bitdefender

ANTIVIRUS 2008

Manual de utilizare

BitDefender Antivirus 2008

Manual de utilizare

Publicat 2007.09.19

Termeni legali


bitdefender

Cuprins

Licență şi garanție

DACĂ NU SUNTEȚI DE ACORD CU ACEŞTI TERMENI ŞI CU ACESTE CONDIȚII NU INSTALAȚI ACEST SOFT. SELECTÂND "ACCEPT", "OK", "CONTINUĂ", "DA" SAU INSTALÂND SAU UTILIZÂND SOFTUL ÎN ORICE FEL INDICAȚI COMPLETA ÎNȚELEGERE ŞI ACCEPTARE A TERMENILOR CONTRACTULUI DE LICENȚĂ.

Aceşti Termeni acoperă soluțiile şi serviciile BitDefender, incluzând documentația asociată şi orice fel de actualizare a aplicației furnizată dumneavoastră în baza licenței achiziționate sau orice înțelegere de servicii asociată, definită în documentație, şi orice copie a acestor obiecte.

Acest Contract de Licență reprezintă o convenție legală între dumneavoastră (ca persoană fizică sau persoană juridică utilizator final) şi BITDEFENDER pentru utilizarea produsului soft identificat mai sus, aparținând BITDEFENDER, care include softul propriu-zis şi serviciile, şi poate include, medii de informație asociate, materiale tipărite şi documentație "on line" sau electronică (referite mai departe ca "BitDefender"). Toate acestea sunt protejate de legislația internațională privind drepturile de autor şi proprietatea intelectuală, precum şi de tratatele internaționale. Prin instalarea, copierea sau utilizarea, în orice alt mod, a produsului BitDefender, acceptați termenii acestui contract.

Dacă nu sunteți de acord cu termenii acestui contract, nu instalați şi nu utilizați produsul BitDefender.

Licența BitDefender. BitDefender este protejat de tratatele şi legile internaționale privind drepturile de autor, precum şi de celelalte legi şi tratate privind proprietatea intelectuală. BitDefender este oferit sub licență şi nu vândut.

ACORDAREA LICENȚEI. BITDEFENDER vă oferă, dumneavoastră şi numai dumneavoastră, următoarea licență ne-exclusivă, limitată, netransferabilă pentru utilizarea produsului BitDefender.

APLICAȚIA SOFTWARE. Puteți instala şi utiliza BitDefender pe oricâte calculatoare este necesar în limita numărului total de licențe de utilizator deținute. Puteți face o singură copie adițională, ca rezervă.

LICENȚA UTILIZATORULUI DE DESKTOP. Această licență se aplică acelui soft BitDefender ce poate fi instalat doar pe un singur calculator şi care nu furnizează servicii pentru rețele. Fiecare utilizator principal poate instala acest soft pe un singur calculator şi poate face doar o singură copie adițională, ca rezervă, pe un dispozitiv diferit. Numărul de utilizatori principali permis este numărul de utilizatori ai licenței.

DURATA LICENȚEI. Licența acordată aici va începe la data la care veți instala BitDefender şi va continua doar până la sfârşitul perioadei pentru care licența a fost achiziționată.

EXPIRARE. Produsul va înceta să mai funcționeze imediat după expirarea licenței.

ACTUALIZĂRI DE PRODUS (UPGRADE-URI). Dacă BitDefender este etichetat ca upgrade, va trebui să dețineți o licență de utilizare a unui produs identificat de BITDEFENDER ca fiind eligibil pentru respectivul upgrade. Un produs BitDefender etichetat ca fiind upgrade, înlocuieşte şi/sau completează produsul care reprezintă baza dreptului dumneavoastră de a beneficia de actualizarea de produs. Puteți utiliza produsul rezultat în urma actualizării numai în concordantă cu termenii specificați în prezentul Contract de Licență. Dacă BitDefender este un upgrade al unei componente a unui pachet de programe soft care v-au fost licențiate ca un singur produs, atunci BitDefender poate fi utilizat sau transferat numai ca parte a acelui pachet individual de produse şi nu poate fi separat pentru utilizarea sa de către mai mulți utilizatori decât numărul de licențe. Termenii şi condițiile acestei licențe înlocuiesc şi prevalează orice alte înțelegeri care ar fi putut exista între dumneavoastră şi BITDEFENDER privind produsul original sau produsul rezultat ca urmare a actualizării.

COPYRIGHT. Toate drepturile, titlurile şi beneficiile ce țin de BitDefender (inclusiv, dar fără a se limita la orice imagine, fotografie, animație, video, audio, muzică, text şi cod, încorporate în produsul BitDefender), toate materialele tipărite care însoțesc produsul şi orice copie a produsului BitDefender sunt proprietatea BITDEFENDER. BitDefender este protejat de legile şi tratatele internaționale privind drepturile de autor şi proprietatea intelectuală. Prin urmare, BitDefender trebuie tratat ca orice alt material supus drepturilor de autor. Nu aveți dreptul să copiați materialele tipărite ce însoțesc BitDefender. Aveți obligația de a prezenta şi include toate notele privind drepturile de autor în forma lor originală în toate copiile create, indiferent de mediul de transmisie sau de forma în care BitDefender există. Sunt interzise sub-licențierea, închirierea, vinderea, cedarea sau împărțirea licenței BitDefender. De asemenea, sunt interzise piratarea, recompilarea, dezasamblarea, crearea de produse derivate, modificarea, traducerea sau orice altă încercare de a descoperi codul sursă al produsului BitDefender.

LIMITAREA GARANȚIEI. BITDEFENDER garantează lipsa oricărui defect al suportului de distribuire al produsului BitDefender timp de 30 de zile de la data achiziționării acestuia. În cazul apariției unui defect al suportului de distribuire, ca unică modalitate de despăgubire pentru încălcarea acestei garanții, BITDEFENDER poate înlocui, la latitudinea sa, suportul defect returnat, cu un altul în schimbul chitanței sau vă poate returna costul produsului BitDefender. BITDEFENDER nu garantează funcționarea neîntreruptă a produsului, lipsa erorilor sau posibilitatea corectării acestora.

BITDEFENDER nu poate garanta ca produsele BitDefender corespund in totalitate cerintelor dumneavoastra.

CU EXCEPȚIA CELOR PRECIZATE ÎN MOD EXPLICIT ÎN ACEASTĂ ÎNȚELEGERE, BITDEFENDER ÎŞI DECLINĂ RESPONSABILITATEA PENTRU ORICE ALTE GARANȚII, EXPLICITE SAU IMPLICITE, CE PRIVESC PRODUSELE, ÎMBUNĂTĂȚIRILE, ÎNTREȚINEREA SAU SUPORTUL LEGAT DE ACESTEA, SAU ORICE ALTE MATERIALE (TANGIBILE SAU INTANGIBILE) SAU SERVICII FURNIZATE. BITDEFENDER DECLINĂ ÎN MOD EXPLICIT ORICE GARANȚII ŞI CONDIȚII IMPLICITE, INCLUZÂND, FĂRĂ LIMITARE, GARANȚIILE IMPLICITE ALE VANDABILITĂȚII, UTILIZĂRII ÎNTR-UN ANUMIT SCOP, TITLULUI, NON-INTERFERENȚEI, ACURATEȚEI DATELOR, A CONȚINUTULUI INFORMAȚIONAL, INTEGRĂRII SISTEMULUI ŞI NEÎNCĂLCĂRII DREPTURILOR UNOR TERȚE PĂRȚI PRIN FILTRAREA, DEZACTIVAREA SAU ÎNDEPĂRTAREA SOFTULUI ACESTORA, A APLICAȚIILOR SPYWARE, ADWARE, A FIŞIERELOR COOKIE, MESAJELOR E-MAIL, DOCUMENTELOR, RECLAMELOR SAU A ALTORA DE GENUL, INDIFERENT DACĂ ACEASTA REIESE DIN STATUT, LEGE, FUNCȚIONARE SAU COMERȚ.

