hitelkártyaszámokat és egyéb személyes digitális adatokat lopjanak el különféle rosszindulatú szoftverek *(kártevők)* segítségével. Ez biztosítja, hogy a számítógépen vagy a megosztott hálózaton futó valamennyi alkalmazás megfelelően működik. A Személyazonosság-védelem folyamatosan észleli és letiltja a gyanús viselkedést, és megvédi a számítógépet a legújabb kártevőktől. A Személyazonosság-védelem valósidejű védelmet nyújt a számítógép számára az új és ismeretlen fenyegetések ellen. Figyeli az összes folyamatot *(beleértve a rejtetteket is)* és a több mint 285 különféle viselkedési mintát, annak megállapításához, hogy zajlik-e gyanús tevékenység a rendszeren. Ezért olyan fenyegetéseket is képes azonosítani, amelyek még nem szerepelnek a vírusadatbázisban. Ha ismeretlen kód jut el a számítógépre, a program azonnal elkezdi figyelni, nem káros tevékenységeket hajt-e végre, és nyomon követi a viselkedését. Ha a fájl kártékonynak bizonyul, a Személyazonosság-védelem áthelyezi a kódot a Karanténba, majd visszaállítja a rendszert érintő összes rosszindulatú módosítást *(kódbeszúrás, beállításjegyzék módosításai, portok megnyitása stb.)*. Nem kell vizsgálatot indítania a védelem biztosításához. Ez a technológia rendkívül proaktív, ritkán van szüksége frissítésekre, és mindig készenlétben áll.

A párbeszédpanel vezérlői

A panelen a következő vezérlőket találja:

Engedélyezve / Letiltva – A gomb megjelenése és funkciója is egy közlekedési lámpára hasonlít. Egy kattintással válthat a két pozíció között. A zöld szín az ***Engedélyezve*** értéket jelenti, vagyis hogy a Személyazonosság-védelem biztonsági szolgáltatás aktív és minden funkciója működik. A vörös szín a ***Letiltva*** állapotot jelzi, vagyis hogy a szolgáltatás ki van kapcsolva. Nyomatékosan javasoljuk, hogy ne módosítsa az alapértelmezett biztonsági beállításokat, hacsak nincs jó oka a szolgáltatás kikapcsolására. Az alapértelmezett beállítások garantálják az alkalmazás optimális teljesítményét és a maximális biztonságot. Ha valamiért ki szeretné kapcsolni a szolgáltatást, a rendszer egy vörös ***Figyelmeztetés*** jellel azonnal figyelmezteti a lehetséges kockázatokra, és tájékoztatja, hogy nem teljes körű a védelme. ***Ne feledje a lehető leghamarabb ismét aktiválni a szolgáltatást!***

Beállítások – A gombra kattintva a speciális beállítások felületre ugorhat. Megnyílik a megfelelő panel, és konfigurálhatja a kiválasztott szolgáltatást, vagyis a Személyazonosság-védelem összetevőt. A speciális beállítások felületen szerkesztheti az **AVG Internet Security 2013** programban valamennyi biztonsági szolgáltatásának összes konfigurációját, de a konfigurálás csak tapasztalt felhasználók számára ajánlott!

Részletek – A gombra kattintva a párbeszédpanel alján megjelenik a kiemelt szolgáltatás rövid leírása.

– A párbeszédpanel bal felső részén lévő zöld nyíllal térhet vissza az összetevők áttekintését tartalmazó fő felhasználói felületre.

Sajnos az **AVG Internet Security 2013** termék nem tartalmazza az Identity Alert szolgáltatást. Ha szeretné használni a védelemnek ezt a típusát, kattintson a ***Frissítés az aktiváláshoz*** gombra azon webhelyre történő ugráshoz, ahol megvásárolhatja az Identity Alert licencét.

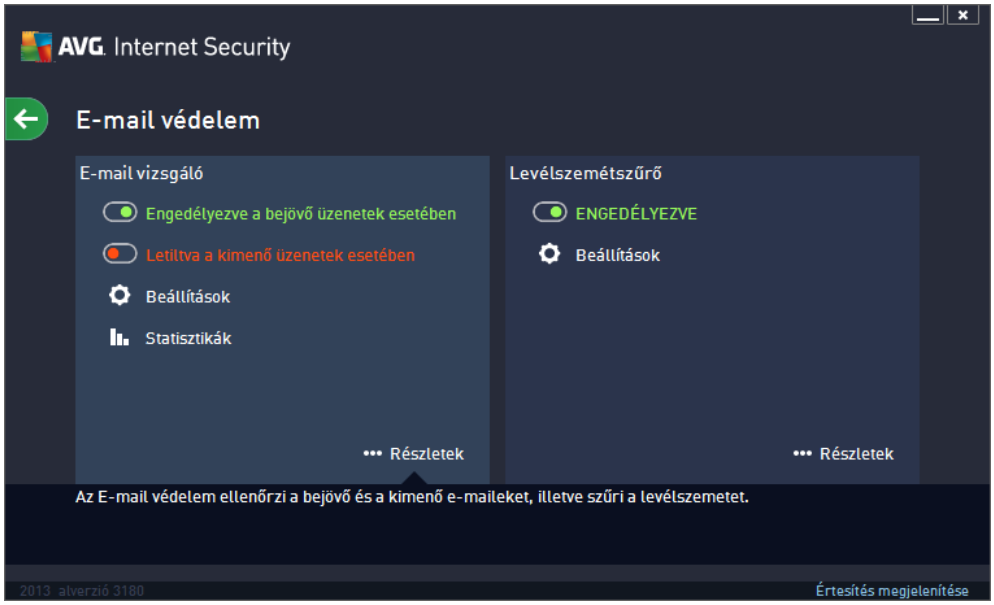
Felhívjuk figyelmét, hogy az Identity Alert szolgáltatás jelenleg még az AVG Premium Security kiadásai esetén is csak bizonyos régiókban (az Egyesült Államokban, az Egyesült Királyságban, Kanadában és Írországban) érhető el.

6.4. E-mailek

Az ***E-mail védelem*** összetevő a következő két biztonsági szolgáltatást tartalmazza: ***E-mail vizsgáló*** és ***Levélszemétszűrő***:

- ***E-mail vizsgáló***: A leggyakoribb vírusok és trójaiak e-mailen keresztül terjednek. Az adathalászatnak és a levélszemétnek köszönhetően az e-mailek egyre nagyobb kockázatot jelentenek. Az ingyenes e-mail postafiókokra nagyobb valószínűséggel érkezik kártékony email *(mivel azok ritkán használnak levélszemétszűrő technológiát)*, és az otthoni felhasználók gyakran megbíznak az ilyen e-mailekben. Az otthoni felhasználók nem megbízható webhelyeket is felkeresnek, és online adatlapokon adják meg személyes adataikat (*pl. e-mail címüket*). Ez szintén növeli az e-mailen keresztül történő támadás veszélyét. A vállalatok gyakran céges e-mail fiókokat használnak, és sokszor például levélszemétszűrőt alkalmaznak a kockázatok csökkentéséhez. Az E-mail védelem összetevő felelős az összes küldött vagy fogadott e-mail vizsgálatáért. Ha vírust észlel egy e-mailben, akkor azt azonnal a Karanténba helyezi. Az összetevő képes kiszűrni bizonyos típusú e-mail mellékleteket, és tanúsítási szöveget fűz hozzá a vírusmentes üzenetekhez. ***Az E-mail vizsgáló használata nem javasolt kiszolgálóplatformokon.***

- ***A Levélszemétszűrő*** ellenőrzi az összes bejövő e-mail üzenetet, és levélszemétként jelöli meg a kéretlen e-maileket *(A levélszemét általában azokat a kéretlen leveleket jelenti, amelyek valamilyen terméket vagy szolgáltatást reklámoznak. Ezeket nagy mennyiségben, egyszerre sok e-mail címre küldik el, megtöltve ezzel a postaládákat. A levélszemét nem vonatkozik a jogszerűen küldött kereskedelmi e-mailekre, amelyeket a felhasználó beleegyezésével küldenek.)*. A Levélszemétszűrő módosítani tudja az *(előtte levélszemétként azonosított)* e-mailek tárgyát úgy, hogy egy különleges szöveges karakterláncot fűz hozzá. Ezután egyszerűen szűrheti e-mailjeit a levelezőprogramban. A Levélszemétszűrő összetevő többféle elemzési módszerrel dolgozza fel az egyes e-maileket, így maximális védelmet nyújt a kéretlen üzenetek ellen. A Levélszemétszűrő rendszeresen frissített adatbázist használ a levélszemét észleléséhez. Használhat RBL-kiszolgálót *(ismert levélszemétküldők e-mail címeinek nyilvános adatbázisa)*, és manuálisan is hozzáadhatja az e-mail címeket az Engedélyezettek listájához *(soha nem levélszemét)* és a Feketelistához *(mindig levélszemét)*.



A párbeszédpanel vezérlői

A párbeszédpanel részei közötti váltáshoz csak kattintson a kívánt szolgáltatáspanel bármelyik részére. A panel ezután világoskék színnel kiemelve jelenik meg. A panel mindkét részén a következő vezérlők találhatók. A funkciójuk mindkét biztonsági szolgáltatás *(E-mail vizsgáló vagy Levélszemétszűrő)* esetén azonos:

Engedélyezve / Letiltva – A gomb megjelenése és funkciója is egy közlekedési lámpára hasonlít. Egy kattintással válthat a két pozíció között. A zöld szín az ***Engedélyezve*** értéket jelenti, vagyis hogy a biztonsági szolgáltatás aktív és minden funkciója működik. A vörös szín a ***Letiltva*** állapotot jelzi, vagyis hogy a szolgáltatás ki van kapcsolva. Nyomatékosan javasoljuk, hogy ne módosítsa az alapértelmezett biztonsági beállításokat, hacsak nincs jó oka a szolgáltatás kikapcsolására. Az alapértelmezett beállítások garantálják az alkalmazás optimális teljesítményét és a maximális biztonságot. Ha valamiért ki szeretné kapcsolni a szolgáltatást, a rendszer egy vörös ***Figyelmeztetés*** jellel azonnal figyelmezteti a lehetséges kockázatokra, és tájékoztatja, hogy nem teljes körű a védelme. ***Ne feledje a lehető leghamarabb ismét aktiválni a szolgáltatást!***

Az E-mail vizsgáló szakaszban látható két „közlekedési lámpa” gomb. Ennek segítségével külön adhatja meg, hogy az E-mail vizsgáló a bejövő, a kimenő vagy mindkét üzenettípust vizsgálja-e. Alapértelmezés szerint a vizsgálat be van kapcsolva a bejövő üzenetekhez és ki van kapcsolva a kimenő üzenetekhez, amelyeknél meglehetősen alacsony a fertőzés kockázata.

Beállítások – A gombra kattintva a speciális beállítások felületre ugorhat. Megnyílik a megfelelő panel, és konfigurálhatja a kiválasztott szolgáltatást, vagyis az E-mail vizsgáló vagy a Levélszemétszűrő összetevőt. A speciális beállítások felületen szerkesztheti az **AVG Internet Security 2013** programban valamennyi biztonsági szolgáltatásának összes konfigurációját, de a konfigurálás csak tapasztalt felhasználók számára ajánlott!

Statisztika – A gombra kattintva a rendszer átirányítja az AVG webhelyének (http://

www.avg.com/) megfelelő oldalára. Ezen az oldalon részletes statisztikai áttekintést talál az **AVG Internet Security 2013** a számítógépen egy adott időtartamon belül, valamint összességében végzett tevékenységeiről.

 ***Részletek*** – A gombra kattintva a párbeszédpanel alján megjelenik a kiemelt szolgáltatás rövid leírása.

 – A párbeszédpanel bal felső részén lévő zöld nyíllal térhet vissza az összetevők áttekintését tartalmazó fő felhasználói felületre.

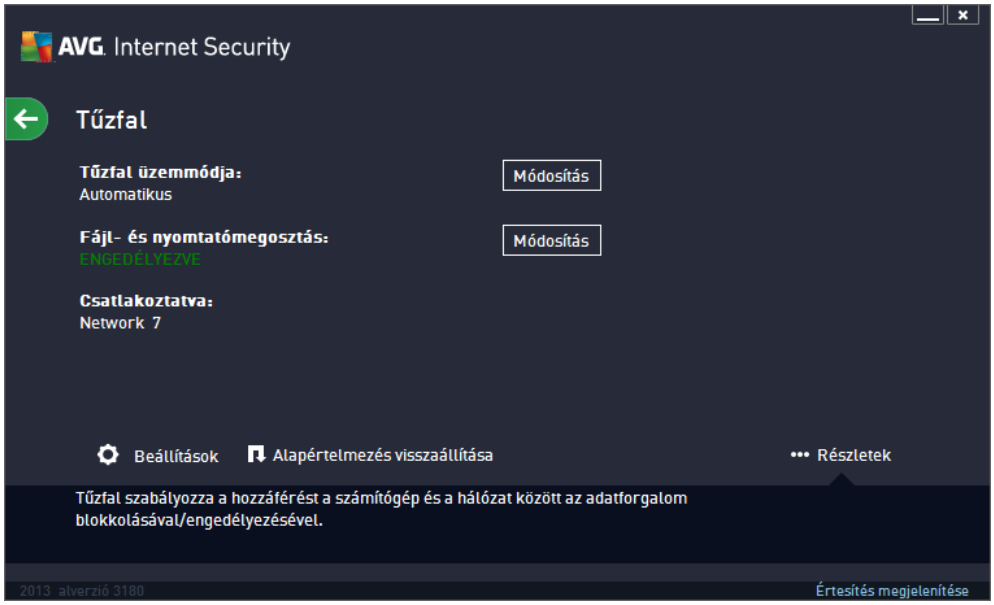
6.5. Tűzfal

A tűzfal olyan rendszer, amely a hálózati adatforgalom blokkolásával, illetve engedélyezésével érvényt szerez a beállított hozzáférés-vezérlési házirendeknek. A tűzfal szabályokat tartalmaz, amelyek védik a belső hálózatot a kívülről *(jellemzően az internetről)* érkező támadásokkal szemben, ezenkívül a tűzfal minden egyes hálózati porton figyeli a kommunikációt. Miután a tűzfal összevetette a kommunikációt a megadott szabályokkal, vagy engedélyezi, vagy blokkolja azt. Ha a tűzfal behatolási kísérletet észlel, akkor „blokkolja" azt, és nem engedi meg a behatolónak, hogy hozzáférjen a számítógéphez. A tűzfal úgy van konfigurálva, hogy engedélyezze vagy tiltsa a belső/ külső kommunikációt *(mindkét irányban)* a megadott portokon és alkalmazásoknál. Például a tűzfalat be lehet úgy állítani, hogy a bejövő és kimenő adatokat csak a Microsoft Explorerben engedélyezze. Ilyenkor más webböngészőkben az adatforgalom nem engedélyezett. megakadályozza, hogy személyes adatai az Ön engedélye nélkül hagyják el a számítógépet. A tűzfal azt is szabályozza, hogy a számítógép hogyan bonyolítsa le az adatcserét a helyi hálózaton vagy az interneten található más számítógépekkel. Egy szervezeten belül az egyes számítógépekre telepített tűzfal a szervezeten belül dolgozók által indított támadásokkal szemben is megvédi a számítógépeket.

Az **AVG Internet Security 2013** ***Tűzfal*** összetevője vezérli a számítógép egyes hálózati portjain keresztülhaladó összes adatforgalmat. A Tűzfal a megadott szabályok alapján elemzi azokat az alkalmazásokat, amelyek a számítógépen futnak *(és amelyek csatlakozni szeretnének az internethez vagy a helyi hálózathoz)*, továbbá azokat, amelyek kívülről próbálnak csatlakozni a számítógéphez. A Tűzfal ezután engedélyezi vagy megtiltja az egyes alkalmazásoknak a hálózati portokon való kommunikációt. Alapértelmezés szerint, ha az alkalmazás ismeretlen *(vagyis nem rendelkezik meghatározott Tűzfal szabállyal)*, akkor a Tűzfal rákérdez, hogy engedélyezze vagy letiltsa a kommunikációs próbálkozást.

Az AVG tűzfalának használata kiszolgálóplatformok védelmére nem javasolt.

Javaslat: *Általában nem ajánlott, hogy egynél több tűzfalat telepítsen a számítógépre. A számítógép biztonsága nem garantált, ha több tűzfalat használ egyszerre. Ugyanis elképzelhető, hogy a két alkalmazás ütközik egymással. Javasoljuk, hogy a számítógépen csak egyetlen tűzfalat használjon, és kapcsolja ki a többit, így csökkentheti egy esetleges szoftverütközés vagy abból adódó probléma kockázatát.*



A Tűzfal elérhető üzemmódjai

A Tűzfal lehetővé teszi, hogy meghatározzon bizonyos biztonsági szabályokat az alapján, hogy a számítógép egy tartományon belül helyezkedik el, különálló számítógép vagy notebook. E lehetőségek mindegyike más és más védelmi szintet kíván, és a szinteket a megfelelő üzemmódok fedik le. A Tűzfal üzemmód tehát a Tűzfal összetevő egy bizonyos konfigurációja, és számos előre meghatározott beállítást használhat.

- ***Automatikus*** – Ebben az üzemmódban a Tűzfal automatikusan kezeli az összes hálózati forgalmat. A program nem kéri, hogy döntéseket hozzon. A Tűzfal valamennyi ismert alkalmazás csatlakozásait engedélyezi, és egyidejűleg létrehoz egy szabályt az alkalmazáshoz, amely szerint az adott alkalmazás a későbbiekben mindig csatlakozhat. Más alkalmazások esetében a Tűzfal az alkalmazás viselkedése alapján dönti el, hogy engedélyezi vagy letiltja a csatlakozást. Ilyen esetben azonban nem jön létre a szabály, és a rendszer újra ellenőrzi az alkalmazást, amikor az kapcsolódni próbál. A legtöbb felhasználónak ez az automatikus, nem feltűnő mód ajánlott.

- ***Interaktív*** – ez a mód akkor hasznos, ha teljes mértékben irányítani kívánja a számítógépe összes bejövő és kimenő hálózati forgalmát. A Tűzfal megfigyeli a forgalmat, és értesíti az összes kommunikációs és adatátviteli kísérletről, így tetszőlegesen engedélyezheti vagy blokkolhatja a kísérleteket. Csak képzett felhasználónak javasolt.

- ***Az internet elérésének blokkolása*** – az internetkapcsolat teljesen le van tiltva, az internet nem érhető el, és semmilyen külső felhasználó nem fér hozzá a számítógépéhez. Csak speciális és rövid idejű használatra szolgál.

- ***Tűzfalas védelem kikapcsolása*** – a Tűzfal kikapcsolása engedélyezi a számítógép minden bejövő és kimenő hálózati forgalmát. Ez a beállítás ezért sebezhetővé teszi a rendszert a hackertámadásokkal szemben. Mindig gondolja át körültekintően a beállítás használatát.

Vegye figyelembe, hogy a Tűzfalon belül egy speciális automatikus mód is elérhető. Ez a háttérben

bekapcsol, ha vagy a Számítógép vagy az Személyazonosság-védelem összetevő ki van kapcsolva, és a számítógépe emiatt sebezhetőbb. A Tűzfal ilyen esetben csak az ismert és a teljesen biztonságos alkalmazásokat engedélyezi automatikusan. Minden egyéb esetben felhasználói döntést fog kérni. Ennek célja, hogy ellensúlyozza a letiltott védelmi összetevőket, és hogy biztosítsa számítógépe biztonságát.

A párbeszédpanel vezérlői

A párbeszédpanel áttekintést nyújt a Tűzfal összetevő állapotával kapcsolatos alapvető információkról:

- ***Tűzfal üzemmódja*** – A Tűzfal aktuálisan kiválasztott üzemmódjáról biztosít információt. Ha az aktuális üzemmódot egy másikra kívánja cserélni, az információk mellett található ***Módosítás*** gomb megnyomásával válthat a Tűzfalbeállítások felületre *(A Tűzfalprofilok használatával kapcsolatos leírásokért és javaslatokért lásd az előző bekezdést)*.

- ***Fájl- és nyomtatómegosztás*** – Tájékoztatja, hogy engedélyezett-e jelenleg a fájl- és nyomtatómegosztás *(mindkét irányba)*. A fájl- és nyomtatómegosztás valójában olyan fájlok vagy mappák megosztását jelenti, amelyeket „Megosztott” állapotúnak jelöl meg Windows rendszeren, közös lemezegységeken, nyomtatókon, szkennereken és minden hasonló eszközön. Az ilyen elemek megosztása csak biztonságosnak ítélt hálózatokon ajánlott *(például otthon, munkahelyen vagy az iskolában)*. Ha azonban nyilvános hálózathoz csatlakozik *(például repülőtéri Wi-Fi hálózathoz vagy internetkávézó hálózatához)*, célszerű, ha semmit nem oszt meg.

- ***Csatlakoztatva:*** – Megadja annak a hálózatnak a nevét, amelyhez jelenleg csatlakozik. Windows XP operációs rendszeren a hálózat neve az adott hálózathoz való első csatlakozáskor választott elnevezésnek felel meg. A Windows Vista és az újabb rendszerek automatikusan átveszik a hálózat nevét a Hálózati és megosztási központból.

A párbeszédpanel a következő vezérlőket tartalmazza:

Módosítás – A gomb használatával módosíthatja egy bizonyos paraméter állapotát. A módosítási folyamat részleteiért tekintse meg az adott paraméterek leírását a fenti bekezdésben.

Beállítások – A gombra kattintva a Tűzfalbeállítások felületre ugorhat, ahol szerkesztheti a Tűzfal teljes konfigurációját. Konfigurálást mindig hozzáértő felhasználó végezzen!

Alapértelmezés visszaállítása – a gomb megnyomásával felülírhatja a Tűzfal aktuális konfigurációját, illetve visszaállíthatja az automatikus észlelésen alapuló alapértelmezett konfigurációt.

Részletek – A gombra kattintva a párbeszédpanel alján megjelenik a kiemelt szolgáltatás rövid leírása.

– A párbeszédpanel bal felső részén lévő zöld nyíllal térhet vissza az összetevők áttekintését tartalmazó fő felhasználói felületre.

6.6. Gyors finomhangolás

A ***Gyors finomhangolás*** összetevő részletes rendszerelemzésre szolgáló eszköz, amely meghatározza, hogy miként javítható a számítógép sebessége és teljesítménye:

A következő hibakategóriák elemezhetők és javíthatók: beállításjegyzék hibái, a szükségtelen fájlok, töredezettség, hibás parancsikonok:

- ***A Beállításjegyzék-hibák*** rész megjeleníti a Windows beállításjegyzék hibáit, amelyek lassíthatják a rendszert, és hibaüzeneteket okozhatnak.
- ***A Szükségtelen fájlok*** rész megjeleníti a merevlemezen lévő feltehetően törölhető fájlok számát. Ezek jellemzően ideiglenes fájlok, valamint a Lomtár elemei.
- ***A Töredezettség*** funkció kiszámítja a merevlemez töredezettségének százalékos mértékét (a töredezettséget az okozza, hogy már sokat használta a merevlemezt, ezért a fájlok a fizikai lemezen több apró darabban, szétszórva helyezkednek el).
- ***A Hibás parancsikonok*** rész megjeleníti a nem működő, például nem létező helyekre mutató parancsikonokat.

A rendszer elemzésének indításához nyomja meg az ***Elemzés*** gombot. Ekkor figyelheti az elemzési folyamatot, majd az eredményeket megtekintheti a diagramon:

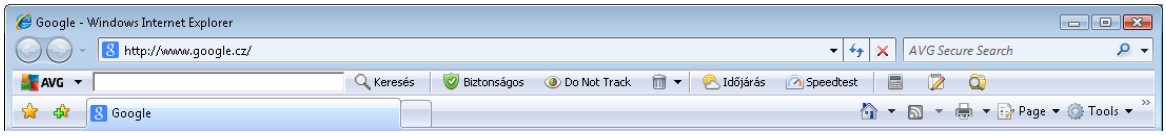
Az eredmények megjelenítik az észlelt rendszerhibák számát (***Hibák***) a vizsgált kategóriák szerint csoportosítva. Az eredmények grafikus formában is megjelennek a ***Súlyossági szint*** oszlopon.

Vezérlőgombok

- ***Elemzés*** (*az elemzés indítása előtt jelenik meg*) – kattintson erre a gombra a számítógép azonnali elemzésének indításához
- ***Javítás*** *(az elemzés után jelenik meg*) – kattintson erre a gombra az összes probléma javításához. A folyamat végén megtekintheti a javítási eredményeket.
- ***Mégse*** – Kattintson erre a gombra a folyamatban lévő elemzés leállításához, és az alapértelmezett AVG fő párbeszédpanelre (*összetevők áttekintése*) történő visszatéréshez az elemzés befejezése után

7. AVG Security Toolbar

Az AVG Security Toolbar egy olyan eszköz, amely szorosan együttműködik a LinkScanner Böngészésvédelem szolgáltatással, és maximális biztonságot garantál, miközben az interneten böngészik. Az **AVG Internet Security 2013** terméken belül az ***AVG Security Toolbar*** telepítése opcionális. A telepítési folyamat során kiválaszthatta, hogy mely összetevők legyenek telepítve. ***Az AVG Security Toolbar*** közvetlenül elérhető a webböngészőből. Jelenleg a támogatott internetböngészők a következők: Internet Explorer (*6.0 vagy újabb verziók*) és/vagy Mozilla Firefox (*3.0 vagy újabb verziók*). A többi böngésző nem támogatott *(ha más böngészőt használ, például az Avant böngészőt, akkor a program nem várt módon viselkedhet).*



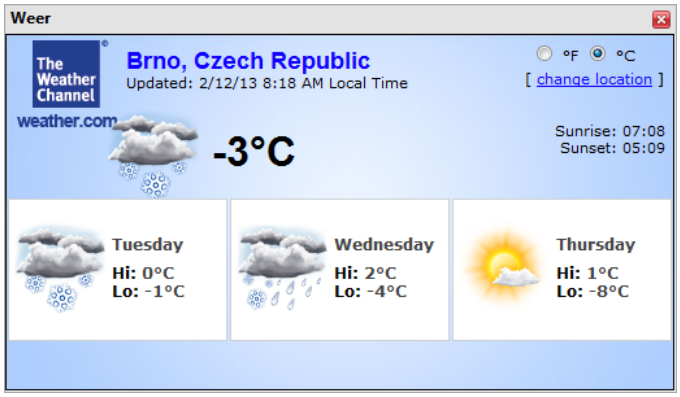
Az AVG Security Toolbar az alábbi elemeket tartalmazza:

- ***Az AVG embléma*** a legördülő menüvel:
    - ***Aktuális fenyegetettségi szint*** – megnyitja a víruslabor weboldalát, ahol grafikus formában ellenőrizheti az aktuális fenyegetettségi szintet az interneten.
    - ***AVG Víruslabor*** – Megnyitja az adott ***AVG Víruslabor*** webhelyet *(a http://www.avgthreatlabs.com címen)*, ahol online információt találhat a különböző webhelyek biztonságáról és az aktuális fenyegetési szintről.
    - ***Toolbar súgó*** – Egy online súgót nyit meg, amely az ***AVG Security Toolbar*** összes funkcióját tartalmazza.
    - ***Visszajelzés küldése a termékről*** – Egy weboldal nyílik meg egy űrlappal, amelyet kitölthet és elmondhatja véleményét az ***AVG Security Toolbar*** eszközről.
    - ***AVG Security Toolbar eltávolítása*** – Megnyit egy weboldalt, amely részletesen ismerteti az ***AVG Security Toolbar*** kikapcsolását minden támogatott webböngészőben.
    - ***Névjegy...*** – Egy új, a jelenleg telepített ***AVG Security Toolbar*** verzióval kapcsolatos adatokat tartalmazó ablakot nyit meg.
- ***Keresési mező*** – Keressen az interneten az ***AVG Security Toolbar*** segítségével, hogy teljesen biztonságban és kényelemben tudhassa magát a 100 százalékban biztonságos keresési eredményeknek köszönhetően. Írja be a kulcsszót vagy a kívánt kifejezést a keresőmezőbe, és kattintson a ***Keresés*** gombra *(vagy nyomja le az Enter billentyűt)*.
- ***Webhelybiztonság*** – Ez a gomb megnyit egy párbeszédpanelt, amely az éppen meglátogatott oldal aktuális fenyegetési szintjéről (*Jelenleg biztonságos*) biztosít információkat. Ez a rövid összefoglaló kibővítve is megjeleníthető a böngészőablak jobb oldalán található oldalhoz kapcsolódó összes biztonsági tevékenység minden részletével együtt (*Teljes jelentés megtekintése*):

- ***Do Not Track*** – a DNT szolgáltatás segítséget nyújt azon webhelyek azonosításában, amelyek online tevékenységeiről gyűjtenek adatokat, és lehetővé teszi ezen tevékenység engedélyezését vagy tiltását. Részletek >>

- ***Törlés*** – a „kuka” gombbal egy legördülő menü érhető el, amelyben kiválaszthatja, hogy a böngészés, a letöltések vagy az online űrlapok adatait szeretné törölni, vagy egyszerre az összes keresési előzményt.

- ***Időjárás*** – Ezzel a gombbal egy új párbeszédpanelt nyit meg, amely a földrajzi helyének megfelelő aktuális időjárásról nyújt információt, valamint megjeleníti a következő két napra vonatkozó előrejelzést. Ez az információ rendszeresen, 3-6 óránként frissül. A párbeszédpanelen manuálisan módosíthatja a kívánt helyszínt, és kiválaszthatja, hogy a hőmérsékletet Celsius vagy Fahrenheit fokban szeretné látni.



- ***Facebook*** – Ezzel a gombbal a Facebook közösségi hálózathoz csatlakozhat közvetlenül az ***AVG Security Toolbarból***.

- ***Sebességteszt*** – Ez a gomb egy olyan online alkalmazáshoz irányítja át, amely segíthet az internetkapcsolat minőségének *(ping),* illetve a le- és feltöltési sebességének ellenőrzésében.

- Gyorsgombok az alábbi alkalmazások gyors eléréséhez: ***Számológép***, ***Jegyzettömb***, ***Windows Intéző***.

8. AVG Do Not Track

Az AVG Do Not Track követéstiltás segítséget nyújt azon webhelyek azonosításában, amelyek online tevékenységeiről gyűjtenek adatokat. Az ***AVG Do Not Track*** (az AVG Security Toolbar egy része) jelzi, ha egy webhely vagy hirdető adatot gyűjt a tevékenységéről, valamint lehetőséget biztosít arra, hogy ezt engedélyezze vagy letiltsa.

- ***Az AVG Do Not Track*** követéstiltás továbbá információkat nyújt az adott szolgáltatások adatvédelmi szabályzatáról, valamint, ha elérhető ilyen, közvetlen hivatkozást biztosít a szolgáltatásról való leiratkozáshoz.
- Ezenkívül az ***AVG Do Not Track*** támogatja a W3C DNT protokollt azon oldalak automatikus értesítéséhez, amelyek esetében nem szeretné, ha nyomon követnék tevékenységét. Az értesítés alapértelmezés szerint engedélyezett, de ennek módosítására bármikor lehetőség van.
- ***Az AVG Do Not Track*** követéstiltás használata az alábbi feltételek elfogadása mellett biztosított.
- ***Az AVG Do Not Track*** alapértelmezés szerint engedélyezett, de bármikor egyszerűen letiltható. Erről útmutatást talál az AVG Do Not Track szolgáltatás letiltása című gyakori kérdések cikkben.
- Az ***AVG Do Not Track*** követéstiltásról további információt talál a webhelyünkön.

Jelenleg az ***AVG Do Not Track*** követéstiltás szolgáltatás működése a Mozilla Firefox, a Chrome és az Internet Explorer böngészőkben támogatott.

8.1. AVG Do Not Track felülete

Az internet használata közben az ***AVG Do Not Track*** követéstiltás figyelmezteti, amint bármilyen adatgyűjtési tevékenységet észlel. Ebben az esetben megváltozik az AVG Security Toolbar eszköztáron található ***AVG Do Not Track*** ikon kinézete. Az ikonon megjelenő apró szám mutatja az azonosított adatgyűjtési szolgáltatások számát:  Az ikonra kattintva a következő párbeszédpanel jelenik meg:

Az összes észlelt adatgyűjtési szolgáltatás fel van sorolva a ***Nyomkövetők ezen az oldalon*** áttekintésében. Az ***AVG Do Not Track*** három típusú adatgyűjtési tevékenységet ismer fel:

- ***Web Analytics (Webes elemzés)*** *(alapértelmezés szerint engedélyezett):* Ezen szolgáltatások az adott webhely teljesítményének és élményének növelésére szolgálnak. Ebben a kategóriában olyan szolgáltatások találhatók, mint például a Google Analytics, az Omniture vagy a Yahoo Analytics. Nem javasolt a webes elemzési szolgáltatások blokkolása, mivel az akadályozhatja a webhely működését is.

- ***Ad Networks (hirdetési hálózatok)*** *(némelyik alapértelmezés szerint blokkolt):* Olyan szolgáltatások, amelyek az online tevékenységéről közvetve vagy közvetlenül adatokat gyűjtenek vagy osztanak meg több webhelyen, hogy személyre szabott hirdetéseket biztosítsanak a tartalomalapú hirdetések helyett. A működésüket az egyes hirdetési hálózatok webhelyén elhelyezett adatvédelmi nyilatkozat határozza meg. Némely hirdetési hálózat alapértelmezés szerint blokkolva van.

- ***Social Buttons (Közösségi hálózatok gombjai)*** *(alapértelmezés szerint engedélyezett):* A közösségi hálózatok által nyújtott élmény növelésére szolgáló elemek. A közösségi hálózatok gombjait a közösségi hálózatok biztosítják a látogatott oldalakon. Az online tevékenységéről gyűjtenek adatokat mialatt be van jelentkezve azokra. A közösségi gombok közé tartoznak például a Facebook közösségi bővítmények, a Twitter gomb vagy a Google +1.

Megjegyzés: *Attól függően, hogy a webhely hátterében milyen szolgáltatások futnak, előfordulhat, hogy nem jelenik meg az előző három rész mindegyike az AVG Do Not Track párbeszédpanelen.*

A párbeszédpanel vezérlői

- ***Mi az a nyomkövetés?*** – Kattintson erre a hivatkozásra a párbeszédpanel felső részében, hogy eljusson egy olyan webhelyre, amely a nyomkövetési alapelvek részletes információit és az egyes nyomkövetési típusok leírását tartalmazza.

- ***Az összes letiltása*** – Kattintson a párbeszédpanel alsó részében található gombra, ha egyáltalán nem kívánja engedélyezni az adatgyűjtési tevékenységeket *(részleteket a Nyomkövetési folyamatok blokkolása című fejezetben talál).*

- ***Do Not Track beállításai*** – Kattintson erre a gombra a párbeszédpanel alsó részében, ha szeretne eljutni egy olyan webhelyre, ahol megadhatja a különböző ***AVG Do Not Track*** paraméterek beállításait *(további részletes információt az AVG Do Not Track beállításai című fejezetben talál)*

8.2. Információk a nyomkövetési folyamatokról

Az azonosított adatgyűjtési szolgáltatások listája csak az adott szolgáltatás nevét tartalmazza. Ahhoz, hogy megfontolt döntést hozzon azzal kapcsolatban, hogy egy adott szolgáltatás blokkolt vagy engedélyezett legyen, több információra is szüksége lehet. Vigye az egeret az adott listaelem fölé. Megjelenik egy információs buborék, amely részletes adatokat tartalmaz a szolgáltatásról. Ebből megtudhatja, hogy a szolgáltatás a személyes adatait is gyűjti, vagy csak egyéb elérhető adatokat. Valamint azt is, hogy azokat megosztják-e harmadik féllel, illetve tárolják-e azokat esetleges későbbi használat céljából:

Az információs buborék alsó részében található az ***Adatvédelmi nyilatkozat*** hivatkozása, amely átirányítja egy olyan webhelyre, ahol megtalálhatja az adott észlelt szolgáltatás adatvédelmi nyilatkozatát.

8.3. Nyomkövetési folyamatok blokkolása

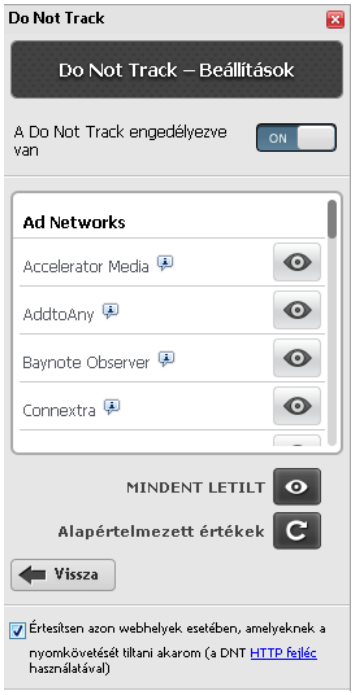
Az Ad Networks/Social Buttons/Web Analytics teljes listáival meghatározhatja, hogy mely szolgáltatásokat kívánja blokkolni. Két módszer közül választhat:

- ***Minden letiltása*** – Kattintson erre, a párbeszédpanel alsó részében található gombra, ha egyáltalán nem kívánja engedélyezni az adatgyűjtési tevékenységeket. *(Viszont azt vegye figyelembe, hogy ezzel a művelettel akadályozhatja a szolgáltatást futtató weboldal működését.)*

-  – Amennyiben nem akarja egyszerre letiltani az összes észlelt szolgáltatást, akkor egyenként is megadhatja, hogy az adott szolgáltatás engedélyezett vagy blokkolt legyen. Engedélyezheti néhány észlelt rendszer futását *(például a webes elemzéseket):* ezek a rendszerek az összegyűjtött adatokat a saját webhelyük optimalizálására használják, és ezzel segítik az internetes környezet fejlesztését az összes felhasználó számára. Ugyanakkor blokkolhatja az összes hirdetési hálózatként azonosított folyamat adatgyűjtési tevékenységét. Csak kattintson az  ikonra az adott szolgáltatás mellett az adatgyűjtés blokkolásához *(ekkor a folyamat neve áthúzva jelenik meg)*, illetve az adatgyűjtés újbóli engedélyezéséhez.

8.4. AVG Do Not Track beállításai

A ***Do Not Track beállításai*** párbeszédpanelen a következő beállítási lehetőségek érhetőek el:



- ***A Do Not Track engedélyezve van*** – A DNT szolgáltatás alapértelmezés szerint aktív *(BE van kapcsolva)*. A szolgáltatás letiltásához állítsa a kapcsolót KI helyzetbe.

- A párbeszédpanel középső részén egy mezőt lát az összes ismert hirdetési hálózatként azonosított adatgyűjtési szolgáltatás nevével. Alapértelmezés szerint a ***Do Not Track***

automatikusan blokkol néhány hirdetési hálózatot, a többiről pedig eldöntheti, hogy azokat is letiltja, vagy meghagyja engedélyezettnek. Ahhoz, hogy ezt megtegye, kattintson a lista alatt található ***Az összes letiltása*** gombra. Vagy az ***Alapértelmezett*** gombbal visszavonhatja a beállítások összes elvégzett módosítását, és visszatérhet az eredeti beállításhoz.

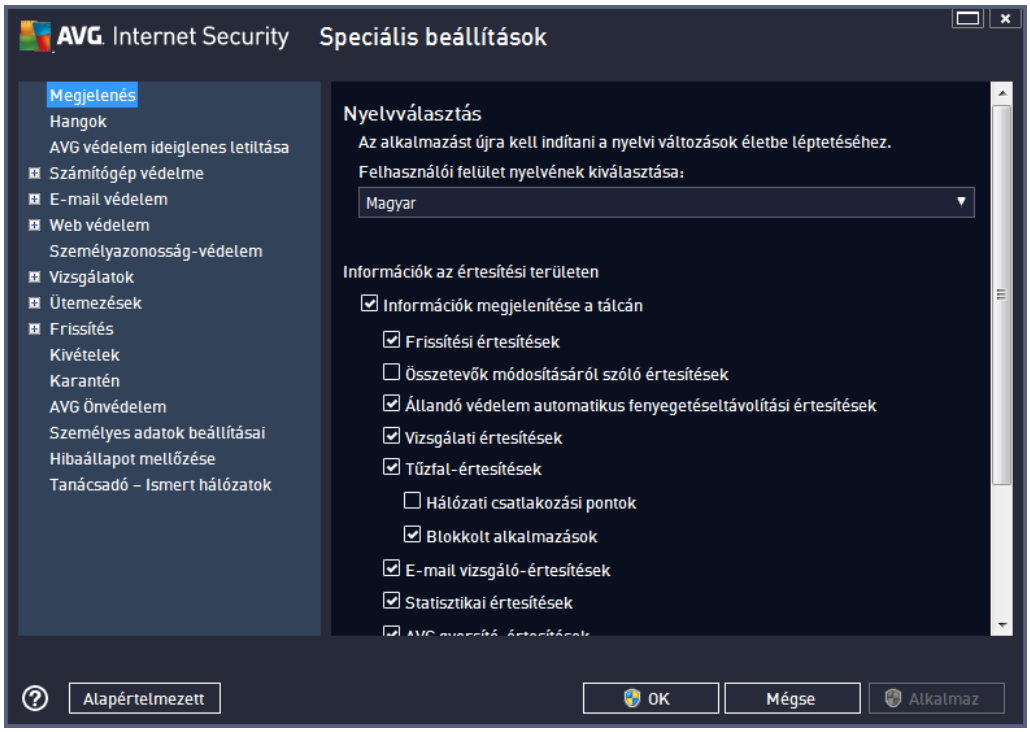
- ***Webhelyek értesítése...*** – Ebben a szakaszban kapcsolható ki és be az ***Azon webhelyek értesítése, amelyek nyomkövetését tiltani akarom*** lehetőség *(alapértelmezés szerint be van kapcsolva).* Hagyja ezt a jelölőnégyzetet bejelölve, ha azt szeretné, hogy a ***Do Not Track*** tájékoztassa az észlelt adatgyűjtési szolgáltatásokat arról, hogy nem szeretné, hogy kövessék.

9. AVG speciális beállítások

Az **AVG Internet Security 2013** egy új ablakot nyit meg ***Speciális AVG beállítások*** néven. Az ablak két részre van osztva: a bal oldali rész fastruktúrába osztott navigációt tesz lehetővé a program beállítási lehetőségei között. Válassza ki a módosítandó összetevőt (*vagy adott részét*), ekkor megnyílik az adott elemhez tartozó szerkesztőablak a jobb oldalon.

9.1. Megjelenés

A navigációs fa első eleme a ***Megjelenés***. Ez az **AVG Internet Security 2013** felhasználói felület általános beállításainak, valamint az alkalmazás viselkedését befolyásoló néhány alapvető beállításnak a megadását teszi lehetővé:



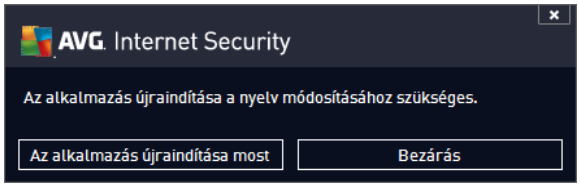
Nyelvválasztás

A ***Nyelvválasztás*** területen választható ki a használni kívánt nyelv egy legördülő menüből. Az itt kiválasztott nyelvet fogja használni az egész **AVG Internet Security 2013** felhasználói felület. A legördülő menüben csak a telepítési folyamat során kiválasztott nyelvek és az angol jelennek meg (*az angol nyelvet alapértelmezés szerint mindig automatikusan telepíti a program*). Az **AVG Internet Security 2013** szoftvert újra kell indítani a nyelválasztás érvényesítéséhez. Kövesse az alábbi lépéseket:

- A legördülő menüben válassza ki az alkalmazásban használni kívánt nyelvet
- A választás megerősítéséhez kattintson az ***Alkalmaz*** gombra *(a párbeszédpanel jobb alsó sarkában)*
- Kattintson az ***OK*** gombra a megerősítéshez

- Egy új párbeszédablak ugrik elő, ami tájékoztatja, hogy a nyelválasztás érvényesítéséhez újra kell indítania az **AVG Internet Security 2013**

- Kattintson ***Az alkalmazás újraindítása most*** gombra a program újraindításának engedélyezéséhez, és várja meg, amíg életbe lép a nyelváltás:

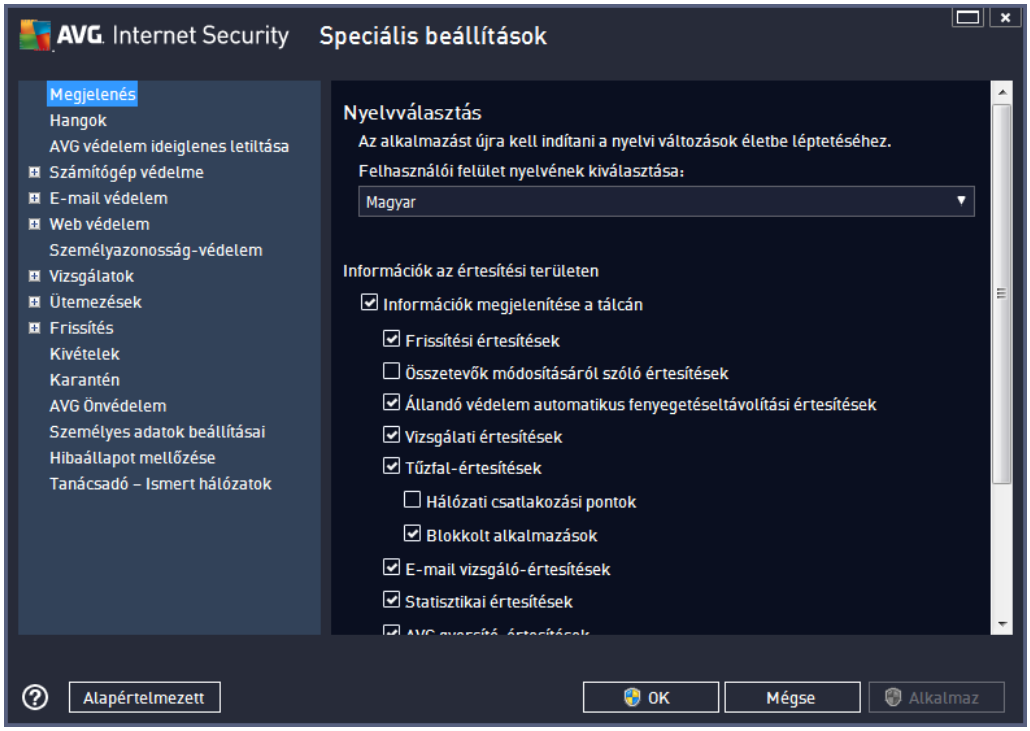


Információk az értesítési területen

Ezen a területen letilthatja az **AVG Internet Security 2013** alkalmazás állapotával kapcsolatos, a tálcán megjelenő értesítéseket. Alapértelmezés szerint a rendszerértesítések megjelenítése engedélyezett. Javasoljuk, hogy ne változtasson ezen a beállításon. Rendszerértesítések tájékoztatnak például a vizsgálati vagy frissítési folyamat indulásáról, valamint az **AVG Internet Security 2013** összetevőinek állapotváltozásáról. Ezeknek a figyelmeztetéseknek szenteljen komoly figyelmet.