DECLINAREA RESPONSABILITĂȚII ÎN CAZ DE DAUNE. Orice persoană care utilizează, testează sau evaluează BitDefender îşi asumă riscul legat de calitatea şi performanța acestuia. BITDEFENDER nu va fi responsabilă, în niciun caz, pentru daune de orice natură, incluzând, fără limitare, daune directe sau indirecte, rezultate din utilizarea, performanța sau livrarea BitDefender, chiar dacă BITDEFENDER a fost informată de existența sau posibilitatea apariției acestora. UNELE STATE INTERZIC LIMITAREA SAU DECLINAREA RESPONSABILITĂȚII ÎN CAZUL DAUNELOR INDIRECTE, DECI CELE MENȚIONATE MAI SUS S-AR PUTEA SĂ NU SE APLICE ÎN CAZUL DUMNEAVOASTRĂ. ÎN NICIUN CAZ, RESPONSABILITATEA BITDEFENDER NU VA DEPĂŞI PREȚUL DE ACHIZIȚIE AL PRODUSULUI BITDEFENDER. Declarațiile de limitare şi declinare a responsabilității de mai sus se vor aplica indiferent dacă acceptați să folosiți, evaluați sau testați BitDefender.

ANUNȚ IMPORTANT PENTRU UTILIZATORI. ACEST SOFT POATE CONȚINE ERORI ŞI NU ESTE PROIECTAT SAU DESTINAT UTILIZĂRII ÎNTR-UN MEDIU CU GRAD MARE DE RISC ŞI CARE NECESITĂ O PERFORMANȚĂ SAU FUNCȚIONARE ÎN CONDIȚII DE SECURITATE ABSOLUTĂ. ACEST PRODUS NU ESTE DESTINAT UTILIZĂRII ÎN OPERAȚIUNI DIN DOMENIUL AVIAȚIEI, SECTORUL NUCLEAR SAU SISTEME DE COMUNICAȚII, SECTORUL ARMAMENTULUI, SISTEME DIRECTE SAU INDIRECTE DE MENȚINERE A VIEȚII, CONTROLUL TRAFICULUI AERIAN SAU ORICE ALTĂ APLICAȚIE SAU INSTALAȚIE ÎN CARE APARIȚIA UNEI EROARI AR PUTEA CAUZA MOARTEA SAU RĂNIREA GRAVĂ A UNOR PERSOANE SAU DAUNE ALE PROPRIETĂȚII.

GENERAL. Această înțelegere se află sub incidența legilor din România şi a regulamentelor şi tratatelor internaționale privind drepturile de autor şi proprietatea intelectuală. Jurisdicția exclusivă şi locația judecării oricărei dispute ce ar putea reieşi din aceşti termeni de licență va fi cea a tribunalelor din Romania.

Prețurile, costurile şi sumele de bani pentru utilizarea BitDefender pot fi modificate fără să fiți anunțat în prealabil.

În eventualitatea invalidității oricărei porțiuni a acestei Înțelegeri, respectiva invaliditate nu va afecta validitatea celorlalte porțiuni ale acestei Înțelegeri.

BitDefender şi simbolurile BitDefender sunt mărci înregistrate ale BITDEFENDER. Toate celelalte mărci înregistrate utilizate în produs sau în materialele asociate sunt proprietatea deținătorilor lor de drept.

Licența se va încheia imediat, fără a fi anunțat, în cazul în care încălcați oricare dintre termenii sau condițiile ei. În urma terminării licenței nu veți fi îndreptățit la returnarea banilor de către BitDefender sau oricare dintre distribuitorii BitDefender. Termenii şi condițiile privind confidențialitatea şi restricțiile de utilizare vor rămâne în vigoare şi după orice terminare a licenței.

BITDEFENDER poate revizui aceşti termeni în orice moment, iar termenii revizuiți se vor aplica în mod automat versiunilor soft corespunzătoare, distribuite cu termenii revizuiți. Dacă oricare parte a acestor termeni este găsită nulă şi neavenită, acest lucru nu va afecta validitatea restului termenilor, ce vor rămâne în vigoare.

În cazul controverselor sau inconsistențelor dintre traducerile acestor termeni în alte limbi, va prevala versiunea în limba engleză publicată de BITDEFENDER.

Contactați BITDEFENDER la Str. Fabrica de Glucoză nr. 5, 72322-Sector 2, Bucureşti, România, sau la numărul de telefon: 40-21-2330780 sau Fax: 40-21-2330763, adresă e-mail: sales@bitdefender.ro.

Prefață

Acest manual se adresează tuturor utilizatorilor care au ales **BitDefender Antivirus 2008** ca soluție de securitate pentru calculatoarele personale. Informațiile incluse în acest manual sunt destinate nu numai utilizatorilor avansați, ci şi oricărei persoane care poate lucra în sistemul Windows.

Acest manual vă prezintă **BitDefender Antivirus 2008**, Compania şi echipa care l-au dezvoltat, vă ghidează în timpul procesului de instalare a produsului şi vă învață cum să-l configurați. Veți afla cum să utilizați **BitDefender Antivirus 2008**, cum să-l actualizați, testați şi personalizați. Veți învăța cum să obțineți beneficii maxime din BitDefender.

Vă dorim o lectură plăcută şi utilă.

1. Convenții utilizate în manual

1.1. Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai uşoară. Aspectul şi semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
`sample syntax`	Exemplele de sintaxă sunt tipărite cu caractere `monospațiate`.
http://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
support@bitdefender.com	Adresele de e-mail sunt inserate în text ca adrese de contact.
“Prefață” (p. xi)	Acesta este un link intern, către o locație din document.
`filename`	Numele fişierelor şi ale directoarelor sunt tipărite cu caractere `monospațiate`.
option	Toate opțiunile produsului sunt tipărite cu caractere **aldine**.

Aspect	Descriere
`sample code listing`	Liniile de cod sunt tipărite cu caractere monospațiate.

1.2. Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Notă
Nota nu este decât o scurtă observație. Deşi pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect asemănător.

Important
Acest lucru necesită atenția dumneavoastră şi nu este recomandat să-l ocoliți. De obicei, aici sunt furnizate informații importante, dar nu cruciale.

Avertisment
Este vorba de informații cruciale, cărora trebuie să le acordați o mare atenție. Dacă urmați indicațiile, nu se va întâmpla nimic rău. Este indicat să citiți şi să înțelegeți despre ce este vorba, deoarece este descris ceva extrem de riscant.

2. Structura manualului

Manualul conține mai multe părți ce acoperă subiectele majore. În plus, vă este oferit un vocabular pentru clarificarea înțelesului anumitor termeni tehnici.

Instalare. Instrucțiuni de instalare pas cu pas a BitDefender pe o stație de lucru. Acesta este un ghid complet pentru instalarea **BitDefender Antivirus 2008**. Începând cu cerințele pentru o instalare corectă, sunteți ghidat de-a lungul întregului proces de instalare. La sfârşit este descrisă şi procedura de dezinstalare a BitDefender, pentru cazul în care doriți să faceți acest lucru.

Administrare elementară. Descriere a administrării elementare a BitDefender.

Administrare avansată a securității. Aceasta este o prezentare detaliată a tipurilor de protecție oferite de BitDefender. Capitolele explică în detaliu toate opțiunile consolei de setări avansate. Sunteți învățat cum să configurați şi să utilizați toate modulele BitDefender astfel încât să vă protejați eficient calculatorul împotriva oricăror amenințări malițioase (viruşi, aplicații spyware, rootkit-uri şi altele).

BitDefender Rescue CD. Aceasta este o descriere a BitDefender Rescue CD. Vă ajută să înțelegeți şi să utilizați funcțiile oferite de acest CD de boot.

Obținere ajutor. Unde să căutați şi unde să cereți ajutor în cazul în care apar situații neprevăzute.

Vocabular. Vocabularul încearcă să explice unii termeni tehnici sau neobişnuiți pe care îi veți găsi în paginile acestui document.

3. Comentarii

Vă invităm să ne ajutați să îmbunătățim acest manual. Am testat şi verificat toate informațiile, în măsura posibilităților noastre. Vă rugăm să ne scrieți despre orice inexactități pe care le veți găsi în această carte sau despre cum credeți că ar putea fi îmbunătățită, pentru a ne ajuta să vă oferim cea mai bună documentație.