Ha valamilyen okból úgy dönt, hogy nem szeretné ezeket az értesítéseket megjeleníteni, vagy csak néhányat kapcsolna be közülük *(például csak egyes AVG Internet Security 2013 összetevőkkel kapcsolatos értesítésekre kíváncsi)*, akkor ezt a következő jelölőnégyzetek bejelölésével vagy jelölésük törlésével teheti meg:

- ***Információk megjelenítése a tálcán*** *(alapértelmezés szerint bekapcsolva)* – Alapértelmezés szerint az összes értesítés megjelenik. Törölje az elem jelölését, ha minden rendszerértesítés megjelenítését ki kívánja kapcsolni. Ha be van kapcsolva, akkor kiválaszthatja, hogy milyen értesítések jelenjenek meg:



- ***Frissítési* értesítések** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy az **AVG Internet Security 2013** frissítés indításával, magával a folyamattal, illetve a befejezéssel kapcsolatban jelenjenek-e meg értesítések.

- ***Összetevők változásával kapcsolatos értesítések*** *(alapértelmezés szerint kikapcsolva)* – meghatározza, hogy az összetevők be- és kikapcsolásával, vagy a lehetséges problémákkal kapcsolatban jelenjenek-e meg értesítések. Az összetevők hibaállapotának jelentésekor ez a beállítás egyenértékű a tálcaikon **AVG Internet Security 2013** összetevőkre vonatkozó hibajelzésével.

- ***Az Állandó védelem automatikus fenyegetéseltávolítási értesítései*** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy a fájlok mentésével, másolásával, illetve folyamatok megnyitásával kapcsolatban jelenjenek-e meg értesítések (*ez a beállítás csak akkor működik, ha az Állandó védelem automatikus javítási szolgáltatása be van kapcsolva*).

- ***Vizsgálati* értesítések** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy az ütemezett vizsgálat indításával, magával a folyamattal, illetve az eredményekkel kapcsolatban jelenjenek-e meg értesítések.

- ***Tűzfalértesítések*** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy a Tűzfal állapotával és folyamataival kapcsolatos értesítések, például az összetevő be- és kikapcsolásával kapcsolatos figyelmeztetések, adatforgalom esetleges blokkolása stb. megjelenjenek-e vagy sem. Ez az elem további két specifikusabb kiválasztási beállítást kínál *(ezek részletes leírását ezen dokumentum Tűzfal című fejezetében találja)*:

  - ***Hálózati csatlakozási pontok*** *(alapértelmezés szerint kikapcsolva)* – hálózathoz történő csatlakozás során a Tűzfal tájékoztatja a felhasználót, hogy ismeri-e a

hálózatot, valamint milyen beállítások vonatkoznak a fájl- és nyomtatómegosztásra.

- ***Blokkolt alkalmazások*** *(alapértelmezés szerint kikapcsolva)* – ha ismeretlen vagy gyanús alkalmazás próbál csatlakozni a hálózathoz, a Tűzfal blokkolja a kísérletet, és értesítést jelenít meg. Ez azért hasznos, mert folyamatosan értesíti a felhasználót, ezért ajánlott a szolgáltatást bekapcsolva hagyni.

- ***Az E-mail vizsgáló*** ***értesítései*** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy megjelenjenek-e értesítések a bejövő és kimenő e-mailek vizsgálatakor.

- ***Statisztikai értesítések*** *(alapértelmezés szerint bekapcsolva)* – jelölje be, ha rendszeresen meg kíván jeleníteni statisztikai értesítéseket a tálcán.

- ***AVG gyorsító értesítései*** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy megjelenjenek-e az ***AVG gyorsító*** tevékenységeivel kapcsolatos értesítések. Az ***AVG gyorsító*** szolgáltatás gördülékenyebbé teszi az online videolejátszást, és megkönnyíti a további letöltéseket.

- ***A rendszerindítás gyorsításával kapcsolatos üzenetek*** *(alapértelmezés szerint kikapcsolva)* – meghatározza, hogy kapjon-e értesítéseket a számítógép rendszerindításának felgyorsulásáról.

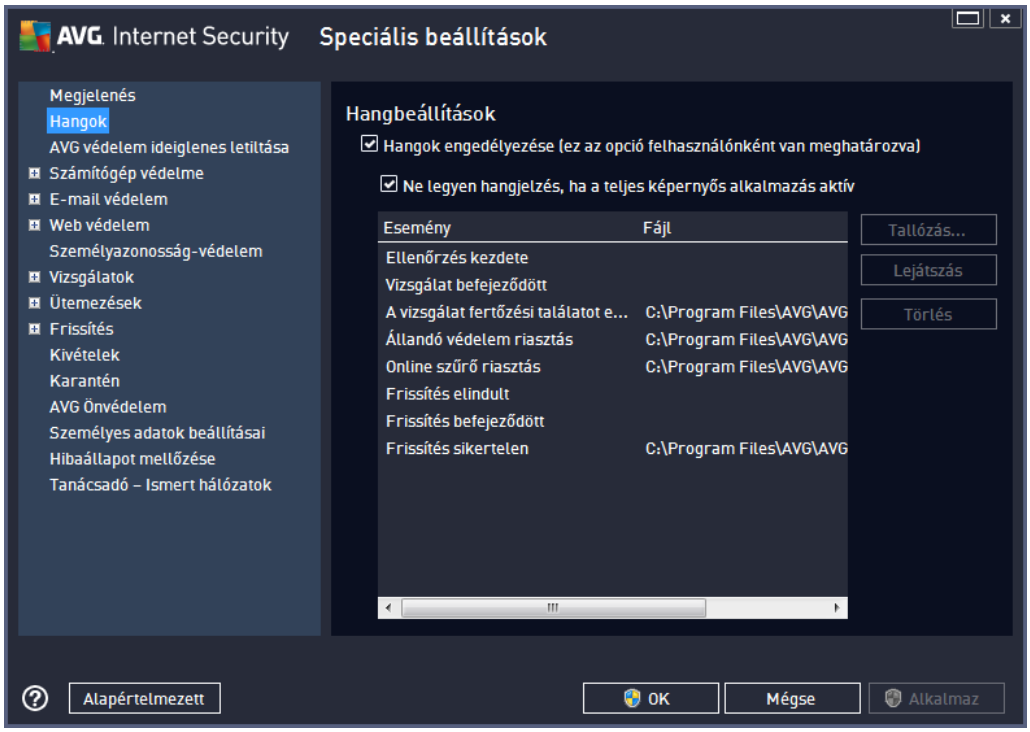
- ***Az AVG tanácsadó értesítései*** *(alapértelmezés szerint bekapcsolva)* – meghatározza, hogy az AVG tanácsadó tevékenységeivel kapcsolatos értesítések megjelenjenek-e a tálcán.

Játék mód

Az AVG ezen szolgáltatása olyan teljes képernyős alkalmazásokra lett kifejlesztve, amelyeknél az AVG által esetlegesen megjelenített üzenet (*pl. ha egy ütemezett vizsgálat elindul*) zavaró lehet (*kis méretűre állíthatják az alkalmazást, és ronthatják a grafikus megjelenítést*). Ezen probléma elkerülése érdekében jelölje be a ***Játékmód engedélyezése teljes képernyős alkalmazások futtatásakor*** opciót (*alapértelmezett beállítás*).

9.2. Hangok

A ***Hangok*** párbeszédpanelen beállíthatja, hogy szeretne-e hangokat hozzárendelni bizonyos **AVG Internet Security 2013** műveletekhez:



A beállítások csak az aktuális felhasználói fiókra vonatkoznak, vagyis a számítógép minden egyes felhasználója külön hangbeállításokat adhat meg. Ha engedélyezni kívánja a hangjelzéseket, hagyja bejelölve a ***Hangjelzések engedélyezése*** beállítást (*a beállítás alapértelmezés szerint be van kapcsolva*), így aktív marad az összes vonatkozó műveletet tartalmazó lista. Ezenkívül érdemes lehet bejelölni a ***Ne legyen hangjelzés, ha a teljes képernyős alkalmazás aktív*** lehetőséget, amellyel letilthatja a hangjelzéseket olyan esetekben, amikor azok zavaróak lehetnek *(részleteket a dokumentum Speciális beállítások/Megjelenés fejezetének Játék mód szakaszában talál)*.

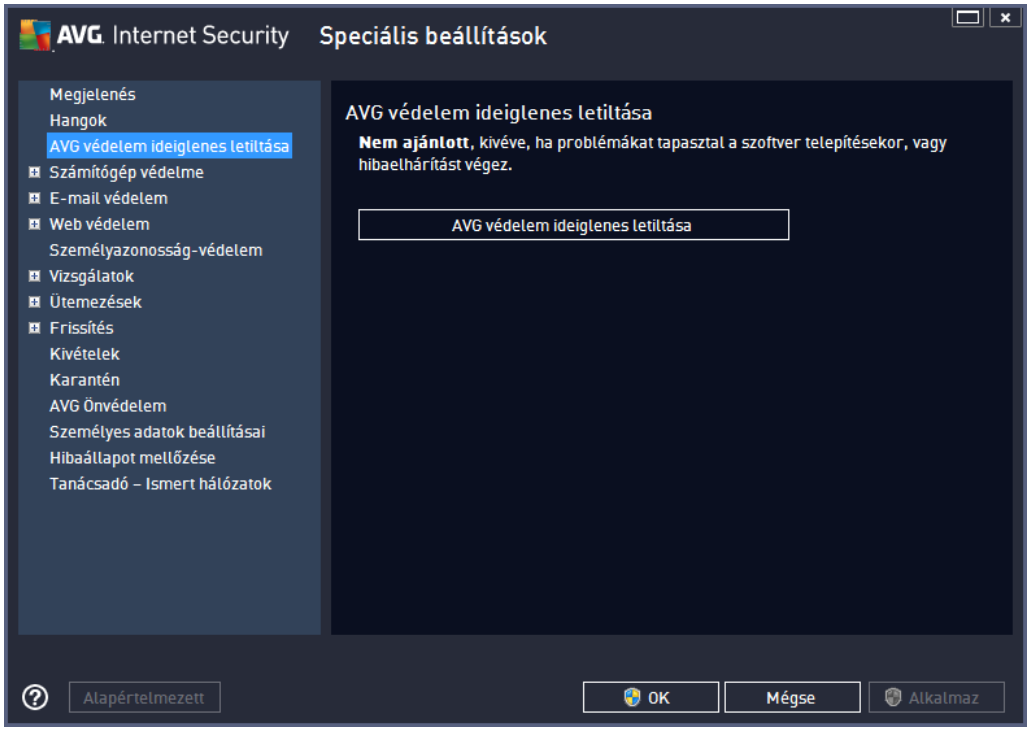
Vezérlőgombok

- ***Tallózás*** – miután kiválasztotta a megfelelő eseményt a listából, a ***Tallózás*** gombra kattintva megkeresheti a számítógépen az eseményhez rendelni kívánt hangfájlt. *(Vegye figyelembe, hogy jelenleg kizárólag a *.wav formátumú fájlok támogatottak.)*
- ***Lejátszás*** – a kiválasztott hang meghallgatásához jelölje ki az eseményt a listán, majd kattintson a ***Lejátszás*** gombra.
- ***Törlés*** – a ***Törlés*** gombbal törölhet egy adott eseményhez társított hangot.

9.3. Az AVG védelem ideiglenes letiltása

Az ***AVG védelem ideiglenes letiltása*** panel lehetővé teszi az **AVG Internet Security 2013** teljes védelmének kikapcsolását.

Ne feledje: ezt a beállítást csak akkor használja, ha feltétlenül szükséges.

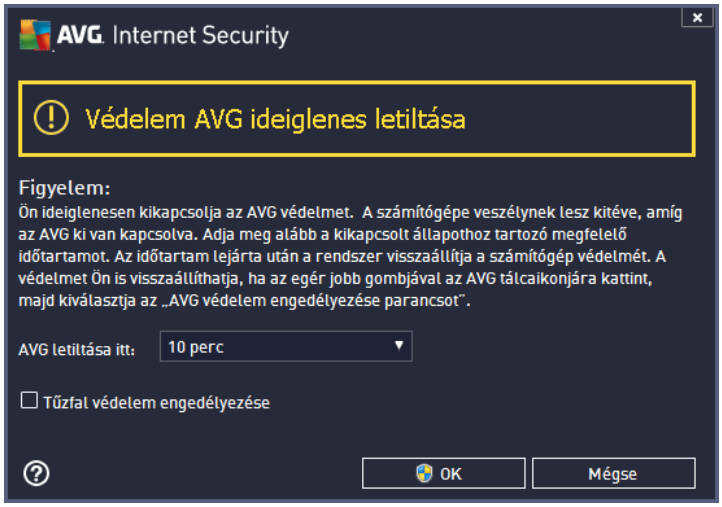


A legtöbb esetben ***nem szükséges*** kikapcsolni az **AVG Internet Security 2013** védelmet új szoftver vagy illesztőprogram telepítése előtt, még akkor sem, ha a telepítő vagy a varázsló javasolja a futó programok és alkalmazások bezárását a telepítési folyamat zavartalansága érdekében. Ha problémákat észlel a telepítések során, akkor először kapcsolja ki az állandó védelmet (*Állandó védelem engedélyezése*). Ha ideiglenesen ki kell kapcsolnia az **AVG Internet Security 2013** védelmet, akkor mielőbb kapcsolja azt vissza. Ha kikapcsolt víruskereső szoftverrel csatlakozik az internethez vagy egy hálózathoz, akkor a számítógépe védtelen a támadásokkal szemben.

Az AVG védelem letiltása

Jelölje be az ***AVG védelem ideiglenes letiltása*** jelölőnégyzetet, és erősítse meg a választást az ***Alkalmaz*** gombra kattintva. A megnyíló ***Az AVG védelem ideiglenes letiltása*** párbeszédpanelen adja meg, mennyi időre kívánja letiltani az **AVG Internet Security 2013** programot. Alapértelmezés szerint a védelem 10 percig lesz kikapcsolva. Ez elegendő idő általános feladatok (például új szoftver telepítése) végrehajtásához. Meghatározhat hosszabb időt, de nem javasoljuk ezt az opciót, hacsak nem feltétlenül szükséges. Ezt követően az összes kikapcsolt összetevő automatikusan újra aktiválódik. Végső esetben, az AVG védelmet a számítógép következő újraindításáig is letilthatja. Egy külön opció érhető el a ***Tűzfal*** összetevő kikapcsolására az ***AVG védelem ideiglenes letiltása*** párbeszédpanelen. Jelölje be a ***Tűzfal védelem letiltása*** jelölőnégyzetet a

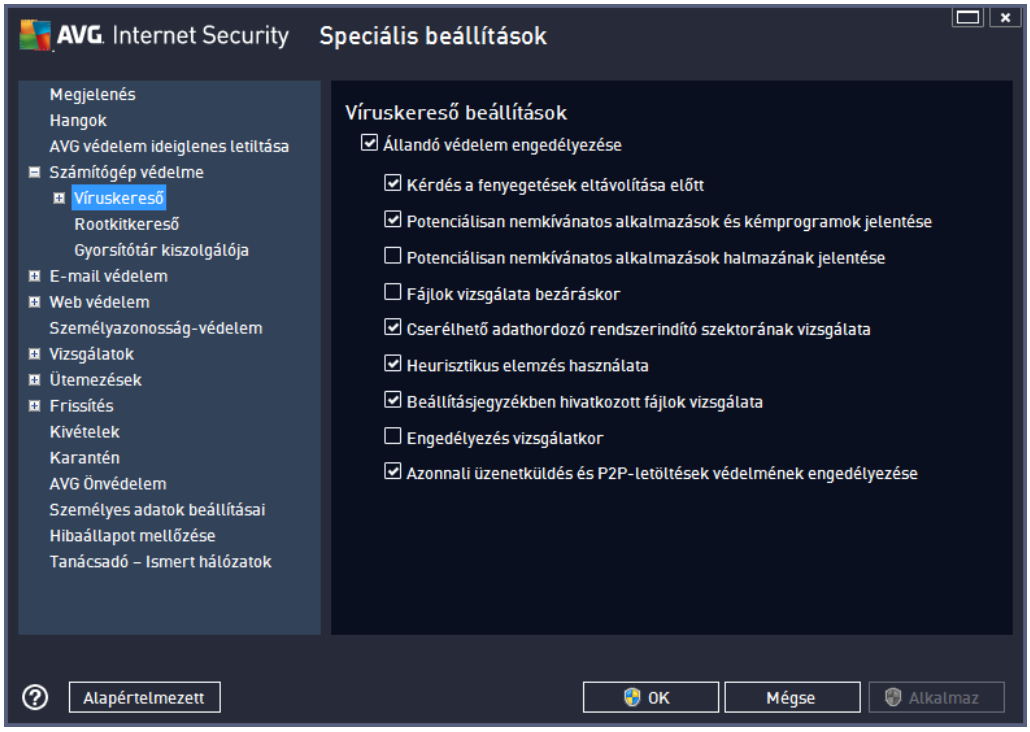
kikapcsolásához.



9.4. Számítógép védelme

9.4.1. Víruskereső

A Víruskereső az ***Állandó védelemmel*** együtt folyamatosan védi a számítógépet az ismert vírusoktól és kémprogramoktól, valamint általában a kártevőktől *(beleértve az úgynevezett alvó és nem aktív kártevőket, amelyek már letöltődtek, de még nem aktiválódtak)*.



Az ***Állandó védelem beállítások*** párbeszédpanelen be- és kikapcsolhatja az állandó védelem funkciót az ***Állandó védelem engedélyezése*** elem segítségével (*alapértelmezés szerint be van kapcsolva*). Kiválaszthatja továbbá, hogy az állandó védelem mely funkciói legyenek aktiválva:

- ***Kérdés a fenyegetések eltávolítása előtt*** (*alapértelmezés szerint bekapcsolva*) – jelölje be ezt annak érdekében, hogy az Állandó védelem ne végezzen el semmit sem automatikusan, hanem megjelenítsen egy párbeszédpanelt, amely a felfedezett fenyegetést írja le, és lehetővé teszi, hogy a teendőkről döntsön. Ha nem jelöli be ezt a lehetőséget, az **AVG Internet Security 2013** automatikusan kijavítja a fertőzést, ha pedig ez nem lehetséges, áthelyezi az objektumot a Karanténba.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** (*alapértelmezés szerint bekapcsolva*) – jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek, és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*) – Jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: ezek olyan programok, amelyek a gyártótól közvetlenül beszerezve ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát, azonban a szolgáltatás legitim programokat is letilthat, ezért a funkció alapértelmezés szerint ki van kapcsolva.

- ***Fájlok vizsgálata bezáráskor*** (*alapértelmezés szerint kikapcsolva*) – A program bezáráskor történő vizsgálatakor az AVG vizsgálja az aktív objektumokat (például alkalmazásokat, dokumentumokat) megnyitáskor és bezáráskor, így védelmet biztosít kifinomultabb vírusokkal szemben is.

- ***Cserélhető adathordozó rendszerindító szektorának vizsgálata*** (*alapértelmezés szerint bekapcsolva*)

- ***Heurisztikus elemzés használata*** (*alapértelmezés szerint bekapcsolva*) – A program heurisztikus elemzést használ a vizsgálat során, vagyis *dinamikusan emulálja a vizsgált objektum utasításait egy virtuális számítógépes környezetben*.

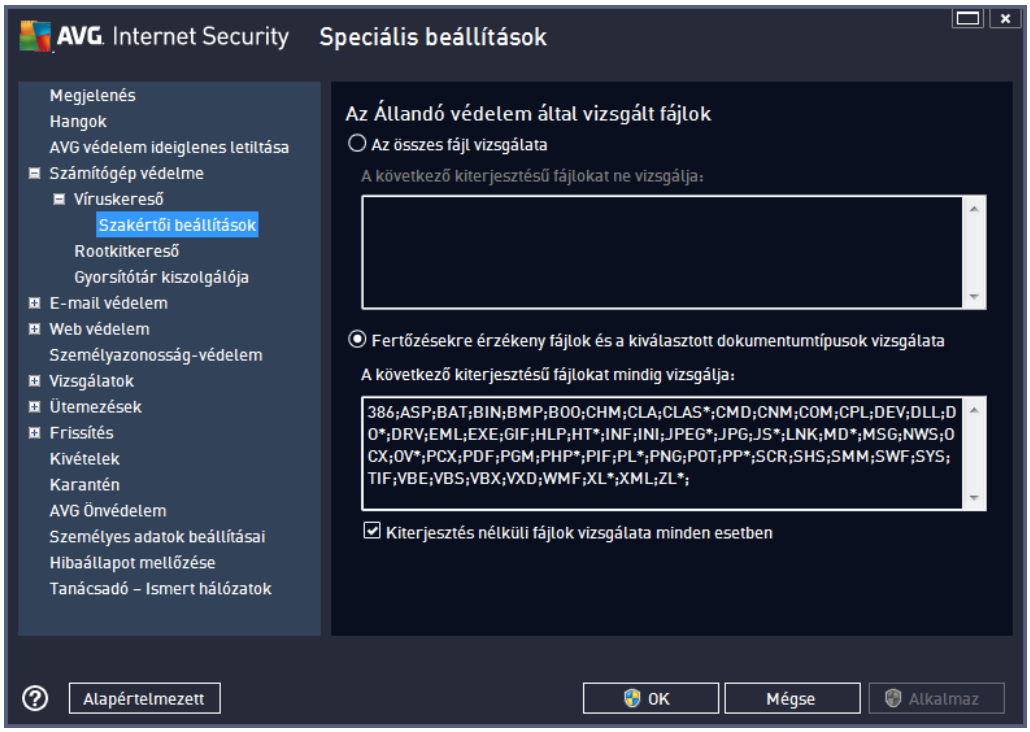
- ***Beállításjegyzékben hivatkozott fájlok vizsgálata*** (*alapértelmezés szerint bekapcsolva*) – Ezzel a paraméterrel beállíthatja, hogy az AVG vizsgálja meg a beállításjegyzékhez hozzáadott összes futtatható fájlt annak érdekében, hogy egy ismert fertőzés ne legyen végrehajtva a számítógép következő indításakor.

- ***Engedélyezés vizsgálatkor*** (*alapértelmezés szerint kikapcsolva*) – Bizonyos helyzetekben (*például extrém vészhelyzetben*) ezen lehetőség bejelölésével aktiválhatja a legátfogóbb vizsgálati algoritmust, amely a lehető legalaposabban vizsgálja át az esetlegesen fenyegetést jelentő objektumokat. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Azonnali üzenetküldés védelem és P2P letöltési védelem engedélyezése*** (*alapértelmezés szerint bekapcsolva*) – Jelölje be ezt az elemet, ha meg szeretne bizonyosodni arról, hogy az azonnali üzenetküldésen alapuló kommunikáció (*például AIM, Yahoo!, ICQ, Skype, MSN Messenger stb.*) és a fájlcserélő hálózatokon *(az ügyfelek között kiszolgáló nélküli, közvetlen kapcsolatot engedélyező hálózatok, amelyek potenciálisan veszélyesek lehetnek; általában zenei fájlok megosztására használatosak)*

keresztül letöltött adatok vírusmentesek.

Az Állandó védelem által vizsgált fájlok párbeszédpanelen beállíthatja, hogy mely fájlokat (*megadott kiterjesztéssel rendelkezőket*) vizsgálja át a program:

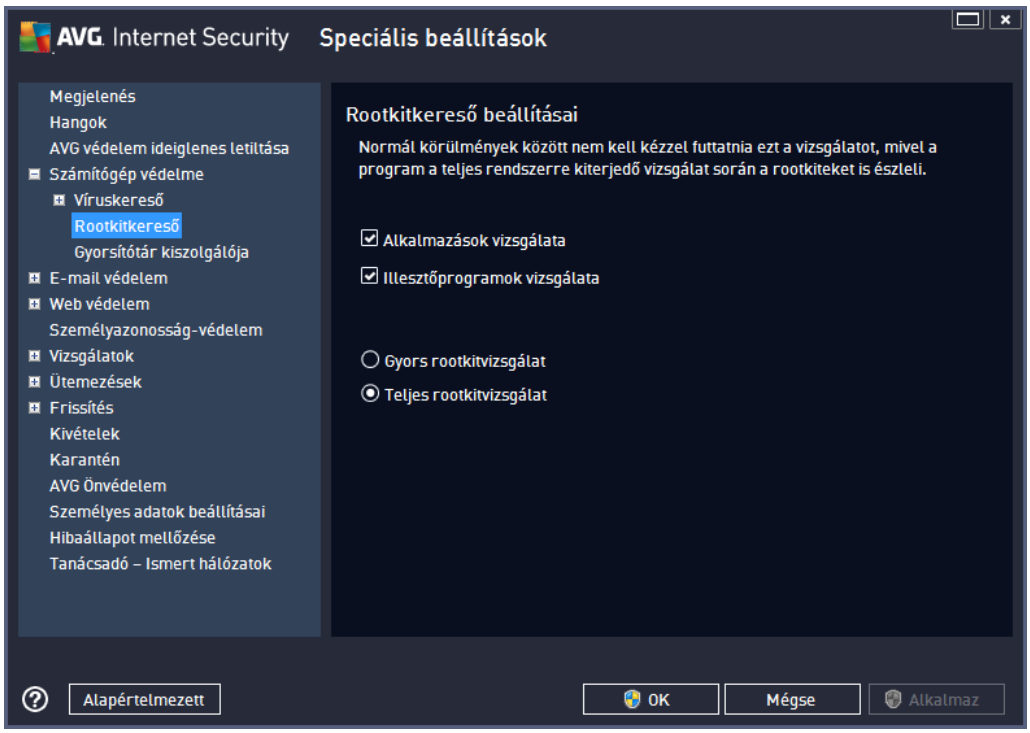


Jelölje be a megfelelő jelölőnégyzetet aszerint, hogy ***Az összes fájl vizsgálatát*** vagy csak a ***Fertőzésekre érzékeny fájlok és a kiválasztott dokumentumtípusok vizsgálatát*** kívánja elvégezni. A vizsgálat felgyorsításához és ezzel egy időben a maximális védelmi szint biztosításához ajánlott megőrizni az alapértelmezett beállításokat. Ilyen módon csak a megfertőzhető fájlokat vizsgálja. A panel megfelelő szakaszában megtalálhatja a vizsgálatban szereplő fájlokat meghatározó kiterjesztések szerkeszthető listáját is.

Jelölje be a ***Kiterjesztés nélküli fájlok vizsgálata minden esetben*** (*alapértelmezés szerint bekapcsolva*) lehetőséget, hogy az Állandó védelem mindig ellenőrizze a kiterjesztés nélküli és az ismeretlen formátumú fájlokat. Javasoljuk, hogy tartsa bekapcsolva ezt az opciót, mert a kiterjesztés nélküli fájlok mindig gyanúsak.

9.4.2. Rootkitkereső

A ***Rootkitkereső beállítások*** párbeszédpanelen szerkesztheti a ***Rootkitkereső*** szolgáltatás beállításait és a rootkitkeresési vizsgálat egyedi paramétereit. A rootkitkeresési vizsgálat a Teljes számítógép-vizsgálat funkció alapértelmezett folyamata:

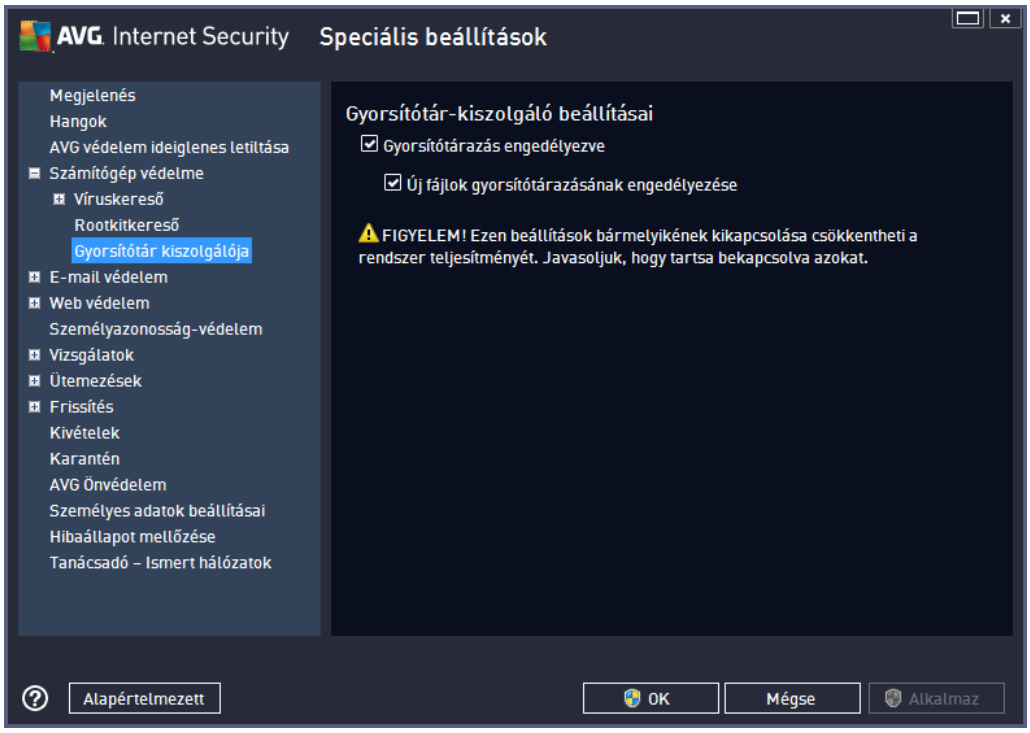


Az ***Alkalmazások vizsgálata*** és az ***Illesztőprogramok vizsgálata*** lehetővé teszi, hogy részletesen meghatározza, mit tartalmazzon a rootkitkeresési vizsgálat. Ezen beállítások módosítása csak haladó felhasználóknak ajánlott. Javasoljuk, hogy mindig tartsa bekapcsolva a beállításokat. Kiválaszthatja a rootkit vizsgálati módját is:

- ***Gyors rootkit vizsgálat*** – az összes futó folyamatot, a betöltött illesztőprogramokat és a rendszermappát (*általában c:\Windows*) ellenőrzi
- ***Teljes rootkit vizsgálat*** – a futó folyamatokat, a betöltött illesztőprogramokat, a rendszermappát (*általában c:\Windows*), valamint az összes helyi lemezt (*flash memóriával együtt, kivéve a floppy-/CD-meghajtókat*) ellenőrzi

9.4.3. Gyorsítótár-kiszolgáló

A ***Gyorsítótár-kiszolgáló beállítások*** párbeszédpanel az **AVG Internet Security 2013** vizsgálatainak felgyorsítására szolgáló gyorsítótár-kiszolgáló műveletekre vonatkozik:



A gyorsítótár-kiszolgáló gyűjti és tárolja a megbízható fájlokkal kapcsolatos adatokat (*egy fájl akkor minősül megbízhatónak, ha egy megbízható forrás digitális aláírásával rendelkezik*). Ezeket a fájlokat a program automatikusan biztonságosnak tekinti, nem szükséges ismét átvizsgálni őket, így ezeket át is ugorja a program a vizsgálatok során.

A ***Gyorsítótár-kiszolgáló beállítások*** párbeszédpanelen a következő lehetőségek érhetők el:

- ***Gyorsítótárazás engedélyezve*** (*alapállapotban bekapcsolva*) – törölje a jelölőnégyzetet a ***Gyorsítótár-kiszolgáló*** kikapcsolásához és a tár törléséhez. Vegye figyelembe, hogy a vizsgálat csökkentheti a számítógép teljesítményét, mivel a rendszer minden használatban lévő fájlt megvizsgál.

- ***Új fájlok gyorsítótárba történő hozzáadásának engedélyezése*** (*alapállapotban bekapcsolva*) – törölje a jelölőnégyzetet, ha nem szeretne több fájlt hozzáadni a gyorsítótárhoz. A rendszer megőrzi a gyorsítótárazott fájlokat a vírusadatbázis következő frissítéséig, illetve a szolgáltatás kikapcsolásáig használja azokat.

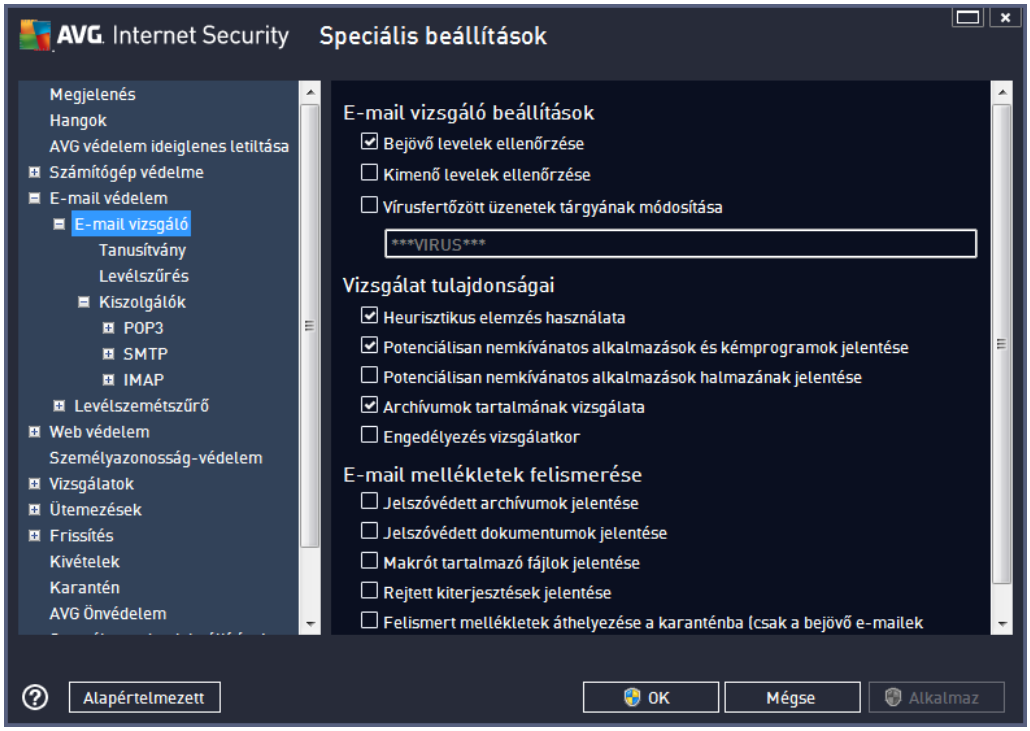
Hacsak nincsen nagyon nyomós indoka a gyorsítótár-kiszolgáló kikapcsolására, azt javasoljuk, hogy tartsa meg az alapértelmezett beállítást, és hagyja bekapcsolva mindkét lehetőséget. Ellenkező esetben jelentősen csökkenhet a rendszer sebessége és teljesítménye.

9.5. E-mail vizsgáló

Ezen a részen szerkesztheti az E-mail vizsgáló és a Levélszemétszűrő részletes konfigurációját:

9.5.1. E-mail vizsgáló

Az ***E-mail vizsgáló*** panel három részből áll:



E-mail vizsgálat

Ezen a részen a bejövő és/vagy kimenő e-mailek következő alapbeállításait adhatja meg:

- ***Bejövő levelek ellenőrzése*** (*alapállapotban bekapcsolva*) – a levelezőprogramba érkező összes e-mail üzenet vizsgálatának be- vagy kikapcsolása
- ***Kimenő levelek ellenőrzése*** (*alapállapotban kikapcsolva*) – a levelezőprogramból kimenő összes e-mail üzenet vizsgálatának be- vagy kikapcsolása
- ***Vírusfertőzött üzenetek tárgyának módosítása*** (*alapállapotban kikapcsolva*) – ha értesítést szeretne kapni arról, hogy a vizsgált e-mail üzenet fertőzött, akkor jelölje be ezt az elemet, és adja meg a kívánt szöveget a szövegmezőben. A szöveg ekkor minden egyes fertőzött e-mail tárgysorához hozzá lesz adva a könnyebb felismerhetőség és szűrés érdekében. A használatra javasolt alapérték a ***VÍRUS***.

Vizsgálat tulajdonságai

Ezen a részen meghatározhatja, hogy az e-mailek miként legyenek megvizsgálva:

- ***Heurisztikus elemzés használata*** (*alapállapotban bekapcsolva*) – jelölje be a heurisztikus észlelési módszer az e-mail üzenetek vizsgálatakor történő használatához. Ha ez a beállítás be van kapcsolva, akkor a mellékleteket nem csak kiterjesztés alapján szűrheti, hanem a tényleges tartalmuk alapján is. A szűrést beállíthatja a Levélszűrés panelen.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** (*alapértelmezés szerint bekapcsolva*) – jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*) – Jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: ezek olyan programok, amelyek a gyártótól közvetlenül beszerezve ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért alapértelmezés szerint ki van kapcsolva.

- ***Archívumok tartalmának vizsgálata*** (*alapállapotban bekapcsolva*) – jelölje be olyan archívumok tartalmának vizsgálatához, amelyek e-mailhez vannak csatolva.

- ***Engedélyezés vizsgálatkor*** (*alapállapotban kikapcsolva*) – bizonyos esetekben (*például ha arra gyanakszik, hogy egy vírus vagy egy támadás megfertőzte a számítógépet*), jelölje be ezt az opciót a legátfogóbb vizsgálati algoritmus bekapcsolásához, amely a számítógép nehezen fertőzhető részeit is ellenőrzi a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

E-mail mellékletek felismerése

Ezen a részen beállíthat további jelentéseket olyan fájlokról, amelyek esetlegesen veszélyesek vagy gyanúsak. Vegye figyelembe, hogy semmilyen figyelmeztető párbeszédpanel nem jelenik meg, csak egy tanúsító üzenettel egészül ki az e-mail üzenet, és minden ilyen jelentés az E-mail védelem észlelései párbeszédpanelen lesz megtalálható:

- ***Jelszóvédett archívumok jelentése*** – a jelszóval védett (*ZIP, RAR stb.*) archívumok nem vizsgálhatók. A jelölőnégyzet bejelölésével potenciálisnak veszélyesnek minősítheti ezeket a fájlokat.

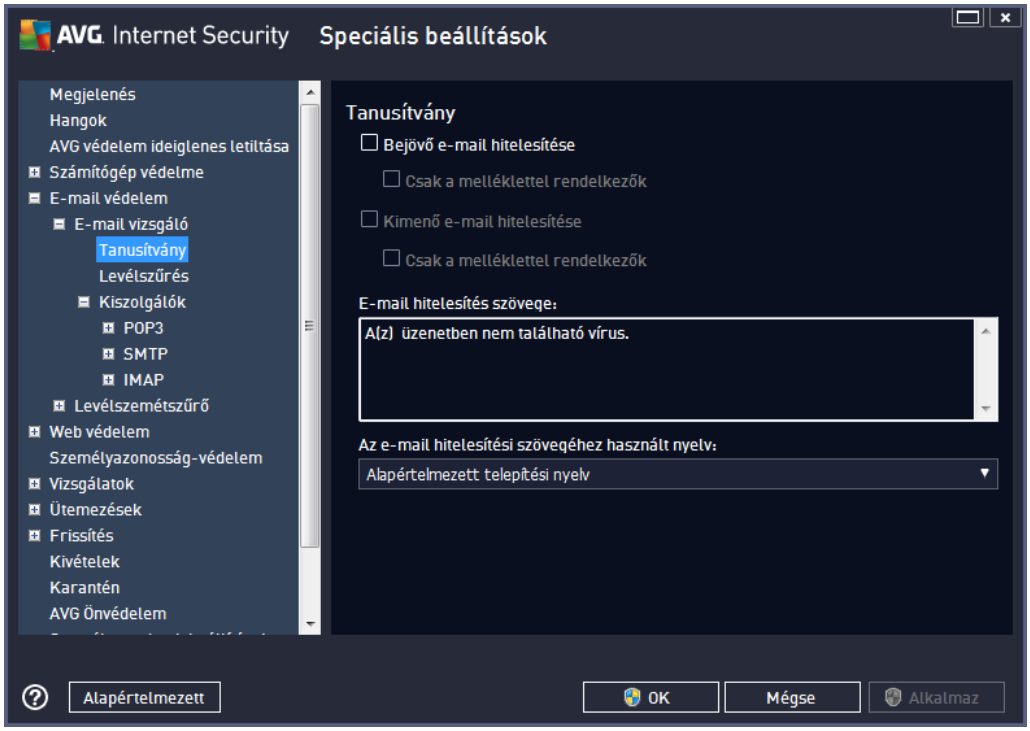
- ***Jelszóvédett dokumentumok jelentése*** – a jelszóval védett dokumentumokat nem lehet vizsgálni. A jelölőnégyzet bejelölésével potenciálisnak veszélyesnek minősítheti ezeket a fájlokat.

- ***Makrókat tartalmazó fájlok jelentése*** – a makró előre meghatározott műveleti lépések folyamata, amely bizonyos feladatokat könnyít meg a felhasználó számára (*az MS Word makrók például széles körben ismertek*). A makróazonban potenciálisan veszélyes utasításokat is tartalmazhat, ezért jelölje be ezt az opciót a makrófájlok gyanúsnak minősítéséhez!

- ***Rejtett kiterjesztések jelentése*** – a rejtett kiterjesztésű fájlok olyan gyanús „valami.txt.exe” futtatható fájlok is lehetnek, amelyek ártatlan „valami.txt” szövegfájlnak álcázzák magukat. A jelölőnégyzet bejelölésével potenciálisnak veszélyesnek minősítheti ezeket a fájlokat.

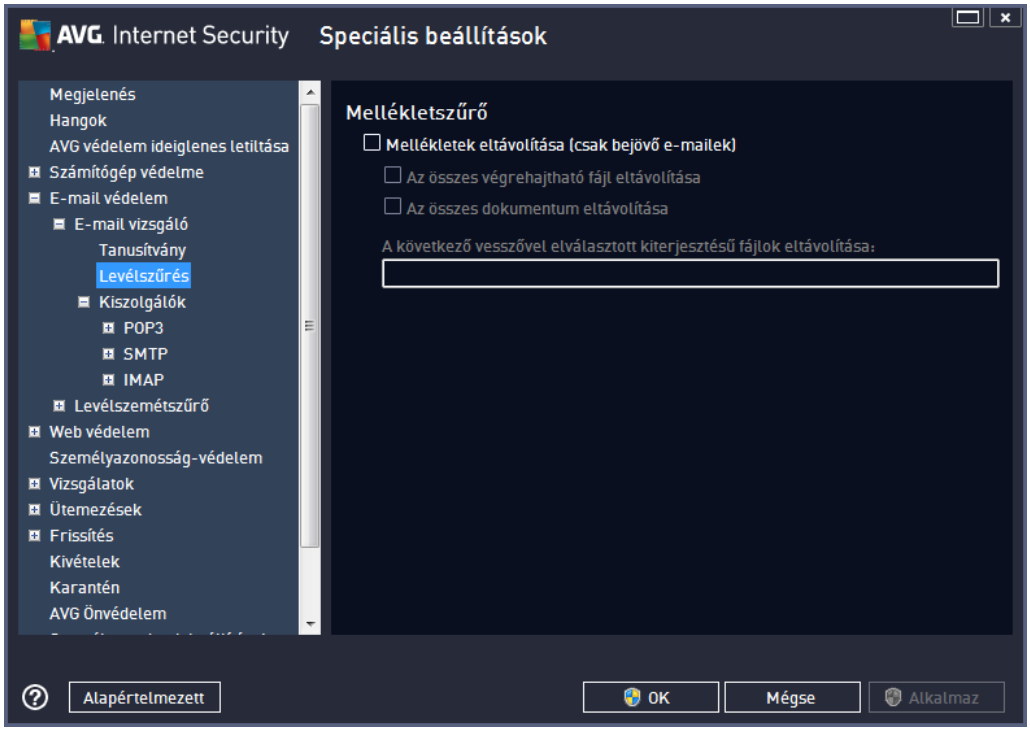
- ***Mellékletek áthelyezése a Karanténba*** – döntse el, hogy szeretne-e tájékoztatást kapni e-mailben a jelszóvédett archívumokról és dokumentumokról, a makrókat tartalmazó fájlokról és/vagy rejtett kiterjesztésű fájlokról, amelyek egy ellenőrzött e-mailhez vannak csatolva. Adja meg, hogy ha ilyen üzenetet azonosít a program a vizsgálat során, a fertőzött objektum a Karanténba kerüljön-e.

A ***Tanúsítvány*** párbeszédpanelen bejelölheti az adott jelölőnégyzeteket, és így megadhatja, kér-e tanúsítást a bejövő levelek esetén (***Bejövő e-mail hitelesítése***) és/vagy a kimenő levelek esetén (***Kimenő e-mail hitelesítése***). Mindegyik lehetőség esetén később megadhatja a ***Csak a melléklettel rendelkezők*** paramétert, hogy a tanúsítványt csak a melléklettel rendelkező e-mail üzenetekhez adja hozzá a program:



Alapértelmezett állapotban a tanúsítvány szövege csak alapinformációkat tartalmaz, amely szerint *az üzenetben nem található vírus.* Azonban ez az információ bővíthető vagy módosítható az igényeinek megfelelően: írja be a kívánt tanúsítási szöveget az ***E-mail tanúsítási szövege*** mezőbe. ***Az e-mail tanúsítási szövegéhez használt nyelv*** részben megadhatja a tanúsítás automatikusan létrehozott részének (*Az üzenetben nem található vírus*) nyelvét. Az üzenet ezután ezen a nyelven jelenik meg.

Megjegyzés: *Vegye figyelembe, hogy csak az alapértelmezett szöveg jelenik meg a kiválasztott nyelven, és a testreszabott szöveget nem fordítja le automatikusan a program.*



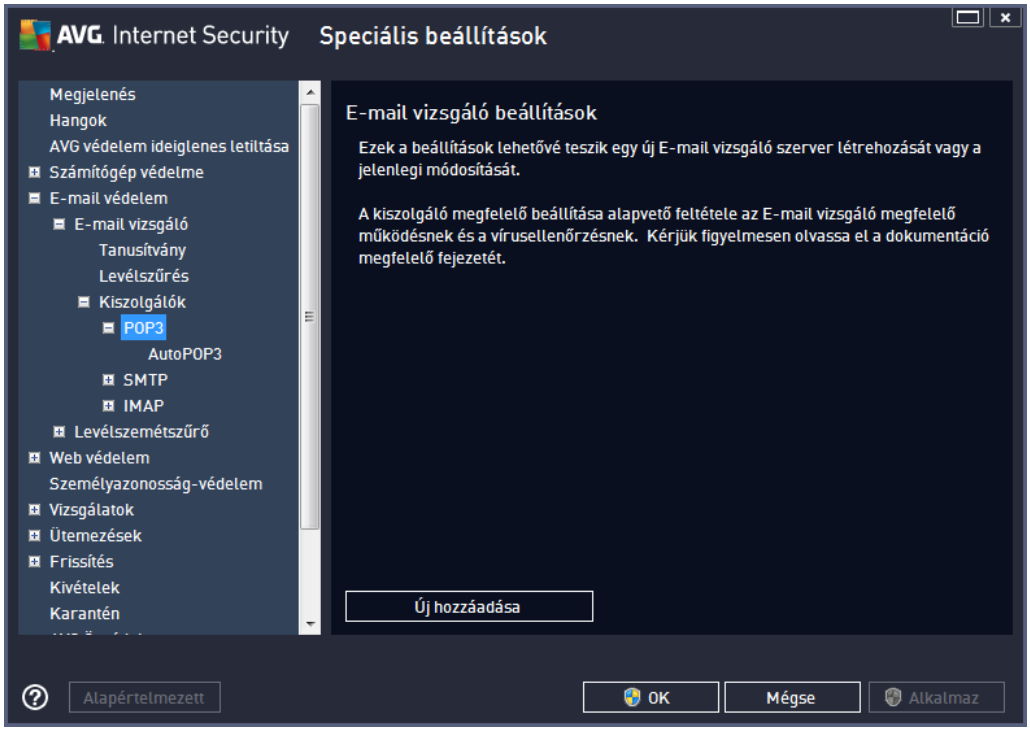
A ***Mellékletszűrő*** párbeszédpanel használatával beállíthatja az e-mail mellékletek vizsgálatának paramétereit. Alapállapotban a ***Mellékletek eltávolítása*** lehetőség ki van kapcsolva. Ha úgy dönt, hogy bekapcsolja, akkor a fertőzött vagy potenciálisan veszélyesnek azonosított csatolmányok automatikusan el lesznek távolítva. Ha meg akarja határozni az eltávolítandó mellékletek különböző típusait, akkor válasszon az opciók közül:

- ***Az összes végrehajtható fájl eltávolítása*** – minden *.exe fájl törölve lesz
- ***Összes dokumentum eltávolítása*** – minden *.doc, *.docx, *.xls, *.xlsx fájl törölve lesz
- ***A vesszővel elválasztott kiterjesztésű fájlok eltávolítása*** – törli az összes meghatározott kiterjesztésű fájlt

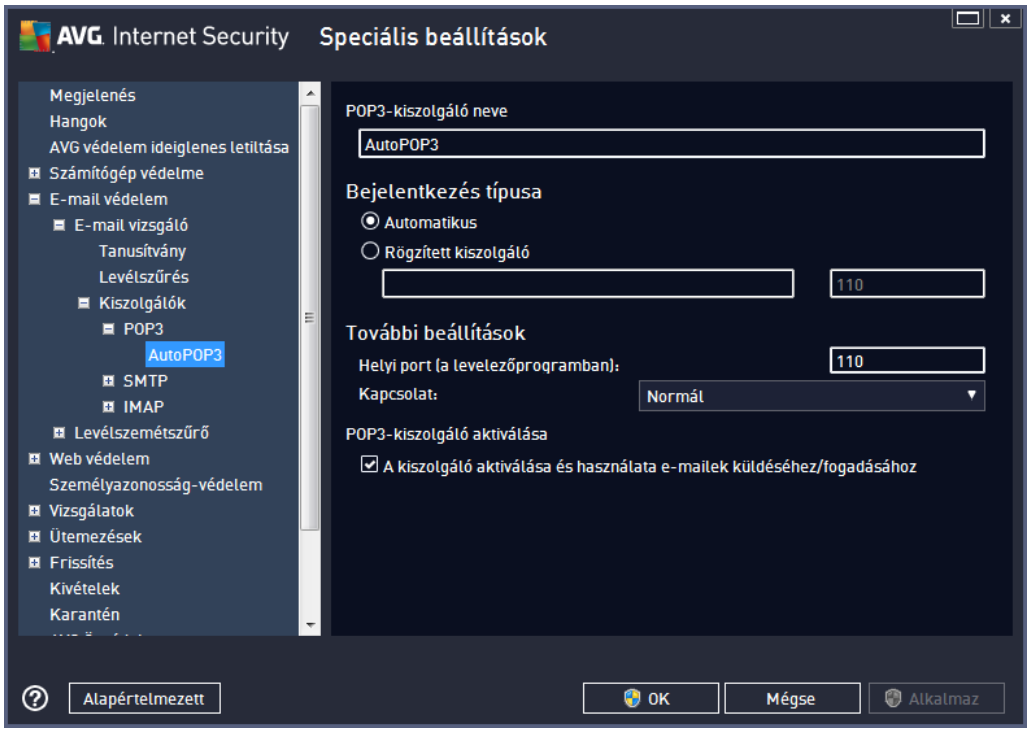
A ***Kiszolgálók*** területen szerkesztheti az E-mail vizsgáló kiszolgálók paramétereit:

- POP3 kiszolgáló
- SMTP-kiszolgáló
- IMAP-kiszolgáló

Ezenkívül meghatározhat új kiszolgálókat a bejövő és a kimenő levelek kezelésére. Ehhez kattintson az ***Új kiszolgáló hozzáadása*** gombra.



Ebben az ablakban megadhat egy új, POP3 protokollt használó E-mail vizsgáló kiszolgálót a bejövő levelekhez:



- ***POP3-kiszolgáló neve*** – ebben a mezőben megadhatja az újonnan hozzáadott kiszolgálók

nevét (*egy POP3-kiszolgáló hozzáadásához kattintson az egér jobb gombjával a bal oldali navigációs menü POP3 elemére*). Az automatikusan létrehozott „AutoPOP3” kiszolgálóknál ez a mező ki van kapcsolva.

- ***Bejelentkezés típusa*** – megadja, hogy az E-mail vizsgáló milyen módszert határozzon a bejövő levelek levelezési kiszolgálójának meghatározására:

    - ***Automatikus*** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik.

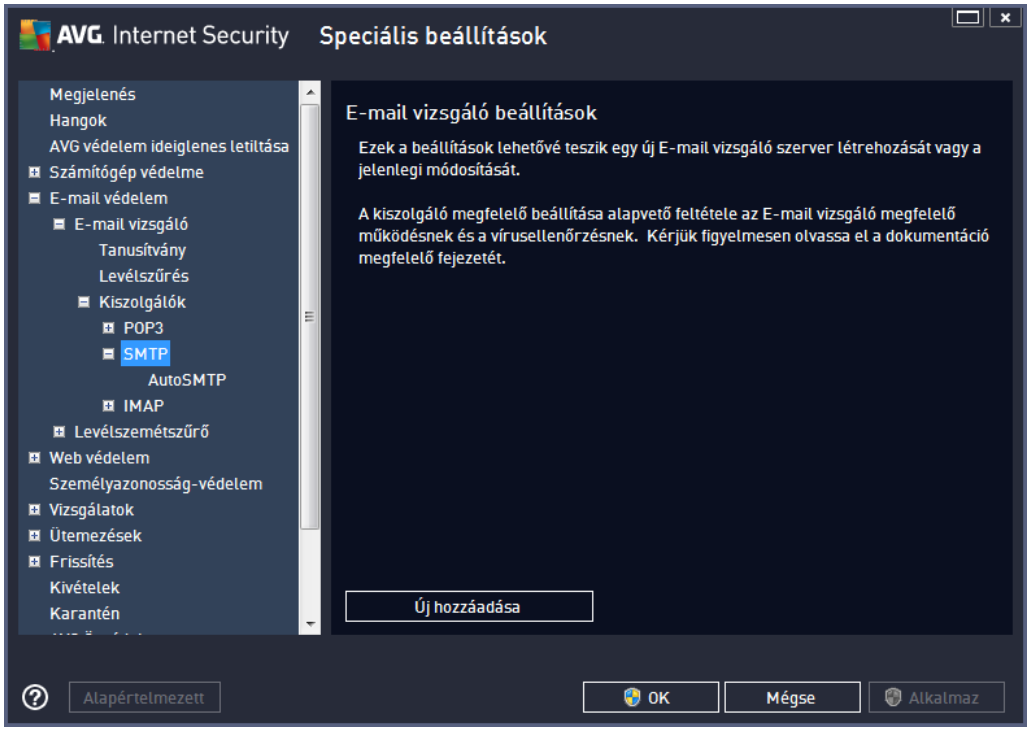
    - ***Rögzített kiszolgáló*** – ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A bejelentkezési név nem változik. A névnél tartománynevet (*például: pop.acme.com*) vagy IP-címet (*például: 123.45.67.89*) használhat. Ha a levelezési kiszolgáló nem szabványos portot használ, akkor a portot is meg lehet adni, kettősponttal elválasztva a kiszolgálónév után (*például: pop.acme.com:8200*). A POP3 kommunikáció szabványos portja 110.

- ***További beállítások*** – további paramétereket adhat meg:

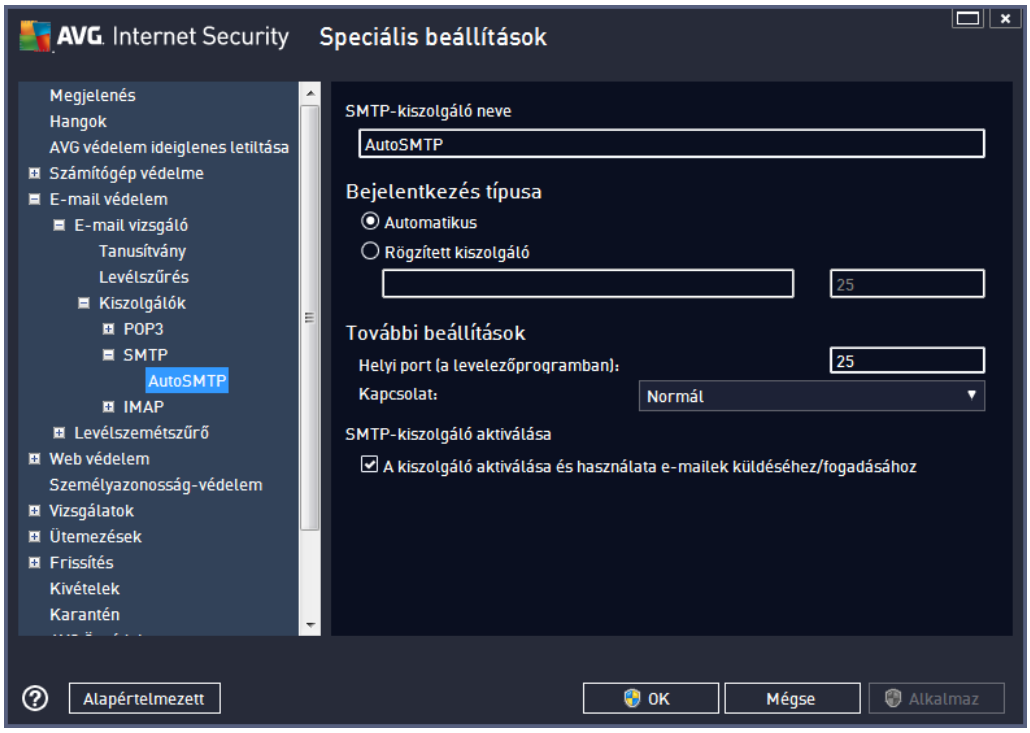
    - ***Helyi port*** – meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítani a POP3 kommunikációhoz.

    - ***Kapcsolat*** – ebben a legördülő menüben meghatározhatja, hogy milyen kapcsolatot használjon a program (*normál/SSL/SSL alapértelmezett*). Ha az SSL kapcsolatot választja, az adatok titkosítva lesznek továbbítva, annak a veszélye nélkül, hogy egy kívülálló nyomon követhetné vagy megfigyelhetné azokat. Ez a funkció is csak akkor áll rendelkezésre, ha a levelezési kiszolgáló támogatja.

- ***Levelezőprogram POP3-kiszolgálójának aktiválása*** – jelölje be/törölje ezt az elemet a megadott POP3-kiszolgáló aktiválásához vagy kikapcsolásához



Ebben az ablakban megadhat egy új, SMTP protokollt használó E-mail vizsgáló kiszolgálót a kimenő levelekhez:



- ***SMTP-kiszolgáló neve*** – ebben a mezőben megadhatja az újonnan hozzáadott

kiszolgálók nevét (*egy SMTP-kiszolgáló hozzáadásához kattintson az egér jobb gombjával a bal oldali navigációs menü SMTP elemére*). Az automatikusan létrehozott „AutoSMTP” kiszolgálóknál ez a mező ki van kapcsolva.

- ***Bejelentkezés típusa*** – megadja, hogy az E-mail vizsgáló milyen módszert használjon a kimenő levelek levelezési kiszolgálójának meghatározásához:

    - ***Automatikus*** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik

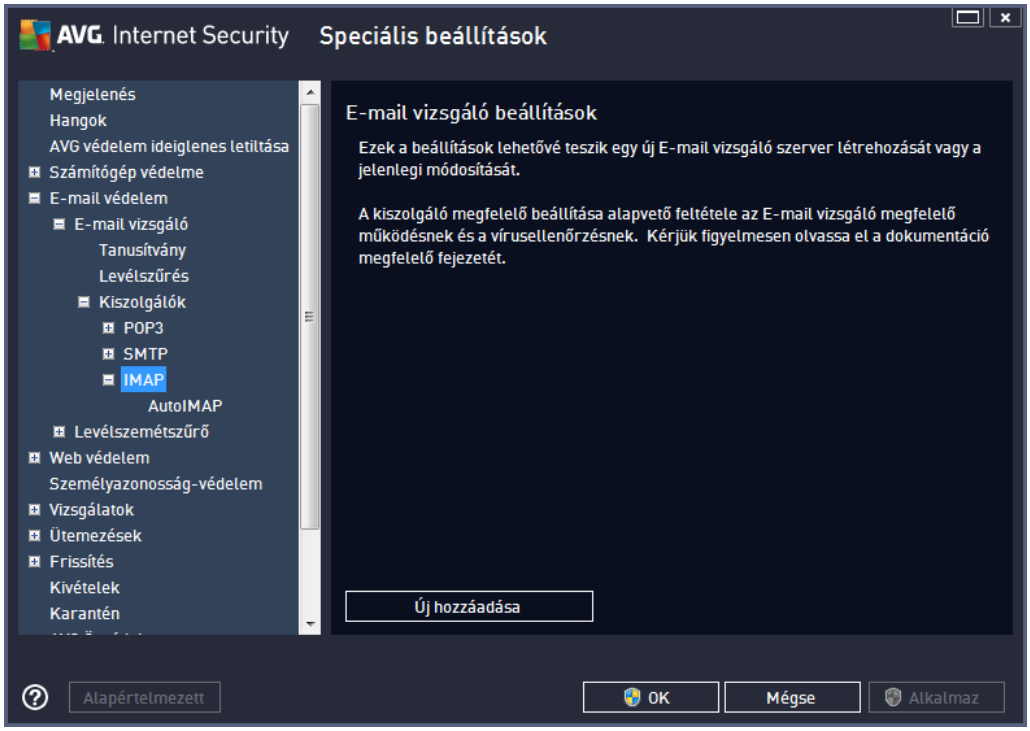
    - ***Rögzített kiszolgáló*** – ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A névnél tartománynevet (*például, smtp.acme.com*), illetve IP-címet (*például, 123.45.67.89*) használhat. Ha a levelezési kiszolgáló nem a standard portot használja, akkor a portot is meg lehet adni, kettősponttal elválasztva a kiszolgálónév után (*például: smtp.acme.com:8200*). Az SMTP-kommunikáció szabványos portja a 25-ös.

- ***További beállítások*** – további paramétereket adhat meg:

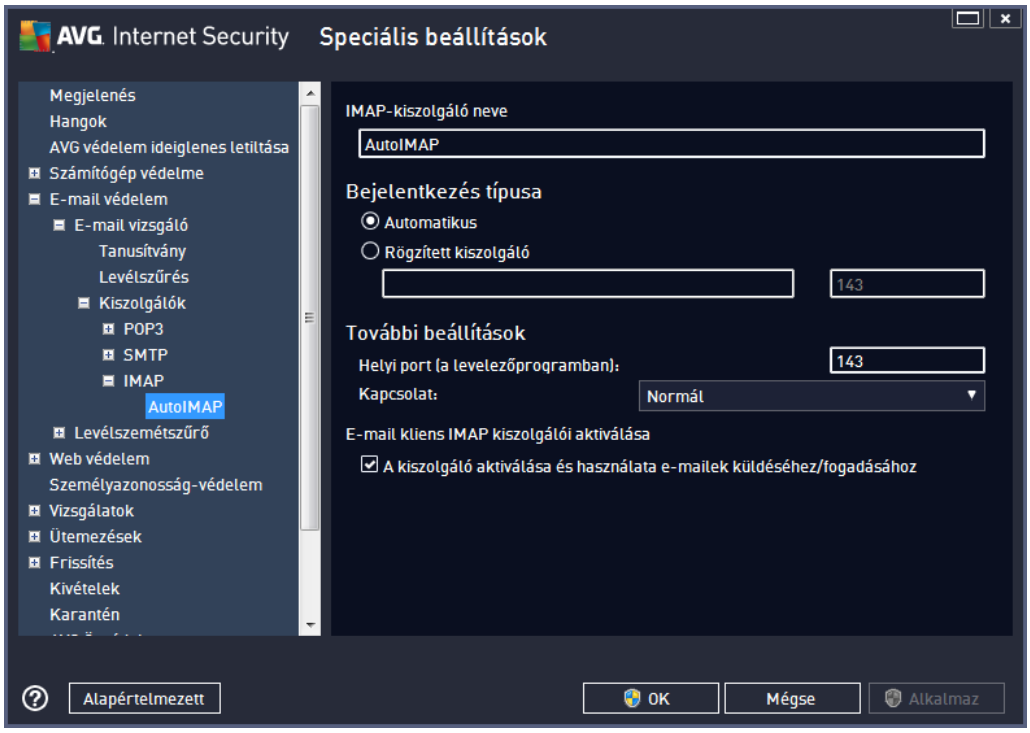
    - ***Helyi port*** – meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítani az SMTP kommunikációhoz.

    - ***Kapcsolat*** – ebben a legördülő menüben meghatározhatja, hogy milyen kapcsolatot használjon a program (*normál/SSL/SSL alapértelmezett*). Ha az SSL kapcsolatot választja, az adatok titkosítva lesznek továbbítva, annak a veszélye nélkül, hogy egy kívülálló nyomon követhetné vagy megfigyelhetné azokat. Ez a funkció csak akkor áll rendelkezésre, ha a célként megadott levelezési kiszolgáló támogatja azt.

- ***Levelezőprogram SMTP-kiszolgálójának aktiválása*** – jelölje be a jelölőnégyzetet vagy törölje jelölést a fent megadott SMTP-kiszolgáló aktiválásához vagy kikapcsolásához



Ezen a párbeszédpanelen megadhat egy új, IMAP protokollt használó E-mail vizsgáló kiszolgálót a kimenő levelekhez:



- ***IMAP-kiszolgáló neve*** – ebben a mezőben megadhatja az újonnan hozzáadott kiszolgálók

nevét (*egy IMAP-kiszolgáló hozzáadásához kattintson az egér jobb gombjával a bal oldali navigációs menü IMAP elemére*). Az automatikusan létrehozott „AutoIMAP” kiszolgálóknál ez a mező ki van kapcsolva.

- ***Bejelentkezés típusa*** – megadja, hogy az E-mail vizsgáló milyen módszert használjon a kimenő levelek levelezési kiszolgálójának meghatározásához:

    - ***Automatikus*** – a bejelentkezés az e-mail ügyfélprogram beállításainak megfelelően automatikusan megtörténik

    - ***Rögzített kiszolgáló*** – ebben az esetben a program mindig az itt megadott kiszolgálót fogja használni. Adja meg a levelezőkiszolgáló címét vagy nevét. A névnél tartománynevet (*például, smtp.acme.com*), illetve IP-címet (*például, 123.45.67.89*) használhat. Ha a levelezési kiszolgáló nem a standard portot használja, akkor a portot is meg lehet adni, kettősponttal elválasztva a kiszolgálónév után (*például: imap.acme.com:8200*). Az IMAP kommunikáció szabványos portja: 143.

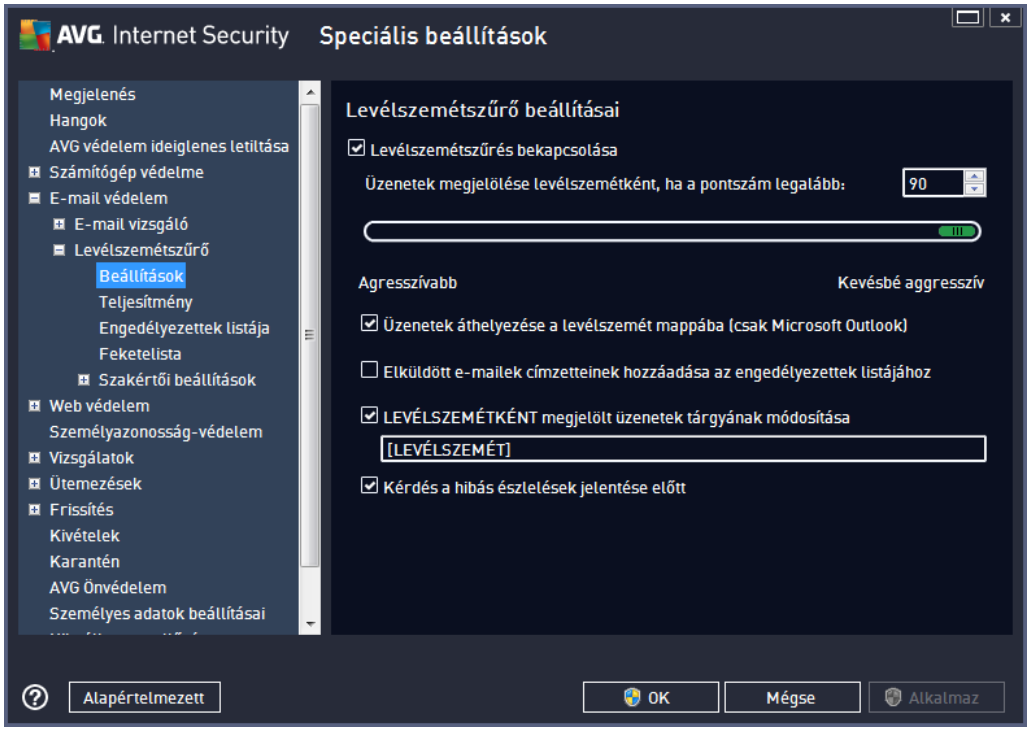
- ***További beállítások*** – további paramétereket adhat meg:

    - ***Helyi port*** – meghatározza azt a portszámot, amelyet a levelező program használni fog. Ezután a levelezőprogramban is ezt a portot kell beállítania az IMAP kommunikációhoz.

    - ***Kapcsolat*** – ebben a legördülő menüben meghatározhatja, hogy milyen kapcsolatot használjon a program (*normál/SSL/SSL alapértelmezett*). Ha az SSL kapcsolatot választja, az adatok titkosítva lesznek továbbítva, annak a veszélye nélkül, hogy egy kívülálló nyomon követhetné vagy megfigyelhetné a levelek tartalmát. Ez a funkció csak akkor áll rendelkezésre, ha a célként megadott levelezési kiszolgáló támogatja azt.

- ***Levelezőprogram IMAP-kiszolgálójának aktiválása*** – jelölje be/törölje ezt a jelölőnégyzetet a fent megadott IMAP-kiszolgáló aktiválásához vagy kikapcsolásához

9.5.2. Levélszemétszűrő



A ***Levélszemétszűrő beállításai*** párbeszédpanelen használja a ***Levélszemétszűrés bekapcsolása*** jelölőnégyzetet az e-mailek levélszemétszűrési vizsgálatának engedélyezéséhez/letiltásához. A beállítás alapértelmezés szerint be van kapcsolva, és mint mindig, javasoljuk, hogy ne módosítsa a konfigurációt, hacsak nincs rá nyomós oka.

A következőkben szigorú vagy kevésbé szigorú pontozási módszereket is beállíthat. ***A Levélszemétszűrő*** többféle dinamikus ellenőrzési módszer segítségével minden üzenethez társít egy pontszámot (*amely azt jelzi, hogy mennyire hasonlít az üzenet tartalma a LEVÉLSZEMÉTHEZ*) Szabályozhatja az ***Üzenet megjelölése levélszemétként, ha a pont nagyobb mint*** beállítást: vagy közvetlen érték megadásával vagy a csúszka jobbra vagy balra történő mozgatásával (*50-90 között állítható*).

Általában az 50-90 közötti értékeket javasoljuk, azonban ha bizonytalan, akkor használja a 90-et. Íme egy általános áttekintés a pontozási küszöbökről:

- ***80-90 közötti érték*** – a valószínűsíthetően levélszemét e-mail üzeneteket kiszűri a rendszer. Ez a beállítás bizonyos üzeneteket tévesen is kiszűrhet.
- ***60-79 közötti érték*** – ez már meglehetősen szigorú beállításnak számít. A program minden olyan üzenetet kiszűr, amelyik levélszemét lehet. Valószínűleg egyes, nem levélszemét üzeneteket is kiszűr a rendszer.
- ***50-59 közötti érték*** – ez egy különösen szigorú beállítás. A nem levélszemétnek számító e-maileket ugyanolyan valószínűséggel szűri ki a program, mint levélszemetet. Ezen értékek használatát nem javasoljuk mindennapos használatra.

A ***Levélszemétszűrő beállításai*** párbeszédpanelen meghatározhatja, hogyan kezelje a program a levélszemétnek minősülő e-mail üzeneteket:

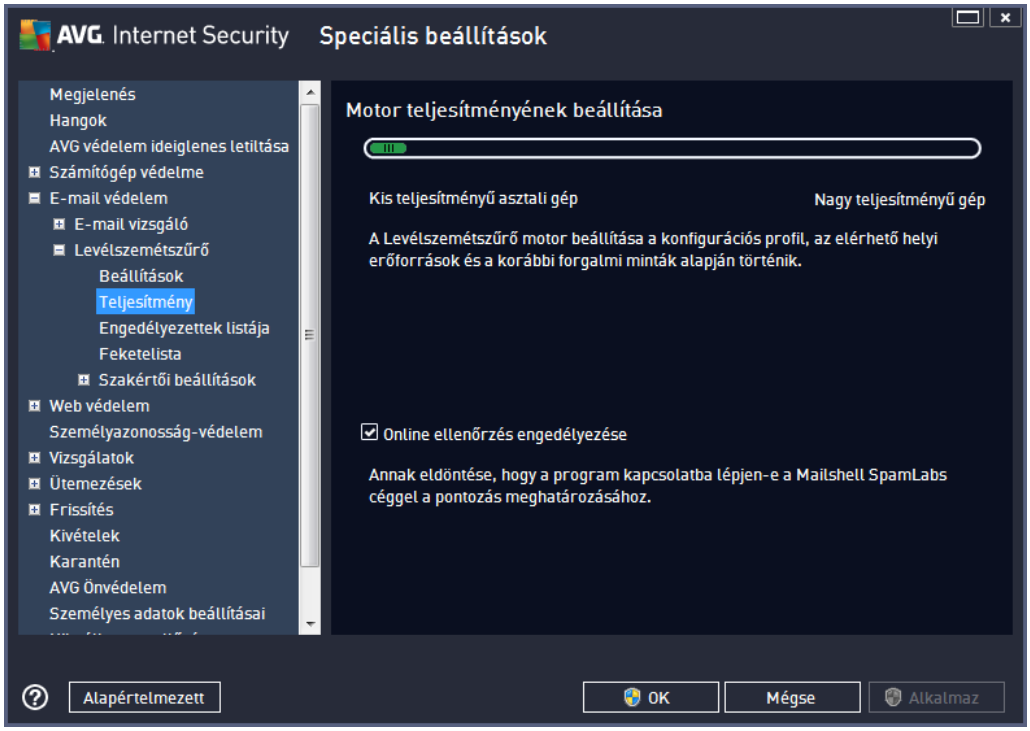
- ***Üzenetek áthelyezése a levélszemét mappába*** *(csak Microsoft Outlook)* – jelölje be ezt a jelölőnégyzetet, ha azt szeretné, hogy minden észlelt levélszemét automatikusan átkerüljön az MS Outlook levelezőprogram levélszemét mappájába. A szolgáltatás más levelezőprogramok esetében jelenleg nem támogatott.

- ***Elküldött e-mailek címzetteinek hozzáadása az engedélyezettek listájához*** – jelölje be ezt a jelölőnégyzetet annak megerősítéséhez, hogy a kimenő e-mailek minden címzettje megbízható, illetve hogy az e-mail fiókjukról érkező valamennyi e-mail üzenet kézbesíthető.

- ***LEVÉLSZEMÉTKÉNT megjelölt üzenetek tárgyának módosítása*** – jelölje be ezt a jelölőnégyzetet, ha az összes levélszemétként azonosított e-mailt meg szeretné jelölni egy bizonyos szóval vagy karakterrel a tárgy mezőben. A kívánt szöveget megadhatja az aktivált szövegmezőben.

- ***Kérdés a hibás észlelések jelentése előtt*** − csak akkor jelenik meg, ha a telepítési folyamat során beleegyezett az Adatvédelmi beállítások projektben való részvételbe. Ha igen, azzal engedélyezte az észlelt fenyegetések jelentését az AVG részére. A jelentés automatikusan jön létre. Ha azonban meg kíván győződni arról, hogy a levélszemétként észlelt üzenetek valóban levélszemetek, ezért azt szeretné, hogy a rendszer az AVG vállalatnak való elküldés előtt megerősítést kérjen, akkor bejelölheti ezt a jelölőnégyzetet.

A ***Motor teljesítményének beállítása*** párbeszédpanelen (*a bal oldali navigációs tábla* ***Teljesítmény*** *eleméből érhető el*) megadhatja a ***Levélszemétszűrő*** összetevő teljesítménybeállításait:



Mozgassa a csúszkát balra vagy jobbra a teljesítményszint módosításához az ***Kis teljesítmény*** / ***Nagy teljesítmény*** módok között.

- ***Kis teljesítmény*** – a program nem használ szabályokat az ellenőrzés során. Kizárólag a

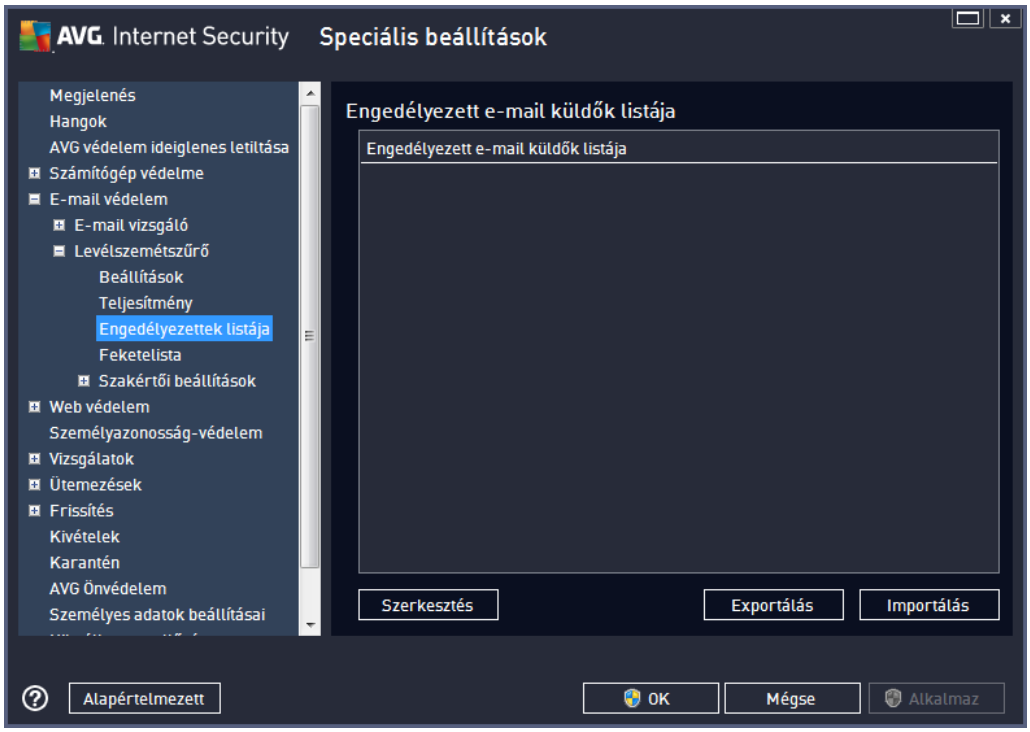
betanított adatok alapján történik az azonosítás. Ez a mód nem ajánlott általános használatra, hacsak nem nagyon elavult a számítógép hardvert használ.

- ***Nagy teljesítmény*** – ez a mód sok memóriát igényel. A vizsgálati folyamat során a levélszemét azonosításához a következő funkciókat használja a program: szabályok és levélszemét adatbázis-gyorsítótár, alap és speciális szabályok, levélszemétküldők IP-címei és adatbázisai.

Az ***Online ellenőrzés engedélyezése*** elem alapértelmezés szerint be van kapcsolva. Még pontosabb levélszemét azonosítást tesz lehetővé a Mailshell kiszolgálókkal való kommunikációnak köszönhetően, azaz azáltal, hogy vizsgált adatokat összeveti a Mailshell online adatbázisaival.

Általában érdemes megtartania az alapbeállításokat, és csak akkor módosítsa azokat, ha feltétlenül szükséges. A beállítások megváltoztatását csak haladó felhasználóknak ajánljuk!

Az ***Engedélyezettek listája*** elem megnyitja az ***Engedélyezett feladók listáját*** azon feladók e-mail címeinek és tartományneveinek globális listájával, amelyek üzenetei soha nem számítanaklevélszemétnek.



A szerkesztőfelületen összeállíthat egy listát azon feladókból, akik soha nem küldenének Önnek nem kívánatos üzeneteket (levélszemetet). A listába olyan teljes tartományneveket is felvehet (*pl. avg.com*), amelyekről soha nem fog levélszemetet kapni. Ha előkészítette a feladók és/vagy tartománynevek előkészített listáját, megadhatja őket a következő módszerekkel: közvetlen bevitel, vagy a teljes címlista egyszerre történő importálása.

Vezérlőgombok

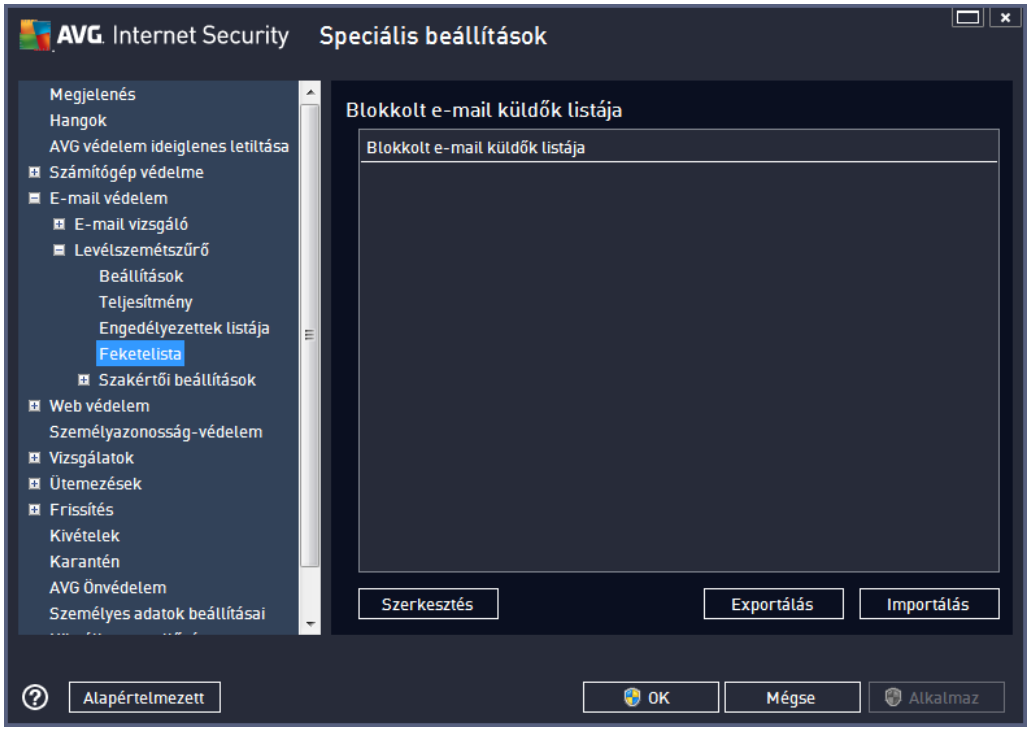
Az alábbi vezérlőgombok érhetők el:

- ***Szerkesztés*** – a gomb megnyomásával megnyit egy olyan párbeszédpanelt, ahol manuálisan megadhat egy címlistát (*használhatja a másolás és beillesztés módszerét is*). Soronként egy elemet (*küldő vagy tartománynevet*) illesszen be.

- ***Exportálás*** – ha valamilyen célból, például biztonsági mentés miatt exportálni szeretné a bejegyzéseket, akkor megteheti ezzel a gombbal. A program ekkor minden bejegyzést egy egyszerű szöveges fájlba másol.

- ***Importálás*** – ha az e-mail címeket és tartományneveket egy szöveges fájlba írta, ezzel a gombbal egyszerűen importálhatja a fájlt. A fájl kizárólag egyetlen elemet tartalmazhat (*cím, tartománynév*) soronként.

A ***Feketelista*** elem megnyitja a tiltott feladók e-mail címeinek és tartományneveinek globális listáját. Az ezekről a címekről érkező üzenetek mindig levélszemétnek számítanak.



Összeállíthat egy listát azon feladókból, akiktől nemkívánatos üzenetekre *(levélszemétre)* számíthat. A listába olyan teljes tartományneveket is felvehet (*például a levelszemetkuldovallalat.hu címet*), amelyekről várhatóan levélszemetet fog kapni. A felvett tartományba tartozó címekről érkező e-maileket mindig levélszemétként azonosítja a program. Ha előkészítette a feladók és/vagy tartománynevek előkészített listáját, megadhatja őket a következő módszerekkel: közvetlen bevitel vagy a teljes címlista egyszerre történő importálása.

Vezérlőgombok

Az alábbi vezérlőgombok érhetők el:

- ***Szerkesztés*** – a gomb megnyomásával megnyit egy olyan párbeszédpanelt, ahol manuálisan megadhat egy címlistát (*használhatja a másolás és beillesztés módszerét is*). Soronként egy elemet (*küldő vagy tartománynevet*) illesszen be.

- ***Exportálás*** – ha valamilyen célból, például biztonsági mentés miatt exportálni szeretné a bejegyzéseket, akkor megteheti ezzel a gombbal. A program ekkor minden bejegyzést egy egyszerű szöveges fájlba másol.

- ***Importálás*** – ha az e-mail címeket és tartományneveket egy szöveges fájlba írta, ezzel a gombbal egyszerűen importálhatja a fájlt.

A Szakértői beállítások szakasz részletes beállítási lehetőségeket tartalmaz a Levélszemétszűrő funkcióhoz. Ezen beállítások módosítását csak haladó felhasználóknak ajánljuk. Jellemzően azon hálózati rendszergazdáknak, akiknek részletesen meg kell adniuk a levélszemétszűrő beállításait az e-mail kiszolgálók legjobb védelme érdekében. Ezért nincs külön súgó az egyes párbeszéd-ablakokhoz, bár egy rövid leírást találhat a felhasználói felület megfelelő részén. Különösen javasoljuk, hogy ne változtassa meg ezen beállításokat, hacsak nincsen teljesen tisztában a Spamcatcher (MailShell Inc.) speciális beállításaival. A nem megfelelő módosítások gyenge teljesítményhez vagy a levélszemétszűrő helytelen működéséhez vezethetnek.

Ha továbbra is megváltoztatná a Levélszemétszűrő beállításait, akkor kövesse a felhasználói felületen megjelenő utasításokat. Általában mindegyik párbeszédablakban egy adott szerkeszthető funkciót talál. A leírás mindig magában a párbeszédablakban olvasható. A következő paramétereket szerkesztheti:

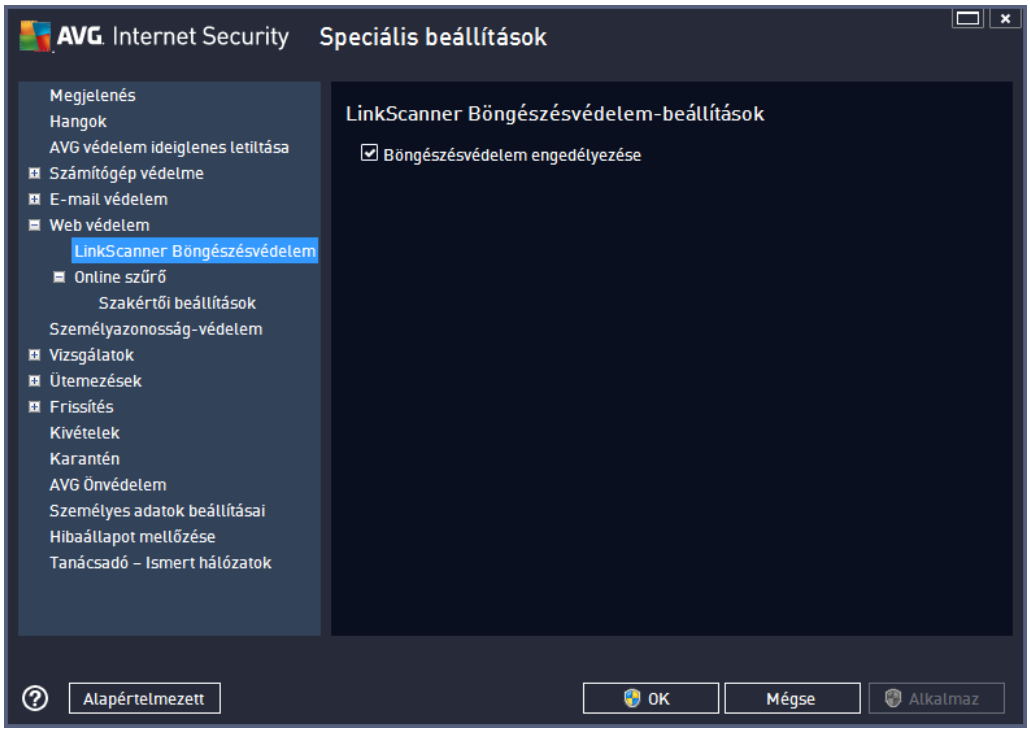
- ***Szűrés*** – nyelvi lista, országlista, engedélyezett IP-címek, blokkolt IP-címek, blokkolt országok, blokkolt karakterkészletek, hamisított feladók

- ***RBL*** – Valósidejű feketelyuk lista kiszolgálók, több találat, küszöb, időtúllépés, maximum IP-k

- ***Internetkapcsolat*** – időtúllépés, proxykiszolgáló, proxy hitelesítése

9.6. Webes böngésző védelme

A ***LinkScanner beállítások*** párbeszédpanel lehetővé teszi a következő szolgáltatások bekapcsolását/kikapcsolását:



- ***Böngészésvédelem engedélyezése*** – (*alapértelmezés szerint bekapcsolva*): aktív (*valósidejű*) védelem kockázatos weboldalak ellen a hozzáférés során. Az ismert kártékony oldalak és veszélyes tartalmuk megjelenítése a webböngészőben, illetve *bármely más, HTTP-t használó alkalmazásban is* le lesz tiltva.

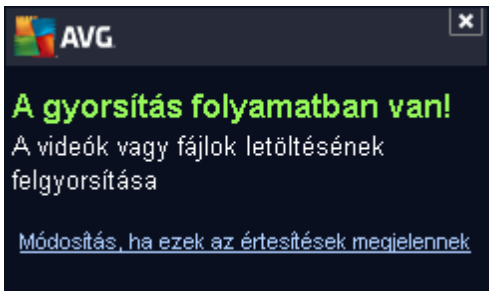
- ***„Secured by LinkScanner" üzenet hozzáadása...*** – (*alapértelmezés szerint kikapcsolva*): jelölje be ezt a lehetőséget ahhoz, hogy a LinkScanner által ellenőrzöttként legyen megjelölve minden, a Facebook / MySpace közösségi oldalakról küldött üzenet, amelyek aktív hivatkozásokat tartalmaznak.

9.6.1. Online szűrő

Az ***Online szűrő*** párbeszédpanel a következő beállítási lehetőségeket tartalmazza:

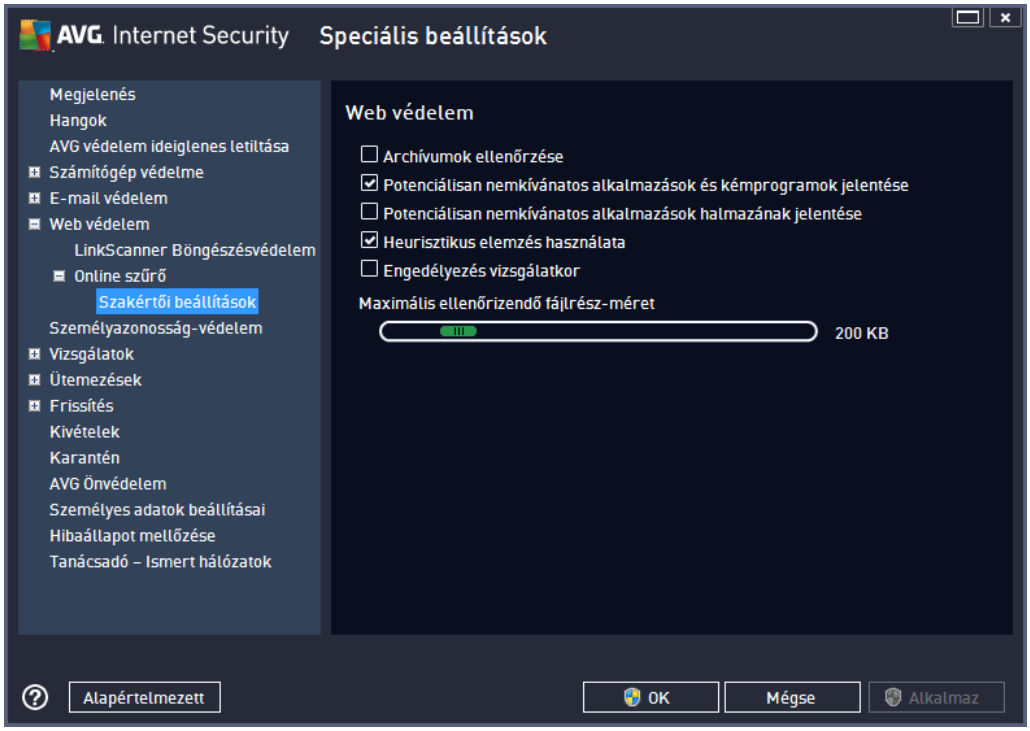
- ***Online szűrő engedélyezése*** *(alapértelmezés szerint bekapcsolva)* – Aktiválja/deaktiválja a teljes ***Online szűrő*** szolgáltatást. Az ***Online szűrő*** speciális beállításainak megadásához használja a következő, Webes védelem elnevezésű párbeszédpanelt.