Aveți la dispoziție următoarea adresă de e-mail documentation@bitdefender.com.

Important
Vă rugăm să scrieți în engleză sau română mailurile către adresa de mai sus pentru a le putea procesa cât mai eficient.

Instalare

1. Instalarea BitDefender Antivirus 2008

Secțiunea **Instalarea BitDefender Antivirus 2008** a acestui manual de utilizare conține următoarele subiecte:

- Cerințe de sistem
- Etapele instalării
- Asistent inițial de configurare
- Actualizarea versiunii de produs
- Repararea sau dezinstalarea BitDefender

1.1. Cerințe de sistem

Pentru funcționarea corespunzătoare a produsului, înainte de instalare, asigurați-vă că unul dintre următoarele sisteme de operare rulează pe calculatorul dumneavoastră şi că sunt îndeplinite cerințele de sistem aferente:

- Platformă de operare: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (sau superior)

Windows 2000

- Procesor de 800 MHz sau superior
- Minimum 256 MB memorie RAM (512 MB recomandat)
- Minimum 60 MB spațiu disponibil pe hard disc

Windows XP

- Procesor de 800 MHz sau superior
- Minimum 256 MB memorie RAM (1 GB recomandat)
- Minimum 60 MB spațiu disponibil pe hard disc

Windows Vista

- Procesor de 800 MHz sau superior
- Minimum 512 MB memorie RAM (1 GB recomandat)
- Minimum 60 MB spațiu disponibil pe hard disc

BitDefender Antivirus 2008 poate fi descărcat pentru evaluare de la adresa http://www.bitdefender.ro, pagina web a corporației BITDEFENDER dedicată securității datelor.

1.2. Etapele instalării

Localizați fișierul de instalare şi faceți dublu-clic. Astfel, va fi lansat programul asistent care vă va ghida pe parcursul procesului de instalare.

Înainte de lansarea programului asistent, BitDefender va căuta versiuni mai noi ale fișierului de instalare. Dacă o versiune mai nouă este disponibilă, vi se va cere să o descărcați. Apăsați pe **Da** pentru a descărca versiunea mai nouă sau pe **Nu** pentru a continua instalarea utilizând versiunea din fișierul de instalare.

Etapele instalării

Urmați aceşti paşi pentru a instala BitDefender Antivirus 2008:

1. Apăsați pe **Înainte** pentru a continua sau pe **Anulare** dacă doriți să părăsiți procesul de instalare.
2. Apăsați pe **Înainte**.

   BitDefender Antivirus 2008 vă alertează dacă aveți un alt produs antivirus instalat pe calculatorul dumneavoastră. Apăsați pe **Şterge** pentru a dezinstala produsul corespunzător. Dacă doriți să continuați fără a dezinstala produsele detectate, apăsați pe **Înainte**.

   Avertisment
   Este recomandat să dezinstalați produsele antivirus detectate înainte de a instala BitDefender. Rularea a două sau mai multor produse antivirus în acelaşi timp, pe acelaşi calculator, provoacă în general instabilitatea sistemului de operare.

3. Vă rugam să citiți cu atenție Contractul de Licență, selectați **Sunt de acord cu termenii contractului** şi apăsați pe **Înainte**. Dacă nu sunteți de acord cu prevederile acestui contract apăsați pe **Anulare**. Procesul de instalare va fi abandonat şi veți părăsi programul asistent.
4. În mod implicit, BitDefender Antivirus 2008 va fi instalat în `C:\Program Files\BitDefender\BitDefender 2008`. Dacă doriți să schimbați calea de instalare, apăsați pe butonul **Caută** şi selectați directorul în care doriți să fie instalat BitDefender Antivirus 2008.

   Apăsați pe **Înainte**.
5. Selectați opțiuni referitoare la procesul de instalare. Unele dintre acestea vor fi selectate implicit:
   - **Deschide fişierul readme** - pentru deschiderea fişierului readme la sfârşitul instalării.
   - **Creează un shortcut pe desktop** - pentru a crea o scurtătură (shortcut) către BitDefender Antivirus 2008 pe desktop la sfârşitul instalării.
   - **Scoate CD când instalarea este finalizată** - pentru a scoate CD-ul din unitate la sfârşitul instalării; această opțiune apare atunci când instalați produsul de pe CD.
   - **Dezactivează Windows Defender** - pentru a dezactiva aplicația Windows Defender; această opțiune apare doar pe Windows Vista.

   Apăsați pe **Instalare** pentru a lansa instalarea programului.

   Important
   În timpul procesului de instalare va apărea un asistent de configurare. Acesta vă va ajuta să înregistrați **BitDefender Antivirus 2008**, să creați un cont BitDefender şi să setați BitDefender să execute sarcini importante de securitate.

Finalizați procesul de configurare ghidat de programul asistent pentru a trece la pasul următor.

6. Apăsați pe **Terminare** pentru a încheia instalarea produsului. După instalare, dacă ați acceptat setările de cale implicite, veți observa că în directorul `Program Files` apare subdirectorul `BitDefender`, conținând un alt subdirector, `BitDefender 2008`.

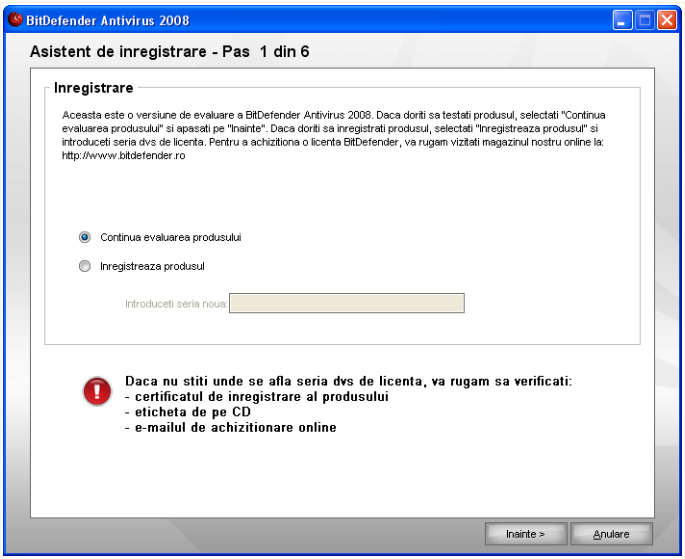
Notă
Este posibil ca la finalul instalării să vi se ceară să reporniți sistemului.

1.3. Asistentul inițial de configurare

În timpul procesului de instalare va apărea un asistent de configurare. Acesta vă va ajuta să înregistrați **BitDefender Antivirus 2008**, să creați un cont BitDefender şi să setați BitDefender să execute sarcini importante de securitate.

Nu este obligatoriu să urmați paşii programului asistent. Totuşi, vă recomandăm să faceți acest lucru pentru a economisi timp şi pentru a vă asigura că sistemul dumneavoastră nu era infectat înainte de a instala BitDefender Antivirus 2008.

1.3.1. Pasul 1/6 - Înregistrați BitDefender Antivirus 2008



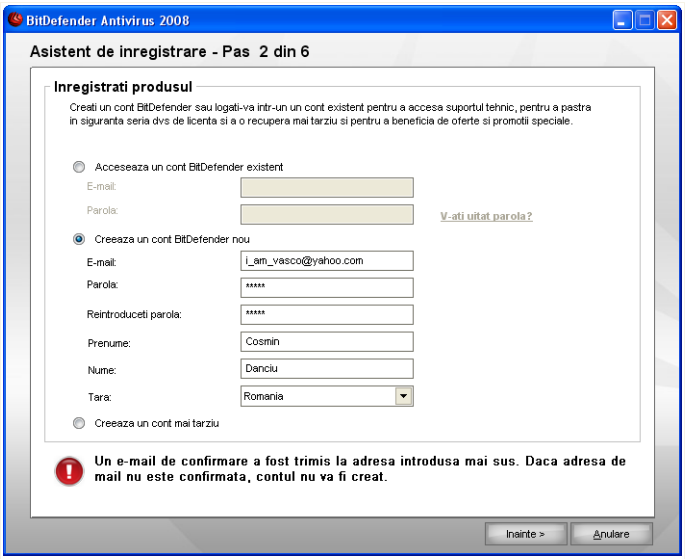
Înregistrare

Selectați **Înregistrează produsul** pentru a înregistra **BitDefender Antivirus 2008**. Introduceți seria de înregistrare în câmpul **Introduceți seria nouă**.