- ***AVG gyorsító engedélyezése*** *(alapértelmezés szerint bekapcsolva)* – Aktiválja/deaktiválja az AVG gyorsítót. Az AVG gyorsító folyamatosabb online videolejátszást tesz lehetővé, és megkönnyíti a további letöltéseket. Amikor videogyorsítás van folyamatban, a tálcán megjelenik egy felugró ablak:



Fenyegetés értesítés mód

A panel alsó részén válassza ki, hogy miként kíván értesítést kapni az észlelt fenyegetésekről: normál felbukkanó ablak, buborék értesítés vagy ikonjelzés a rendszerterületen.



A ***Web védelem*** ablakban szerkesztheti az összetevő beállításait a honlapok tartalmi vizsgálatának szempontjából. A szerkesztőfelület lehetővé teszi a következő alapvető opciók beállítását:

- ***Webes védelem engedélyezése*** – ez az opció biztosítja, hogy az ***Online szűrő*** ellenőrizze a honlapok tartalmát. Ha az opció be van kapcsolva (*alapértelmezés szerint*), akkor a következő elemeket kapcsolhatja be és ki:

    - ***Archívumok ellenőrzése*** – (*alapállapotban kikapcsolva*): ellenőrzi a megjelenítendő oldalba ágyazott esetleges archívumok, tömörített fájlok tartalmát.

    - ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** – *(alapértelmezés szerint bekapcsolva)*: jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

    - ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** – (*alapállapotban kikapcsolva*): jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez; olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért a funkció alapértelmezés szerint ki van kapcsolva.

    - ***Heurisztikus elemzés használata*** – (*alapállapotban bekapcsolva*): a megjelenítendő oldal tartalmának ellenőrzése a heurisztikus elemzés módszerével (*a vizsgált objektum utasításainak dinamikus emulálása veszélytelen módon, egy virtuális számítógépes környezetben*).

- ***Engedélyezés vizsgálatkor*** (*alapértelmezés szerint kikapcsolva*) – bizonyos esetekben (*például ha vírusfertőzésre gyanakszik*) ezzel a beállítással aktiválhatja a legalaposabb vizsgálati algoritmusokat, amelyek még a számítógép ritkán megfertőződő részeit is ellenőrzik a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

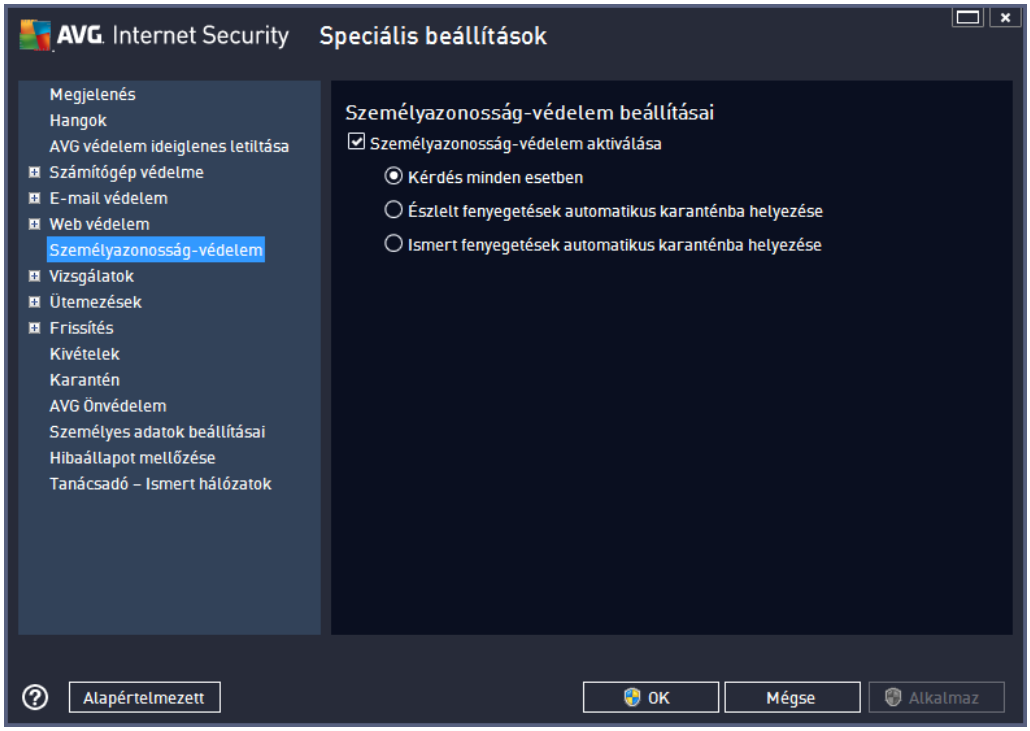
- ***Maximális ellenőrzendő fájlméret*** – ha beágyazott fájlok találhatók egy megjelenítendő weboldalban, akkor még azelőtt ellenőrizheti a tartalmukat, mielőtt azok letöltődnének a számítógépre. Azonban a nagy fájlok vizsgálata időbe telhet, és a weboldal betöltődése jelentősen lelassulhat. Használja a csúszkát az ***Online szűrővel*** vizsgálandó fájlok maximális méretének beállításához. Ha a letöltött fájl nagyobb a megadott méretnél, és az Online szűrő nem ellenőrzi, de természetesen Ön ilyenkor is védve van: ugyanis az esetleges fertőzést az ***Állandó védelem*** azonnal észleli.

- ***Kiszolgáló/IP/tartomány kizárása*** – a szövegmezőbe beírhatja egy szerver (*kiszolgáló, IP-cím, IP-cím maszkkal vagy URL*) pontos nevét vagy egy tartományt, amit az ***Online szűrőnek*** nem kell ellenőriznie. Csak olyan kiszolgálókat zárjon ki, amelyben teljesen biztos, hogy nem fognak veszélyes tartalmat nyújtani.

9.7. Személyazonosság-védelem

A Személyazonosság-védelem olyan, kártevőktől védő összetevő, amely mindenféle kártevő (*kémprogramok, robotprogramok, személyes adatokat eltulajdonító programok stb.*) ellen véd, viselkedésalapú technológiát használ, és azonnali védelmet biztosít a legújabb vírusok ellen *(az összetevők működésének részletes leírásáért tekintse meg a Személyazonosság fejezetet*).

A ***Személyazonosság-védelem beállításai*** panel lehetővé teszi a Személyazonosság-védelem alapvető funkcióinak ki- és bekapcsolását:



Identity Protection aktiválása (*alapállapotban bekapcsolva*) – törölje a jelölőnégyzet jelölését a Személyazonosság összetevő kikapcsolásához.

Javasoljuk, hogy ezt a beállítást ne kapcsolja ki, hacsak ez nem elkerülhetetlen.

Ha a Személyazonosság-védelem be van kapcsolva, akkor meghatározhatja, hogy mi történjen egy fenyegetés észlelésekor:

- ***Kérdés minden esetben*** (*alapállapotban bekapcsolva*) – ha a program fenyegetést észlel, akkor rákérdez, hogy áthelyezze-e azt a karanténba, így elkerülhető, hogy a futtatni kívánt alkalmazásokat a program eltávolítsa.
- ***Észlelt fenyegetések automatikus karanténba helyezése*** – jelölje be ezt a jelölőnégyzetet az összes észlelt fenyegetés automatikus és azonnali áthelyezéséhez az Karanténjába. Az alapértelmezett beállítások szerint egy új fenyegetés észlelésekor a program rákérdez, hogy karanténba helyezze-e azt (így csak azon alkalmazásokat távolítja el, amelyeket Ön nem kíván futtatni).
- ***Ismert fenyegetések automatikus karanténba helyezése*** – jelölje be a kártevők automatikus és azonnali áthelyezéséhez a Karanténba.

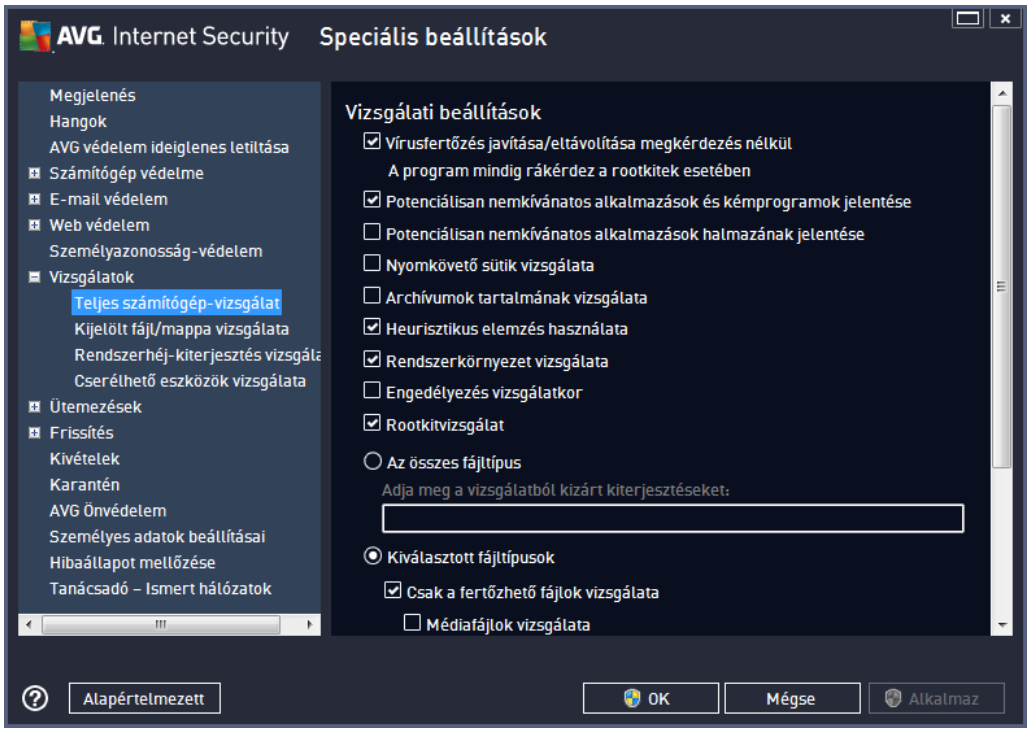
9.8. Vizsgálatok

A haladó vizsgálati beállítások négy kategóriára vannak osztva, és a szoftver gyártója által meghatározott bizonyos vizsgálati típusokra vonatkoznak:

- ***Teljes számítógép-vizsgálat*** – A teljes számítógép előre meghatározott normál vizsgálata
- ***Rendszerhéj-kiterjesztés vizsgálata*** – egy adott objektum vizsgálata közvetlenül a Windows Intézőből
- ***Kijelölt fájl/mappa vizsgálata*** – a számítógép kiválasztott területeinek előre meghatározott, általános vizsgálata
- ***Cserélhető eszközök vizsgálata*** – a számítógéphez csatlakoztatott cserélhető eszközök vizsgálata

9.8.1. Vizsgálat a teljes számítógépen

A ***Számítógép teljes vizsgálata*** lehetővé teszi a szoftvergyártó által előre meghatározott vizsgálatok paramétereinek szerkesztését, Számítógép teljes vizsgálata:



Vizsgálati beállítások

A ***Vizsgálati beállítások*** részen a vizsgálati paraméterek listáját találhatja, melyeket tetszőlegesen be- és kikapcsolhat:

- ***Fertőzés javítása/eltávolítása kérdés nélkül*** (*alapértelmezés szerint bekapcsolva*) – ha a rendszer vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl automatikusan nem javítható, az objektumot áthelyezi a Karanténba.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** (*alapértelmezés szerint bekapcsolva*) – jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*) – Jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: ezek olyan programok, amelyek a gyártótól közvetlenül beszerezve ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért a funkció alapértelmezés szerint ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** (*alapértelmezés szerint kikapcsolva*) – Ez a paraméter meghatározza, hogy a rendszer észlelje-e a cookie-kat; (*a HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*).

- ***Archívumok tartalmának vizsgálata*** *(alapértelmezés szerint kikapcsolva)* – Ez a paraméter meghatározza, hogy vizsgálatkor a program ellenőrizze az archívumokban (például ZIP, RAR, stb.) tárolt fájlokat.

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*) – a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*) – a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Engedélyezés vizsgálatkor*** (*alapértelmezés szerint kikapcsolva*) – bizonyos esetekben (*például ha vírusfertőzésre gyanakszik*) ezzel a beállítással aktiválhatja a legalaposabb vizsgálati algoritmusokat, amelyek még a számítógép ritkán megfertőződő részeit is ellenőrzik a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Rootkitek keresése*** (*alapértelmezés szerint bekapcsolva*) – A Rootkitkereső az esetleges rootkiteket, vagyis olyan programokat és technológiákat keres a számítógépen, melyek a kártékony tevékenységeket fedik el. Ha a program rootkitet észlel, akkor az nem jelenti automatikusan azt, hogy a számítógép fertőzött. Bizonyos esetekben a program egyes eszközillesztőket, vagy legitim alkalmazások részeit is – tévesen – rootkitként észlel.

El kell döntenie továbbá, hogy a program mely fájlokat vizsgálja

- ***Az összes fájltípus*** kivételek megadásánál lehetőségével. Ezen fájlkiterjesztéseket vesszővel válassza el (*mentés után a vesszők pontosvesszőkre változnak*);

- ***Kiválasztott fájltípusok*** – megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek fertőzöttek lehetnek (*a nem fertőzhető fájlokat, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem ellenőrzi a program*), pl. médiafájlok (*video-, audiofájlok – ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg azokat*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

- Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** – ez az opció alapértelmezés szerint be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell azokat.

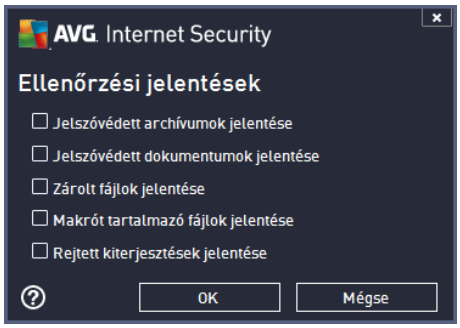
A vizsgálati sebesség beállítása

A ***Vizsgálati sebesség beállítása*** részben meghatározhatja a vizsgálat sebességét a rendszer erőforrásainak függvényében. Alapállapotban ez az érték *felhasználótól által függő* automatikus erőforráshasználatra van állítva. Ha azt szeretné, hogy a vizsgálat gyorsabban fusson, akkor kevesebb idő szükségeltetik, de a rendszererőforrások használata jelentősen megnő, és lelassíthatja a PC-n zajló egyéb tevékenységeket (*ezt az opciót akkor használhatja, ha a*

számítógép be van kapcsolva, és senki nem dolgozik rajta jelenleg). Másrészt csökkentheti a rendszererőforrások használatát, de ez a vizsgálathoz szükséges idő növekedésével jár.

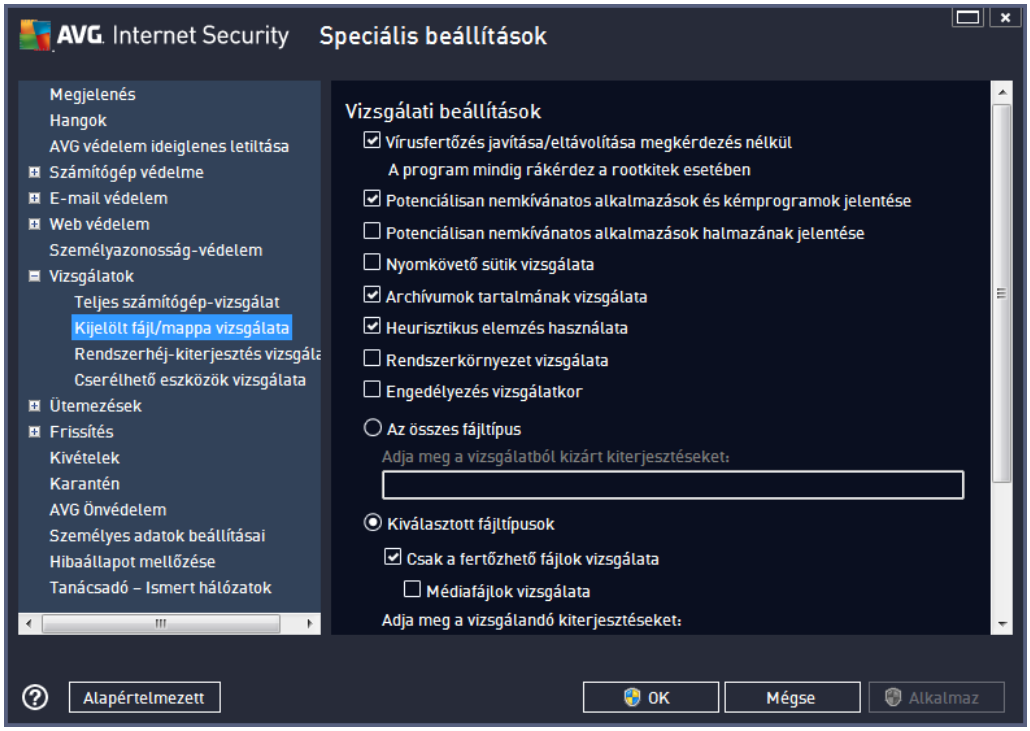
További vizsgálati jelentések beállítása...

Kattintson a ***További vizsgálati jelentések...*** hivatkozásra a ***Vizsgálati jelentések*** panel megnyitásához, ahol számos opciót jelölhet be azzal kapcsolatban, hogy a programnak mit kell jelentenie:



9.8.2. Kijelölt fájl/mappa ellenőrzése

A ***Kijelölt fájlok vagy mappák vizsgálata*** panel megegyzik a Számítógép teljes vizsgálata panellel. Minden beállítási lehetőség ugyanaz, azonban az alapértékek szigorúbbak a Teljes számítógép vizsgálata ablakban:

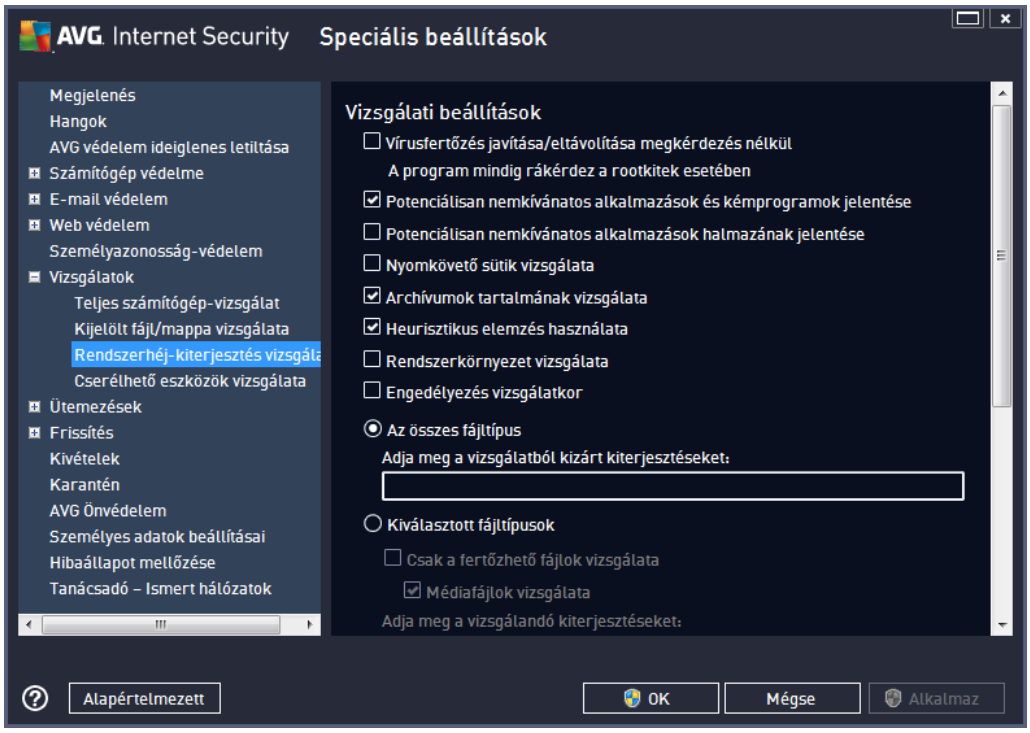


Az összes itt beállított paraméter csak a Bizonyos fájlok vagy mappák vizsgálata opcióra vonatkozik!

Megjegyzés: *Az adott paraméterek leírásával kapcsolatban lásd az AVG speciális beállítások / Vizsgálatok / Teljes számítógép-vizsgálat fejezetet.*

9.8.3. Rendszerhéj-kiterjesztés vizsgálata

Hasonlóan az előző Számítógép teljes vizsgálata elemhez, a ***Héjkiterjesztés vizsgálat*** is lehetővé teszi a számos gyári beállítás módosítását. Itt a beállítások egyedi objektumok Windows Intézőből történő közvetlen vizsgálatára vonatkoznak (*héjkiterjesztés*), lásd a Vizsgálat Windows Intézőben fejezetet:



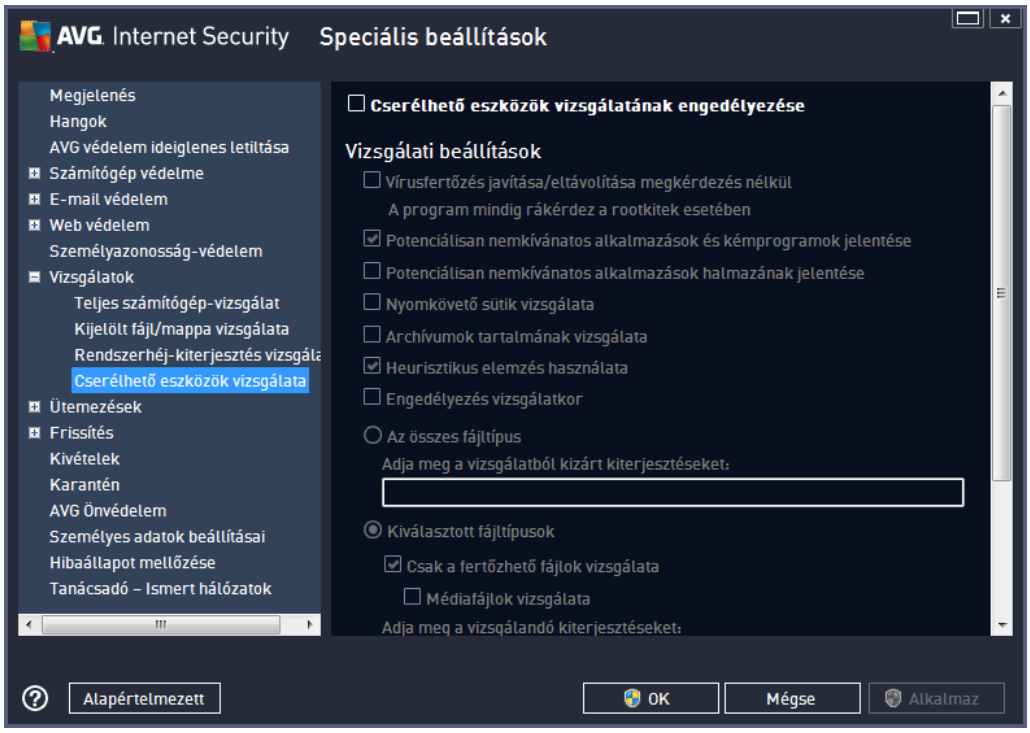
A paraméterek listája megegyezik a Teljes számítógép vizsgálata rész paramétereivel. Az alapértelmezett beállítások azonban eltérnek (*például a Teljes számítógép-vizsgálat szolgáltatás nem vizsgálja a tömörített fájlokat, de ellenőrzi a rendszerkörnyezetet, a Rendszerhéj-kiterjesztés vizsgálata esetében ez fordítva van*).

Megjegyzés: *Az adott paraméterek leírásával kapcsolatban lásd az AVG speciális beállítások / Vizsgálatok / Teljes számítógép-vizsgálat fejezetet.*

A Teljes számítógép-vizsgálat párbeszédpanelhez hasonlóan a ***Rendszerhéj-kiterjesztés vizsgálata*** párbeszédpanel is tartalmazza az ***AVG felhasználói felület egyéb beállításai*** részt, ahol meghatározhatja, hogy a vizsgálati folyamat és a vizsgálat eredménye elérhető legyen-e az AVG felhasználói felületéről. Meghatározhatja azt is, hogy a vizsgálati eredmények csak akkor jelenjenek meg, ha a rendszer fertőzést észlelt.

9.8.4. Cserélhető eszközök vizsgálata

A ***Cserélhető eszközök vizsgálata*** panel felülete hasonlít a Számítógép teljes vizsgálata panel felületéhez:



A ***Cserélhető eszközök vizsgálata*** automatikusan elindul, ha egy cserélhető eszközt csatlakoztat a számítógéphez. Ez a vizsgálat alapértelmezés szerint ki van kapcsolva. Azonban különösen fontos, hogy ellenőrizze a cserélhető eszközöket is, mivel azok potenciális veszélyforrást képviselnek. A vizsgálat beállításához és szükség esetén automatikus elindításához jelölje be a ***Cserélhető eszközök vizsgálata*** lehetőséget.

Megjegyzés: *Az adott paraméterek leírásával kapcsolatban lásd az AVG speciális beállítások / Vizsgálatok / Teljes számítógép-vizsgálat fejezetet.*

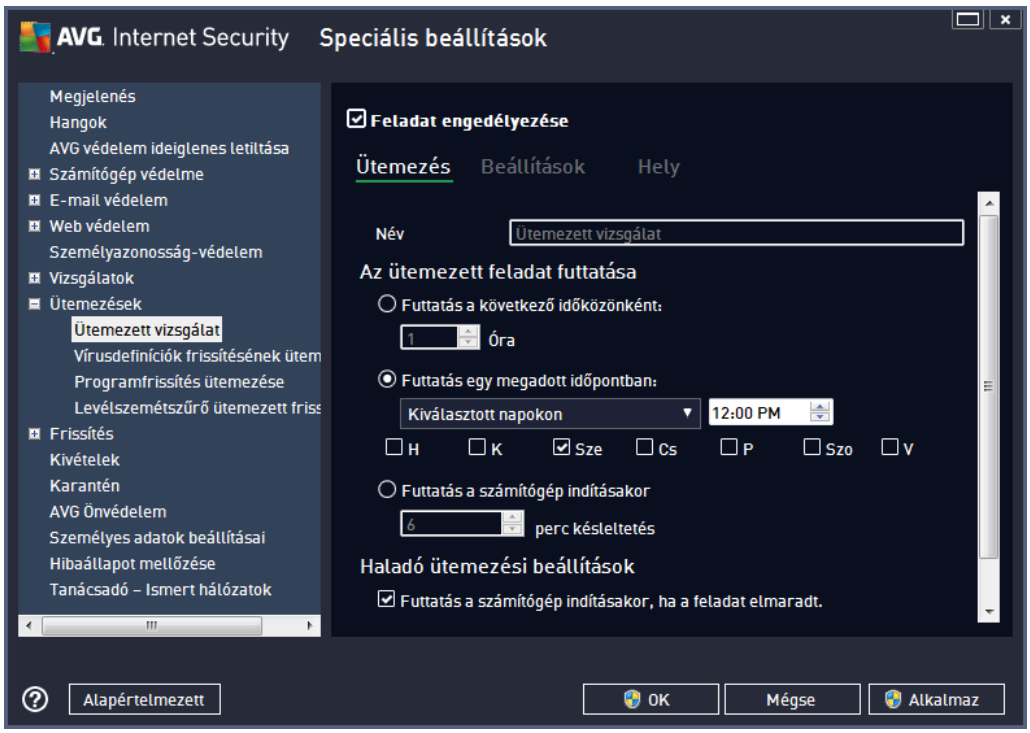
9.9. Ütemezések

Az ***Ütemezések*** részben szerkesztheti a következők alapbeállításait:

- Ütemezett vizsgálat
- Vírusdefiníciók frissítésének ütemezése
- Programfrissítés ütemezése
- Levélszemétszűrő frissítés ütemezése

9.9.1. Ütemezett vizsgálat

Az ütemezett vizsgálat paramétereit három lapon szerkesztheti (*de akár új ütemezést is létrehozhat*). Az egyes füleken be- és kikapcsolhatja a ***Feladat engedélyezése*** opciót az ütemezett vizsgálat ideiglenes letiltásához. Szükség esetén újra bekapcsolhatja azt:



Ezután a ***Név*** mező (*kikapcsolva az alapértelmezett ütemezéseknél*) mutatja a program gyártója által létrehozott nevet ezen ütemezéshez. Az újonnan létrehozott ütemezéseknél (*felvehet egy új ütemezést, ha a jobb gombbal az* ***Ütemezett vizsgálat*** *elemre kattint a bal oldali navigációs sávban*) felvehet egy saját nevet, ekkor a szöveges mező szerkesztésre megnyitható. Próbáljon mindig rövid, jellemző és megfelelő nevet adni a vizsgálatoknak, így később könnyebben megkülönböztetheti majd azokat.

Például: *Nem javasolt, hogy a vizsgálatnak az „Új vizsgálat" vagy „Saját vizsgálat" nevet adja, mivel ez semmit nem mond arról, hogy a vizsgálat valójában mit vizsgál. Ugyanakkor megfelelő leíró név például a „Rendszerterületek vizsgálata" stb. Nem szükséges a névben megadni, hogy a számítógép teljes vagy részleges vizsgálatáról van szó, mivel a saját vizsgálatok minden esetben adott fájlok vagy mappák vizsgálatának minősülnek.*

Ezen a panelen beállíthatja az adott keresés következő paramétereit:

Az ütemezett feladat futtatása

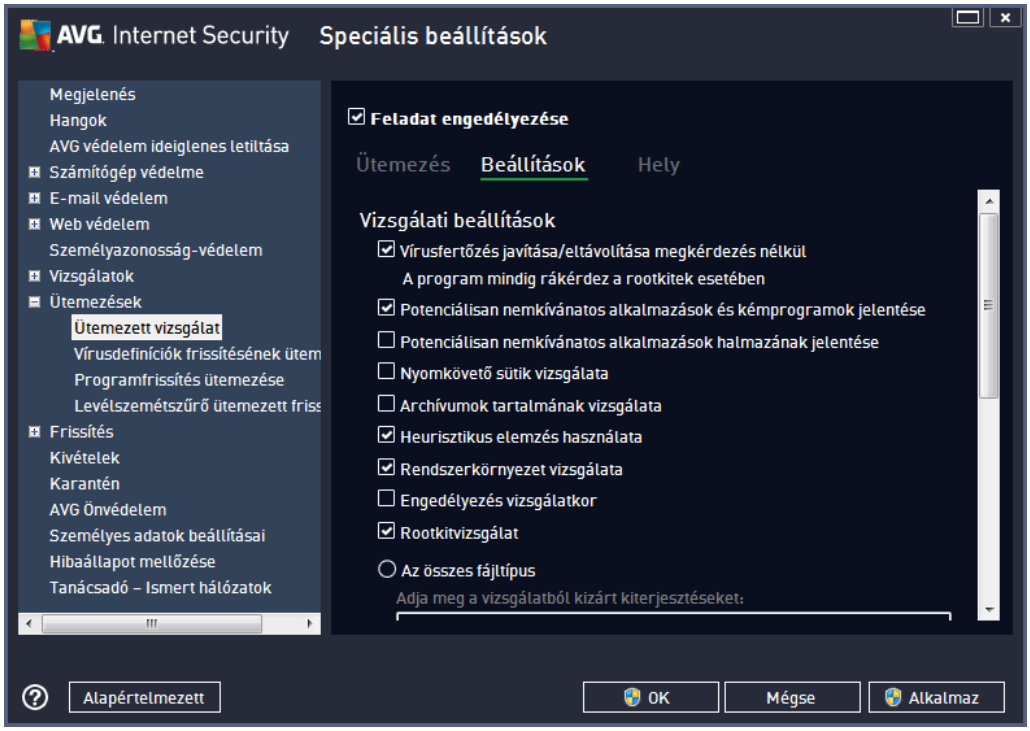
Itt megadhatja, hogy az ütemezett vizsgálatok milyen időközönként fussanak le. Az ütemezés megadható bizonyos időközönként indított ismételt vizsgálatok futtatásával (***Futtatás a következő időközönként:***), vagy egy pontos dátum és időpont megadásával (***Futtatás egy megadott időpontban...***), illetve megadható egy adott eseményhez hozzárendelve is (***Futtatás a számítógép***

indításakor).

Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a vizsgálat mely körülmények között induljon/ne induljon, például ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva. Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy felugró ablakban az AVG tálcaikonjánál.

Egy új AVG tálcaikon jelenik meg (*színes ikon egy zseblámpával*), és tájékoztatja arról, hogy egy ütemezett vizsgálat éppen folyamatban van. Kattintson az egér jobb gombjával az AVG ikonjára egy helyi menü megnyitásához, ahol felfüggesztheti vagy leállíthatja a futó vizsgálatot, illetve megváltoztathatja annak prioritását.



A ***Beállítások*** lapon a vizsgálati paraméterek listáját találhatja, amelyeket tetszőlegesen be- és kikapcsolhat. Alapértelmezés szerint a legtöbb paraméter be van kapcsolva, és működni fog a vizsgálat során. ***Javasoljuk, hogy tartsa meg az alapértelmezett beállításokat, és csak akkor módosítson rajtuk, ha feltétlenül szükséges***:

- ***Fertőzés javítása/eltávolítása kérdés nélkül*** *(alapértelmezés szerint bekapcsolva):* ha a rendszer vírust talál a vizsgálat során, akkor azt automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl automatikusan nem javítható, az objektumot áthelyezi a Karanténba.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** *(alapértelmezés szerint bekapcsolva):* jelölje be a kémprogramok és vírusok kereséséhez.

A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*): jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért a funkció alapértelmezés szerint ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** (*alapértelmezés szerint kikapcsolva*): ez a paraméter meghatározza, hogy a rendszer észlelje-e a cookie-kat a vizsgálat során (*a HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*)

- ***Archívumok tartalmának vizsgálata*** (*alapértelmezés szerint bekapcsolva*): ez a paraméter meghatározza, hogy vizsgálatkor a program ellenőrizze-e az archívumokban (például ZIP, RAR, stb.) tárolt fájlokat is.

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*): a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*): a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Engedélyezés vizsgálatkor*** (*alapértelmezés szerint kikapcsolva):* bizonyos esetekben (*például ha vírusfertőzésre gyanakszik*) ezzel a beállítással aktiválhatja a legalaposabb vizsgálati algoritmusokat, amelyek még a számítógép ritkán megfertőzhető részeit is ellenőrzik a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Rootkitek keresése*** *(alapértelmezés szerint bekapcsolva): a* Rootkitkereső lehetséges rootkiteket, vagyis olyan programokat és technológiákat keres a számítógépen, amelyek kártékony tevékenységeket rejthetnek el. Ha a program rootkitet észlel, akkor az nem jelenti automatikusan azt, hogy a számítógép fertőzött. Bizonyos esetekben a program egyes eszközillesztőket, vagy legitim alkalmazások részeit is – tévesen – rootkitként észlel.

El kell döntenie továbbá, hogy a program mely fájlokat vizsgálja

- ***Az összes fájltípus*** kivételek megadásánál lehetőségével. Ezen fájlkiterjesztéseket vesszővel válassza el (*mentés után a vesszők pontosvesszőkre változnak*);

- ***Kiválasztott fájltípusok*** – megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek fertőzöttek lehetnek (*a nem fertőzhető fájlokat, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem ellenőrzi a program*), pl. médiafájlok (*video-, audiofájlok – ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg azokat*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

- Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** – ez az opció

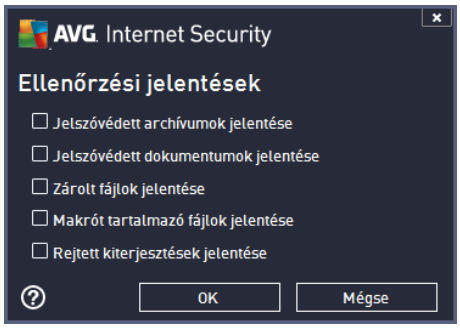
alapértelmezés szerint be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell azokat.

A vizsgálati sebesség beállítása

Ebben a részben hangolhatja a vizsgálat sebességét a rendszer erőforrásainak függvényében. Alapállapotban ez az érték *felhasználófüggő* automatikus erőforrás-használati szintre van állítva. Ha azt szeretné, hogy a vizsgálat gyorsabban fusson, akkor kevesebb idő szükségeltetik, de a rendszererőforrások használata jelentősen megnő, és lelassíthatja a PC-n zajló egyéb tevékenységeket (*ezt az opciót akkor használhatja, ha a számítógép be van kapcsolva, és senki nem dolgozik rajta jelenleg*). Másrészt csökkentheti a rendszererőforrások használatát, de ez a vizsgálathoz szükséges idő növekedésével jár.

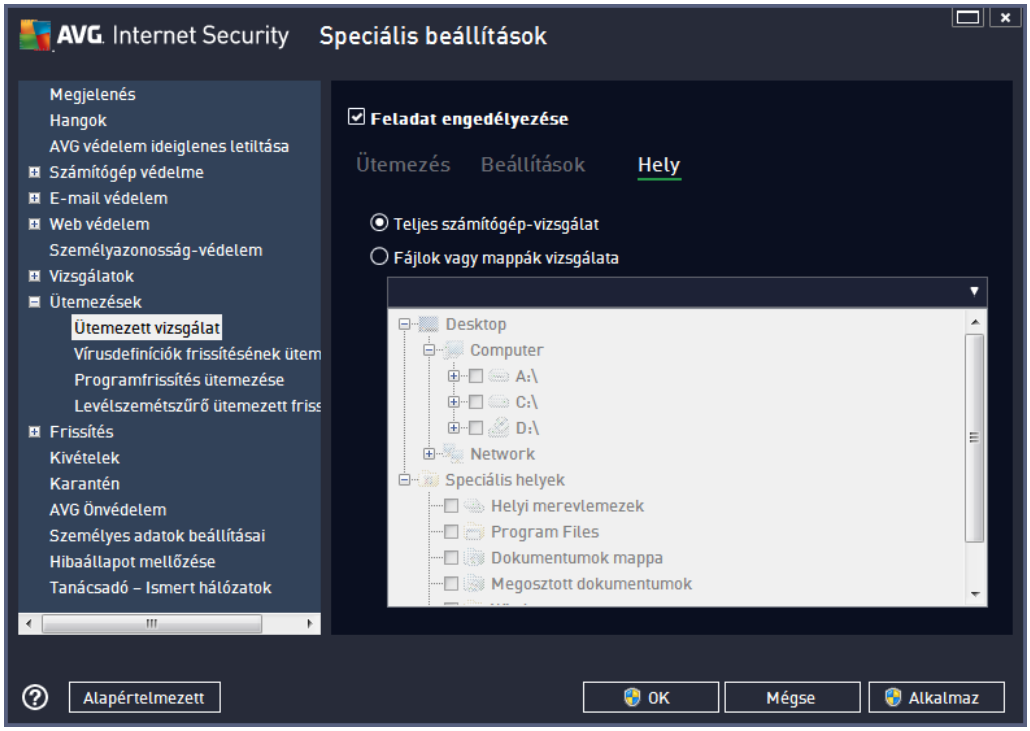
További vizsgálati jelentések beállítása

Kattintson a ***További vizsgálati jelentések...*** hivatkozásra a ***Vizsgálati jelentések*** panel megnyitásához, ahol számos opciót jelölhet be azzal kapcsolatban, hogy a programnak mit kell jelentenie:



Számítógép kikapcsolásának beállításai

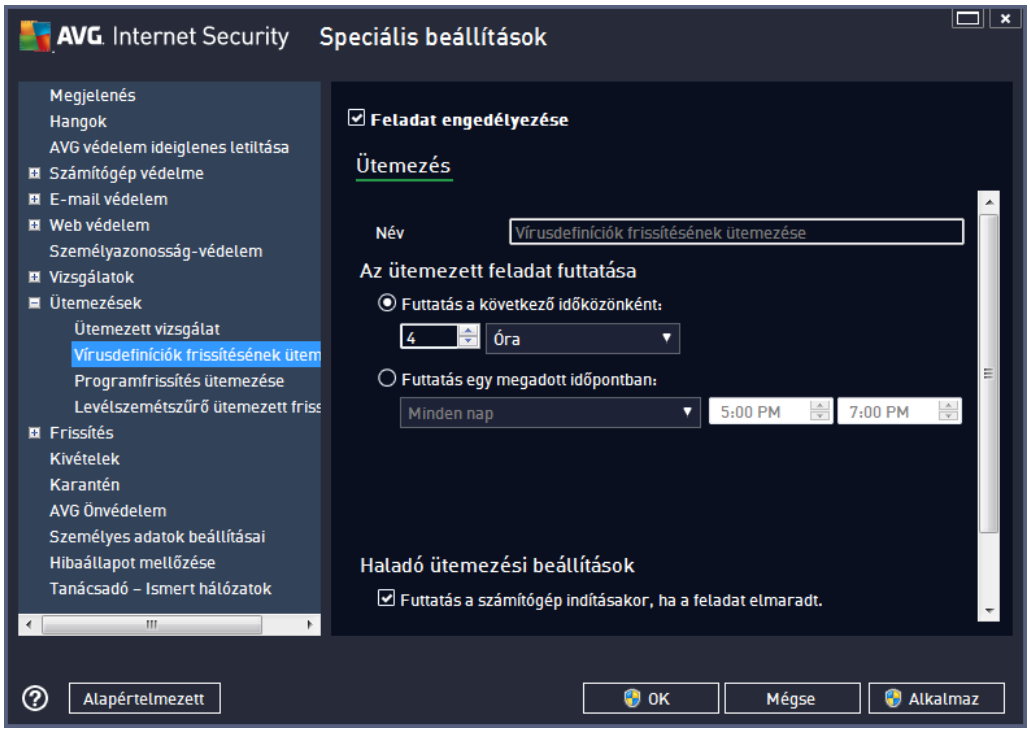
A számítógép kikapcsolásának beállításai szakaszon eldöntheti, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (***Számítógép kikapcsolása a vizsgálat befejezésekor***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Leállítás akkor is, ha a számítógép zárolva van***).



A ***Hely*** lapon meghatározhatja, hogy a számítógép teljes vizsgálatát vagy csak bizonyos fájlok és mappák vizsgálatát szeretné ütemezni. Ha a bizonyos fájlok és mappák vizsgálatát választja, akkor a panel alsó részén a fastruktúra aktiválódik és bejelölheti az ellenőrzendő mappákat.

9.9.2. Vírusdefiníciók frissítésének ütemezése

Ha ***valóban szükséges***, kikapcsolhatja a ***Feladat engedélyezése*** elemet az ütemezett vírusdefiníció-frissítés ideiglenes letiltásához, majd később újra bekapcsolhatja azt:



Ebben az ablakban megadhatja a definíciófrissítés ütemezésének részletes paramétereit. A ***Név*** mező (*kikapcsolva az alapértelmezett ütemezéseknél*) mutatja a program gyártója által létrehozott nevet ezen ütemezéshez.

Az ütemezett feladat futtatása

Ebben a részben adhatja meg, hogy az újonnan ütemezett vírusdefiníció-frissítés milyen gyakran induljon el. Az ütemezést meghatározhatja a rendszeresen történő futtatással (***Futattás minden ...***), dátummal és időponttal (***Futtatás meghatározott időben ...***).

Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a vírusdefiníció-frissítés milyen körülmények között induljon el vagy ne induljon el, ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

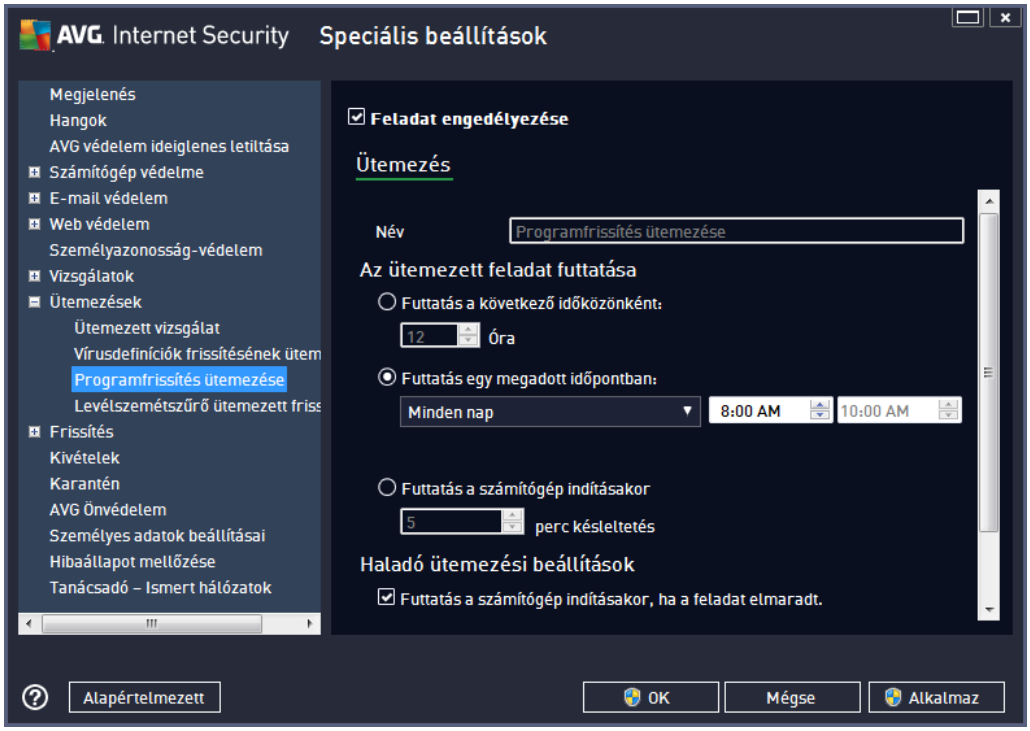
Egyéb frissítési beállítások

Végül jelölje be a ***Futtassa a frissítést újra, amint lesz internetkapcsolat*** lehetőséget, hogy ha az internetkapcsolat megszakad, és a frissítés sikertelen, akkor a folyamat újra lefusson, miután az internetkapcsolat helyreállt. Miután az ütemezett frissítés elindult a megadott időben, erről értesítést

kap egy előugró ablakban az AVG tálcaikonjánál (*feltéve, hogy megtartotta a Speciális beállítások/ Megjelenés panel alapértelmezett beállításait).*

9.9.3. Programfrissítés ütemezése

Ha ***valóban szükséges***, kikapcsolhatja a ***Feladat engedélyezése*** elemet az ütemezett programfrissítés ideiglenes letiltásához. Később újra bekapcsolhatja azt:



A ***Név*** mező (*kikapcsolva az alapértelmezett ütemezéseknél*) mutatja a program gyártója által létrehozott nevet ezen ütemezéshez.

Az ütemezett feladat futtatása

Adja meg, hogy az újonnan ütemezett programfrissítés milyen időközönként fusson le. Az ütemezést meghatározhatja a rendszeresen történő futtatással (***Futtatás minden ...***), dátummal és időponttal (***meghatározott időben ...***), vagy egy adott eseményhez kötheti (***Futtatás számítógép indításakor***).

Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a programfrissítés mely körülmények között induljon/ne induljon (például ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

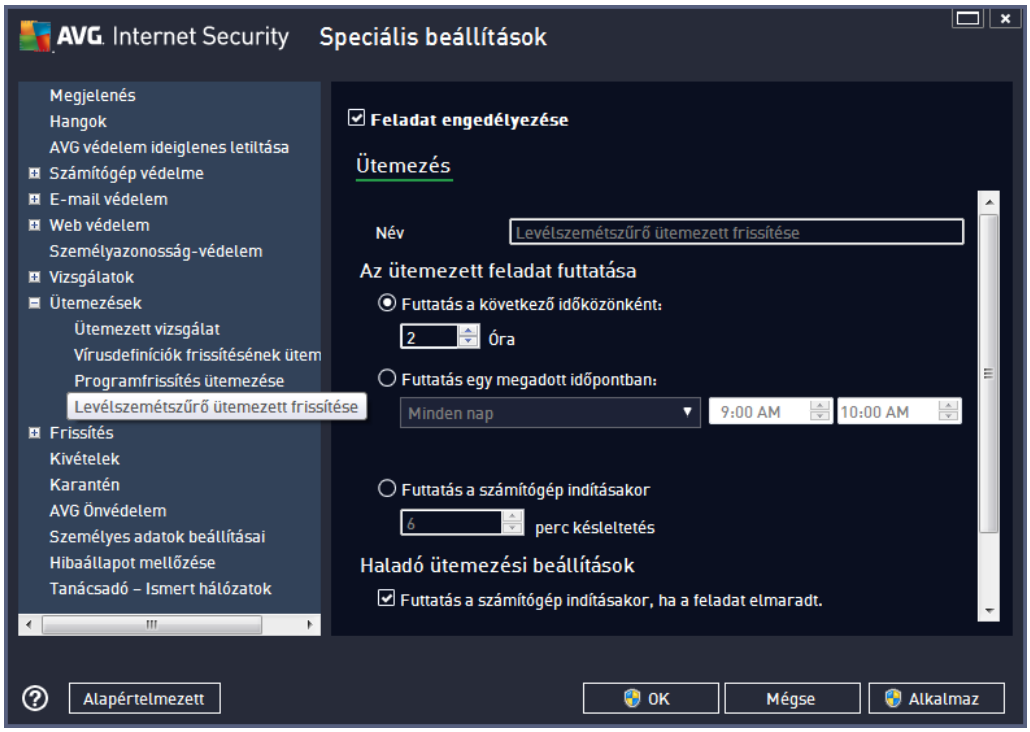
Egyéb frissítési beállítások

Jelölje be a ***Futtassa a frissítést újra, amint lesz internetkapcsolat*** lehetőséget, hogy ha az internetkapcsolat megszakad, és a frissítés sikertelen, akkor a folyamat újra lefusson, miután az internetkapcsolat helyreállt. Miután az ütemezett frissítés elindult a megadott időben, erről értesítést kap egy előugró ablakban az AVG tálcaikonjánál (*feltéve, hogy megtartotta a Speciális beállítások/ Megjelenés panel alapértelmezett beállításait).*

Megjegyzés: *Ha az ütemezett programfrissítés és az ütemezett vizsgálat időben egybeesik, akkor a frissítési folyamatnak van elsődleges prioritása, és a vizsgálat meg lesz szakítva.*

9.9.4. Levélszemétszűrő frissítési ütemezése

Ha valóban szükséges, kikapcsolhatja a ***Feladat engedélyezése*** elemet az ütemezett Levélszemétszűrés frissítésének ideiglenes letiltásához, majd később újra bekapcsolhatja azt:



Ebben az ablakban megadhatja a frissítési ütemezés részletes paramétereit. A ***Név*** mező (*kikapcsolva az alapértelmezett ütemezéseknél*) mutatja a program gyártója által létrehozott nevet ezen ütemezéshez.

Az ütemezett feladat futtatása

Itt az időközt adhatja meg a Levélszemétszűrő újonnan létrehozott frissítési ütemezéseihez. A Levélszemétszűrő ütemezése megadható bizonyos időközönként indított ismételt frissítés futtatásával (***Futtatás a következő időközönként...***), vagy egy pontos dátum és időpont megadásával (***Futtatás egy megadott időpontban***), illetve megadható egy adott eseményhez hozzárendelve is (***A számítógép indításán alapuló művelet***).

Haladó ütemezési beállítások

Ebben a részben meghatározhatja, hogy a Levélszemétszűrő frissítése milyen körülmények között induljon el vagy ne induljon el, ha a számítógép energiatakarékos módban van, vagy teljesen ki van kapcsolva.

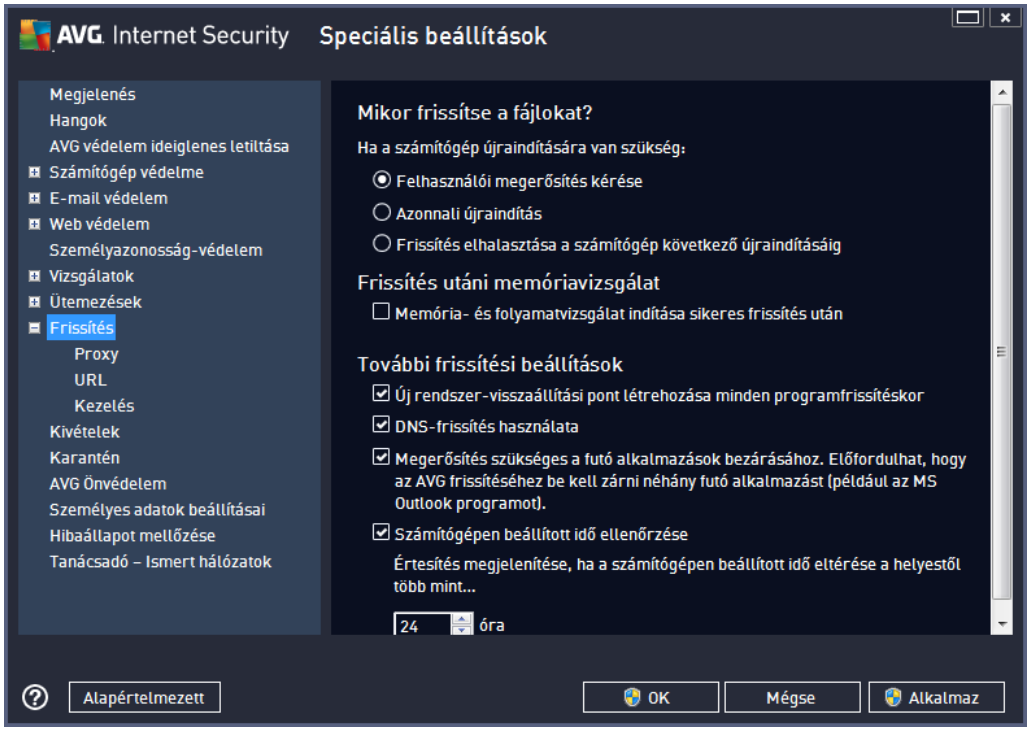
Egyéb frissítési beállítások

Jelölje be a ***Futtassa a frissítést újra, amint lesz internetkapcsolat*** lehetőséget, ha azt szeretné, hogy ha az internetkapcsolat megszakad, és a Levélszemétszűrő frissítése sikertelen, akkor a folyamat újra lefusson, miután az internetkapcsolat helyreállt.

Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy előugró ablakban az AVG tálcaikonjánál (*feltéve, hogy megtartotta a Speciális beállítások/Megjelenés panel alapértelmezett konfigurációit).*

9.10. Frissítés

A ***Frissítés*** navigációs elem egy új ablakot nyit meg, ahol általános paramétereket adhat meg az AVG frissítésekkel kapcsolatban:



Mikor frissítse a fájlokat?

Ezen a részen három különböző lehetőség közül választhat, ha a frissítési folyamathoz újra kell indítania a számítógépet. A frissítés befejezését ütemezheti a számítógép következő újraindítására, vagy akár azonnal is kezdeményezheti az újraindítást:

- ***Felhasználói megerősítés szükséges*** *(alapértelmezett)* – A program felszólítja a

számítógép újraindítására a frissítési folyamat befejezéséhez

- ***Azonnali újraindítás*** – A program azonnal és automatikusan újraindítja a számítógépet, miután a frissítési folyamat befejeződött (nem szükséges az Ön hozzájárulása)

- ***Befejezés a számítógép következő újraindításakor*** – A frissítési folyamat befejezése a számítógép következő újraindításakor történik meg. Vegye figyelembe, hogy ez az opció csak akkor javasolt, ha a számítógépet rendszeresen újraindítja (naponta legalább egyszer).

Frissítés utáni memóriavizsgálat

Jelölje be ezt a négyzetet, ha új memóriavizsgálatot kíván elindítani minden egyes sikeresen befejezett frissítés után. A letöltött frissítés új vírusdefiníciókkal rendelkezhet és azonnal használható a vizsgálat során.

További frissítési opciók

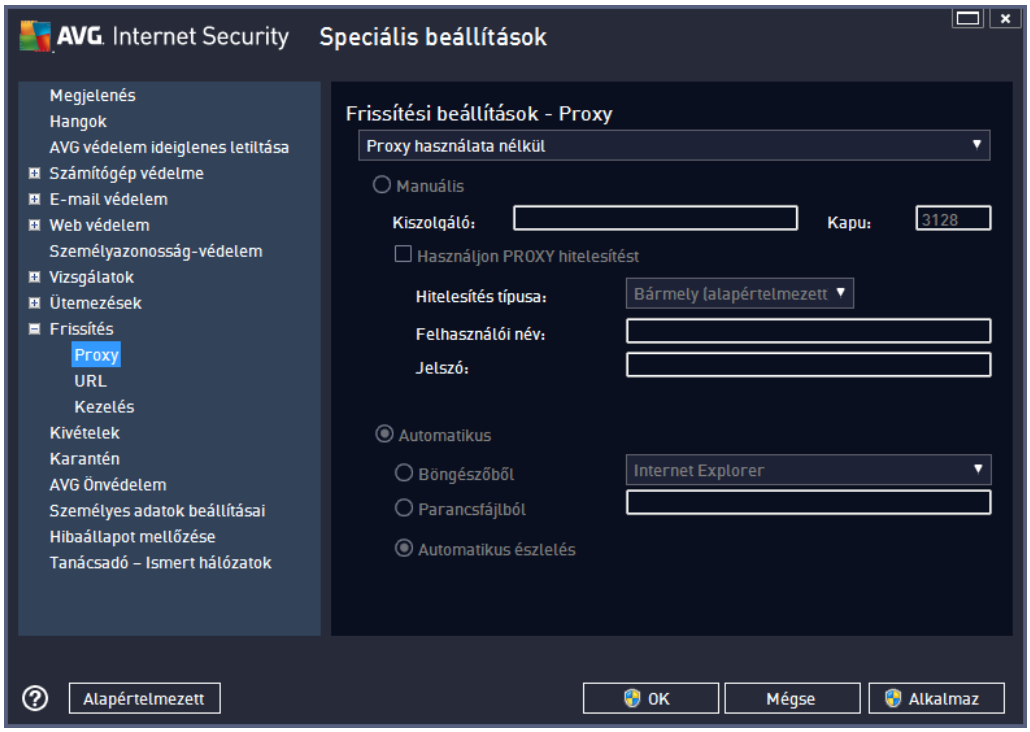
- ***Új rendszer-visszaállítási pont létrehozása programfrissítéskor*** – mielőtt az AVG programfrissítés lefutna, egy rendszer-visszaállítási pont lesz létrehozva. Ha a frissítési folyamat sikertelen, és az operációs rendszer összeomlik, akkor mindig visszaállíthatja a rendszert a korábbi állapotra. Az opció elérhető a Start / Minden program / Kellékek / Rendszereszközök / Rendszer-visszaállítás menüből, de a módosítás csak tapasztalt felhasználóknak javasolt! Hagyja bejelölve ezt az elemet, ha használni akarja a funkciót.

- ***DNS-frissítés használata*** (*alapértelmezés szerint bekapcsolva*) – ha bejelöli ezt a lehetőséget, akkor a frissítés indításakor az **AVG Internet Security 2013** megkeresi a legújabb vírusadatbázist és programverziót a DNS-kiszolgálón. Ekkor csak a legkisebb méretű, feltétlenül szükséges frissítőfájlok töltődnek le és települnek. Így a letöltendő teljes adatmennyiség minimalizálható, és a frissítési folyamat is gyorsabb lesz.

- ***A Megerősítés szükséges a futó alkalmazások bezárásához*** (*alapértelmezés szerint bekapcsolva*) – elem bejelölésével biztosíthatja, hogy egyetlen futó alkalmazást se zárhasson be a program az Ön engedélye nélkül – ha ez szükséges a frissítési folyamat befejezéséhez.

- ***Számítógépen beállított idő ellenőrzése*** – Jelölje be ezt a lehetőséget, amennyiben szeretne értesítést kapni arról, ha a számítógépen beállított idő a megadottnál jobban eltér a tényleges időtől.

9.10.1. Proxy



A proxy kiszolgáló egy különálló kiszolgáló vagy egy számítógépen futó szolgáltatás, amely közvetett hozzáférést nyújt az internethez. A megadott hálózati szabályoknak megfelelően közvetlenül, vagy egy proxykiszolgálón keresztül csatlakozhat az Internethez; illetve a kétfajta csatlakozás egyidejűleg is történhet. A ***Frissítési beállítások – Proxy*** ablak fenti részében választania kell a következőkből:

- ***Proxy használata nélkül*** – alapértelmezett beállítások
- ***Proxy használata***
- ***Csatlakozás megkísérlése proxy használatával. Ha sikertelen, akkor csatlakozzon közvetlenül***

Ha proxy kiszolgálóval választja bármelyik opciót, akkor további adatokat kell megadnia. A kiszolgálóbeállításokat manuálisan vagy automatikusan is megadhatja.

Manuális beállítás

Ha a manuális beállítást választja (jelölje be a ***Manuális*** *opciót az adott elem aktiválásához*), akkor a következőket kell megadnia:

- ***Kiszolgáló*** – a kiszolgáló IP-címe vagy neve
- ***Port*** – az internetkapcsolatot szolgáltató port száma (*(alapértelmezés szerint ez a szám a 3128, de az értéket meg lehet változtatni – ha bizonytalan, forduljon a hálózat rendszergazdájához*)

A proxykiszolgálónál az egyes felhasználókra különböző szabályok vonatkozhatnak. Ha így állítja be a proxy kiszolgálót, akkor jelölje be a ***Használjon PROXY hitelesítést*** opciót, hogy ellenőrizhesse, a kiszolgálón keresztüli internetcsatlakozáshoz megadott felhasználónév és jelszó megfelelő.

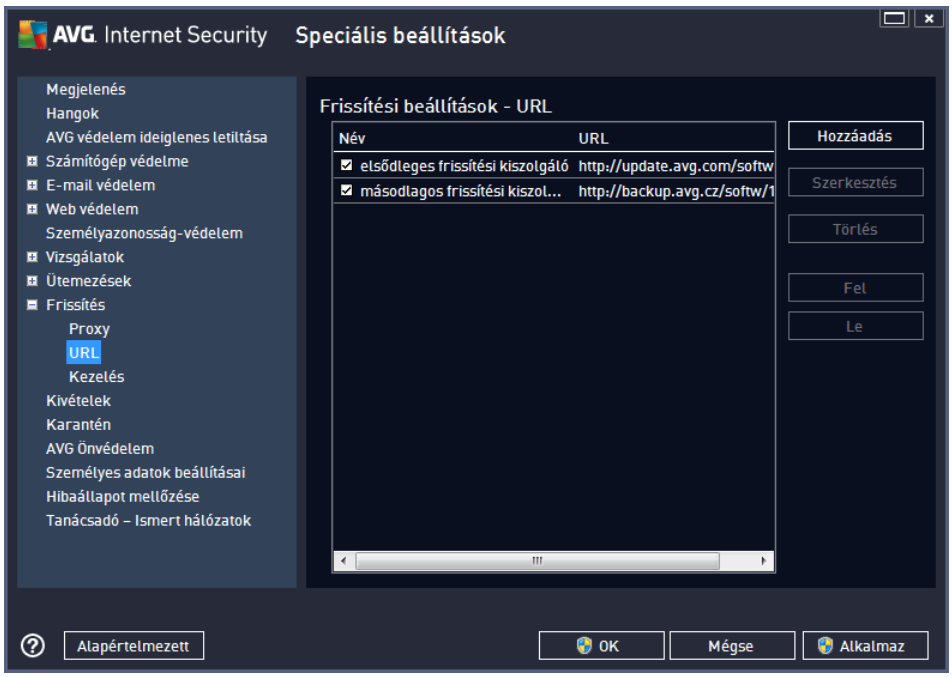
Automatikus beállítás

Ha az automatikus beállítást választja (*jelölje be az **Automatikus** opciót az aktiválásához*), akkor válassza ki, hogy a proxybeállítások honnan legyenek átvéve:

- ***Böngészőből*** – a programbeállításokat az alapértelmezett internetböngészőből olvassa be
- ***Parancsfájlból*** – a beállítások egy proxy címet adó, letöltött parancsfájlból lesznek beolvasva.
- ***Automatikus észlelés*** – beállítások automatikus felismerése a proxy kiszolgálóból

9.10.2. URL

Az ***URL*** párbeszédpanel azon internetes címek listáját tartalmazza, ahonnan a frissítési fájlok letölthetők:



Vezérlőgombok

A lista és a lista elemeinek megváltoztatása a következő kezelőgombokkal történik:

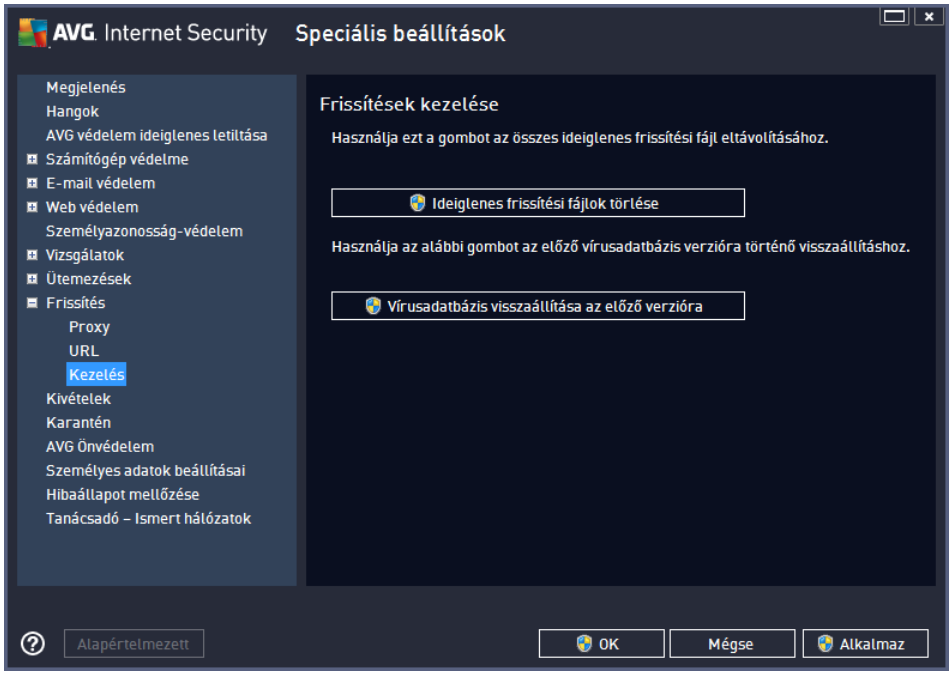
- ***Hozzáadás*** – egy új párbeszédpanelt nyit meg, ahol új URL címeket adhat a listához
- ***Szerkesztés*** - egy párbeszédpanelt nyit meg, ahol módosíthatja a kijelölt URL

paramétereit

- ***Törlés*** – a kijelölt URL törlése a listából
- ***Fel*** – a kijelölt URL előrébb mozdítása a listában egy hellyel
- ***Le*** – a kijelölt URL hátrébb mozdítása a listában egy hellyel

9.10.3. Kezelés

A ***Frissítések kezelése*** párbeszédpanelről két lehetőség érhető el, mégpedig két gomb segítségével:

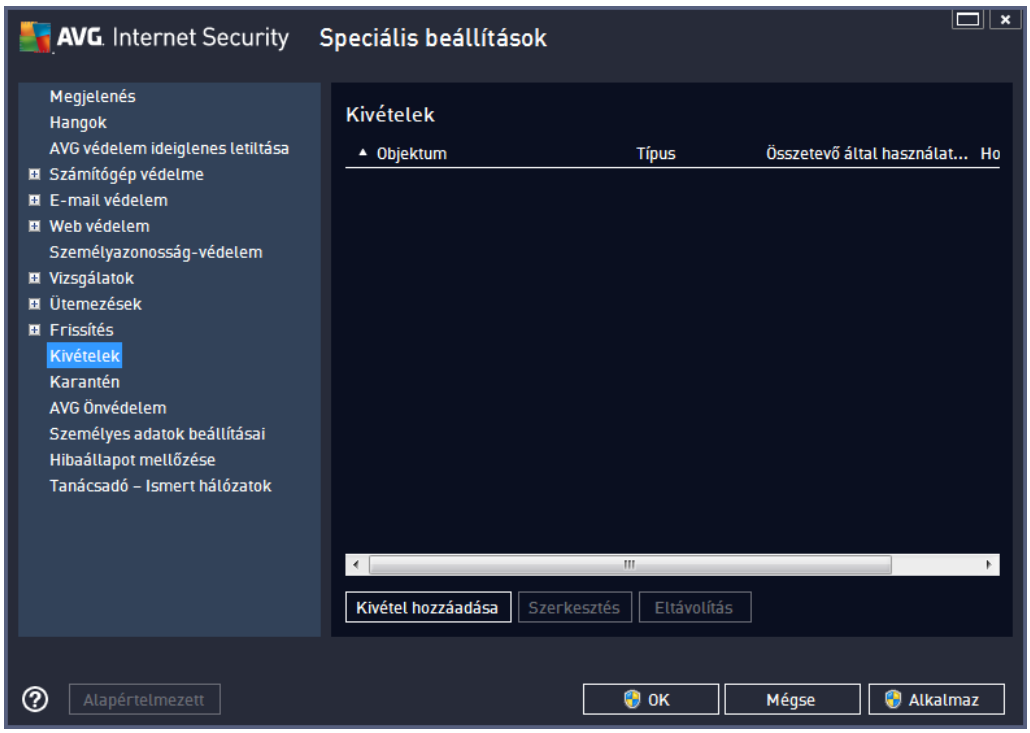


- ***Ideiglenes frissítési fájlok törlése*** – nyomja meg ezt a gombot az összes szükségtelen frissítési fájl törléséhez a merevlemezről (*ezeket a rendszer alapértelmezés szerint 30 napig tárolja*)
- ***Vírusadatbázis visszaállítása az előző verzióra*** – nyomja meg ezt a gombot az aktuális vírusadatbázis törléséhez, és az előző mentett verzióhoz történő visszatéréshez (*az új adatbázis verzió a következő frissítéskor fog települni*)

9.11. Kivételek

A ***Kivételek*** párbeszédpanelen kivételeket, vagyis az **AVG Internet Security 2013** által figyelmen kívül hagyott elemeket adhat meg. Általában akkor kell kivételt megadnia, ha az AVG folyamatosan fenyegetésként észlel egy programot vagy fájlt, illetve egy biztonságos webhelyet veszélyesnek ítélve blokkol. Az ilyen fájlokat vagy webhelyeket adja hozzá a kivételek listájához, így az AVG nem jelenti és nem blokkolja többé ezeket.

Mindig győződjön meg arról, hogy a kérdéses fájl, program vagy webhely tényleg teljesen biztonságos legyen!



A párbeszédpanel táblázatában a kivételek listája található, ha már meg vannak határozva. Mindegyik elem mellett egy-egy jelölőnégyzet található. Ha a jelölőnégyzet be van jelölve, akkor a kivétel érvényben van; ha nincs bejelölve, akkor a kivétel meg van határozva, de jelenleg nincsen érvényben. Az oszlopok fejlécére történő kattintással az engedélyezett elemeket a megfelelő kritériumok szerint rendezheti.

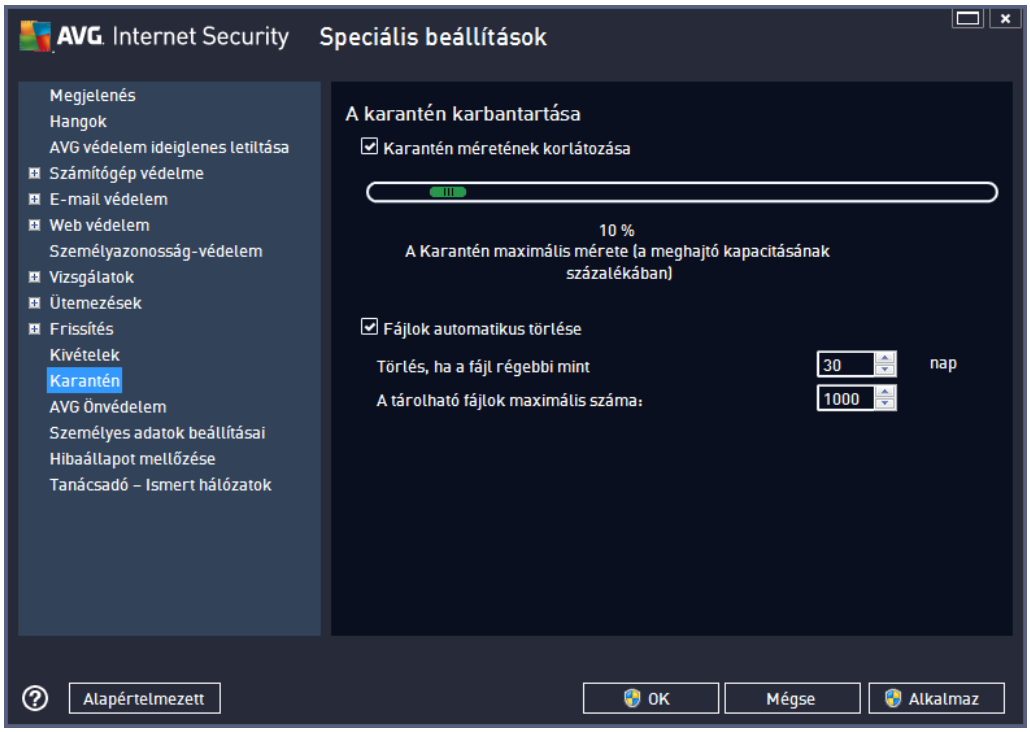
Vezérlőgombok

- ***Kivételek hozzáadása*** – Kattintson egy új párbeszédpanel megnyitásához, ahol lehetőség nyílik az AVG vizsgálat alól mentesülő elemek megadására. Először a program arra kéri, hogy határozza meg az objektum típusát, vagyis, hogy az egy fájl, mappa, vagy egy URL-cím. Ezt követően meg kell keresnie a lemezen, hogy megadja a megfelelő objektum elérési útvonalát vagy beírja az URL-címet. Végül kiválaszthatja, hogy mely AVG funkciók hagyják figyelmen kívül a kiválasztott objektumot *(Állandó védelem, Személyazonosság, Vizsgálat, Rootkitkereső)*.

- ***Szerkesztés*** – Ez a gomb csak akkor aktív, ha néhány kivételt már meghatározott, és azok szerepelnek a táblázatban. Ezt követően a gomb használatával megnyithatja a kiválasztott kivételhez tartozó szerkesztő párbeszédpanelt, és beállíthatja a kivétel paramétereit.

- ***Eltávolítás*** – A gomb használatával visszavonhat egy korábban meghatározott kivételt. Eltávolíthatja azokat egyenként, vagy kijelölheti a kivételek egy csoportját a listában és visszavonhatja a meghatározott kivételeket. Miután visszavonta a kivételt, az AVG ismét ellenőrzi a fájlt, mappát vagy URL-címet. Vegye figyelembe, hogy csak a kivétel lesz eltávolítva, maga a fájl vagy mappa nem!

9.12. Karantén

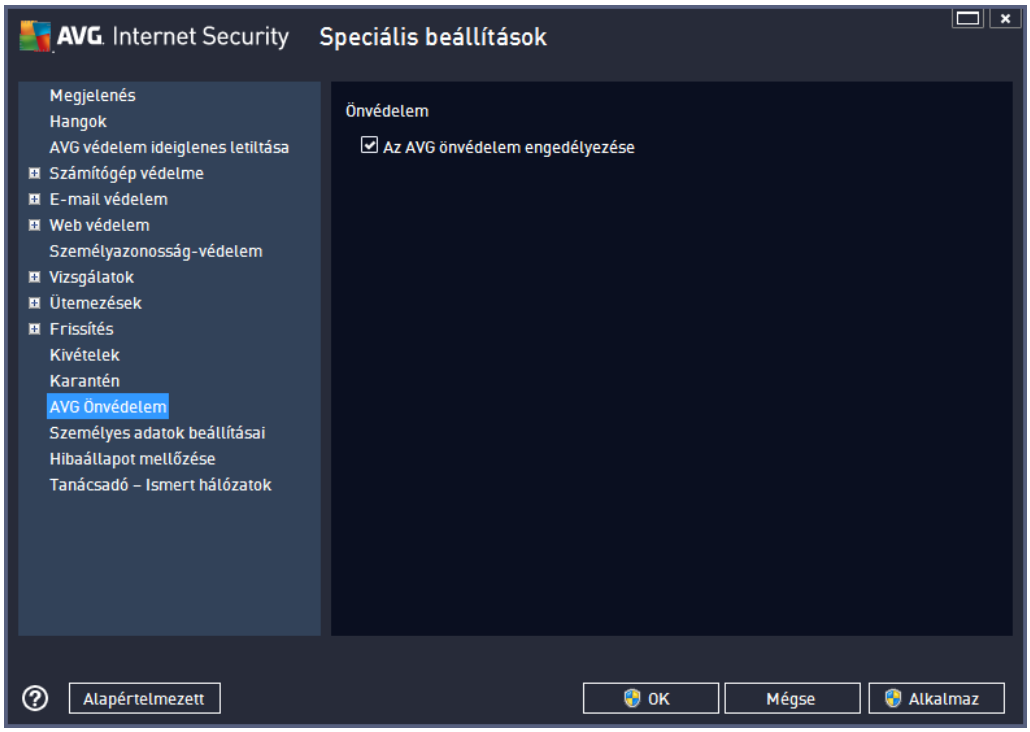


A ***Karantén karbantartása*** ablak lehetővé teszi, hogy számos paramétert határozzon meg a Karanténbantárolt objektumok kezelésével kapcsolatban:

- ***Karantén méretének korlátozása*** – használja a csúszkát a Karantén maximális méretének meghatározásához. Az alapértelmezett méret helyi lemez kapacitásának függvényében, azzal arányosan lesz meghatározva.

- ***Fájlok automatikus törlése*** – ebben a részben meghatározhatja azt az időtartamot, ameddig az objektum a Karanténban marad (***Törlés, ha a fájl régebbi mint ... nap***), illetve a Karanténban tárolható fájlok maximális számát (***Tárolható fájlok maximális száma***).

9.13. AVG önvédelem

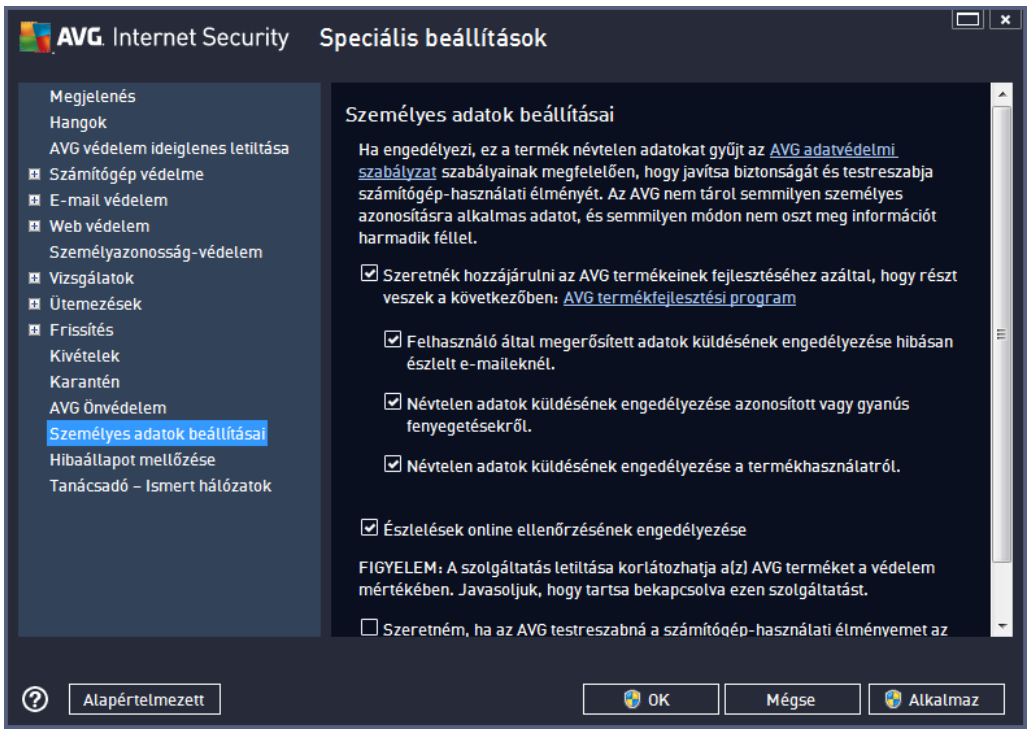


Az ***AVG önvédelem*** lehetővé teszi, hogy az **AVG Internet Security 2013** megvédje a saját folyamatait, fájljait, beállításkulcsait és illesztőprogramjait azok módosításával vagy inaktiválásával szemben. Az ilyen típusú védelem fő oka, hogy néhány kifinomult fenyegetés megpróbálja kikapcsolni a vírusvédelmet, hogy azután szabadon károsíthassa a számítógépet.

Javasolt bekapcsolva tartani ezt a szolgáltatást.

9.14. Személyes adatok beállításai

A ***Személyes adatok beállításai*** párbeszédpanel felkéri, hogy vegyen részt az AVG termékek fejlesztésében, illetve az online biztonság növelésében. A jelentései segítenek nekünk összegyűjteni a legfrissebb információkat a legújabb fenyegetésekről a világ számos pontján, és cserébe továbbfejlesztjük a védelmet mindenki számára. A jelentés teljesen automatikus, ezért nem okoz kényelmetlenséget. A jelentések semmilyen személyes azonosításra alkalmas adatot nem tartalmaznak. Az észlelt fenyegetések jelentése nem kötelező, de kérjük, hogy hagyja ezt a beállítást bekapcsolva, mivel így segít nekünk továbbfejleszteni a védelmet az Ön és más AVG felhasználók számára.



A párbeszédpanelen a következőkövetkezőket állíthatja be:

- ***Szeretnék hozzájárulni az AVG termékfejlesztéséhez az AVG Termékfejlesztési programban való részvétellel*** *(alapértelmezés szerint bekapcsolva)* – Ha szeretne segíteni az **AVG Internet Security 2013** továbbfejlesztésében, akkor hagyja bejelölve a jelölőnégyzetet. Ezzel engedélyezi az észlelt fenyegetések jelentését az AVG számára, így naprakész információkat tudunk gyűjteni a kártevőkről szerte a világon, és jobb védelmet biztosítunk mindenkinek. A jelentés teljesen automatikus, ezért nem okoz kényelmetlenséget, és semmilyen személyes azonosításra alkalmas adatot nem küld el.
    - ***Információk küldése a hibásan észlelt e-mailekről*** *(alapértelmezés szerint bekapcsolva)* – információkat küld a tévesen levélszemétként azonosított e-mailekről vagy az olyan levélszemétről, amelyeket a Levélszemétszűrő szolgáltatás nem észlelt. Ezen információk küldésekor a rendszer megerősítést kér.
    - ***Anonim adatok küldésének engedélyezése az észlelt vagy gyanús fenyegetésekről*** *(alapértelmezés szerint bekapcsolva)* – információkat küld a gyanús, veszélyes vagy szokatlan viselkedést mutató elemekről *(ezek lehetnek vírusok, kémprogramok vagy kártékony weboldalak)* .
    - ***Anonim adatok küldésének engedélyezése a termékhasználatról*** *(alapértelmezés szerint bekapcsolva)* – egyszerű statisztikai adatokat küld az alkalmazás használatáról, például észlelések száma, indított vizsgálatok, sikeres/sikertelen frissítések stb.
- ***Online ellenőrzések engedélyezése*** *(alapértelmezés szerint bekapcsolva)* – a rendszer a vakriasztások kiszűrése érdekében ellenőrzi az észlelt fenyegetéseket.

- ***Szeretném, ha az AVG testreszabná a számítógép-használati élményemet az AVG testreszabás bekapcsolásával*** – ez a szolgáltatás (név nélkül) elemzi a számítógépére telepített

programok és alkalmazások viselkedését. Ezen elemzés alapján az AVG kimondottan az igényeinek megfelelő szolgáltatást tud nyújtani, így teremti meg a maximális biztonságot az Ön számára.

Leggyakoribb fenyegetések

Ma az egyszerű vírusoknál sokkal bonyolultabb fenyegetések is léteznek. A kártékony kódok és a veszélyes weboldalak szerzői rendkívül innovatívak, és rendszeresen tűnnek fel újfajta fenyegetések (jelentős részük az interneten). A következők a legelterjedtebbek:

- ***A vírus*** olyan rosszindulatú kód, mely sokszorosítja önmagát, szétterjed a számítógépen, és gyakran észrevétlen marad egészen addig, amíg kárt nem okoz. Egyes vírusok komoly fenyegetést jelentenek, mivel fájlokat törölnek a lemezről, szándékosan módosítják azokat, míg más vírusok nem okoznak kárt, csak például folyamatosan zenét játszanak. Alapvetően mégis minden vírus veszélyes a sokszorozódási képessége miatt – még egy egyszerű vírus is pillanatok alatt képes megtölteni a számítógép memóriáját, és teljesen lebéníthatja azt.

- ***A féreg*** a vírusok egyik olyan fajtája, mely a vírustól eltérően semmilyen más „hordozóhoz" nem kapcsolódik, hanem egy az egyben küldi el saját magát más számítógépekre (általában e-mailben), és ezzel gyakran túlterheli az e-mail kiszolgálókat illetve a hálózati rendszereket.

- ***A kémprogram*** általában kártevőként kategorizálható (*kártevő = bármely rosszindulatú program, például vírusok*). A rejtőzködő program jellemzően trójai faló, amelynek célja, hogy személyes információkat (jelszavakat, hitelkártyaszámokat) szerezzen, illetve lehetővé tegye, hogy a számítógép feletti irányítást egy külső támadó távolról átvegye. Természetesen mindezt a felhasználó tudta, illetve hozzájárulása nélkül.

- ***A potenciálisan nemkívánatos programok*** olyan kémprogramok, melyek nem feltétlenül veszélyesek a számítógépre. A PUP-ra jó példa a reklámprogram, mely olyan kód, aminek célja reklámok terjesztése jellemzően felbukkanó ablakok formájában – bosszantó de nem feltétlenül káros módon.

- ***A nyomkövető sütik*** is egyfajta kémprogramnak minősülnek. Ezen apró fájlokat a rendszer a webböngészőben tárolja, és automatikusan elküldi a forrásoldalra a következő látogatáskor. A következő adatokat tartalmazhatják: böngészési előzmények vagy egyéb hasonló információk.

- ***Az exploit*** olyan kártékony kód, mely az operációs rendszer, az internetböngésző vagy egyéb fontos program hibáját illetve sérülékenységét használja ki

- ***Az adathalászat*** érzékeny és személyes adatok megszerzésére irányuló kísérlet, melynek során a támadó egy megbízható és jól ismert szervezet álcája mögé bújik. A potenciális áldozatokat általában nagy mennyiségben kiküldött e-mailben keresik meg, és arra kérik őket, hogy például frissítsék bankszámlával kapcsolatos adataikat. Ehhez csak egy adott hivatkozást kell követniük, amely egy hamis banki webhelyre vezet.

- ***A hoax*** olyan nagy mennyiségben kiküldött e-mail, amely veszélyes, pánikkeltő vagy egyszerűen csak idegesítő és haszontalan információkat tartalmaz. Számos feljebb ismertetett fenyegetés hoax e-maileket használ a terjedéshez.

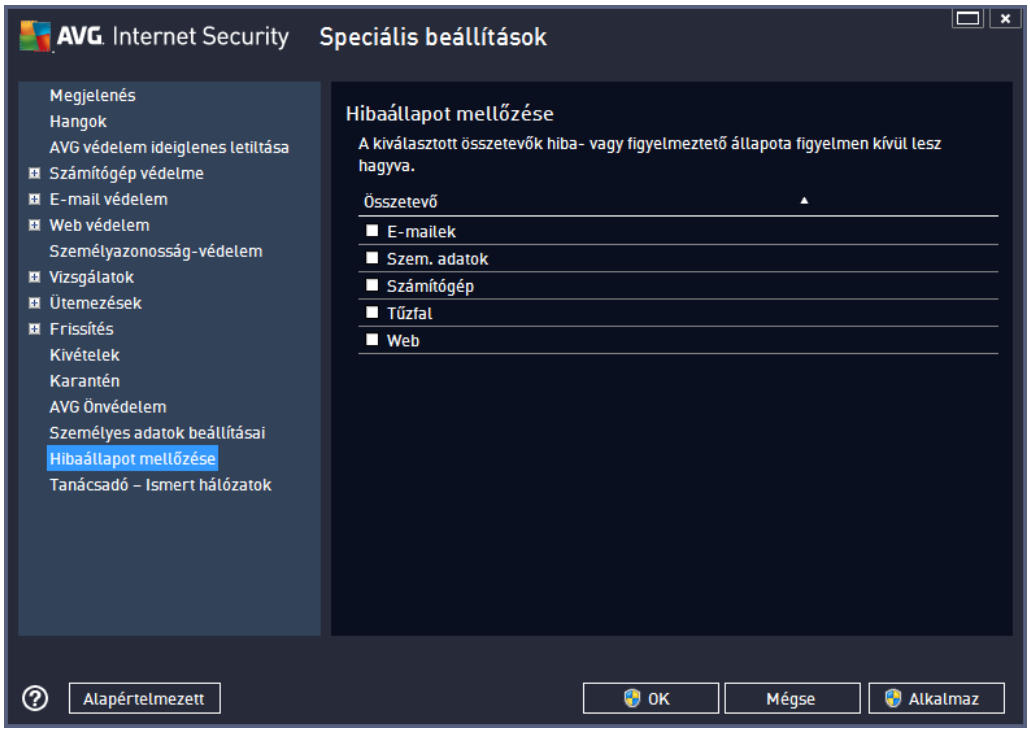
- ***A káros weboldalak*** szándékosan telepítenek kártékony kódot a felhasználó

számítógépére. A feltört oldalak ugyanezt csinálják, azzal a különbséggel, hogy ezek legitim oldalak, melyeket a látogatók megfertőzésére használnak fel.

Az összes fent felsorolt fenyegetés elleni védelem érdekében az AVG Internet Security 2013. az Összetevők áttekintése [című fejezetben ismertetett egyedi alprogramokat](#) tartalmazza.

9.15. Hibaállapot mellőzése

A ***Hibaállapot mellőzése*** párbeszédpanelen bejelölheti azon összetevőket, amelyekről nem akar értesítéseket kapni:



Alapállapotban egy összetevő sincs kiválasztva a listán. Ez azt jelenti, hogy ha valamelyik összetevő hibaállapotba lép, akkor Ön erről azonnal értesítést kap:

- [ikon a tálcán](#) – ha az AVG összes összetevője megfelelően működik, akkor az ikon négy színben jelenik meg. Viszont ha hiba történik, akkor az ikon sárga felkiáltójelre vált,
- a fennálló probléma szöveges leírása a [Biztonsági állapot információk](#) részen az AVG főablakán

Elképzelhető olyan szituáció, hogy valamilyen okból átmenetileg ki kell kapcsolnia egy összetevőt. ***Ez nem javasolt, az összes összetevőt bekapcsolva és az alapértelmezett konfigurációjában kell tartania***, de átmenetileg előfordulhat ilyen helyzet. Ekkor a tálcaikon automatikusan jelzi az összetevő hibaállapotát. Ebben az esetben viszont nem beszélhetünk tényleges hibáról, mivel az összetevőt Ön szándékosan kapcsolta ki, és tudatában van a biztonsági kockázatoknak. Ugyanakkor, mivel az ikon már szürkére váltott, nem tud további esetleges hibákat jelezni.