Pentru a evalua produsul în continuare, selectați **Continuă evaluarea produsului**.

Apăsați pe **Înainte**.

1.3.2. Pasul 2/6 - Creați un cont BitDefender



Creare cont

Nu am un cont BitDefender

Pentru a beneficia de suport tehnic gratuit şi alte servicii BitDefender gratuite trebuie să creați un cont. Selectați **Creează un nou cont BitDefender** şi furnizați informațiile cerute. Informațiile furnizate aici vor rămâne confidențiale.

Notă
Dacă doriți să creați un cont mai târziu, selectați opțiunea corespunzătoare.

Introduceți o adresă de mail validă în câmpul **E-mail**. Alegeți o parolă şi introduceți-o în câmpul **Parolă**. Confirmați parola în câmpul **Reintroduceți parola**. Utilizați adresa de mail şi parola pentru a accesa contul dumneavoastră la http://myaccount.bitdefender.com.

Notă
Parola trebuie să conțină minim patru caractere.

Introduceți numele şi prenumele dumneavoastră şi selectați țara în care locuiți.

Pentru a crea un cont trebuie mai întâi să vă activați adresa de mail. Verificați-vă adresa de mail şi urmați instrucțiunile din e-mailul trimis de serviciul de înregistrare BitDefender.

Apăsați pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

Deja am un cont BitDefender

Dacă aveți deja un cont activ, introduceți adresa de mail şi parola contului dumneavoastră. Dacă parola introdusă este incorectă, vi se va cere să o reintroduceți când apăsați pe **Înainte**. Apăsați pe **Ok** pentru a reintroduce parola sau pe **Anulare** pentru a părăsi programul asistent.

Dacă v-ați uitat parola, apăsați pe **V-ați uitat parola?** şi urmați instrucțiunile.

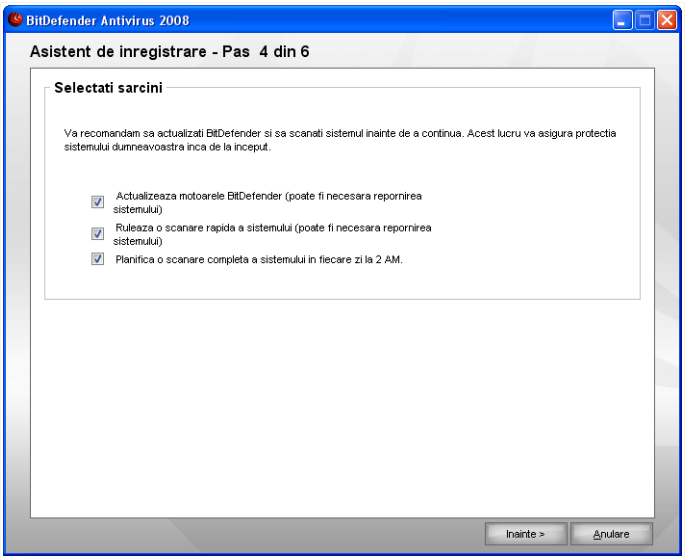
Apăsați pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

1.3.3. Pasul 3/6 - Învățați despre RTVR

Informații despre RTVR

Apăsați pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

1.3.4. Pasul 4/6 - Selectați sarcinile ce vor fi rulate



Selectare sarcini

Configurați BitDefender Antivirus 2008 să execute sarcini importante privind securitatea sistemului dumneavoastră.

Următoarele opțiuni sunt disponibile:

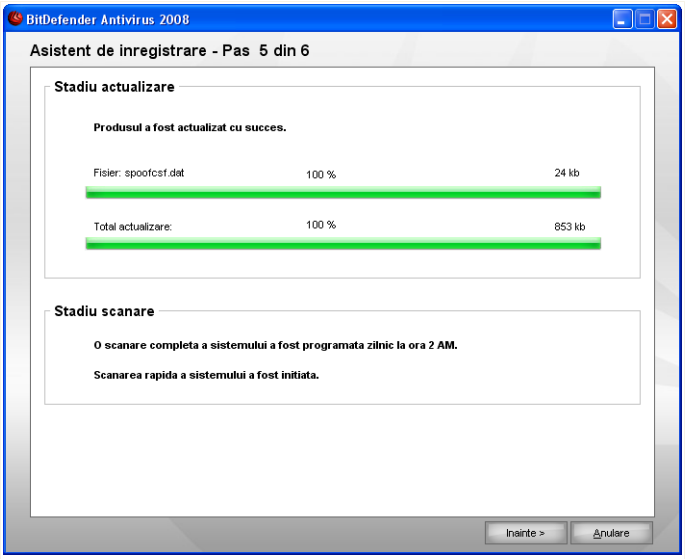
- **Actualizeaza motoarele BitDefender (poate fi necesara repornirea sistemului)** - în timpul pasului următor va fi efectuată o actualizare a motoarelor BitDefender pentru a vă proteja sistemul împotriva celor mai noi amenințări.
- **Ruleaza o scanare rapida a sistemului (poate fi necesara repornirea sistemului)** - în timpul pasului următor va fi efectuată o scanare rapida a sistemului ce va permite BitDefender să se asigure că fişierele dumneavoastră din directoarele `Windows` şi `Program Files` nu sunt infectate.
- **Planifică o scanare completă a sistemului în fiecare zi la 2 AM** - rulează o scanare completă a sistemului în fiecare zi la ora 2.

Important
Vă recomandăm să păstrați aceste opțiuni selectate înainte de a trece la pasul următor pentru a asigura securitatea sistemului dumneavoastră.

Dacă selectați doar ultima opțiune sau nicio opțiune, veți sări peste pasul următor.

Apăsați pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

1.3.5. Pasul 5/6 - Aşteptați finalizarea sarcinilor

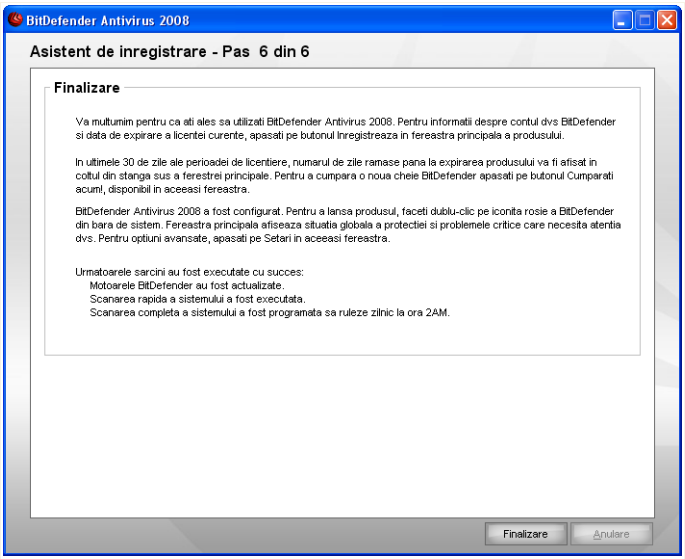


Stare sarcini

Aşteptați ca sarcinile să fie finalizate. Puteți vedea starea sarcinilor selectate în pasul anterior.

Apăsați pe **Înainte** pentru a continua sau pe **Anulare** pentru a părăsi programul asistent.

1.3.6. Pasul 6/6 - Examinați rezumatul



Finalizare

Acesta este ultimul pas al asistentului de configurare.

Apăsați pe **Finalizare** pentru a finaliza asistentul şi a continua procesul de instalare.

1.4. Actualizarea versiunii de produs

Procedura de actualizare a produsului poate fi realizată prin una dintre următoarele metode:

- **Instalați fără înlăturarea versiunii precedente - doar pentru v8 sau versiuni superioare, exceptând Internet Security.**

  Faceți dublu-clic pe fişierul de instalare şi urmați paşii programului asistent descris în secțiunea "*Etapele instalării*" (p. 3).

Important
În timpul instalării va apărea un mesaj de eroare cauzat de `serviciul Filespy`. Apăsați pe **OK** pentru a continua procesul de instalare.

- **Dezinstalați vechea versiune şi instalați-o pe cea nouă - valabilă pentru toate versiunile BitDefender.**

  În primul rând va trebui să dezinstalați vechea versiune, apoi să reporniți calculatorul şi să instalați noua versiune conform instrucțiunilor din secțiunea "*Etapele instalării*" (p. 3).

Important
Dacă faceți o actualizare de produs pentru o versiune v8 sau superioară, vă recomandăm să salvați setările BitDefender, lista de prieteni şi lista de spammeri. După finalizarea procesului de actualizare, veți putea să le încărcați.

1.5. Repararea sau dezinstalarea BitDefender

Dacă doriți să reparați sau să dezinstalați **BitDefender Antivirus 2008**, urmați calea din meniul Start al Windows: **Start** → **Programe** → **BitDefender 2008** → **Reparare sau Dezinstalare**.

Vi se va solicita să confirmați alegerea prin apăsarea butonului **Înainte**. Va apărea o nouă fereastră, de unde puteți selecta:

- **Reparare** - pentru reinstalarea tuturor componentelor programului instalate anterior.

  Important
  Înainte de a repara produsul vă recomandăm să salvați lista de prieteni şi lista de spammeri. De asemenea, puteți salva setările BitDefender şi baza de date bayesiană. Astfel, după finalizarea procesului de reparare, le veți putea încărca.

  Dacă alegeți să reparați BitDefender, va apărea o nouă fereastră. Apăsați pe **Repară** pentru a iniția procesul de reparare.

  Reporniți calculatorul atunci când vi se va cere acest lucru şi, după repornire, apăsați pe **Instalare** pentru a reinstala BitDefender Antivirus 2008.

  După finalizarea procesului de instalare, va apărea o nouă fereastră. Apăsați pe **Finalizare**.
- **Dezinstalare** - pentru dezinstalarea tuturor componentelor instalate.

Notă

Vă recomandăm să alegeți **Dezinstalare** pentru a asigura o reinstalare corectă.

Dacă alegeți să dezinstalați BitDefender, va apărea o nouă fereastră.

Important

Dezinstalând BitDefender, nu veți mai fi protejat împotriva amenințărilor malițioase, precum viruşii şi aplicațiile spyware. Dacă doriți activarea Windows Defender după dezinstalarea BitDefender, selectați căsuța corespunzătoare. Această opțiune apare doar pe Windows Vista.

Apăsați pe **Dezinstalare** pentru a iniția dezinstalarea BitDefender Antivirus 2008.

În timpul procesului de dezinstalare, vi se va cere să ne trimiteți comentariile şi sugestiile dumneavoastră legate de BitDefender. Apăsați pe **OK** pentru a răspunde unui chestionar online constând în cel mult cinci întrebări scurte. Dacă nu doriți să completați chestionarul, apăsați pe **Anulare**.

După finalizarea procesului de dezinstalare, va apărea o nouă fereastră. Apăsați pe **Finalizare**.

Notă

După ce procesul de dezinstalare este finalizat, vă recomandăm să ştergeți subdirectorul `BitDefender` din directorul `Program Files`.

A apărut o eroare în timpul dezinstalării BitDefender

Dacă în timpul dezinstalării BitDefender apare o eroare, procesul de dezinstalare este oprit şi va apărea o nouă fereastră. Apăsați pe **Rulează utilitar de dezinstalare** pentru a vă asigura că BitDefender a fost dezinstalat complet. Utilitarul de dezinstalare va şterge toate fişierele şi cheile din regiştri care nu au fost şterse în timpul procesului automatizat de dezinstalare.

Administrare elementară

2. Introducere

O dată ce ați instalat BitDefender, calculatorul dumneavoastră este protejat. Puteți deschide oricând doriți Centrul de securitate al BitDefender pentru a verifica situația securității sistemului, pentru a lua măsuri preventive sau pentru a configura produsul.

Pentru a accesa consola de administrare, utilizați meniul Windows Start, urmând calea **Start → Programe → BitDefender 2008 → BitDefender Antivirus 2008** sau, mai rapid, făcând dublu-clic pe **icoana BitDefender** din bara de sistem.

Centrul de securitate al BitDefender

Centrul de securitate al BitDefender conține două zone:

- Zona **Status**: conține informații referitoare la vulnerabilitățile securității calculatorului dumneavoastră şi vă ajută să le rezolvați. Puteți vedea cu uşurință câte probleme afectează securitatea calculatorului dumneavoastră. Apăsând pe butonul roşu **Repară probleme**, vulnerabilitățile calculatorului dumneavoastră vor fi remediate imediat sau veți fi ghidat pentru a le putea remedia uşor. În acelaşi timp, sunt disponibile patru butoane de stare corespunzătoare unui număr de patru tipuri de

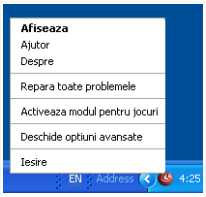
securitate. Un buton de stare verde indică absența oricărui risc. Un buton de stare galben sau roşu indică riscuri de securitate medii, respectiv ridicate. Pentru a le rezolva, apăsați pe butonul galben/roşu şi apoi pe butoanele **Repară**, unul câte unul sau pe butonul **Repară tot**. Culoarea gri indică o componentă neconfigurată.

- Zona **Sarcini rapide**: vă ajută să vă protejați sistemul şi datele.

În plus, Centrul de securitate BitDefender conține mai multe linkuri utile.

Link	*Descriere*
Cumpărați acum!	Deschide o pagină de unde puteți cumpăra produsul.
Contul meu	Deschide pagina contului dumneavostră BitDefender.
Înregistrează	Porneşte asistentul de înregistrare.
Ajutor	Deschide fişierul de ajutor.
Suport	Deschide pagina de suport a BitDefender.
Setări	Deschide consola de setări avansate.
Istoric	Deschide o fereastră conținând istoricul şi evenimentele BitDefender.

Pentru o administrare mai rapidă a produsului, puteți folosi şi iconița BitDefender din bara de sistem.



Meniul contextual

Dacă faceți dublu-clic pe această iconiță, se va deschide Centrul de securitate BitDefender. De asemenea, apăsând dreapta pe ea, un meniu contextual vă va oferi posibilitatea unei administrări rapide a BitDefender.

- **Afişează** - deschide Centrul de securitate BitDefender.
- **Ajutor** - deschide documentația electronică.
- **Despre** - deschide pagina web a BitDefender.

- **Repară toate problemele** - vă ajută să remediați problemele ce afecteaza securitatea sistemului.
- **Activează modul pentru jocuri** - dezactivează alertele şi ferestrele de tip pop-up şi setează protecția în timp real la nivel permisiv.
- **Deschide setări avansate** - permite accesul la consola de setări avansate.
- **Ieşire** - opreşte aplicația.

2.1. Scanare manuală BitDefender

Dacă doriți să scanați rapid un anumit fişier, puteți utiliza scanarea manuală BitDefender.

Pentru a accesa programul asistent de scanare manuală, utilizați meniul Windows Start, urmând calea **Start → Programe → BitDefender 2008 → Scanare manuală BitDefender**.

Tot ce trebuie să faceți este să căutați directorul în listă, să îl selectați şi să apăsați pe **OK**.

3. Status securitate

Statusul securității afişează o listă organizată sistematic şi uşor de gestionat a vulnerabilităților de securitate de pe calculatorul dumneavoastră. BitDefender Antivirus 2008 vă va înştiința de fiecare dată când o problemă afectează securitatea calculatorului dumneavoastră.