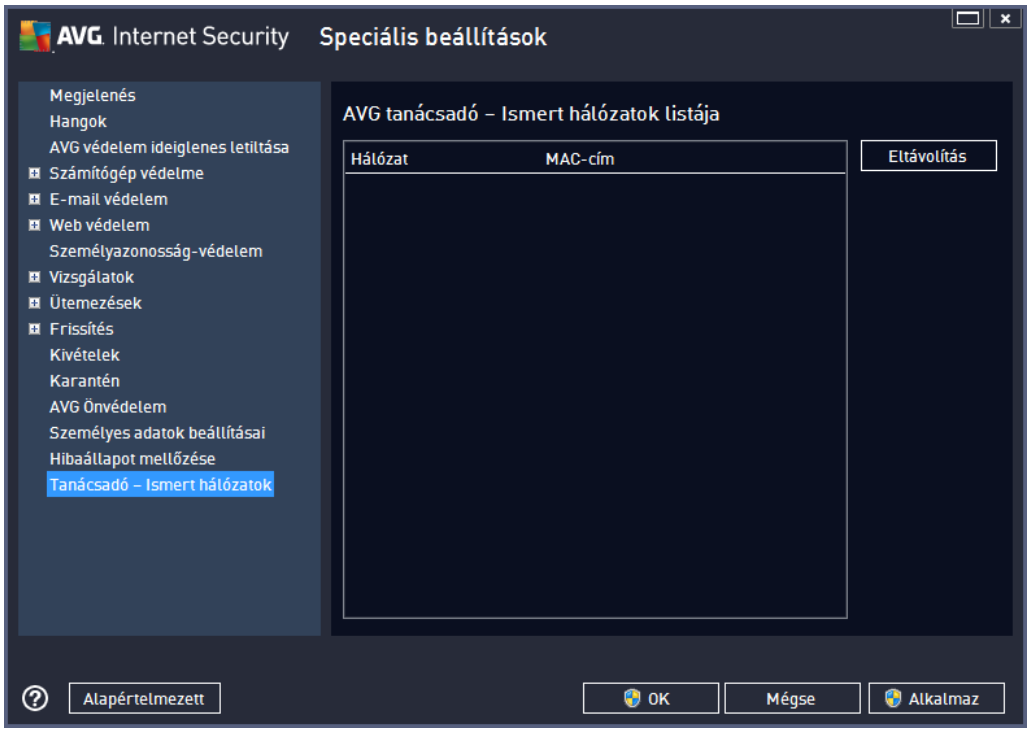
Ezért a ***Hibaállapot figyelmen kívül hagyása*** panelen kiválaszthatja azokat az összetevőket, amelyek hibaállapotban vannak (*vagy ki vannak kapcsolva*), és nem kíván értesítést kapni róluk.

Kattintson az ***OK*** gombra a megerősítéshez.

9.16. Tanácsadó – Ismert hálózatok

Az AVG Tanácsadó olyan szolgáltatást is tartalmaz, amely a csatlakozott hálózatokat figyeli, és ha új hálózatot észlel *(egy már használatban lévő hálózati névvel, ami félrevezető lehet)*, értesítést küld, és javasolja a hálózat biztonságosságának ellenőrzését. Ha úgy dönt, hogy az új hálózat biztonságos a csatlakozáshoz, mentheti azt erre a listára *(Az AVG tanácsadó rendszertálca-értesítésében található hivatkozáson keresztül, amely megjelenik a rendszertálca fölött, amint egy ismeretlen hálózatot észlel. A részletekért tekintse meg az AVG tanácsadó fejezetet)*. Az AVG tanácsadó ezután emlékezni fog a hálózat egyedi attribútumaira *(különösen a MAC-címre)*, és legközelebb nem jeleníti meg az értesítést. A rendszer minden olyan hálózatot, amelyhez kapcsolódik, ismert hálózatként kezel, és hozzáadja azokat a listához. Az egyes bejegyzéseket törölheti, ha megnyomja az ***Eltávolítás*** gombot; ezt követően az adott hálózatot a rendszer újra ismeretlenként és potenciálisan nem biztonságosként kezeli.

Ezen a párbeszédpanelen ellenőrizheti, mely hálózatokat tekint ismertnek a rendszer:



Megjegyzés: *A Windows XP 64 bites verziója nem támogatja az AVG tanácsadó ismert hálózatok szolgáltatását.*

10. Tűzfalbeállítások

A Tűzfal beállítások új ablakban nyílnak meg, ahol megadhatja az összetevő speciális beállításait. A Tűzfal beállításai új ablakban nyílnak meg, ahol több konfigurációs párbeszédpanelen szerkesztheti az összetevő speciális paramétereit. A konfiguráció egyszerű vagy szakértői módban is megjeleníthető. Amikor először lép be a konfigurációs ablakba, az egyszerű verzióban nyílik meg, és a következő paraméterek szerkesztését teszi lehetővé:

- Általános
- Alkalmazások
- Fájl- és nyomtatómegosztás

A párbeszédpanel alján található a ***Szakértői mód*** gomb. A gomb megnyomásával további navigációs elemeket jeleníthet meg a párbeszédpanelen, amelyekkel rendkívül speciális tűzfalbeállításokat hajthat végre:

- Speciális beállítások
- Megadott hálózatok
- Rendszerszolgáltatások
- Naplók

A szoftver szállítója beállította az összes AVG Internet Security 2013 összetevőt, hogy azok optimális teljesítményt nyújtsanak. Javasoljuk, hogy ne változtassa meg az alapértelmezett beállításokat, hacsak nem feltétlenül szükséges. A beállítások változtatását mindig hozzáértő felhasználó végezze!

10.1. Általános

Az ***Általános információ*** párbeszédpanel áttekintést biztosít az összes elérhető Tűzfal módról. Az aktuálisan kiválasztott Tűzfal mód megváltoztatható egy másik mód kiválasztásával a menüből.

A szoftver szállítója beállította az összes AVG Internet Security 2013 összetevőt, hogy azok optimális teljesítményt nyújtsanak. Javasoljuk, hogy ne változtassa meg az alapértelmezett beállításokat, hacsak nem feltétlenül szükséges. Bármely változtatást hozzáértő felhasználónak kell végeznie!

A Tűzfal lehetővé teszi, hogy meghatározzon bizonyos biztonsági szabályokat az alapján, hogy a számítógép egy tartományon belül helyezkedik el, különálló számítógép vagy notebook. E lehetőségek mindegyike más és más védelmi szintet kíván, és a szinteket a megfelelő üzemmódok fedik le. A Tűzfal üzemmód tehát a Tűzfal összetevő egy bizonyos konfigurációja, és számos előre meghatározott beállítást használhat.

- ***Automatikus*** – Ebben az üzemmódban a Tűzfal automatikusan kezeli az összes hálózati forgalmat. A program nem kéri, hogy döntéseket hozzon. A Tűzfal valamennyi ismert alkalmazás csatlakozásait engedélyezi, és egyidejűleg létrehoz egy szabályt az alkalmazáshoz, amely szerint az adott alkalmazás a későbbiekben mindig csatlakozhat. Más alkalmazások esetében a Tűzfal az alkalmazás viselkedése alapján dönti el, hogy engedélyezi vagy letiltja a csatlakozást. Ilyen esetben azonban nem jön létre a szabály, és a rendszer újra ellenőrzi az alkalmazást, amikor az kapcsolódni próbál. ***A legtöbb felhasználónak ez az automatikus, nem feltűnő mód ajánlott.***

- ***Interaktív*** – ez a mód akkor hasznos, ha teljes mértékben irányítani kívánja a számítógépre összes bejövő és kimenő hálózati forgalmát. A Tűzfal megfigyeli a forgalmat, és értesíti az összes kommunikációs és adatátviteli kísérletről, így tetszőlegesen engedélyezheti vagy blokkolhatja a kísérleteket. Csak képzett felhasználónak javasolt.

- ***Az internet elérésének blokkolása*** – az internetkapcsolat teljesen le van tiltva, az internet nem érhető el, és semmilyen külső felhasználó nem fér hozzá a számítógépéhez. Csak speciális és rövid idejű használatra szolgál.

- ***Tűzfalas védelem kikapcsolása*** – a Tűzfal kikapcsolása engedélyezi a számítógép minden bejövő és kimenő hálózati forgalmát. Ez a beállítás ezért sebezhetővé teszi a rendszert a hackertámadásokkal szemben. Mindig gondolja át körültekintően a beállítás használatát.

Vegye figyelembe, hogy a Tűzfalon belül egy speciális automatikus mód is elérhető. Ez a háttérben bekapcsol, ha vagy a Számítógép vagy az Személyazonosság-védelem összetevő ki van kapcsolva,

és a számítógépe emiatt sebezhetőbb. A Tűzfal ilyen esetben csak az ismert és a teljesen biztonságos alkalmazásokat engedélyezi automatikusan. Minden egyéb esetben felhasználói döntést fog kérni. Ennek célja, hogy ellensúlyozza a letiltott védelmi összetevőket, és hogy biztosítsa számítógépe biztonságát.

10.2. Alkalmazások

Az ***Alkalmazás*** panel felsorolja mindazon alkalmazásokat, amelyek már megpróbáltak a hálózaton kommunikálni, illetve megjeleníti a hozzájuk rendelt műveleteket:

Az ***Alkalmazások listája*** felületen a program által a számítógépen észlelt alkalmazások jelennek meg (*amelyekhez megfelelő műveleteket is rendelt a program*) . A következő művelettípusokat lehet használni:

- – kommunikáció engedélyezése az összes hálózaton
- – kommunikáció tiltása
- – megadott speciális beállítások

Vegye figyelembe, hogy csak már telepített alkalmazásokat ismer fel a program. Alapértelmezés szerint, ha egy új alkalmazás első alkalommal próbál csatlakozni a hálózatra, akkor a tűzfal automatikusan létrehoz egy szabályt a megbízható adatbázis alapján, vagy Önnek kell eldöntenie, hogy engedélyezi-e vagy letiltja a kommunikációt. Az utóbbi esetben válaszát elmentheti állandó szabályként (amely megjelenik ezen a panelen).

Természetesen azonnal létrehozhat szabályokat az új alkalmazásokhoz – nyomja meg ezen a panelen a ***Hozzáadás*** gombot, és adja meg az alkalmazás részleteit.

Az alkalmazásokat leszámítva a lista két külön elemet tartalmaz. Az ***Elsődleges alkalmazásszabályok*** (*a lista tetején*) tetszőlegesek, és mindig az alkalmazásszabályok előtt

kerülnek alkalmazásra. ***Az Egyéb alkalmazásszabályokat*** (*a lista alján*) utolsóként alkalmazza a rendszer, ha semmilyen más szabály nem lép érvénybe, pl. ismeretlen vagy nem meghatározott alkalmazások esetén. Válassza ki az elindítandó műveletet, amikor egy ilyen alkalmazás a hálózaton keresztül próbál meg kommunikálni: Tiltás *(mindig tiltja a kommunikációt)*, Engedélyezés *(a kommunikáció bármely hálózaton engedélyezett)*, Rákérdez *(a program megkérdezi, hogy engedélyezze vagy tiltsa a kommunikációt)*. ***Ezen elemek más beállításokkal rendelkeznek, mint a normál alkalmazások, és módosításukat csak tapasztalt felhasználóknak javasoljuk. Javasoljuk, hogy ne módosítsa a beállításokat.***

Vezérlőgombok

A lista szerkesztése a következő kezelőgombokkal történik:

- ***Hozzáadás*** – megnyit egy üres párbeszédpanelt új alkalmazásszabályok meghatározásához.
- ***Szerkesztés*** – megnyitja ugyanezen párbeszédpanelt egy meglévő alkalmazás-szabálykészlet szerkesztéséhez.
- ***Törlés*** – a kijelölt alkalmazás törlése a listából.

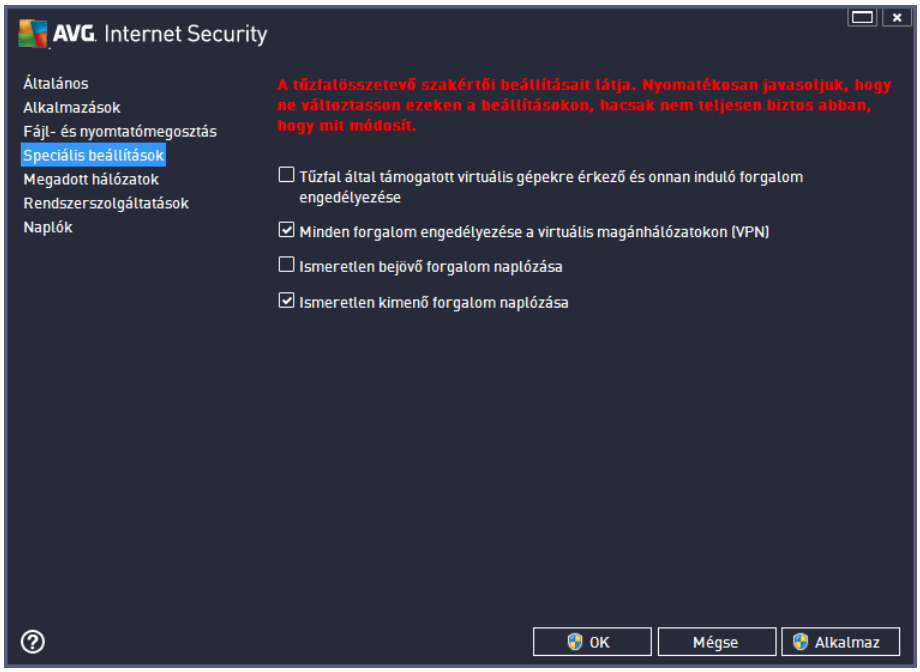
10.3. Fájl- és nyomtatómegosztás

A fájl- és nyomtatómegosztás valójában olyan fájlok vagy mappák megosztását jelenti, amelyeket „Megosztott” állapotúnak jelöl meg Windows rendszeren, közös lemezegységeken, nyomtatókon, szkennereken és minden hasonló eszközön. Az ilyen elemek megosztása csak biztonságosnak ítélt hálózatokon kívánatos *(például otthon, munkahelyen vagy az iskolában)*. Ha azonban nyilvános hálózathoz csatlakozik *(például repülőtéri Wi-Fi hálózathoz vagy internetkávézó hálózatához)*, célszerű, ha semmit nem oszt meg. Az AVG Tűzfal könnyedén képes letiltani vagy engedélyezni a megosztást, és lehetővé teszi a már használt hálózatok beállításainak mentését.

A ***Fájl- és nyomtatómegosztás*** párbeszédpanelen szerkesztheti a fájl- és nyomtatómegosztás és az aktuálisan csatlakozott hálózatok konfigurációját. Windows XP operációs rendszeren a hálózat neve az adott hálózathoz való első csatlakozáskor választott elnevezésnek felel meg. A Windows Vista és az újabb rendszerek automatikusan átveszik a hálózat nevét a Hálózati és megosztási központból.

10.4. Speciális beállítások

Bármely beállítás módosítása a Speciális beállítások panelen CSAK TAPASZTALT FELHASZNÁLÓK RÉSZÉRE javasolt.

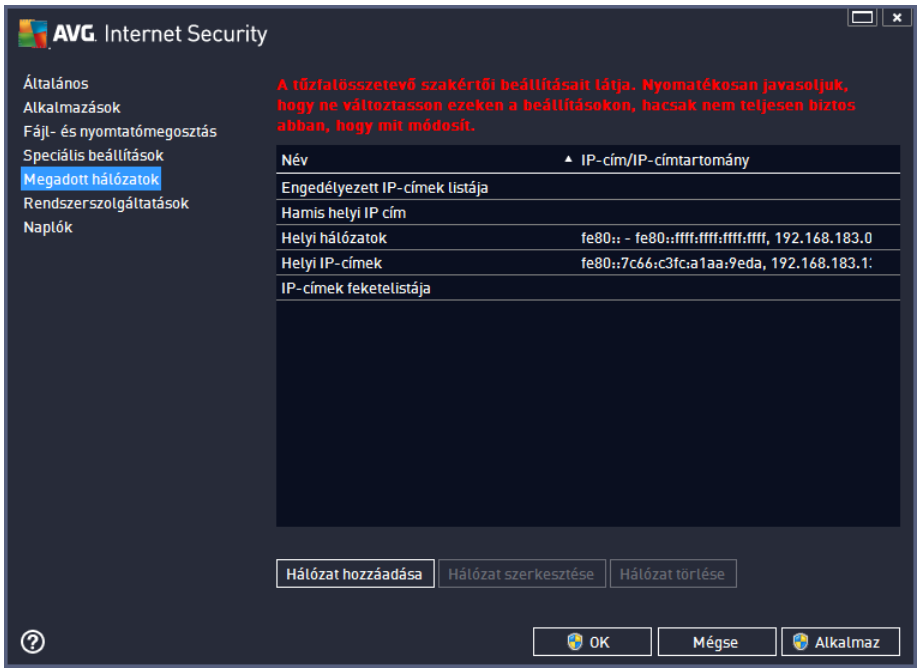


A ***Speciális beállítások*** párbeszédpanel lehetővé teszi az alábbi tűzfalparaméterek bekapcsolását/ kikapcsolását:

- ***Tűzfal által támogatott virtuális gépekre érkező és onnan induló forgalom engedélyezése*** – hálózati kapcsolat támogatása virtuális gépeken, például a VMWare rendszerben.
- ***Minden forgalom engedélyezése a virtuális magánhálózatokon (VPN)*** – VPN kapcsolatok *támogatása (távoli számítógépekhez történő csatlakozáshoz)*.
- ***Ismeretlen bemenő/kimenő forgalom naplózása*** – a rendszer az ismeretlen alkalmazások alapján az összes *(bemenő/kimenő)* kommunikációs kísérletet rögzíti a Tűzfalnaplóban.

10.5. Megadott hálózatok

Bármely beállítás módosítása a Megadott hálózatok panelen CSAK TAPASZTALT FELHASZNÁLÓK RÉSZÉRE javasolt.

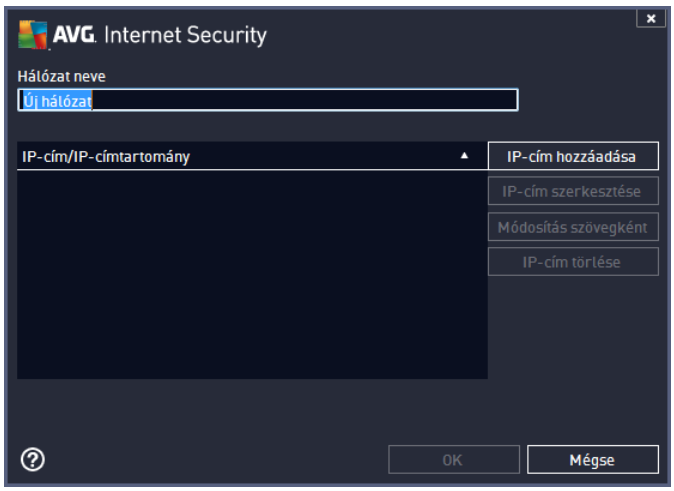


A ***Megadott hálózatok*** panel felsorolja az összes hálózatot, amelyhez a számítógép csatlakozik. A lista a következő információkat tartalmazza minden egyes észlelt hálózattal kapcsolatban:

- ***Hálózatok*** – Felsorolja az összes hálózatot, amelyhez a számítógép csatlakozik.
- ***IP-címtartomány*** – Minden egyes hálózatot automatikusan észlel a rendszer, és IP-címtartományként határoz meg.

Vezérlőgombok

- ***Hálózat hozzáadása*** – Megnyit egy új párbeszédpanelt, ahol szerkesztheti az újonnan meghatározott hálózat paramétereit, vagyis megadhatja a ***Hálózat nevét*** és az ***IP-cím tartományát***:

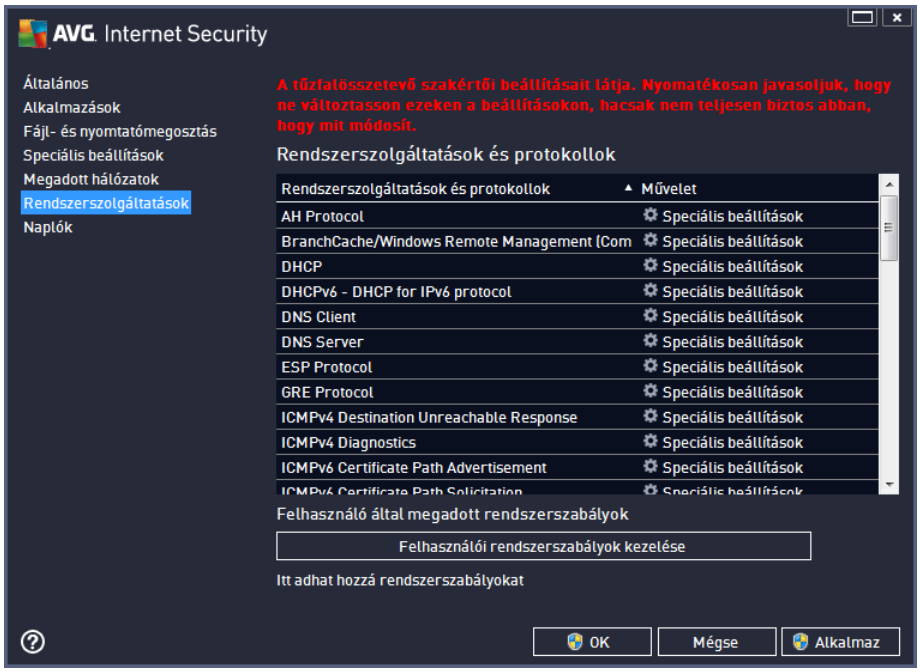


- ***Hálózat szerkesztése*** – Megnyitja a ***Hálózat tulajdonságai*** párbeszédpanelt (*lásd fent*), ahol egy már meghatározott hálózat paramétereit szerkesztheti (*a párbeszédpanel megegyezik az új hálózatok hozzáadására szolgáló ablakkal, lásd az előző bekezdés leírását*).

- ***Hálózat törlése*** – Eltávolítja a kijelölt hálózat hivatkozását a listából.

10.6. Rendszerszolgáltatások

Bármely beállítás módosítása a Rendszerszolgáltatások és protokollok panelen CSAK TAPASZTALT FELHASZNÁLÓK RÉSZÉRE javasolt.



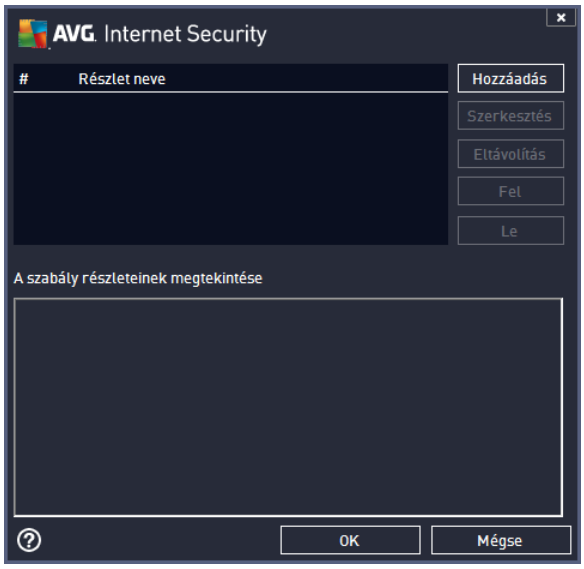
A ***Rendszerszolgáltatások és protokollok*** panel felsorolja azon normál Windows rendszerszolgáltatásokat és protokollokat, amelyeknek szükségük van a hálózati kommunikációra. Ez a rész a következő oszlopokat tartalmazza:

- ***Rendszerszolgáltatás és protokollok*** – Ez az oszlop a kapcsolódó rendszerszolgáltatás nevét jeleníti meg.
- ***Művelet*** – Ez az oszlop a kapcsolódó művelet ikonját jeleníti meg:
  - o Kommunikáció engedélyezése az összes hálózaton
  - o Kommunikáció tiltása

A lista elemeinek (*és hozzárendelt műveleteinek*) szerkesztéséhez kattintson a jobb gombbal, majd válassza a ***Szerkesztés*** lehetőséget. ***A rendszerszabályok módosítását kizárólag haladó felhasználók végezzék. A szabályok módosítását nem javasoljuk!***

Felhasználó által megadott rendszerszabályok

Egy új párbeszédpanel megnyitásához a rendszerszolgáltatási szabályok megadása érdekében (*lásd az alábbi képet*) nyomja meg a ***Felhasználói rendszerszabályok kezelése*** gombot. Ugyanaz a párbeszédpanel nyílik meg, ha a rendszerszolgáltatások és a protokollok lista bármely meglévő eleme beállításának szerkesztése mellett dönt. A panel felső részén a jelenleg szerkesztés alatt álló rendszerszabály részleteit láthatja, míg az alsó rész a kiválasztott szabályt mutatja. A szabályokat szerkesztheti, hozzáadhatja vagy törölheti a megfelelő gombbal:



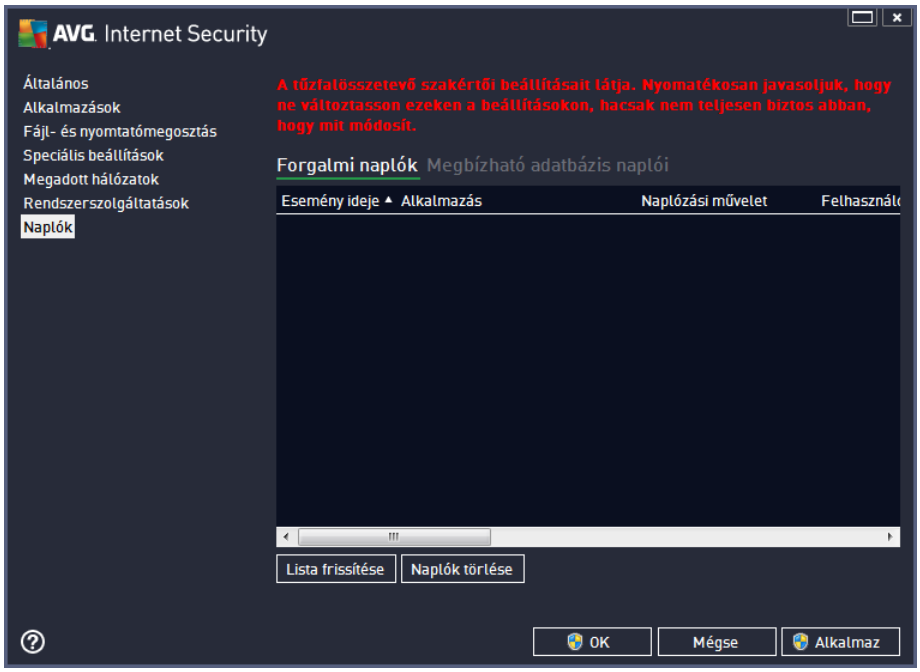
Vegye figyelembe, hogy a részletes szabálybeállítások összetettek, és elsősorban hálózati rendszergazdáknak szólnak, akiknek teljes felügyeletre van szükségük a tűzfal-konfiguráció felett. Ha nem ismeri a kommunikációs protokollokat, hálózati portszámokat, IP-címeket stb., akkor ne módosítsa ezen beállításokat! Ha mégis módosítania kell a konfigurációt, akkor további információkért forduljon a súgóhoz.

10.7. Naplók

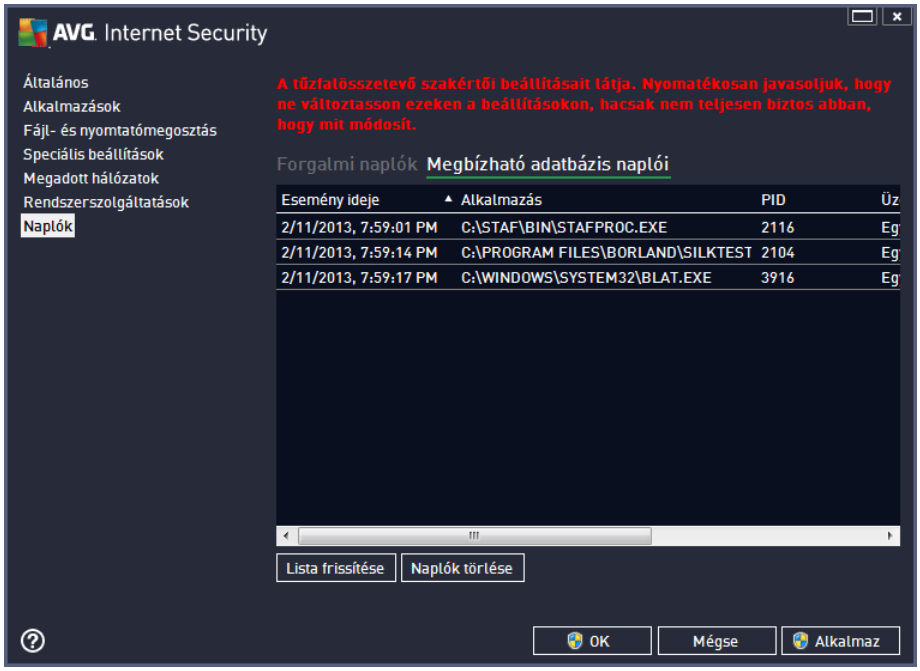
Bármely beállítás módosítása a Naplók párbeszédpanelen CSAK TAPASZTALT FELHASZNÁLÓK RÉSZÉRE javasolt.

A ***Naplók*** párbeszédpanel lehetővé teszi, hogy áttekintse a két lapon megjelenített Tűzfal műveletek és események részletes naplóját:

- ***Forgalmi naplók*** – Ez a lap információkat biztosít a hálózatot elérni kívánó összes alkalmazás tevékenységéről. Valamennyi elemre vonatkozóan információt talál az esemény ideje, az alkalmazás neve, a kapcsolódó naplóművelet, a felhasználó neve, a PID, a forgalom iránya, a protokoll típusa, a távoli és a helyi portok száma és a helyi és távoli IP cím vonatkozásában.



- ***Megbízható adatbázis naplói*** – *A Megbízható adatbázis* egy olyan belső AVG adatbázis, amely információkat gyűjt a megbízható és tanúsított alkalmazásokról (amelyek mindig kommunikálhatnak az interneten). Ha egy új alkalmazás csatlakozni próbál a hálózatra (*és még nincs tűzfalszabály meghatározva az alkalmazáshoz*), akkor Önnek kell eldöntenie, hogy engedélyezi-e a hálózati kommunikációt az adott alkalmazás számára. Az AVG ellenőrzi a *Megbízható adatbázist*, és ha az alkalmazás megtalálható benne, akkor azt automatikusan kiengedi a hálózatra. Ha a program nem talál semmilyen információt az alkalmazásról az adatbázisban, akkor Ön egy külön párbeszédpanelen engedélyezheti az alkalmazás számára a hálózati hozzáférést.



Vezérlőgombok

- ***Lista frissítése*** – Az összes naplózott paramétert a következők alapján lehet rendezni: időrendben (*dátum*) vagy ABC sorrendben (*egyéb oszlopk*) - csak kattintson az adott oszlopra. Használja a ***Lista frissítése*** gombot a megjelenített információk frissítéséhez.

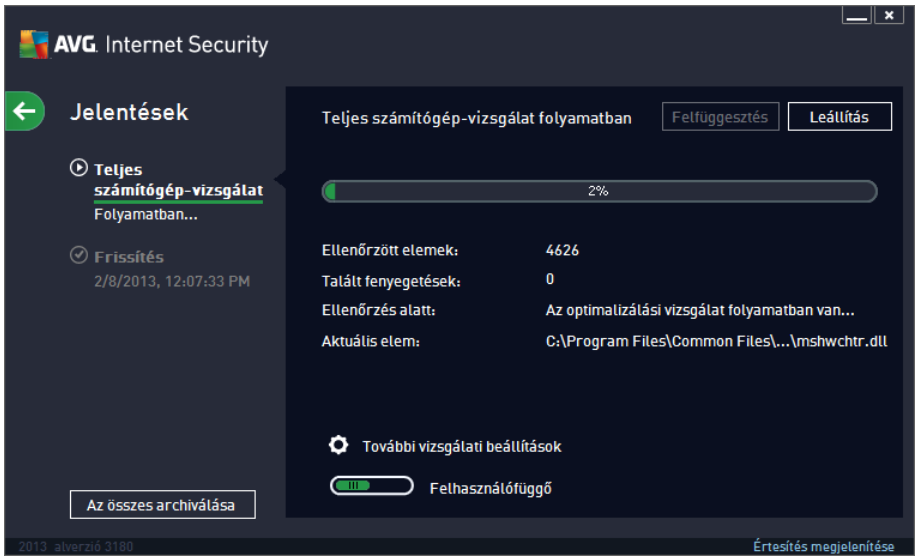
- ***Naplók törlése*** – kattintson ide a táblázatban található összes bejegyzés törléséhez.

11. AVG vizsgálat

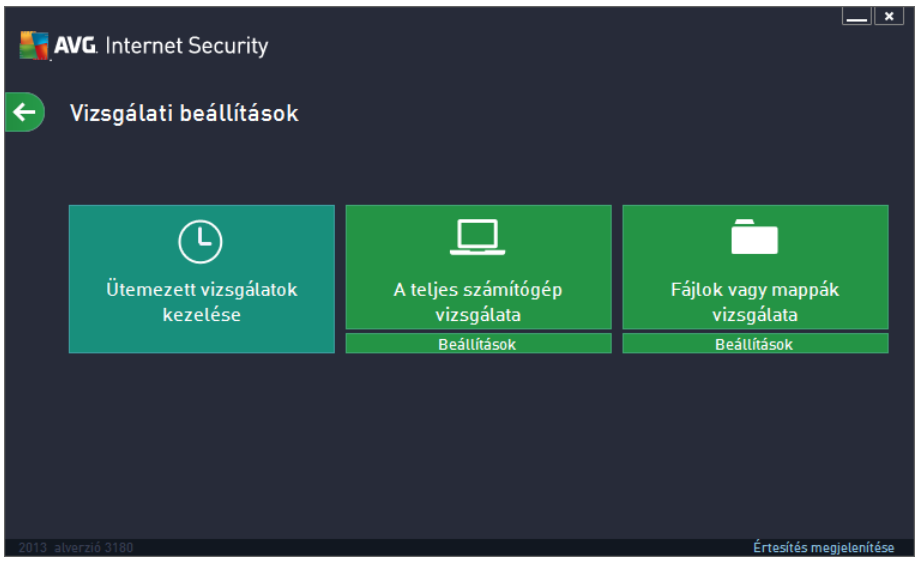
Alapértelmezés szerint az **AVG Internet Security 2013** nem futtat semmilyen vizsgálatot, hiszen az első vizsgálat után *(amely indítására felkéri a program)* Ön teljes védelemben részesül az **AVG Internet Security 2013** állandó összetevőinek köszönhetően, amelyek folyamatosan készenlétben állnak, és nem hagyják, hogy kártékony kódok férjenek hozzá a számítógépéhez. Természetesen rendszeres időközönként ütemezhet vizsgálatokat, vagy tetszés szerint manuálisan is elindíthat egy vizsgálatot.

Az AVG vizsgálati felület a fő felhasználói felületről, a grafikusan két részre osztott gombbal érhető el: 

- ***Vizsgálat indítása*** – Nyomja meg a gombot a Teljes számítógép-vizsgálat azonnali indításához. Az állapot és az eredmények az automatikusan megnyíló Jelentések ablakban tekinthetők meg:



- ***Beállítások*** – Válassza ezt a gombot *(grafikusan három vízszintes vonalként jelenik meg egy zöld mezőn)* a ***Vizsgálati beállítások*** párbeszédpanel megnyitásához, ahol az ütemezett vizsgálatokat kezelheti és a Teljes számítógép-vizsgálat / Kiválasztott fájlok és mappák vizsgálata funkció paramétereit szerkesztheti.



A ***Vizsgálati beállítások*** párbeszédpanelen három fő vizsgálati konfigurációs részt talál:

- ***Ütemezett vizsgálatok kezelése*** – Kattintson erre a beállításra egy új párbeszédpanel megnyitásához, amely az összes vizsgálati ütemezés áttekintését tartalmazza. Mielőtt meghatározza a saját vizsgálatait, csak egy, a szoftvergyártó által előre meghatározott ütemezett vizsgálat lesz látható a táblázatban. A vizsgálat alapértelmezés szerint ki van kapcsolva. A bekapcsolásához kattintson rá az egér jobb gombjával, és válassza a *Feladat engedélyezése* lehetőséget a helyi menüből. Amint engedélyezi az ütemezett vizsgálatot, szerkesztheti annak konfigurációját a *Szerkesztés* gomb segítségével. A *Hozzáadás* gombra kattintva új, saját vizsgálati ütemezést hozhat létre.

- ***A teljes számítógép vizsgálata / Beállítások*** – Ez a gomb két részre van osztva. Kattintson a *Teljes számítógép vizsgálata* lehetőségre a teljes számítógép vizsgálatának azonnali elindításához *(a teljes számítógép vizsgálatának részleteiért tekintse meg az Előre meghatározott vizsgálatok / A teljes számítógép vizsgálata című fejezetet)*. Az alsó *Beállítások* részre kattintva megnyílik a teljes számítógép-vizsgálat konfigurációs párbeszédpanelje.

- ***Kiválasztott fájlok és mappák vizsgálata / Beállítások*** – Ez a gomb is két részre van osztva. Kattintson a *Kiválasztott fájlok és mappák vizsgálata* lehetőségre a számítógépen kiválasztott területek vizsgálatának azonnali indításához *(a kiválasztott fájlok és mappák vizsgálatának részleteiért tekintse meg az Előre meghatározott vizsgálatok / Kiválasztott fájlok és mappák vizsgálata című fejezetet)* . Az alsó *Beállítások* részre kattintva megnyílik a kiválasztott fájlok és mappák vizsgálatának konfigurációs párbeszédpanelje.

11.1. Előre meghatározott vizsgálatok

Az **AVG Internet Security 2013** vírusirtó egyik legfontosabb funkciója az azonnali vizsgálat. Az azonnali keresés a számítógép különböző részeinek vizsgálatára szolgál, ha vírusfertőzés gyanúja merül fel. Azt ajánljuk, hogy az ilyen teszteket rendszeresen végezze el, még akkor is, ha úgy gondolja, hogy a számítógépen nincs vírus.

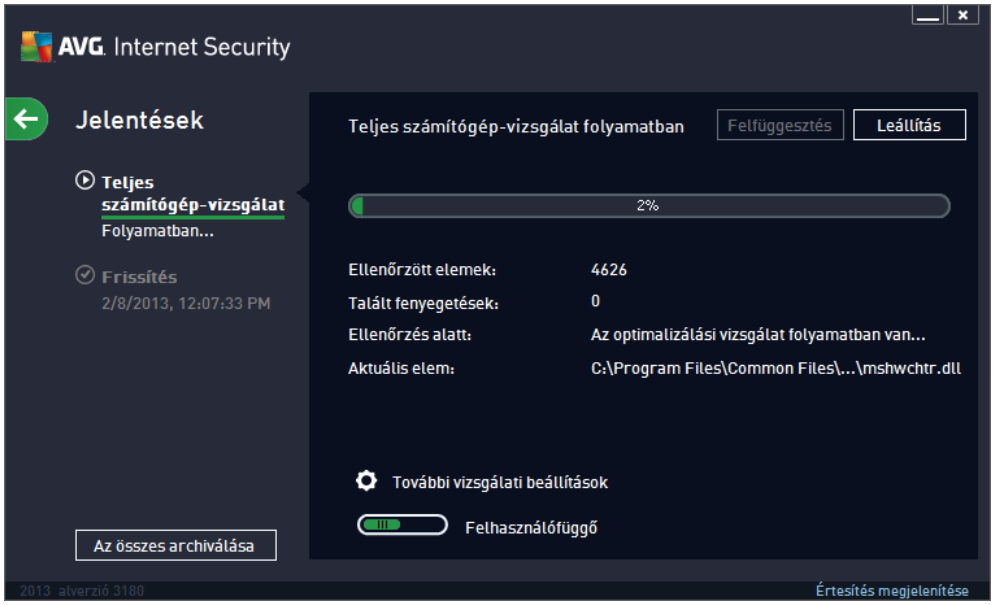
Az **AVG Internet Security 2013** programban a következő előre meghatározott vizsgálatokat találhatja, amelyeket a szoftver gyártója állított be:

11.1.1. A teljes számítógép vizsgálata

A Teljes számítógép-vizsgálat megvizsgálja az egész számítógépet esetleges fertőzések és/vagy nemkívánatos programokat keresve. A vizsgálatkor a számítógép összes merevlemezét ellenőrzi, azonosítja és javítja a fertőzött fájlokat, vagy áthelyezi azokat a Karanténba. A teljes számítógép vizsgálatát javasoljuk heti legalább egyszer elvégezni.

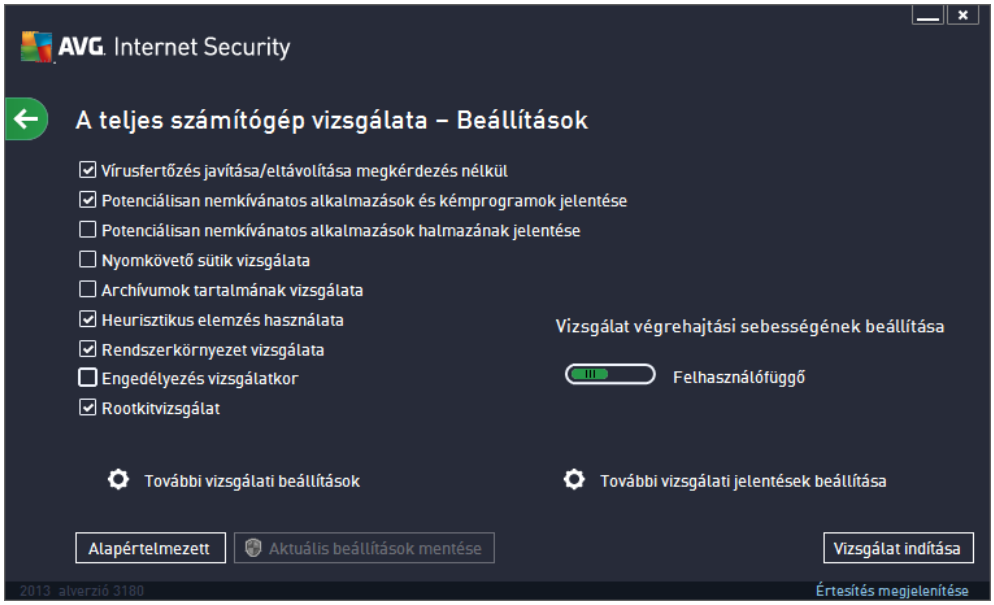
Vizsgálat indítása

A ***Teljes számítógép-vizsgálat*** közvetlenül a fő felhasználói felületről indítható a ***Vizsgálat indítása*** gombra kattintva. Semmilyen egyéb beállítás nem szükséges ehhez a vizsgálathoz, a folyamat azonnal indul. A ***Teljes számítógép-vizsgálat folyamatban*** párbeszédpanelen (*lásd a képernyőképet*) tekintheti meg a folyamat állapotát és az eredményeket. A vizsgálatot ideiglenesen szüneteltetheti (***Felfüggesztés***) vagy teljesen le is állíthatja (***Leállítás***), ha szükséges.



Vizsgálati beállítások szerkesztése

A ***Teljes számítógép-vizsgálat*** konfigurációját ***A teljes számítógép vizsgálata – Beállítások*** párbeszédpanelen *szerkesztheti (a párbeszédpanel a Vizsgálati beállítások párbeszédpanel Teljes számítógép-vizsgálat területének Beállítások hivatkozásán keresztül érhető el).* ***Érdemes megtartani az alapértelmezett beállításokat, és csak akkor módosítsa azokat, ha feltétlenül szükséges!***



A listában tetszés szerint be- és kikapcsolhatja az adott vizsgálati paramétereket:

- ***Fertőzés javítása/eltávolítása kérdés nélkül*** *(alapértelmezés szerint bekapcsolva)* – Ha a rendszer vírust talál a vizsgálat során, akkor automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl automatikusan nem javítható, az objektumot áthelyezi a Karanténba.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** *(alapértelmezés szerint bekapcsolva)* – Jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** *(alapértelmezés szerint kikapcsolva)* – Jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: ezek olyan programok, amelyek a gyártótól közvetlenül beszerezve ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért a funkció alapértelmezés szerint ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** *(alapértelmezés szerin kikapcsolva)* – Ez a paraméter meghatározza, hogy a rendszer észlelje-e a cookie-kat (*a HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma).*

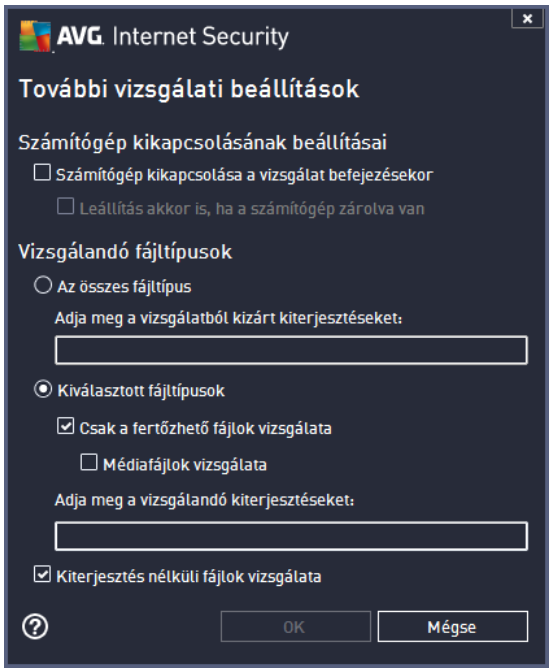
- ***Archívumok tartalmának vizsgálata*** *(alapértelmezés szerint kikapcsolva)* – Ez a paraméter határozza meg, hogy vizsgálatkor a program ellenőrizze-e az archívumokban (például ZIP, RAR, stb.) tárolt fájlokat.

- ***Heurisztikus elemzés használata*** *(alapértelmezés szerint bekapcsolva)* – A heurisztikus elemzés *(a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben)* lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet vizsgálata*** *(alapértelmezés szerint bekapcsolva)* – A vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Engedélyezés vizsgálatkor*** *(alapértelmezés szerint kikapcsolva)* – Bizonyos esetekben *(például ha vírusfertőzésre gyanakszik)* ezzel a beállítással aktiválhatja a legalaposabb vizsgálati algoritmusokat, amelyek még a számítógép ritkán megfertőződő részeit is ellenőrzik a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***További vizsgálati beállítások*** – ez a link megnyit egy új További vizsgálati beállítások panelt, ahol a következő paramétereket adhatja meg:



  - ***A számítógép kikapcsolásának beállításai*** – döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (***Számítógép kikapcsolása a vizsgálat befejezésekor***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Leállítás akkor is, ha a számítógép zárolva van***).

  - ***Vizsgálandó fájltípusok*** – el kell döntenie azt is, hogy a program mely fájlokat vizsgálja:

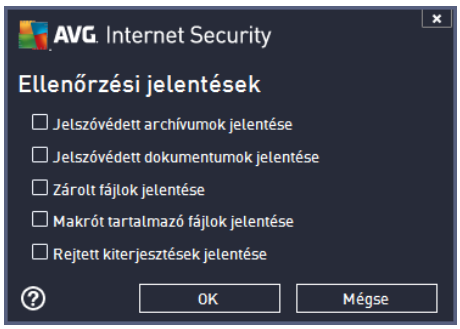
    - ***Az összes fájltípus***, kivételek megadásának lehetőségével, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszővel válassza el;

    - ***Kiválasztott fájltípusok*** – megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek fertőzöttek lehetnek (*a nem fertőzhető fájlokat, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem ellenőrzi a program*), pl. médiafájlok (*video-, audiofájlok – ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg azokat*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

➢ Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** – ez az opció alapértelmezés szerint be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell azokat.

- ***Vizsgálat sebességének beállítása*** – használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapértelmezés szerint ez az érték *felhasználófüggő* automatikus erőforrás-használati szintre van állítva. A vizsgálati folyamatot állíthatja lassabbra, ekkor a rendszer-erőforrások minimálisan lesznek kihasználva, (*ez akkor hasznos, ha dolgoznia kell a számítógépen, és mindegy, hogy a vizsgálat mennyi időt vesz igénybe*), illetve állíthatja gyorsabbra nagyobb rendszer-erőforrás használattal (*pl. ha a számítógépet ideiglenesen magára hagyja*).

- ***További vizsgálati jelentések beállítása*** – a hivatkozás megnyit egy új ***Vizsgálati jelentések*** panelt, ahol kiválaszthatja, hogy milyen találati típusokat jelentsen a program:



Figyelmeztetés: *Ezek a beállítások megegyeznek az újonnan létrehozott vizsgálatok beállításaival – az AVG Vizsgálat / Vizsgálat ütemezése / Hogyan keressen a program fejezetben leírtaknak megfelelően. Ha úgy dönt, hogy megváltoztatja az alapértelmezett konfigurációt a* ***Teljes számítógép vizsgálata*** *részben, akkor elmentheti az új beállításokat alapértelmezettként, és azok lesznek használva a jövőben minden teljes vizsgálathoz.*

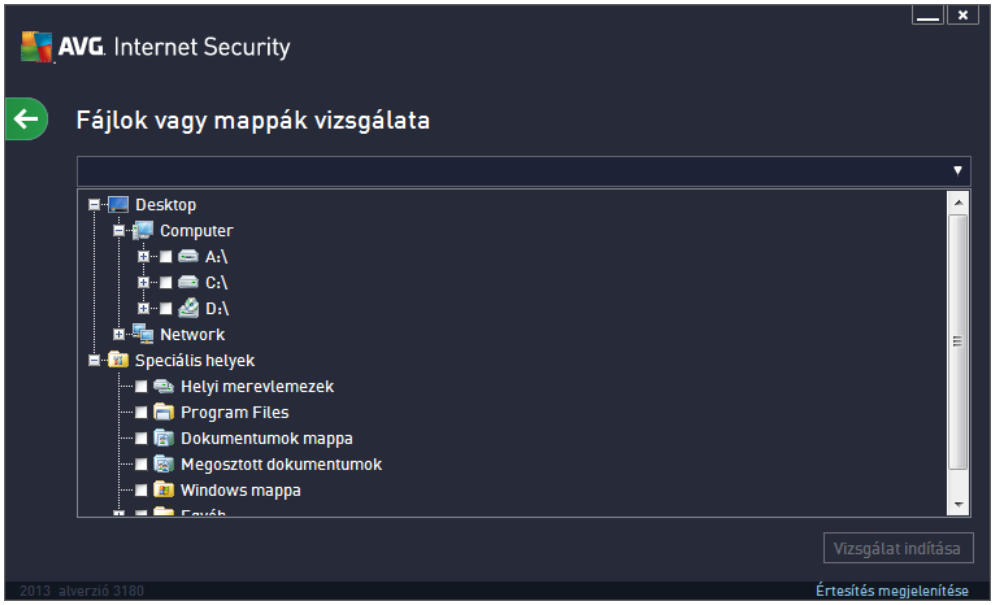
11.1.2. Kiválasztott fájlok és mappák vizsgálata

Kijelölt fájlok vagy mappák ellenőrzése – csak azokat a rendszerterületeket ellenőrzi, amelyeket Ön előzőleg kiválasztott (*meghatározott mappák, merevlemezek, floppylemezek, CD-k stb.*). A vírusok észlelése és javítása során a folyamat megegyezik a teljes számítógép vizsgálati folyamatával: a program minden vírusfertőzést javít vagy Karanténba helyez. Az adott fájlokat vagy mappákat saját vizsgálatba is felveheti, és tetszőlegesen ütemezheti a kereséseket.

Vizsgálat indítása

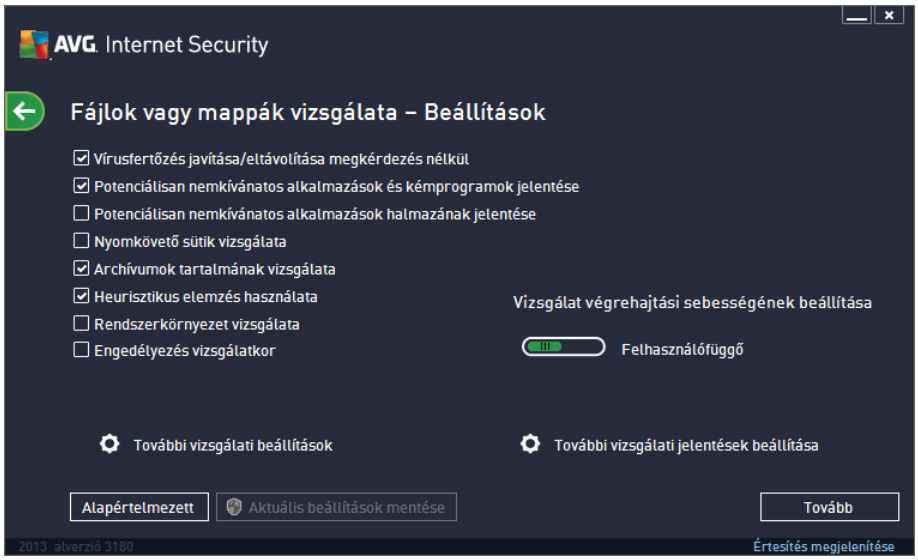
A ***Kiválasztott fájlok és mappák vizsgálata*** közvetlenül a Vizsgálati beállítások párbeszédpanelről indítható el a **Kiválasztott fájlok és mappák vizsgálata** gombra kattintva. A ***Válasszon ki bizonyos fájlokat vagy mappákat az ellenőrzéshez*** panel megjelenik. Válassza ki a számítógép fastruktúrájából a vizsgálni kívánt mappákat. A kiválasztott mappák elérési útja automatikusan megjelenik a párbeszédpanel felső részén látható szövegdobozban. Lehetősége van arra is, hogy egy bizonyos mappát almappák kihagyásával végezzen vizsgálatot. Ehhez adjon egy mínuszjelet „**-**” az automatikusan létrehozott elérési útvonal elé (*lásd a képernyőképet*). Egy teljes mappa vizsgálatból való kizárásához használja a „**!**” jelet paraméter. Végül a vizsgálat indításához nyomja meg a ***Vizsgálat indítása*** gombot. A vizsgálati folyamat alapvetően megegyezik a Teljes

számítógép-vizsgálat funkcióval.



Vizsgálati beállítások szerkesztése

A ***Kiválasztott fájlok és mappák vizsgálata*** konfigurációt a ***Kiválasztott fájlok és mappák vizsgálata – Beállítások*** párbeszédpanelen *szerkesztheti (a párbeszédpanel a Vizsgálati beállítások párbeszédpanel Kiválasztott fájlok és mappák vizsgálata területének Beállítások hivatkozásával érhető el).* ***Érdemes megtartani az alapértelmezett beállításokat, és csak akkor módosítsa azokat, ha feltétlenül szükséges!***



A listában tetszés szerint be- és kikapcsolhatja az adott vizsgálati paramétereket:

- ***Fertőzés javítása/eltávolítása kérdés nélkül*** *(alapértelmezés szerint bekapcsolva):* Ha a rendszer vírust talál a vizsgálat során, akkor az automatikusan javítja, amennyiben ez

lehetséges. Ha a fertőzött fájl automatikusan nem javítható, az objektumot áthelyezi a Karanténba.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** *(alapértelmezés szerint bekapcsolva)*: Jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** *(alapértelmezés szerint kikapcsolva)*: Jelölje be ezt a jelölőnégyzetet a kémprogramok speciális változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért a funkció alapértelmezés szerint ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** *(alapértelmezés szerin kikapcsolva)* – Ez a paraméter meghatározza, hogy a rendszer észlelje-e a cookie-kat *(a HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma)*.

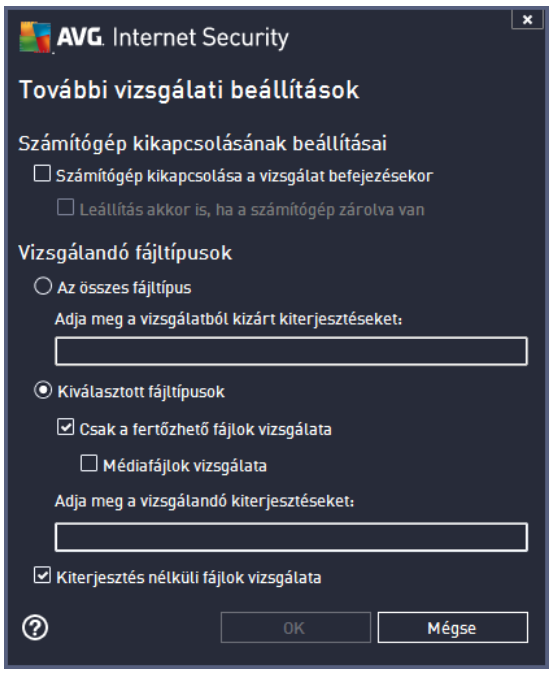
- ***Archívumok tartalmának vizsgálata*** *(alapértelmezés szerint bekapcsolva)* : Ez a paraméter meghatározza, hogy vizsgálatkor a program ellenőrizze-e az archívumokban (például ZIP, RAR, stb.) tárolt fájlokat.

- ***Heurisztikus elemzés használata*** *(alapértelmezés szerint bekapcsolva)*: A heurisztikus elemzés *(a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben)* lesz az egyik víruskeresési módszer a vizsgálat során.

- ***Rendszerkörnyezet vizsgálata*** *(alapértelmezés szerint kikapcsolva)*: A vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Engedélyezés vizsgálatkor*** *(alapértelmezés szerint kikapcsolva)*: Bizonyos esetekben *(például ha vírusfertőzésre gyanakszik)* ezzel a beállítással aktiválhatja a legalaposabb vizsgálati algoritmusokat, amelyek még a számítógép ritkán megfertőződő részeit is ellenőrzik a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***További vizsgálati beállítások*** – Ez a hivatkozás megnyit egy új ***További vizsgálati beállítások*** panelt, ahol a következő paramétereket adhatja meg:



- ***A számítógép kikapcsolásának beállításai*** – döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (***Számítógép kikapcsolása a vizsgálat befejezésekor***), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (***Leállítás akkor is, ha a számítógép zárolva van***).

- ***Vizsgálandó fájltípusok*** – el kell döntenie azt is, hogy a program mely fájlokat vizsgálja:

  - ***Az összes fájltípus,*** kivételek megadásának lehetőségével, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszővel válassza el;

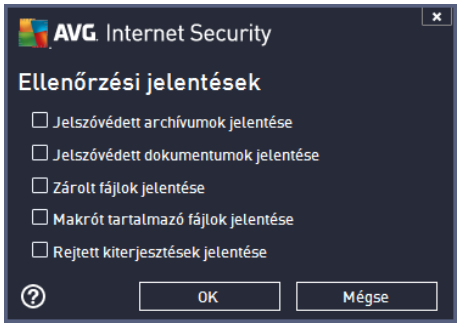
  - ***Kiválasztott fájltípusok*** – megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek fertőzöttek lehetnek (*a nem fertőzhető fájlokat, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem ellenőrzi a program*), pl. médiafájlok (*video-, audiofájlok – ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem valószínű, hogy vírus fertőzné meg azokat*). A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

  - Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** – ez az opció alapértelmezés szerint be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell azokat.

- ***Vizsgálat sebességének beállítása*** – használja a csúszkát a vizsgálati folyamat prioritásának módosításához. Alapértelmezés szerint ez az érték *felhasználófüggő* automatikus erőforrás-használati szintre van állítva. Alapállapotban a vizsgálati folyamatot lassabbra állíthatja, ekkor a rendszer minimális erőforrást használ (*hasznos, ha a számítógépen kell dolgoznia, és nem számít a gyorsaság*); vagy gyorsabbra állíthatja,

ekkor a rendszer több erőforrást használ (*a számítógépet ideiglenesen felügyelet nélkül hagyhatja*).

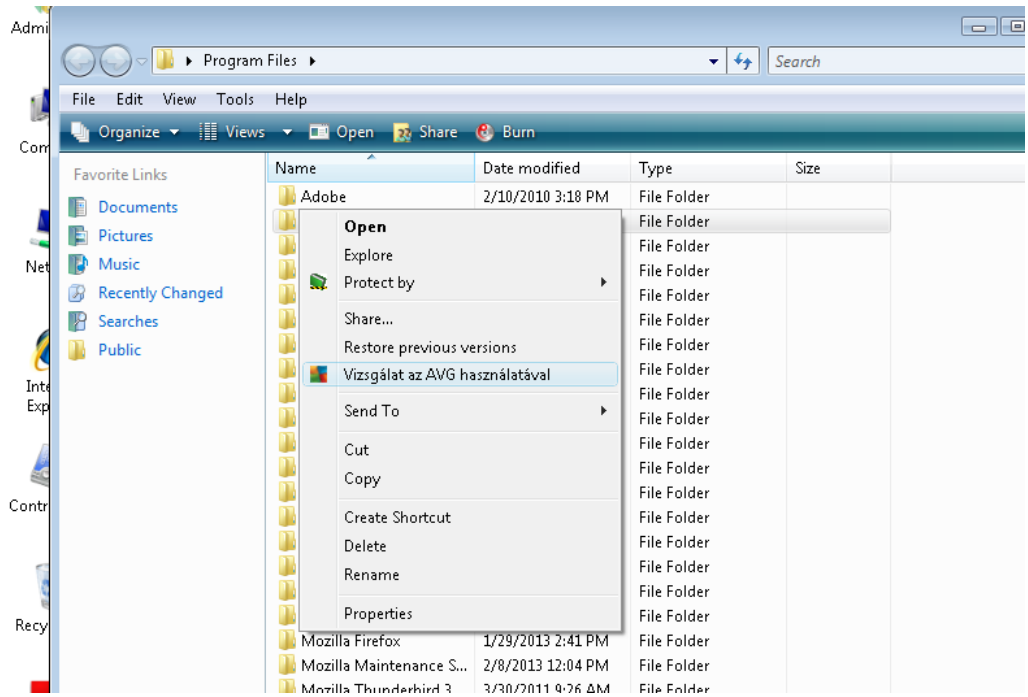
- ***További vizsgálati jelentések beállítása*** – a hivatkozás megnyit egy új ***Vizsgálati jelentések*** panelt, ahol kiválaszthatja, hogy milyen találati típusokat jelentsen a program:



Figyelmeztetés: *Ezek a beállítások megegyeznek az újonnan létrehozott vizsgálatok beállításaival – az AVG Vizsgálat / Vizsgálat ütemezése / Hogyan keressen a program fejezetben leírtaknak megfelelően. Ha úgy dönt, hogy megváltoztatja az alapbeállításokat a* ***Kijelölt fájlok vagy mappák ellenőrzése*** *részben, akkor elmentheti az új beállításokat alapértelmezettként, és azok lesznek használva a jövőben minden meghatározott fájl vagy mappa vizsgálatához. Továbbá ez a beállítás sablonként lesz használva minden újonnan létrehozott ütemezett vizsgálathoz (az egyéni keresések a Meghatározott fájlok vagy mappák vizsgálata rész aktuális beállításaitól függnek).*

11.2. Vizsgálat a Windows Intézőben

A számítógép teljes vagy részleges ellenőrzéséhez meghatározott vizsgálatokon kívül az **AVG Internet Security 2013** lehetővé teszi adott objektumok ellenőrzését közvetlenül a Windows Intézőből. Ha egy ismeretlen fájlt nyitna meg, de nem biztos a tartalmában, akkor elképzelhető, hogy előtte ellenőrizni szeretné. Kövesse az alábbi lépéseket:



- A Windows Intézőben jelölje ki a vizsgálni kívánt fájlt *(vagy mappát)*
- Kattintson a jobb gombbal az objektumra a helyi menü megnyitásához
- Válassza ki a ***Vizsgálat AVG-vel*** lehetőséget a fájl ellenőrzéséhez **AVG Internet Security 2013**

11.3. Parancssori vizsgálat

Az **AVG Internet Security 2013** terméken belül lehetőség van vizsgálat indítására parancssorból is. Ezt használhatja például kiszolgálókon, vagy a számítógép indításakor automatikusan lefutó kötegszkriptek létrehozásakor. A vizsgálatot az AVG grafikus felhasználói felületen elérhető legtöbb paraméterrel indíthatja a parancssorból.

Az AVG parancssorból történő indításához futtassa a következő parancsot abból a mappából, ahol az AVG telepítve van:

- ***avgscanx*** 32 bites operációs rendszerhez
- ***avgscana*** 64 bites operációs rendszerhez

A parancs formája

A parancs formája a következő:

- ***avgscanx /paraméter*** … pl. ***avgscanx /comp*** a számítógép teljes vizsgálatához
- ***avgscanx /paraméter /paraméter*** .. több paraméter egy sorban legyen szóközzel és „/” jellel elválasztva

- ha a paraméter használatához egyedi érték megadására van szükség (pl. a ***/scan*** paraméter, melynél meg kell adni a számítógép vizsgálandó területeit pontos elérési útvonal formájában), akkor ezen értékek pontosvesszővel legyenek elválasztva, például: ***avgscanx /scan=C:\;D:***

Vizsgálati paraméterek

Az elérhető paraméterek teljes listájához gépelje be az adott parancsot a /? paraméterrel vagy /HELP (pl. ***avgscanx /?***). Az egyetlen kötelező paraméter a /SCAN, mely meghatározza, hogy a számítógép mely részeit kell vizsgálni. Az opciók részletesebb leírásához lásd a parancssori paraméterek áttekintését.

A vizsgálat indításához nyomja meg az ***Enter*** gombot. A vizsgálatot megszakíthatja a ***Ctrl+C*** vagy ***Ctrl+Pause*** gomb megnyomásával.

A parancssori vizsgálat elindult a grafikus felületről

Ha a számítógépet Windows csökkentett módban futtatja, akkor elindíthatja a parancssori vizsgálatot a grafikus felhasználói felületről is. A vizsgálat a parancssorból fog futni. A ***Parancssori szerkesztő*** panel lehetővé teszi, hogy kényelmesen meghatározza a legtöbb vizsgálati paramétert a grafikus felhasználói felületen.

Mivel ez a panel csak a Windows csökkentett módból érhető el, a részletes leírásért forduljon a közvetlenül a panelből megnyitható súgóhoz.

11.3.1. Parancssori vizsgálat paraméterek

Az alábbiakban megtalálhatja a parancssori vizsgálathoz szükséges összes paramétert:

- /SCAN — Kiválasztott fájlok és mappák vizsgálata /SCAN=útvonal;útvonal *(például /SCAN=C:\;D:\)*
- /COMP — Teljes számítógép-vizsgálat
- /HEUR — Heurisztikus elemzés használata
- /EXCLUDE — Elérési út vagy fájlok kihagyása a vizsgálatból
- /@ — Parancsfájl /fájlnév/
- /EXT — Ezen kiterjesztések vizsgálata /például: EXT=EXE,DLL/
- /NOEXT — Ne vizsgálja ezeket a kiterjesztéseket /például: NOEXT=JPG/
- /ARC — Archívumok vizsgálata
- /CLEAN — Automatikus javítás
- /TRASH — Fertőzött fájlok karanténba helyezése

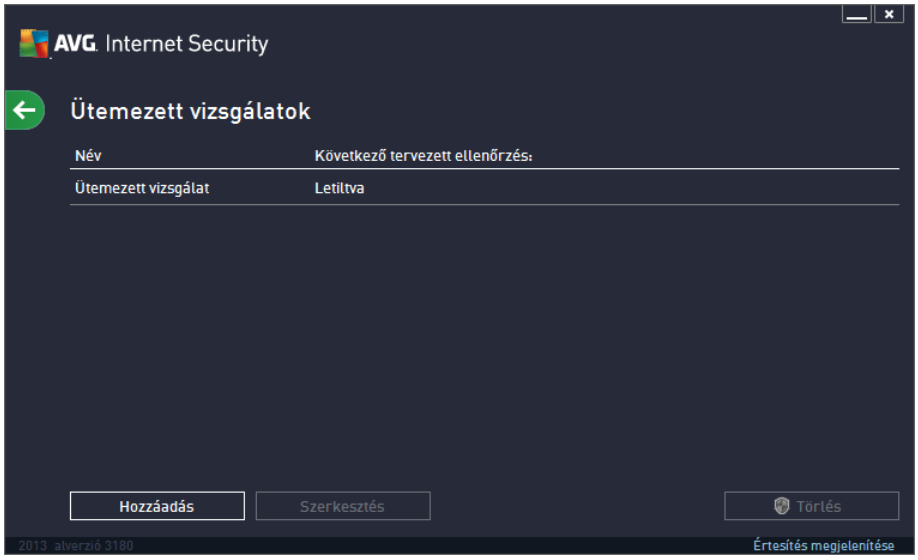
- /QT Gyorsvizsgálat
- /LOG Vizsgálati eredményfájl létrehozása
- /MACROW Makrók jelentése
- /PWDW Jelszóval védett fájlok jelentése
- /ARCBOMBSW Levélbombák *(többszörösen tömörített archívumok)*
- /IGNLOCKED Zárolt fájlok mellőzése
- /REPORT Jelentéskészítés fájlba /fájlnév/
- /REPAPPEND Hozzáfűzés a jelentésfájlhoz
- /REPOK Nem fertőzött fájlok jelentése OK-ként
- /NOBREAK A CRTL+BREAK billentyű kombinációval való megszakítás tiltása
- /BOOT MBR/RENDSZERTÖLTŐ SZEKTOR ellenőrzés engedélyezése
- /PROC Aktív folyamatok vizsgálata
- /PUP Potenciálisan nemkívánatos programok
- /PUPEXT Potenciálisan nemkívánatos alkalmazások halmazának jelentése
- /REG Rendszerleíró-adatbázis vizsgálata
- /COO Cookie-k vizsgálata
- /? Súgó megjelenítése a témakörről
- /HELP Súgó megjelenítése a témakörről
- /PRIORITY Vizsgálati prioritás beállítása /Alacsony, Automatikus, Magas/ *(lásd: Speciális beállítások / Vizsgálatok)*
- /SHUTDOWN Számítógép kikapcsolása a vizsgálat befejezésekor
- /FORCESHUTDOWN A számítógép kényszerített leállítása a vizsgálat befejezésekor
- /ADS Alternatív adatfolyamok vizsgálata *(csak NTFS)*
- /HIDDEN Rejtett kiterjesztésű fájlok jelentése
- /INFECTABLEONLY Csak fertőzhető kiterjesztésű fájlok vizsgálata
- /THOROUGHSCAN Engedélyezés vizsgálatkor
- /CLOUDCHECK Vakriasztások keresése

- /ARCBOMBSW Újratömörített archívumfájlok jelentése

11.4. Vizsgálatok ütemezése

Az **AVG Internet Security 2013** segítségével bármikor elindíthat egy keresést *(például ha gyanítja, hogy a számítógépen vírus található)* vagy egy ütemezett vizsgálatot. Javasoljuk, hogy ütemezések alapján futtasson le vizsgálatokat: így biztosíthatja, hogy a számítógép védve van mindenféle fertőzésveszélytől, és nem kell aggódnia, hogy mikor és hogyan indítson el egy keresést. Rendszeresen, legalább hetente egyszer futtassa le a Teljes számítógép-vizsgálat szolgáltatást. Azonban amennyiben lehetséges, a teljes számítógép vizsgálata napi szinten javasolt – az alapértelmezett vizsgálati ütemezésben is ez szerepel. Ha a számítógép mindig be van kapcsolva, akkor a vizsgálatot célszerű a munkaidőn kívülre ütemezni. Ha számítógép néha ki van kapcsolva, akkor a vizsgálatot ütemezheti a számítógép indítási idejére, amennyiben egy feladat kimaradt, mivel a kikapcsolt időszakra volt időzítve.

Az vizsgálatok ütemezése az ***Ütemezett vizsgálatok*** panelen hozhatók létre / szerkeszthetők, amely a Vizsgálati beállítások panel ***Ütemezett vizsgálatok kezelése*** gombján keresztül érhető el. Az új ***Ütemezett vizsgálat*** panelen az összes aktuálisan ütemezett vizsgálat teljes áttekintését láthatja:

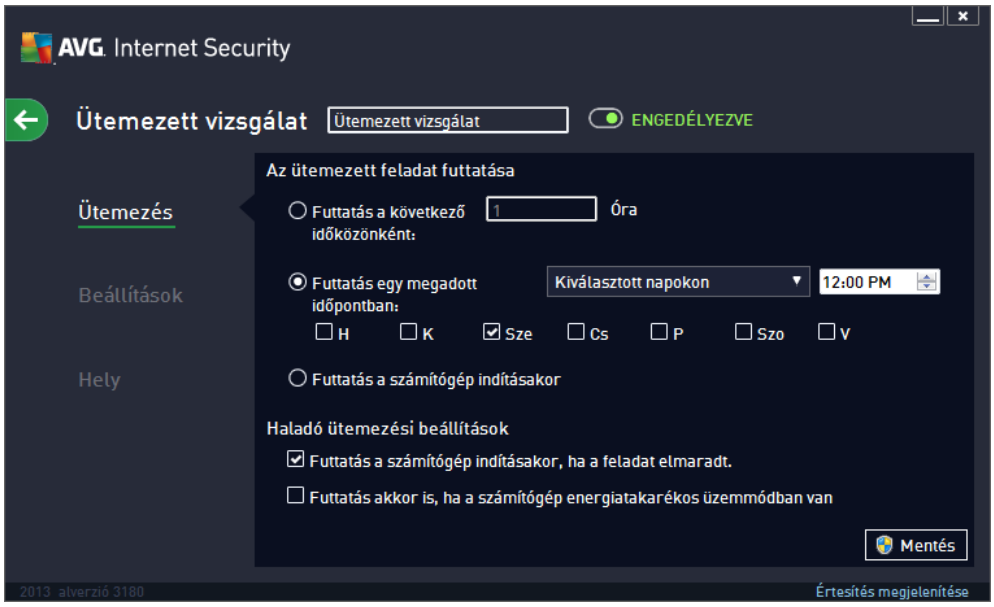


Mielőtt meghatározza a saját vizsgálatait, csak egy, a szoftvergyártó által előre meghatározott ütemezett vizsgálat lesz látható a táblázatban. A vizsgálat alapértelmezés szerint ki van kapcsolva. A bekapcsolásához kattintson rá az egér jobb gombjával, és válassza a ***Feladat engedélyezése*** lehetőséget a helyi menüből. Amint engedélyezi az ütemezett vizsgálatot, szerkesztheti annak konfigurációját a ***Szerkesztés*** gomb segítségével. A ***Vizsgálati ütemezés hozzáadása*** gombra is kattinthat új, saját vizsgálati ütemezés létrehozásához. Az ütemezett vizsgálat paramétereit három lapon szerkesztheti (*de akár új ütemezést is létrehozhat*):

- Ütemezés
- Beállítások
- Hely

Mindegyik lapon egyszerűen kikapcsolhatja a „közlekedési lámpa” gombot az ütemezett vizsgálat ideiglenes letiltásához, majd szükség esetén újra bekapcsolhatja:

11.4.1. Ütemezés



Az ***Ütemezés*** lap felső részén találhatja azt a szövegmezőt, amelyben megadhatja a jelenleg meghatározás alatt álló vizsgálati ütemezés nevét. Próbáljon mindig rövid, jellemző és megfelelő nevet adni a vizsgálatoknak, így később könnyebben megkülönböztetheti majd azokat. Nem javasolt például, hogy a vizsgálatnak az „Új vizsgálat” vagy „Saját vizsgálat” nevet adja, mivel ez semmit nem mond arról, hogy a vizsgálat valójában mit ellenőriz. Ugyanakkor megfelelő leíró név például a „Rendszerterületek vizsgálata” stb.

Ezen a panelen beállíthatja az adott keresés következő paramétereit:

- ***Az ütemezett feladat futtatása*** – Itt megadhatja, hogy az ütemezett vizsgálatok milyen időközönként fussanak le. Az ütemezés megadható bizonyos időközönként indított ismételt vizsgálatok futtatásával *(Futtatás a következő időközönként:)*, vagy egy pontos dátum és időpont megadásával *(Futtatás egy megadott időpontban...)*, illetve megadható egy adott eseményhez hozzárendelve is *(Futtatás a számítógép indításakor)*.

- ***Speciális ütemezési beállítások*** – Ebben a részben meghatározhatja, hogy a vizsgálat mely körülmények között induljon/ne induljon, például ha a számítógép energiatakarékos módban van vagy teljesen ki van kapcsolva. Miután az ütemezett vizsgálat elindult a megadott időben, erről értesítést kap egy felugró ablakban az AVG tálcaikonjánál. Egy új AVG tálcaikon jelenik meg (színes ikon egy zseblámpával), és tájékoztatja arról, hogy egy ütemezett vizsgálat éppen folyamatban van. Kattintson az egér jobb gombjával az AVG ikonjára egy helyi menü megnyitásához, ahol felfüggesztheti vagy leállíthatja a futó vizsgálatot, illetve megváltoztathatja annak prioritását.

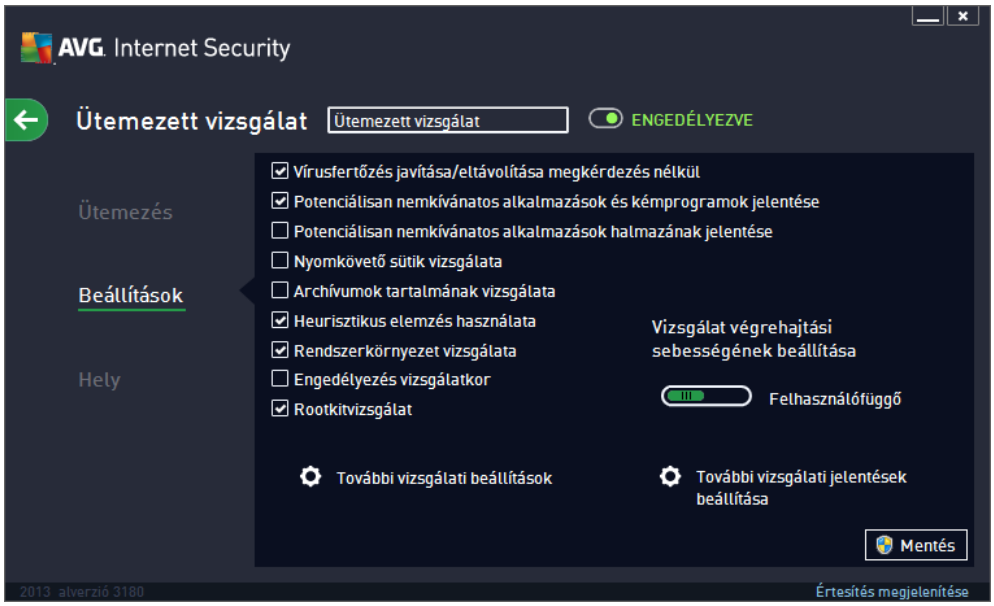
A párbeszédpanel vezérlői

- ***Mentés*** – A lapon vagy a párbeszédpanel többi lapján végrehajtott összes módosítást

menti, és visszatér az Ütemezett vizsgálatok áttekintéséhez. Ezért ha be szeretné állítani a vizsgálati paramétereket az összes lapon, akkor csak abban az esetben nyomja meg ezt a gombot, ha végzett az összes beállítással.

- – A párbeszédpanel bal felső részén lévő nyíllal térhet vissza az Ütemezett vizsgálatok áttekintésére.

11.4.2. Beállítások



A ***Beállítások*** lap felső részén találhatja azt a szövegmezőt, amelyben megadhatja a jelenleg meghatározás alatt álló vizsgálati ütemezés nevét. Próbáljon mindig rövid, jellemző és megfelelő nevet adni a vizsgálatoknak, így később könnyebben megkülönböztetheti majd azokat. Nem javasolt például, hogy a vizsgálatnak az „Új vizsgálat” vagy „Saját vizsgálat” nevet adja, mivel ez semmit nem mond arról, hogy a vizsgálat valójában mit ellenőriz. Ugyanakkor megfelelő leíró név például a „Rendszerterületek vizsgálata” stb.

A ***Beállítások*** lapon a vizsgálati paraméterek listáját találhatja, amelyeket tetszőlegesen be- és kikapcsolhat. ***Javasoljuk, hogy tartsa meg az alapértelmezett beállításokat, és csak akkor módosítson rajtuk, ha feltétlenül szükséges***:

- ***Fertőzés javítása/eltávolítása kérdés nélkül*** *(alapértelmezés szerint bekapcsolva):* ha a rendszer vírust talál a vizsgálat során, akkor azt automatikusan javítja, amennyiben ez lehetséges. Ha a fertőzött fájl automatikusan nem javítható, az objektumot áthelyezi a Karanténba.

- ***Potenciálisan nemkívánatos alkalmazások és kémprogramok jelentése*** *(alapértelmezés szerint bekapcsolva):* jelölje be a kémprogramok és vírusok kereséséhez. A kémprogramok külön kártevő kategóriát képviselnek és komoly biztonsági kockázatot jelentenek. Nagy részüket a felhasználók mégis szándékosan telepítik. Javasoljuk, hogy tartsa bekapcsolva ezt az eszközt, mivel így növelheti számítógépe biztonságát.

- ***Potenciálisan nemkívánatos alkalmazások halmazának jelentése*** (*alapértelmezés szerint kikapcsolva*): jelölje be ezt a jelölőnégyzetet a kémprogramok speciális

változatainak észleléséhez: olyan programok kereséséhez, amelyek ártalmatlanok, de később kártékony célokra használhatók. Ezzel tovább növelheti a számítógép biztonságát. Lehetséges, hogy a szolgáltatás legitim programokat is letilt, ezért a funkció alapértelmezés szerint ki van kapcsolva.

- ***Nyomkövető sütik vizsgálata*** (*alapértelmezés szerint kikapcsolva*): ez a paraméter meghatározza, hogy a rendszer észlelje-e a cookie-kat a vizsgálat során (*a HTTP cookie-kat hitelesítéshez, nyomkövetéshez és bizonyos adatok gyűjtéséhez használják a felhasználókról, pl. honlap preferenciák vagy online vásárlás során a kosár tartalma*)

- ***Archívumok tartalmának vizsgálata*** (*alapértelmezés szerint bekapcsolva*): ez a paraméter meghatározza, hogy vizsgálatkor a program ellenőrizze-e az archívumokban (például ZIP, RAR, stb.) tárolt fájlokat is.

- ***Heurisztika használata*** (*alapállapotban bekapcsolva*): a heurisztikus elemzés (*a vizsgált objektum utasításainak dinamikus emulációja egy virtuális környezetben*) lesz az egyik víruskeresési módszer a vizsgálat során.

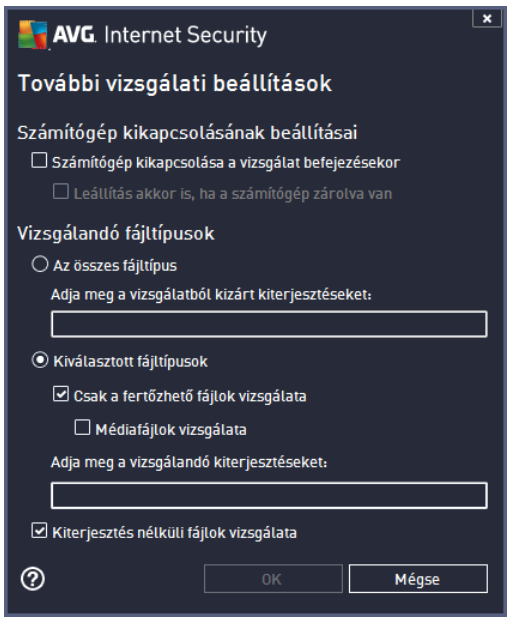
- ***Rendszerkörnyezet ellenőrzése*** (*alapállapotban bekapcsolva*): a vizsgálat a számítógép rendszerterületeit is ellenőrzi.

- ***Engedélyezés vizsgálatkor*** (*alapértelmezés szerint kikapcsolva):* bizonyos esetekben (*például ha vírusfertőzésre gyanakszik*) ezzel a beállítással aktiválhatja a legalaposabb vizsgálati algoritmusokat, amelyek még a számítógép ritkán megfertőzhető részeit is ellenőrzik a biztonság kedvéért. Ne feledje, hogy ez a módszer meglehetősen időigényes.

- ***Rootkitek keresése*** *(alapértelmezés szerint bekapcsolva): a* Rootkitkereső lehetséges rootkiteket, vagyis olyan programokat és technológiákat keres a számítógépen, amelyek kártékony tevékenységeket rejthetnek el. Ha a program rootkitet észlel, akkor az nem jelenti automatikusan azt, hogy a számítógép fertőzött. Bizonyos esetekben a program egyes eszközillesztőket, vagy legitim alkalmazások részeit is – tévesen – rootkitként észlel.

További vizsgálati beállítások

Ez a hivatkozás megnyit egy új ***További vizsgálati beállítások*** panelt, ahol a következő paramétereket adhatja meg:



- ***A számítógép kikapcsolásának beállításai*** – döntse el, hogy a számítógép automatikusan kikapcsoljon-e, miután a vizsgálati folyamat véget ért. Miután megerősítette ezt a beállítást (*Számítógép kikapcsolása a vizsgálat befejezésekor*), egy új opció aktiválódik, mely lehetővé teszi, hogy akkor is leállítsa a számítógépet, ha az éppen zárolt (*Leállítás akkor is, ha a számítógép zárolva van*).

- ***Vizsgálandó fájltípusok*** – el kell döntenie azt is, hogy a program mely fájlokat vizsgálja:

  - ***Az összes fájltípus,*** kivételek megadásának lehetőségével, amelyek kimaradnak a vizsgálatból. Ezen fájlkiterjesztéseket vesszővel válassza el;

  - ***Kiválasztott fájltípusok*** – megadhatja, hogy a program csak olyan fájlokat vizsgáljon, amelyek fertőzöttek lehetnek *(a nem fertőzhető fájlokat, mint pl. a sima szöveges fájlok vagy egyéb nem futtatható fájlok, nem ellenőrzi a program)*, pl. médiafájlok *(video-, audiofájlok – ha nem jelöli be ezt a négyzetet, akkor tovább csökken a vizsgálati idő, mivel ezen fájlok általában túl nagyok, és egyébként sem túl valószínű, hogy vírus fertőzné meg azokat)*. A kiterjesztések segítségével megadhatja, hogy mely fájlokat vizsgálja a program.

  - Megadhatja azt is, hogy ***a program vizsgálja a kiterjesztés nélküli fájlokat*** – ez az opció alapértelmezés szerint be van kapcsolva és javasolt, hogy tartsa is így. A kiterjesztés nélküli fájlok különösen gyanúsak, ezért mindig ellenőrizni kell azokat.

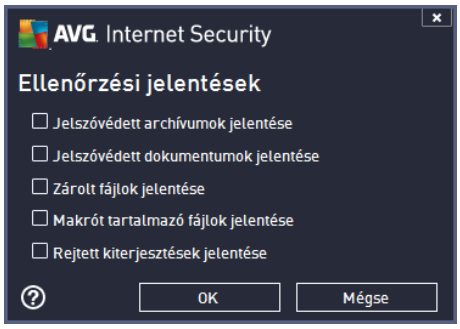
A vizsgálati sebesség beállítása

Ebben a részben hangolhatja a vizsgálat sebességét a rendszer erőforrásainak függvényében. Alapállapotban ez az érték *felhasználófüggő* automatikus erőforrás-használati szintre van állítva. Ha azt szeretné, hogy a vizsgálat gyorsabban fusson, akkor kevesebb idő szükségeltetik, de a rendszererőforrások használata jelentősen megnő, és lelassíthatja a PC-n zajló egyéb tevékenységeket (*ezt az opciót akkor használhatja, ha a számítógép be van kapcsolva, és senki nem dolgozik rajta jelenleg*). Másrészt csökkentheti a rendszererőforrások használatát, de ez a

vizsgálathoz szükséges idő növekedésével jár.

További vizsgálati jelentések beállítása

Kattintson a ***További vizsgálati jelentések...*** hivatkozásra a ***Vizsgálati jelentések*** panel megnyitásához, ahol számos opciót jelölhet be azzal kapcsolatban, hogy a programnak mit kell jelentenie:

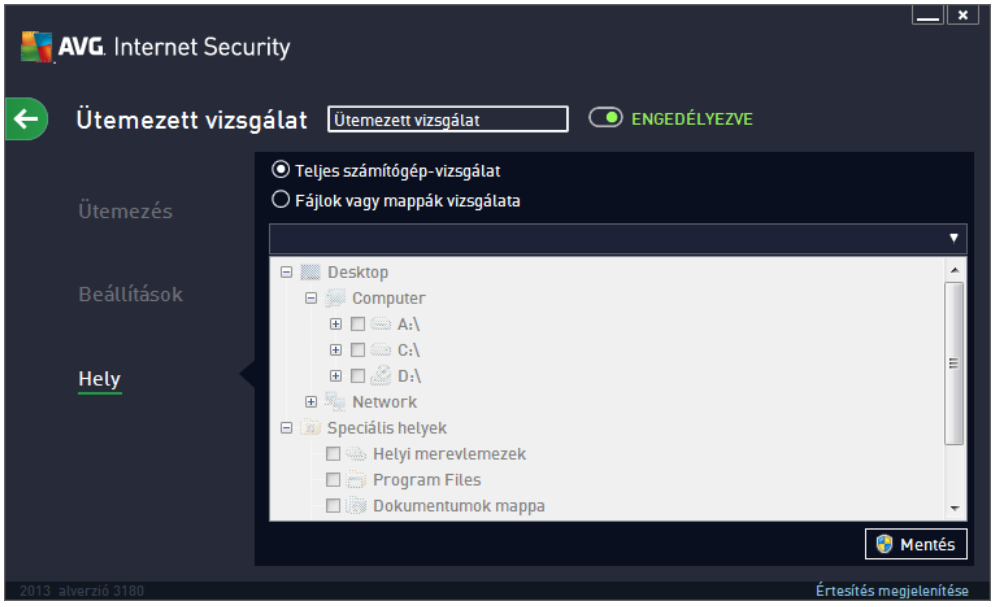


A párbeszédpanel vezérlői

- ***Mentés*** – A lapon vagy a párbeszédpanel többi lapján végrehajtott összes módosítást menti, és visszatér az Ütemezett vizsgálatok áttekintéséhez. Ezért ha be szeretné állítani a vizsgálati paramétereket az összes lapon, akkor csak abban az esetben nyomja meg ezt a gombot, ha végzett az összes beállítással.

- – A párbeszédpanel bal felső részén lévő nyíllal térhet vissza az Ütemezett vizsgálatok áttekintésére.

11.4.3. Hely



A ***Hely*** lapon meghatározhatja, hogy a számítógép teljes vizsgálatát vagy csak bizonyos fájlok és mappák vizsgálatát szeretné ütemezni. Ha bizonyos fájlok és mappák vizsgálatát választja, akkor a párbeszédpanel alsó részén a fastruktúra aktiválódik, és bejelölheti a vizsgálni mappákat (*kattintson a plusz jelre a kívánt mappa kiválasztásához*). Több mappát is kiválaszthat egyszerre az adott dobozok bejelölésével. A kiválasztott mappák megjelennek a szövegmezőben a párbeszédpanel tetején, míg a legördülő menü eltárolja a vizsgálati előzményeket későbbi használatra. Akár manuálisan is megadhatja a kívánt mappa teljes elérési útvonalát (*ha több útvonalat ír be, akkor pontosvesszővel válassza el őket, szóköz nélkül*).

A fastruktúrában láthat egy ***Különleges helyek*** ágat. Az alábbiakban láthatja azon helyeket, amelyeket a rendszer megvizsgál, ha az adott jelölőnégyzetet bejelöli:

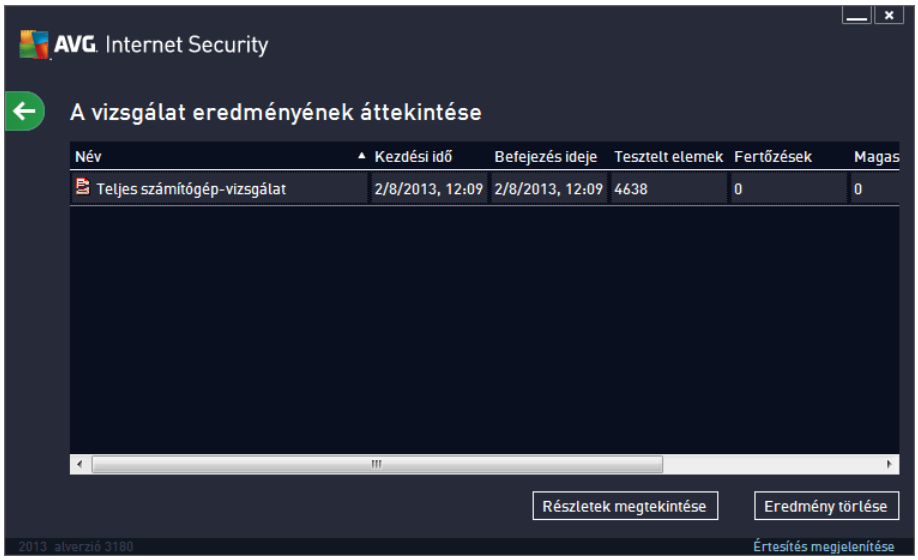
- ***Helyi merevlemezek*** – A számítógép összes merevlemeze
- ***Program Fájlok***
  - C:\Program Files\
  - *a 64-bit verziónál:* C:\Program Files (x86)
- ***Dokumentumok mappa***
  - *Windows XP-nél:* C:\Documents and Settings\Default User\My Documents\
  - *Windows Vista/7 rendszereknél*: C:\Users\user\Documents\
- ***Megosztott dokumentumok***
  - *Windows XP-nél*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7 rendszereknél*: C:\Users\Public\Documents\
- ***Windows mappa*** – C:\Windows\
- ***Egyéb***
  - *Rendszermeghajtó* – az a merevlemez, amelyen az operációs rendszer telepítve van (általában C:)
  - *Rendszermappa* – C:\Windows\System32\
  - *Ideiglenes fájlok mappa* – C:\Documents and Settings\User\Local\ (*Windows XP*); vagy C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Ideiglenes internetes fájlok* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); vagy C: \Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

A párbeszédpanel vezérlői

- ***Mentés*** – A lapon vagy a párbeszédpanel többi lapján végrehajtott összes módosítást menti, és visszatér az Ütemezett vizsgálatok áttekintéséhez. Ezért ha be szeretné állítani a vizsgálati paramétereket az összes lapon, akkor csak abban az esetben nyomja meg ezt a gombot, ha végzett az összes beállítással.