Există patru butoane de status al securității:

- **ANTIVIRUS**
- **CONFIDENȚIALITATE**
- **ANTIPHISING**
- **Actualizare**

De asemenea, în partea stângă, puteți vedea numărul de probleme ce afectează securitatea calculatorului dumneavoastră şi un buton roşu, **Repară probleme**.

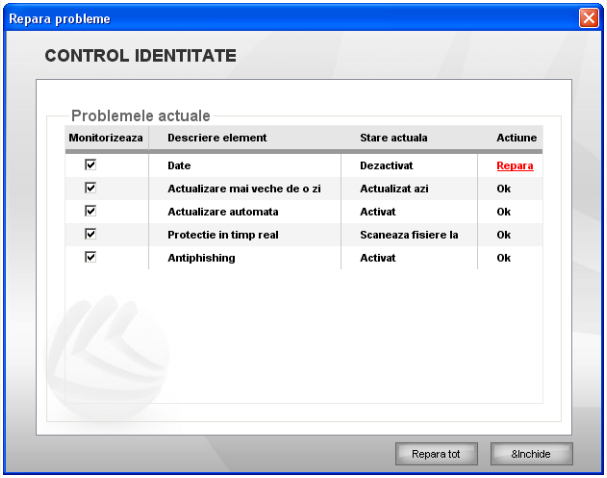
Cele patru butoane de status pot fi colorate în verde, galben, roşu sau gri, în funcție de nivelul curent de protecție.

- **Verdele** indică un risc scăzut de securitate.
- **Galbenul** indică un risc mediu de securitate.
- **Roşul** indică un risc ridicat de securitate.
- **Griul** indică o componentă care nu este configurată.

Remedierea problemelor de securitate se face printr-o simplă apăsare pe butonul **Repară probleme**.

Veți vedea o listă a problemelor de securitate şi o scurtă descriere a lor.

Pentru a remedia o anumită problemă, apăsați pe butonul **Repară** corespunzător. Problema va fi rezolvată imediat sau după ce urmați paşii unui program asistent. Dacă decideți să remediați toate problemele, apăsați pe butonul **Repară tot** şi urmați paşii programului asistent corespunzător.



Probleme de securitate

Pentru a remedia problemele mai târziu, apăsați pe **Închide**.

Important
În dreptul fiecărei probleme există o căsuță bifată în mod implicit. Dacă nu doriți ca o anumită problemă să fie luată în considerare atunci când se calculează riscul de securitate, debifați căsuța corespunzătoare. Vă rugăm să folosiți această opțiune cu grijă, deoarece este foarte uşor să creşteți riscul de securitate la care calculatorul dumneavostră este expus.

3.1. Buton de stare antivirus

Dacă butonul de stare antivirus este verde, atunci totul este în regulă. Altfel, dacă butonul este galben, roşu sau gri, calculatorul dumneavoastră este expus unui risc mediu sau ridicat de securitate.

Culoarea butoanelor de stare se poate schimba atât atunci când configurați setări ce afectează securitatea calculatorului dumneavoastră, cât şi atunci când uitați să executați sarcini importante. De exemplu, dacă a trecut mult timp de la ultima scanare a sistemului, butonul de stare al securității va fi galben. Dacă a trecut foarte mult timp, atunci acesta va fi roşu.

Tabelul de mai jos furnizează informații despre elementele luate în considerare atunci când se calculează riscul de securitate.

Problemă	Culoare
A trecut mult timp de la ultima scanare.	Galben
A trecut foarte mult timp de la ultima scanare a sistemului.	Roşu
Protecția în timp real este dezactivată.	Roşu
Protecția antivirus este setată la nivelul permisiv.	Galben

Pentru a remedia problemele, urmați aceşti paşi:

1. Apăsați pe butonul de stare antivirus.
2. Apăsați fie pe butoanele **Repară**, pentru a le remedia pe rând, fie pe butonul **Repară tot**, pentru a le remedia pe toate imediat.
3. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

3.2. Butonul de stare Confidențialitate

Dacă butonul de stare Confidențialitate este verde, atunci totul este în regulă. Altfel, dacă acesta este roşu sau gri, calculatorul dumneavoastră este expus unui risc ridicat de securitate.

Tabelul de mai jos furnizează informații despre elementele luate în considerare atunci când se calculează riscul de securitate.

Problemă	Culoare
Protecția confidențialității este configurată şi activată.	Verde
Protecția confidențialității este configurată şi dezactivată.	Roşu
Protecția confidențialității nu este configurată.	Gri

Pentru a remedia problemele, urmați aceşti paşi:

1. Apăsați pe butonul de stare Confidențialitate.
2. Apăsați fie pe butoanele **Repară**, pentru a le remedia pe rând, fie pe butonul **Repară tot**, pentru a le remedia pe toate imediat.
3. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

3.3. Butonul de stare Antiphishing

Dacă butonul de stare Antiphishing este verde, atunci totul este în regulă. Altfel, dacă acesta este roşu, calculatorul dumneavoastră este expus unui risc ridicat de securitate.

Tabelul de mai jos furnizează informații despre elementele luate în considerare atunci când se calculează riscul de securitate.

Problemă	*Culoare*
Protecția antiphishing este activată.	Verde
Protecția antiphishing este dezactivată.	Roşu

Pentru a remedia problemele, urmați aceşti paşi:

1. Apăsați pe butonul de stare Antiphishing.
2. Apăsați fie pe butoanele **Repară**, pentru a le remedia pe rând, fie pe butonul **Repară tot**, pentru a le remedia pe toate imediat.
3. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

3.4. Butonul de stare Actualizare

Dacă butonul de stare Actualizare este verde, atunci totul este în regulă. Altfel, dacă acesta este roşu, calculatorul dumneavoastră este expus unui risc ridicat de securitate.

Tabelul de mai jos furnizează informații despre elementele luate în considerare atunci când se calculează riscul de securitate.

Problemă	*Culoare*
Actualizarea automată este activată.	Verde
Actualizarea automată este dezactivată.	Roşu
A trecut o zi de la ultima actualizare.	Roşu

Pentru a remedia problemele, urmați aceşti paşi:

1. Apăsați pe butonul de stare Actualizare.
2. Apăsați fie pe butoanele **Repară**, pentru a le remedia pe rând, fie pe butonul **Repară tot**, pentru a le remedia pe toate imediat.
3. Dacă o problemă nu este remediată automat, urmați paşii programului asistent.

4. Sarcini rapide

Sub cele patru butoane de stare se găseşte zona **Sarcini rapide**.

4.1. Securitate

BitDefender conține un modul de securitate care vă ajută să îl actualizați şi să vă protejați sistemul de viruşi.

Pentru a accesa modulul de securitate, apăsați pe tabul **Securitate**.

Următoarele butoane sunt disponibile:

- **Actualizează acum** - inițiază o actualizare discretă.
- **Scanează Documentele mele** - inițiază o scanare rapidă a documentelor şi setărilor dumneavoastră.
- **Scanare completă sistem** - inițiază o scanare completă a calculatorului dumneavoastră.

4.1.1. Actualizare

Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului şi, în acelaşi timp, orice vulnerabilitate va fi exclusă.

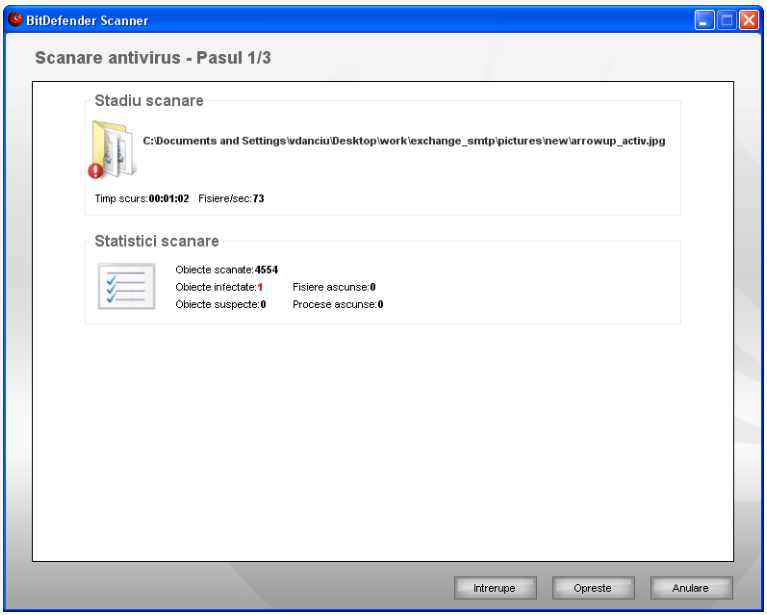
4.1.2. Programul asistent de scanare

Atunci când inițiați un proces de scanare la cerere, fie o scanare rapidă sau completă a sistemului, va apărea programul asistent de scanare.

Urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



Scanare

Puteți vedea stadiul şi statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse şi altele).

Notã
Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

Pentru a opri temporar procesul de scanare, apăsați pe **Întrerupe**. Va trebui să apăsați pe **Reia** pentru a relua scanarea.

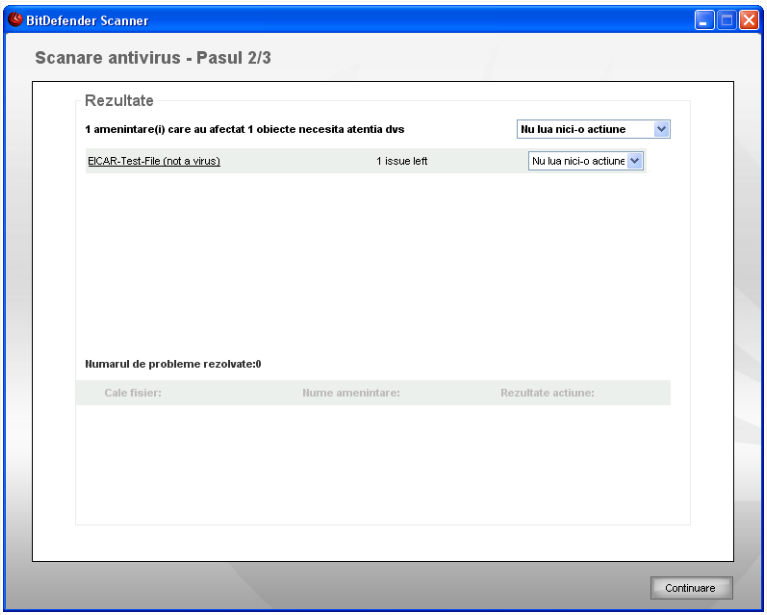
Puteți opri scanarea oricând doriți apăsând pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent.

Notã
Dacă au fost detectate fişiere suspecte în timpul scanării, vi se va cere să le trimiteți laboratorului BitDefender.

Aşteptați ca BitDefender să finalizeze scanarea.

Pasul 2/3 - Selectați acțiunile

După ce scanarea a fost finalizată, va apărea o nouă fereastră, unde puteți vedea rezultatele scanării.



Acțiuni

Puteți vedea numărul problemelor care vă afectează sistemul.

Problemele sunt afişate pe grupuri. Apăsați pe căsuța cu “+” pentru a deschide un grup sau pe căsuța cu “-” pentru a închide un grup.

Puteți alege o acțiune globală care să fie luată asupra fiecărui grup de probleme sau puteți alege acțiuni separate pentru fiecare problemă în parte.

Următoarele opțiuni pot apărea pe meniu:

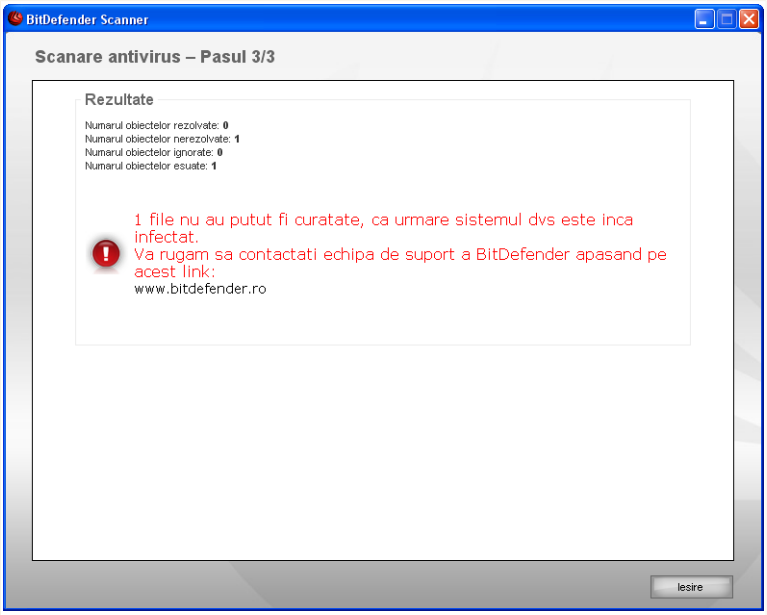
Acțiune	Descriere
Nicio acțiune	Nu se va lua nicio acțiune asupra fişierelor detectate.

Acțiune	Descriere
Dezinfectează	Dezinfectează fişierele infectate.
Şterge	Şterge fişierele detectate.
Demască	Face vizibile obiectele ascunse.

Apăsați pe **Repară probleme** pentru a aplica acțiunile specificate.

Pasul 3/3 - Examinați rezultatele

Atunci când BitDefender a remediat toate problemele apărute, rezultatele scanării vor fi afişate într-o nouă fereastră.



Rezumat

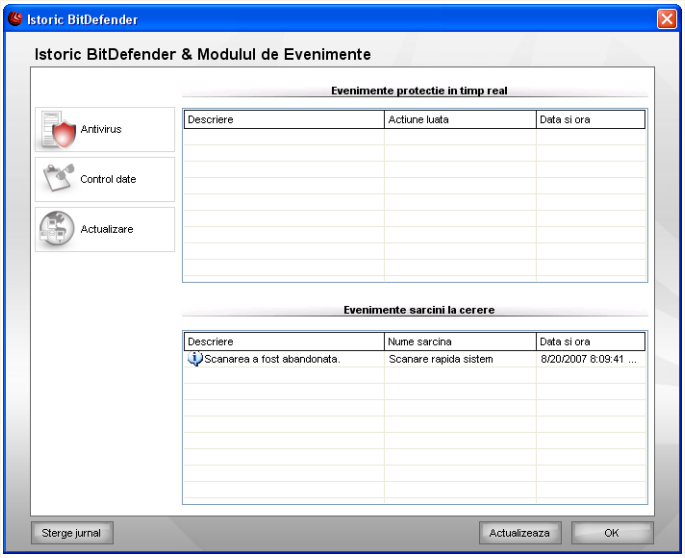
Puteți vedea un rezumat al rezultatelor.

Fişierul de raport este salvat automat în secțiunea Rapoarte din fereastra de **Proprietăți** a sarcinii respective.

Avertisment
Dacă sunt probleme care nu au fost remediate, vă recomandăm să contactați echipa de suport a BitDefender pe pagina web www.bitdefender.ro.

5. Istoric

Linkul **Istoric**, situat în partea de jos a Centrului de securitate BitDefendere, deschide o nouă fereastră conținând istoricul şi evenimentele BitDefender. Această fereastră vă furnizează un sumar al evenimentelor legate de securitate. De exemplu, puteți vedea uşor dacă actualizarea a fost realizată cu succes, dacă au fost detectate aplicații malițioase pe calculatorul dumneavoastră, dacă sarcinile de backup au rulat fără erori etc.



Evenimente

Pentru a gestiona mai uşor istoricul şi evenimentele BitDefender, următoarele categorii sunt oferite în partea stângă:

- **Antivirus**
- **Control date**
- **Actualizare**

Pentru fiecare categorie este disponibilă o listă de evenimente. Următoarele informații sunt furnizate pentru fiecare eveniment: o scurtă descriere, acțiunea luată de

BitDefender atunci când evenimentul a avut loc şi data şi timpul când a avut loc. Dacă doriți mai multe informații în legătură cu un anumit eveniment din listă, faceți dublu-clic pe evenimentul respectiv.