- – A párbeszédpanel bal felső részén lévő nyíllal térhet vissza az Ütemezett vizsgálatok áttekintésére.

11.5. A vizsgálat eredménye



A ***Vizsgálat eredményeinek áttekintése*** párbeszédpanel az összes eddig végrehajtott vizsgálat eredményeinek listáját tartalmazza. A táblázat a következő információkat tartalmazza az egyes vizsgálati eredményekről:

- ***Ikon*** – Az első oszlopban a vizsgálat állapotát leíró információs ikon található:
  - o Nem található fertőzés, a vizsgálat kész
  - o Nem található fertőzés, megszakítva befejezés előtt
  - o A rendszer fertőzést talált, nem történt javítás, a vizsgálat kész
  - o A rendszer fertőzést talált, nem történt javítás, megszakítva befejezés előtt
  - o A rendszer fertőzéseket talált és eltávolította vagy törölte azokat, a vizsgálat kész
  - o A rendszer fertőzéseket talált és eltávolította vagy törölte azokat, megszakítva befejezés előtt

- ***Név*** – Ez az oszlop az adott vizsgálat nevét tartalmazza. Ez vagy a két előre meghatározott vizsgálat egyike, vagy az Ön saját ütemezett vizsgálata.

- ***Kezdési idő*** – A vizsgálat indításának pontos dátumát és idejét adja meg.

- ***Befejezési idő*** – A vizsgálat befejezésének, felfüggesztésének vagy megszakításának pontos dátumát és idejét adja meg.
- ***Tesztelt objektumok*** – Az összes vizsgált objektum teljes számát mutatja.
- ***Fertőzések*** – Az eltávolított és talált fertőzések teljes számát jeleníti meg.
- ***Magas / Közepes / Alacsony*** – A következő három oszlopban a magas, közepes és alacsony súlyossági szintű fertőzések száma található.
- ***Rootkitek*** – A vizsgálat során talált rootkitek teljes számát mutatja.

A párbeszédpanel vezérlői

Részletek megtekintése – A gombra kattintva megtekintheti a kiválasztott vizsgálat részletes információit *(a fenti táblázatban kiemelve)*.

Eredmények törlése – A gombra kattintva eltávolíthatja a táblázatból a kiválasztott vizsgálati eredményeket.

– A párbeszédpanel bal felső részén lévő zöld nyíllal térhet vissza az összetevők áttekintését tartalmazó fő felhasználói felületre.

11.6. Vizsgálati eredmények részletei

Egy adott vizsgálati eredmény részletes információinak áttekintését a ***Részletek megtekintése*** gombra kattintva érheti el a Vizsgálati eredmények áttekintése párbeszédpanelen. A rendszer ugyanarra a párbeszédpanelre irányítja át, amely részletesen ismerteti egy vizsgálati eredmény információit. Az információk három lapon jelennek meg:

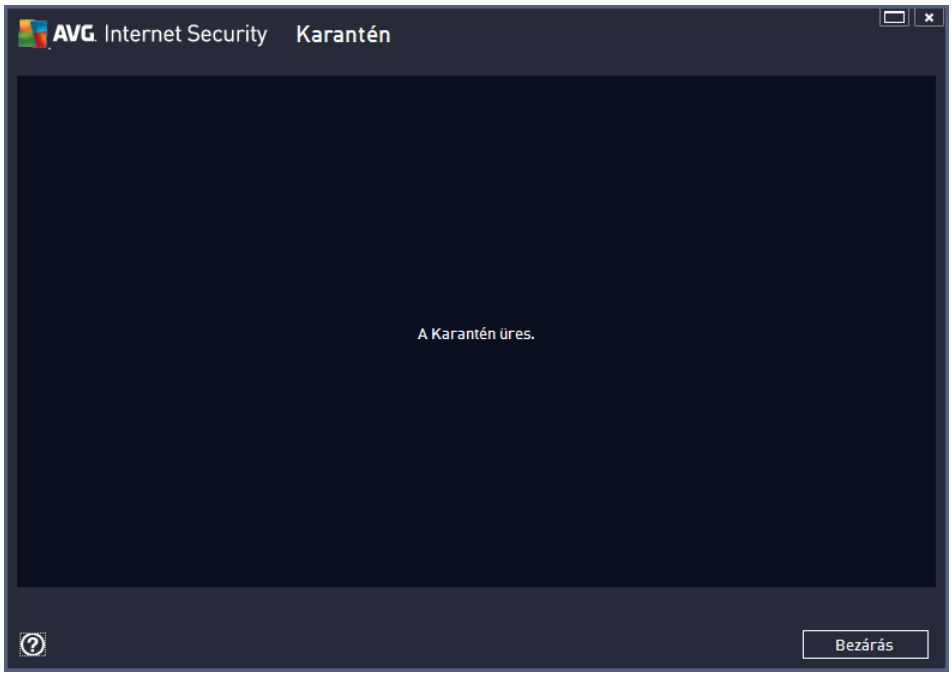
- ***Összegzés*** – A lap alapvető információkat biztosít a vizsgálatról: arról, hogy sikeresen fejeződött-e be, talált-e a rendszer fenyegetéseket, és hogy mi történt azokkal.
- ***Részletek*** – A lap a vizsgálat összes információját megjeleníti, beleértve az észlelt fenyegetések részleteit is. A jelentés exportálása fájlba lehetővé teszi, hogy elmentse ezt egy .csv fájlba.
- ***Észlelések*** – A lap csak akkor jelenik meg, ha a rendszer fenyegetést észlelt a vizsgálat alatt, és részletes információkat biztosít a fenyegetésekről:

  Alacsony súlyosság: információk vagy figyelmeztetések, nem valódi fenyegetések. Általában makrókat tartalmazó dokumentumok, jelszóval védett dokumentumok vagy archívumok, zárolt fájlok stb.

  Közepes súlyosság: általában PUP *(potenciálisan nemkívánatos programok, például reklámprogramok*) vagy nyomkövető cookie-k

  Magas súlyosság: komoly fenyegetések, például vírusok, trójai falovak, biztonsági rések kihasználása stb. Ezenkívül a Heurisztika észlelési módszer által észlelt objektumok, vagyis a vírusadatbázisban még nem leírt fenyegetések.

12. Karantén



A Karantén biztonságos környezetet nyújt az AVG tesztjei során azonosított gyanús/fertőzött fájlok kezeléséhez. Ha a vizsgálat során az AVG vírusirtó fertőzött objektumot talál, és nem tudja automatikusan megjavítani, a program megkérdezi, hogy mihez kezdjen a gyanús objektumokkal. Azt ajánljuk, hogy helyezze át az objektumot a ***Karanténba*** a további műveletekhez. A ***Karantén*** lényege, hogy bármely törölt fájlt megőrizzen egy bizonyos ideig, így meggyőződhet róla, hogy a fájlra nincs szüksége az eredeti helyen. Amennyiben a fájl hiánya problémákat okoz, küldje el a fájlt elemzésre, vagy állítsa vissza az eredeti helyére.

A ***Karantén*** felület külön ablakban nyílik meg, és áttekintést nyújt az elkülönített fertőzött objektumokról:

- ***Tárolás dátuma*** – Azt a dátumot és időt adja meg, amikor a gyanús fájlt a program azonosította és áthelyezte a Karanténba.
- ***Súlyossági szint*** – Ha telepítette a Személyazonosság összetevőt az **AVG Internet Security 2013** programon belül, a kockázati szint grafikus formában jelenik meg egy négyszintű skálán a kifogástalantól *(három zöld pont)* a rendkívül veszélyesig *(három piros pont)*. A fertőzés típusa szintén megjelenik (*a fertőzöttségi szint alapján az objektumok egyértelműen vagy potenciálisan fertőzöttek lehetnek*).
- ***Észlelés neve*** – A felismert fertőzés nevét adja meg az online vírusenciklopédia alapján.
- ***Forrás*** – Megadja, hogy az **AVG Internet Security 2013** melyik összetevője észlelte az adott fenyegetést.
- ***Üzenetek*** – Nagyon ritkán előfordulhat, hogy ebben az oszlopban megjegyzések jelennek az adott észlelt fenyegetésről.

Vezérlőgombok

A következő vezérlőgombok érhetők el a ***Karantén*** felületről:

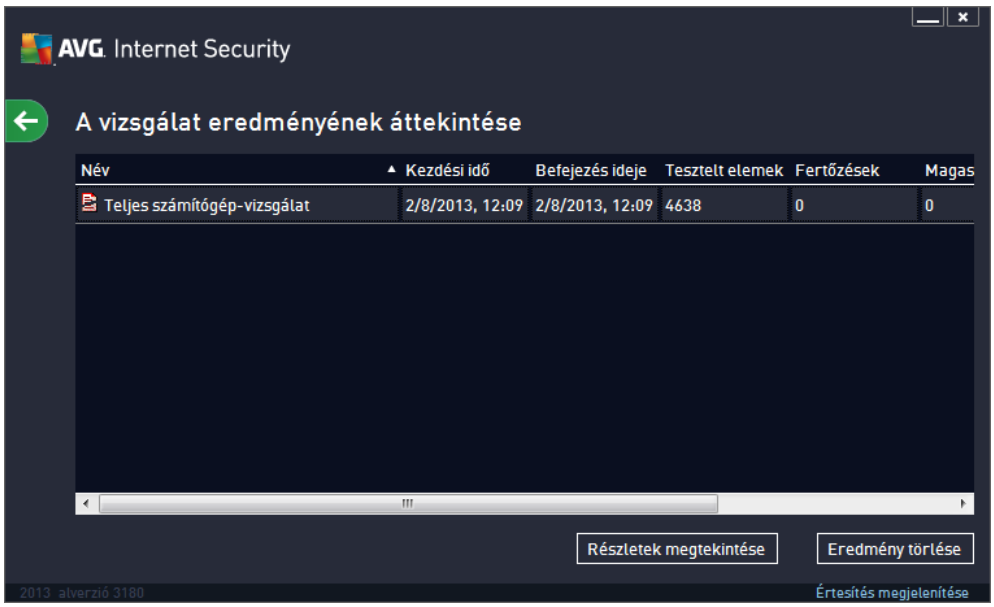
- ***Visszaállítás*** – visszahelyezi a fertőzött fájlt az eredeti helyére a lemezen.
- ***Visszaállítás más néven*** – áthelyezi a fertőzött fájlt egy kiválasztott mappába.
- ***Részletek*** – egy ***Karanténba*** helyezett adott fenyegetés részletes információinak megtekintéséhez jelölje ki a kiválasztott elemet a listán, majd kattintson a ***Részletek*** gombra az észlelt fenyegetés leírását tartalmazó új párbeszédpanel megnyitásához.
- ***Törlés*** – véglegesen és visszavonhatatlanul törli a fertőzött fájlt a ***Karanténból***.
- ***Karantén kiürítése*** – törli a ***Karantén*** tartalmát. A fájlok ***Karanténból*** történő eltávolításával a fájlok véglegesen törlődnek a lemezről (*nem a Lomtárba kerülnek át*).

13. Előzmények

Az ***Előzmények*** szakasz tartalmazza az összes múltbeli esemény *(például a frissítések, vizsgálatok, észlelések stb.) információit* és az ezekről az eseményekről készített jelentéseket. Ez a szakasz a fő felhasználói felületről a ***Beállítások / Előzmények*** elemen keresztül érhető el. Emellett az összes rögzített esemény előzménye a következő részekre van osztva:

- A vizsgálat eredménye
- Állandó védelem találatai
- Az E-mail védelem észlelései
- Az Online szűrő találatai
- Eseménynapló
- Tűzfalnapló

13.1. A vizsgálat eredménye



A ***Vizsgálat eredményének áttekintése*** párbeszédpanel a ***Beállítások / Előzmények / Vizsgálat eredménye*** menüelemen keresztül érhető el az **AVG Internet Security 2013** főablakának felső navigációs sávjáról. A párbeszédpanel tartalmazza az összes korábban indított vizsgálatot és azok eredményeit:

- ***Név*** – vizsgálattól függ; lehet valamelyik alapértelmezett vizsgálat neve, vagy olyan név, melyet Ön adott egy saját ütemezett vizsgálatnak. Minden név tartalmaz egy ikont a vizsgálat eredményére vonatkozólag:

  – a zöld ikon azt jelenti, hogy a program nem talált fertőzést a vizsgálat során

– a kék ikon azt jelenti, hogy a program talált fertőzést a vizsgálat során, de azt automatikusan eltávolította

– a piros ikon azt jelenti, hogy a program talált fertőzést a vizsgálat során, de nem tudta azt eltávolítani!

Mindegyik ikon teljes vagy félbevágott alakú lehet – a teljes azt jelenti, hogy a vizsgálat rendben befejeződött; míg a félbevágott ikon azt jelenti, hogy a vizsgálat megszakadt vagy leállították.

Megjegyzés: *Mindegyik vizsgálattal kapcsolatos további információkért nézze meg a Vizsgálat eredménye ablakot a Részletek megtekintése gombbal (az ablak alján).*

- ***Kezdési idő*** – a dátum és idő a vizsgálat indításakor
- ***Befejezés ideje*** – a dátum és idő a vizsgálat befejezésekor
- ***Vizsgált objektumok*** – a vizsgálat során ellenőrzött objektumok száma
- ***Fertőzések*** – a felismert / eltávolított vírusfertőzések száma
- ***Magas / Közepes*** / ***Alacsony*** – ezekben az oszlopokban található az összes eltávolított/ talált fertőzés száma, valamint a magas, közepes és alacsony súlyossági szintű fertőzések száma
- ***Információk*** – a vizsgálat folyamatával és eredményével kapcsolatos információk *(jellemzően befejezéskor vagy megszakításkor)*
- ***Rootkitek*** – észlelt rootkitek

Vezérlőgombok

A vezérlőgombok a ***Vizsgálat eredményének áttekintése*** ablakban a következők:

- ***Részletek megtekintése*** – nyomja meg ezt a gombot a Vizsgálati eredmények párbeszédpanel megjelenítéséhez és a kijelölt vizsgálat részletes adatainak megtekintéséhez
- ***Eredmény törlése*** – nyomja meg ezt a gombot a kijelölt elem vizsgálati eredményekből történő eltávolításához
- – az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése)* a párbeszédpanel bal felső sarkában található nyíllal térhet vissza

13.2. Állandó védelem találatai

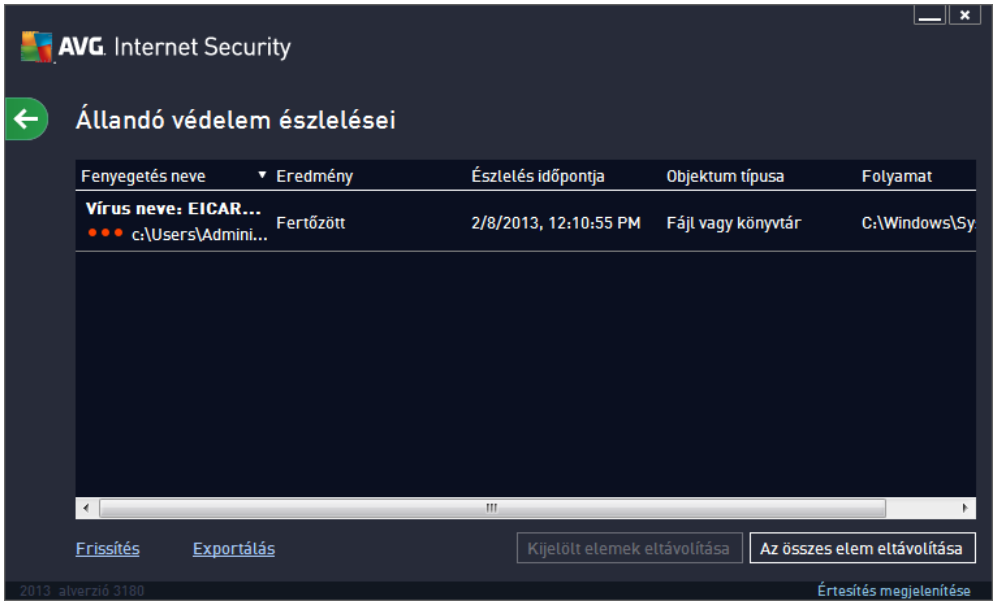
Az ***Állandó védelem*** szolgáltatás a ***Számítógép*** összetevő része és a fájlokat azok másolása, megnyitása és elmentése esetén vizsgálja. Ha a rendszer fenyegetést észlel, akkor azonnal riaszt a következő ablakkal:

Ezen a panelen információt találhat azokról az objektumokról, amelyeket fertőzöttnek minősített a program (*Név*), továbbá itt jelenik meg néhány leíró jellegű tény a felismert fertőzésről (*Leírás*). A Részletek megjelenítése hivatkozás átirányítja az online vírusenciklopédiához, ahol részletes információkat talál az észlelt fertőzésről, ha azok ismertek. A párbeszédpanelben található egy áttekintés is az észlelt fenyegetések kezelésének elérhető megoldásairól. A lehetőségek egyike ajánlottként lesz megjelölve: ***Védelem (ajánlott). Amennyiben lehetséges, mindig válassza ezt a lehetőséget!***

Megjegyzés: *Előfordulhat, hogy az észlelt objektum mérete túllépi a Karantén szabad helyének méretét. Ebben az esetben egy figyelmeztető üzenet jelenik meg, ha Ön fertőzött objektumot próbál áthelyezni a Karanténba. A Karantén mérete módosítható. Ezt az értéket a merevlemez valódi méretének adott százalékában határozhatja meg. A Karantén méretének növeléséhez menjen a Karantén párbeszédpanelre az AVG speciális beállítások részen a „Karantén méretének korlátozása" opcióra.*

A panel alsó részén található a ***Részletek mutatása*** hivatkozás. Kattintson rá egy új ablak megnyitásához, amely részletes adatokat jelenít meg a fertőzés észlelésekor futó folyamatról, illetve a folyamat azonosításáról.

Az Állandó védelem valamennyi találatának listája áttekinthető az ***Állandó védelem találatai*** párbeszédpanelen. A párbeszédpanel a ***Beállítások / Előzmények / Állandó védelem találatai*** menüelemen keresztül érhető el az **AVG Internet Security 2013** főablakának felső navigációs sávjáról. A párbeszédablak megmutatja az állandó védelem által azonosított és veszélyesnek minősített elemeket, amelyek javítása vagy áthelyezése a Karanténba megtörtént.



Minden észlelt objektumnál a következő információk állnak rendelkezésre:

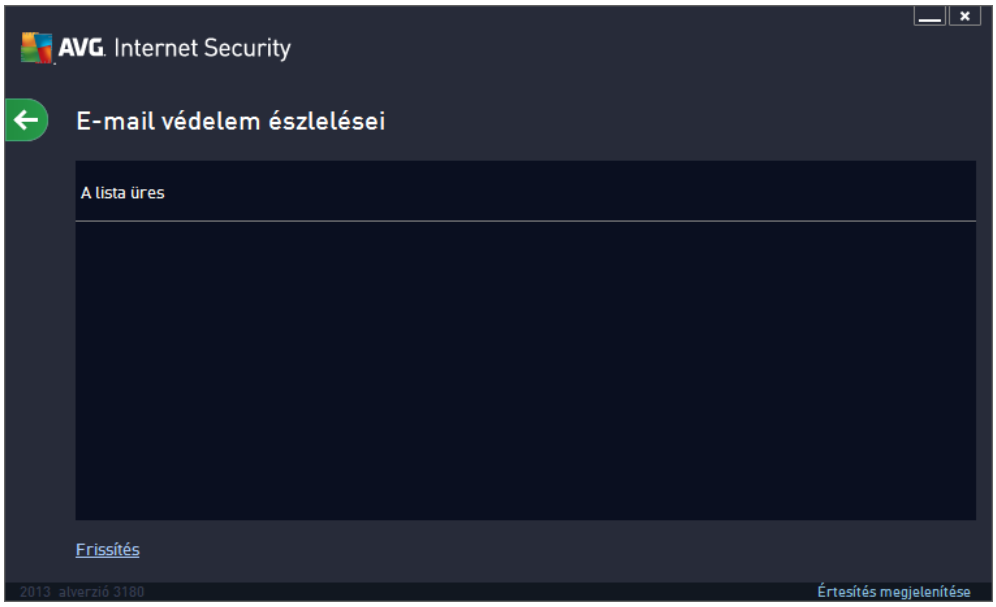
- ***Észlelés neve*** – az észlelt objektum és helyének leírása (*neve*)
- ***Eredmény*** – az észlelt objektumon végzett művelet
- ***Észlelési idő*** – azon dátum és időpont, amikor a program észlelte és letiltota a fenyegetést
- ***Objektum típusa*** – az észlelt objektum típusa
- ***Folyamat*** – milyen művelet váltotta ki a potenciálisan veszélyes objektum megjelenését illetve észlelését

Vezérlőgombok

- ***Frissítés*** – frissíti az ***Online szűrő***
- ***Exportálás*** – exportálja az észlelt elemek teljes listáját egy fájlba
- ***Kijelölt elemek eltávolítása*** – a listában kijelölheti a kiválasztott bejegyzéseket, és ezzel a gombbal törölheti a kiválasztott elemeket
- ***Összes fenyegetés eltávolítása*** – a gomb használatával törölheti a párbeszédablakban megjelenített összes bejegyzést
- – az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése)* a párbeszédpanel bal felső sarkában található nyíllal térhet vissza

13.3. Az E-mail védelem észlelései

Az ***E-mail védelem észlelései*** párbeszédpanel a ***Beállítások/Előzmények/E-mail védelem észlelései*** menüelemen keresztül érhető el az **AVG Internet Security 2013** főablakának felső navigációs sávjáról.



A párbeszédpanel megjeleníti az E-mailek összetevő által észlelt összes találat listáját. Minden észlelt objektumnál a következő információk állnak rendelkezésre:

- ***Észlelés neve*** – az észlelt objektum és forrásának leírása *(esetleg neve is)*
- ***Eredmény*** – az észlelt objektumon végzett művelet
- ***Észlelési idő*** – megmutatja a gyanús objektum azonosításának dátumát és idejét
- ***Objektum típusa*** – az észlelt objektum típusa
- ***Folyamat*** – milyen művelet váltotta ki a potenciálisan veszélyes objektum megjelenését illetve észlelését

A párbeszédpanel alsó részén, a lista alatt, az észlelt objektumok teljes számával kapcsolatos információkat talál. Exportálhatja az észlelt elemek teljes listáját egy fájlba (***Lista exportálása fájlba***), és törölheti az észlelt elemek összes bejegyzését is (***Lista ürítése***).

Vezérlőgombok

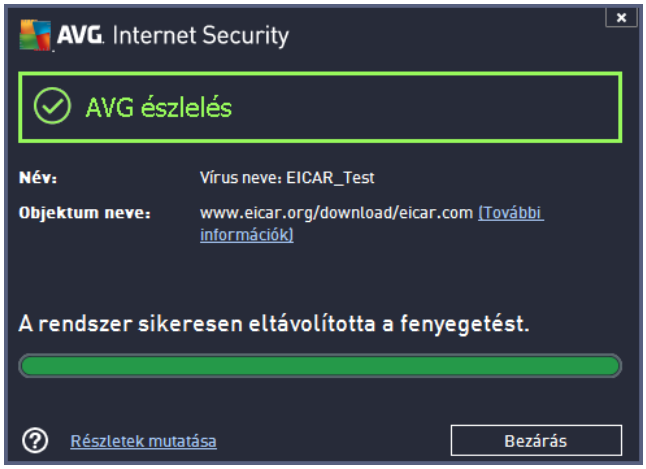
A vezérlőgombok az ***E-mail vizsgáló*** felületen a következők:

- ***Lista frissítése*** – frissíti az észlelt fenyegetések listáját.
- – az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése)* a

párbeszédpanel bal felső sarkában található nyíllal térhet vissza

13.4. Az Online szűrő találatai

Az Online szűrő ellenőrzi a meglátogatandó weboldalakat (és az esetlegesen beágyazott dokumentumokat), mielőtt azok megjelennének a webböngészőben vagy letöltődnének a számítógépre. Ha fenyegetést észlel, akkor azonnal riaszt a következő ablakkal:

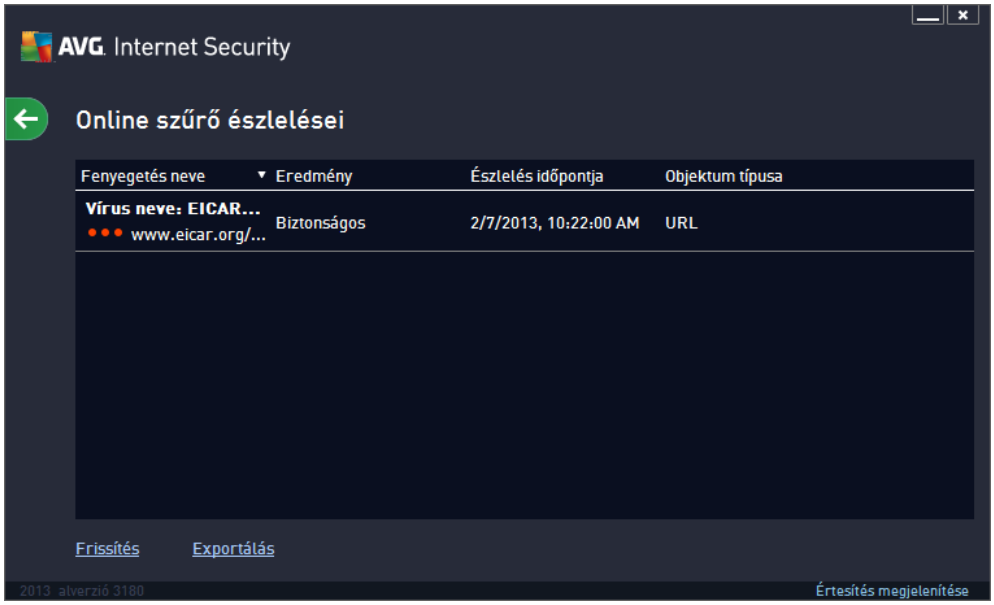


Ezen a panelen információt találhat azokról az objektumokról, amelyeket fertőzöttnek minősített a program (*Név*), továbbá itt jelenik meg néhány leíró jellegű tény a felismert fertőzésről (*Leírás*). A Részletek megjelenítése hivatkozás átirányítja az online vírusenciklopédiához, ahol részletes információkat talál az észlelt fertőzésről, ha azok ismertek. A párbeszédpanel a következő vezérlőelemeket tartalmazza:

- ***Részletek megjelenítése*** – kattintson a hivatkozásra egy új felbukkanó ablak megnyitásához, ahol információkat találhat a fertőzés észlelésekor futó folyamatról, illetve a folyamat azonosításáról.

- ***Bezár*** – kattintson erre a gombra a panel bezárásához.

A gyanús oldal nem lesz megnyitva, és a program a fenyegetést naplózza az ***Online szűrő találataiban***. Az észlelt fenyegetések áttekintése a ***Beállítások / Előzmények / Online szűrő találatai*** menüelemen keresztül érhető el az **AVG Internet Security 2013** főablakának felső navigációs sávjáról.



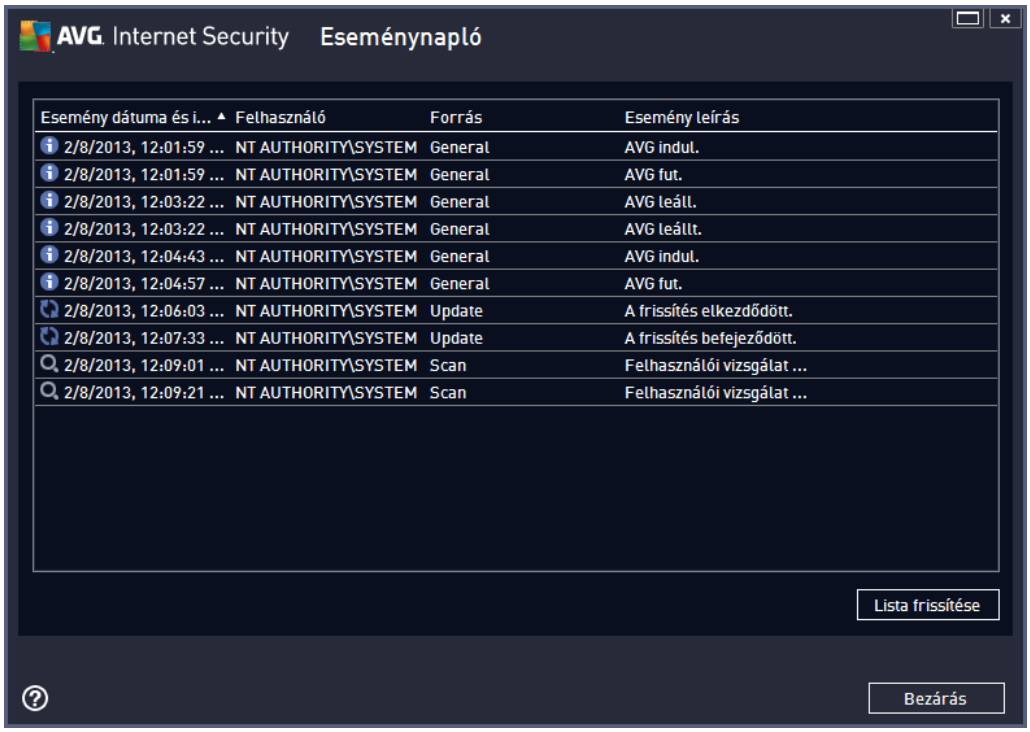
Minden észlelt objektumnál a következő információk állnak rendelkezésre:

- ***Észlelés neve*** – az észlelt objektum és forrásának (*weboldalának*) leírása (*esetleg neve is*)
- ***Eredmény*** – az észlelt objektumon végzett művelet
- ***Észlelési idő*** – azon dátum és időpont, amikor a program észlelte és letiltota a fenyegetést
- ***Objektum típusa*** – az észlelt objektum típusa
- ***Folyamat*** – milyen művelet váltotta ki a potenciálisan veszélyes objektum megjelenését illetve észlelését

Vezérlőgombok

- ***Frissítés*** – frissíti az ***Online szűrő***
- ***Exportálás*** – exportálja az észlelt elemek teljes listáját egy fájlba
- – az alapértelmezett AVG fő párbeszédpanelre *(összetevők áttekintése)* a párbeszédpanel bal felső sarkában található nyíllal térhet vissza

13.5. Eseménynapló



Az ***Eseménynapló*** párbeszédpanel a ***Beállítások / Előzmények / Eseménynapló*** menüelemen keresztül érhető el az **AVG Internet Security 2013** főablakának felső navigációs sávjáról. Ezen a panelen az **AVG Internet Security 2013** működése közben fellépett fontosabb események összegzését tekintheti át. A párbeszédpanel a következő típusú események bejegyzéseit tartalmazza: információ az AVG alkalmazás frissítéséről; információ a vizsgálat kezdetéről, végéről és leállításáról (*beleértve az automatikusan elvégzett teszteket*); a vírusészleléshez kapcsolódó eseményekről szóló információk (*állandó védelem vagy keresés* segítségével) az előfordulás helyével együtt; és egyéb fontos események.

Az egyes eseményeknél a következő adatok találhatók:

- ***Az Esemény dátuma és ideje*** az esemény bekövetkezésének pontos dátumát és idejét adja meg.
- ***A Felhasználó*** az esemény bekövetkezésekor aktuálisan bejelentkezett felhasználó nevét mutatja.
- ***A Forrás*** a forrás összetevőjének adatait vagy az AVG rendszer más, az eseményt kiváltó részét mutatja.
- ***Az Esemény leírása*** röviden leírja, hogy mi történt.

Vezérlőgombok

- ***Lista frissítése –*** a gomb megnyomásával az összes bejegyzést frissítheti az események listájában

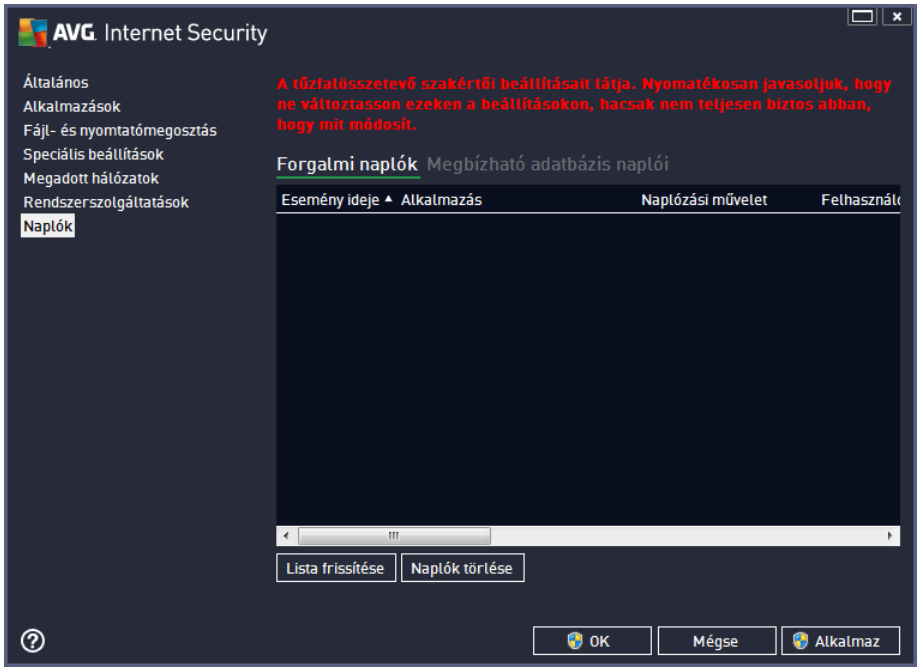
- ***Bezárás*** – a gomb lenyomásával visszatérhet a **AVG Internet Security 2013** fő ablakhoz

13.6. Tűzfalnapló

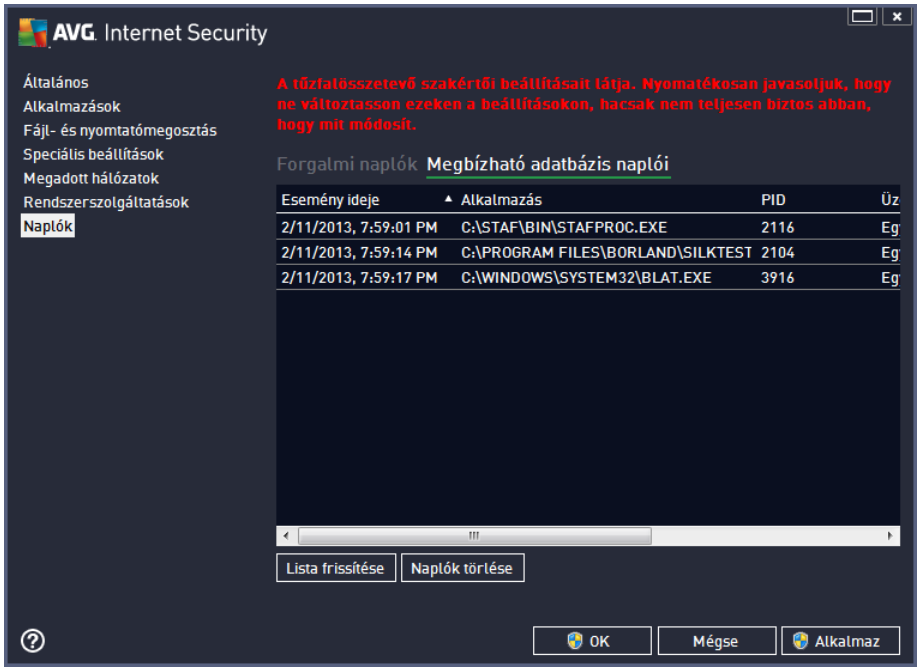
Ez a párbeszédpanel a speciális beállítások megadására szolgál, és javasoljuk, hogy ne módosítsa ezeket a beállításokat, csak ha teljesen biztos a dolgában.

A ***Naplók*** párbeszédpanel lehetővé teszi, hogy áttekintse a két lapon megjelenített Tűzfal műveletek és események részletes naplóját:

- ***Forgalmi naplók*** – Ez a lap információkat biztosít a hálózatot elérni kívánó összes alkalmazás tevékenységéről. Valamennyi elemre vonatkozóan információt talál az esemény ideje, az alkalmazás neve, a kapcsolódó naplóművelet, a felhasználó neve, a PID, a forgalom iránya, a protokoll típusa, a távoli és a helyi portok száma és a helyi és távoli IP cím vonatkozásában.



- ***Megbízható adatbázis naplói*** – *A Megbízható adatbázis* egy olyan belső AVG adatbázis, amely információkat gyűjt a megbízható és tanúsított alkalmazásokról (amelyek mindig kommunikálhatnak az interneten). Ha egy új alkalmazás csatlakozni próbál a hálózatra (*és még nincs tűzfalszabály meghatározva az alkalmazáshoz*), akkor Önnek kell eldöntenie, hogy engedélyezi-e a hálózati kommunikációt az adott alkalmazás számára. Az AVG ellenőrzi a *Megbízható adatbázist*, és ha az alkalmazás megtalálható benne, akkor azt automatikusan kiengedi a hálózatra. Ha a program nem talál semmilyen információt az alkalmazásról az adatbázisban, akkor Ön egy külön párbeszédpanelen engedélyezheti az alkalmazás számára a hálózati hozzáférést.



Vezérlőgombok

- ***Lista frissítése*** – Az összes naplózott paramétert a következők alapján lehet rendezni: időrendben (*dátum*) vagy ABC sorrendben (*egyéb oszlopk*) - csak kattintson az adott oszlopra. Használja a ***Lista frissítése*** gombot a megjelenített információk frissítéséhez.

- ***Naplók törlése*** – kattintson ide a táblázatban található összes bejegyzés törléséhez.

14. AVG frissítések

Semmilyen biztonsági szoftver nem garantálhat védelmet a különböző típusú fenyegetések ellen, ha az nincs rendszeresen frissítve. A vírusok készítői mindig újabb és újabb kihasználható hibákat keresnek az egyes szoftverekben és operációs rendszerekben. Új vírusok, rosszindulatú kódok és hackelési stratégiák jelennek meg minden egyes nap. Ezért a szoftvergyártók folyamatosan adnak ki frissítéseket és biztonsági javításokat újonnan felfedezett biztonsági rések betöméséhez.

Tekintettel az újonnan megjelenő számítógépes fenyegetések természetére és elterjedésük gyorsaságára, alapvető fontosságú az **AVG Internet Security 2013** rendszeres frissítése. A legjobb megoldás, ha megtartja az alapértelmezett beállításokat, amelyek szabályozzák az automatikus frissítést is. Felhívjuk figyelmét, hogy amennyiben az **AVG Internet Security 2013** vírusadatbázisa nem naprakész, a program nem képes felismerni a legújabb veszélyforrásokat.

Kulcsfontosságú, hogy rendszeresen frissítse az AVG programot. A vírusdefiníciós adatbázisokat lehetőleg naponta frissítse. A kevésbé fontos programfrissítéseket elég hetente elvégezni.

14.1. Frissítés indítása

A lehető legnagyobb biztonság elérése érdekében az **AVG Internet Security 2013** alapértelmezés szerint négy óránként ellenőrzi a vírusadatbázis frissítéseit. Mivel az AVG frissítések nem előre meghatározott ütemezés szerint jelennek meg, hanem az új fenyegetések mértéke és súlyossága alapján, ezért az ellenőrzés nagyon fontos az AVG vírusadatbázisának naprakészen tartásához.

Ha azonnal ellenőrizni kívánja a frissítéseket, használja a fő felhasználói felületen található Frissítés gyorshivatkozást. A hivatkozás mindig, az összes felhasználói felületi ablakból elérhető. Amikor elindítja a frissítést, az AVG először ellenőrzi, hogy elérhetők-e új frissítési fájlok. Ha igen, akkor az **AVG Internet Security 2013** elindítja a letöltést és a frissítési folyamatot. Az AVG tálcaikon feletti párbeszédpanelen látja a frissítés eredményeit.

Ha csökkenteni kívánja a frissítés-ellenőrzések számát, megadhatja saját beállításait is. Azonban ***határozottan ajánlott a frissítést naponta legalább egyszer elindítani.*** A beállítást a Speciális beállítások/Ütemezések szakaszban lehet elvégezni, a következő párbeszédpaneleken:

- Vírusdefiníciók frissítésének ütemezése
- Programfrissítés ütemezése
- Levélszemétszűrő frissítés ütemezése

14.2. Frissítési szintek

Az AVG Internet Security 2013 kétféle frissítési szintet kínál:

- ***Az adatbázisfrissítés*** a vírusok, levélszemetek és rosszindulatú programok elleni megbízható védelemhez szükséges módosításokat tartalmazza. A kód módosítását általában nem foglalja magában, csak a vírusadatbázis frissítésére szolgál. A frissítést rögtön alkalmazni kell, amint elérhető.
- ***A Programfrissítés*** a program különböző módosításait, javításait és fejlesztéseit tartalmazza.

A frissítés ütemezésekor mindkét frissítési szint paraméterei megadhatók:

- Vírusdefiníciók frissítésének ütemezése
- Programfrissítés ütemezése

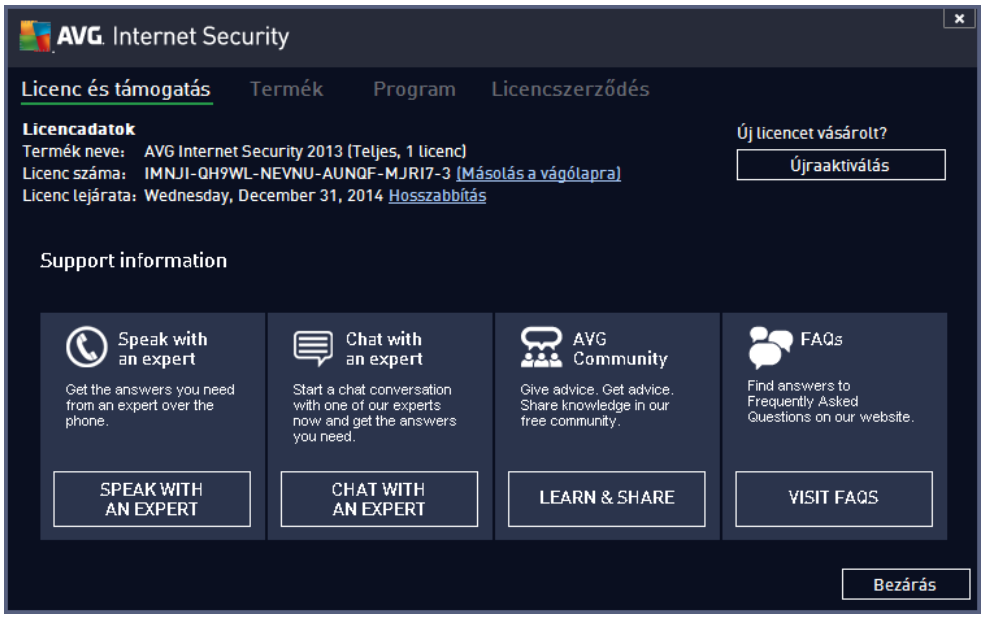
Megjegyzés: *Ha az ütemezett programfrissítés és az ütemezett vizsgálat időben egybeesik, akkor a frissítési folyamatnak van elsődleges prioritása, és a vizsgálat meg lesz szakítva.*

15. Gyakori kérdések és műszaki támogatás

Ha az **AVG Internet Security 2013**termékkel kapcsolatban bármilyen értékesítési vagy technikai problémája van, több módon is segítséghez juthat. Kérjük, válasszon a következő lehetőségek közül:

- ***Támogatás kérése***: Közvetlenül az AVG alkalmazásból elérheti az AVG webhelyén található, e célra létrehozott ügyfél-támogatási oldalt (http://www.avg.com/). Válassza a főmenü ***Súgó/Támogatás kérése*** lehetőségét az AVG webhelyére történő ugráshoz és a támogatás eléréséhez. A folytatáshoz kövesse a weboldalon megjelenő utasításokat.

- *Támogatás (főmenü hivatkozás)*: az AVG alkalmazás menüben (*a fő felhasználói felület tetején*) megtalálható a ***Támogatás*** hivatkozás, amely egy új párbeszédpanelt nyit meg. Ezen az összes szükséges információ megtalálható a segítségkéréshez. A párbeszédpanel a telepített AVG program alapvető adatait (*program / adatbázis-verzió*), a licencadatokat, és a gyorstámogatási hivatkozások listáját tartalmazza:



- ***A súgófájlban található hibaelhárítás***: Az **AVG Internet Security 2013** súgófájljának részeként közvetlenül elérhető egy új ***Hibaelhárítás*** nevű szakasz *(a súgófájl megnyitásához az alkalmazás bármelyik párbeszédpanelén nyomja meg az F1 billentyűt)*. Ez a szakasz a leggyakrabban előforduló olyan helyzetek listáját tartalmazza, amikor egy felhasználónak szakértői segítségre van szüksége egy technikai problémával kapcsolatban. Válassza ki azt a szituációt, amely a legjobban leírja a problémáját, és kattintson rá a probléma megoldását részletesen leíró útmutatás megnyitásához.

- ***AVG webhely támogatási központ***: Az AVG webhelyén (http://www.avg.com/) is kereshet megoldást a problémájára. ***A Támogató központ*** szakaszban tematikus csoportok strukturált listáját találja, melyek mind értékesítési, mind technikai problémákkal foglalkoznak.

- ***Gyakori kérdések***: Az AVG webhelyén (http://www.avg.com/) egy, a gyakori kérdésekkel foglalkozó, különálló és részletesen kidolgozott szakaszt is talál. Ez a szakasz a ***Támogatási központ / GYIK*** menüponton keresztül érhető el. A kérdések itt is jól

rendszerezve, értékesítés, technikai problémák illetve vírus kategóriákba sorolva tekinthetők meg.

- ***Vírusokról és fenyegetésekről***: Az AVG webhely (http://www.avg.com/) egy külön fejezete foglalkozik a vírusokkal kapcsolatos problémákkal *(a weboldal a főmenüből érhető el a Súgó / A vírusok és fenyegetések ismertetése)*. Az online fenyegetésekkel kapcsolatos strukturált információkat tartalmazó oldalra történő belépéshez a menüben válassza a ***Támogatási központ / Vírusokról és fenyegetésekről*** lehetőséget. Itt a vírusok és kémprogramok eltávolításához talál útmutatót, valamint tanácsokat azzal kapcsolatban, hogyan tudhatja számítógépét mindig biztonságban.

- ***Vitafórum***: Használhatja az AVG felhasználók a http://forums.avg.com webhelyen található vitafórumát is.