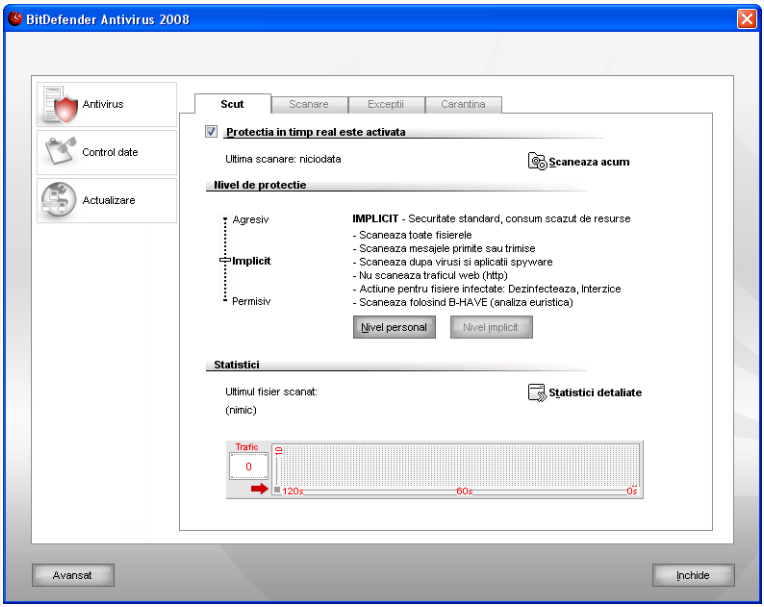
Apăsați pe **Şterge jurnal** dacă doriți să ştergeți rapoartele vechi sau pe **Actualizare** pentru a vă asigura că şi ultimele evenimente sunt afişate.

Administrare avansată a securității

6. Introducere

BitDefender Antivirus 2008 este dotat cu o consolă de setări centralizată, care permite configurarea şi administrarea avansată a BitDefender.

Pentru a accesa consola de setări, apăsați pe linkul **Setări**, situat în partea de jos a Centrului de Securitate.



Consola de setări

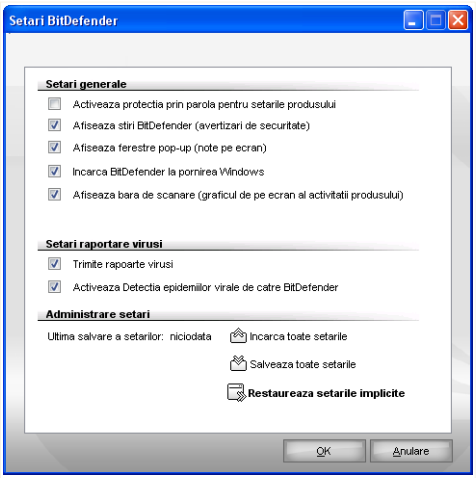
Consola de setări este organizată în module: **Antivirus**, **Control date** şi **Actualizare**. Acest lucru permite administrarea facilă a BitDefender, în funcție de tipul problemelor de securitate căruia se adresează.

În partea stângă a consolei de setări puteți vedea selectorul de module:

- Antivirus - în această secțiune puteți configura modulul **Antivirus**.
- Control date - în această secțiune puteți configura modulul **Control date**.
- Actualizare - în această secțiune puteți configura modulul **Actualizare**.

6.1. Configurarea setărilor generale

Pentru a configura setări generale ale BitDefender Antivirus 2008 şi pentru a-i gestiona setările, apăsați pe **Avansat**. Va apărea o nouă fereastră.



Setări generale

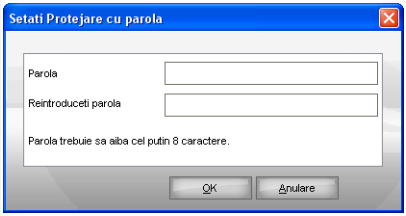
Aici puteți seta comportamentul general al produsului. BitDefender se încarcă la pornirea Windows iar apoi rulează minimizat în bara de sistem.

6.1.1. Setări generale

- **Activează protecția prin parolă pentru setările produsului** - permite setarea unei parole pentru a proteja configurația consolei de administrare a BitDefender.

  Notă
  Dacă nu sunteți singura persoană cu drepturi administrative care foloseşte acest calculator, este recomandat să vă protejați setările BitDefender cu o parolă.

  Dacă selectați această opțiune, va apărea următoarea fereastră:



Confirmarea parolei

Introduceți parola în câmpul **Parolă**, reintroduceți-o în câmpul **Reintroduceți parola** şi apăsați pe **OK**.

Din acest moment, dacă doriți să schimbați opțiunile de configurare ale BitDefender, veți fi rugat să introduceți parola.

Important
Dacă uitați parola va fi nevoie să reparați produsul pentru a schimba configurarea BitDefender.

- **Afişează ştiri BitDefender (avertizări de securitate)** - afişează din când în când notificări de securitate referitoare la noi viruşi descoperiți, trimise de serverul BitDefender.
- **Afişează ferestre pop-up (note pe ecran)** - afişează ferestre de informare cu privire la starea produsului.
- **Încarcă BitDefender la pornirea Windows** - lansează BitDefender automat, la pornirea sistemului de operare. Această opțiune este recomandată.
- **Afişează bara de scanare (graficul de pe ecran al activității produsului)** - activează/dezactivează bara de scanare.

6.1.2. Setări raportare viruşi

- **Trimite rapoarte viruşi** - trimite Laboratorului BitDefender rapoarte referitoare la viruşii identificați în calculatorul dumneavoastră. Astfel ne ajutați să ținem evidența noilor viruşi.

  Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, şi nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar numele viruşilor şi vor fi folosite doar pentru a crea rapoarte statistice.
- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, şi nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar potențialul virus şi vor fi folosite doar pentru a detecta noi viruşi.

6.1.3. Administrare setări

Folosiți butoanele **Salvează toate setările** / **Încarcă toate setările** pentru a salva setările BitDefender într-o anumită locație sau pentru a le încărca dintr-o anumită locație. Astfel, puteți folosi aceleaşi setări şi după ce ați reinstalat sau ați reparat produsul BitDefender.

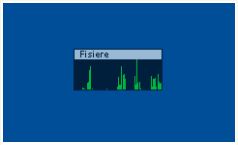
Important
Doar utilizatorii cu drepturi administrative pot salva sau încărca setări.

Pentru a încărca setările implicite, apăsați pe **Restaurează setările implicite**.

6.2. Utilizarea barei de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră.

Barele verzi (zona **Fişiere**) reprezintă numărul de fişiere scanate pe secundă, pe o scară de la 0 la 50.



Bara de scanare

Notă
Bara de scanare vă va avertiza când protecția în timp real este dezactivată prin afişarea unui X roşu deasupra zonei **Fişiere**.

Puteți utiliza **Bara de scanare** pentru a scana obiecte. În acest scop, trageți obiectele care doriți să fie scanate peste ea.

Notă
Pentru mai multe informații, consultați "*Scanare prin drag&drop*" (p. 57).

Când nu mai doriți să vedeți reprezentarea grafică, faceți doar clic-dreapta pe ea şi selectați **Închide**. Pentru a ascunde permanent această fereastră, apăsați pe **Avansat** în consola de setări şi debifați opțiunea **Afişează bara de scanare (graficul de pe ecran al activității produsului)**.

7. Antivirus

BitDefender vă protejează calculatorul împotriva oricăror amenințări malițioase (viruşi, troieni, aplicații spyware, rootkituri şi altele).

Pe lângă scanarea clasică bazată pe semnături de aplicații malițioase, BitDefender va efectua şi o analiză euristică a fişierelor scanate. Scopul scanării euristice este de a identifica noi viruşi pe baza anumitor elemente şi algoritmi, înainte ca semnătura acestor viruşi să fie cunoscută. Pot apărea şi alarme false. Când este detectat un fişier de acest gen, el este clasificat ca suspect. În aceste cazuri, este recomandat să trimiteți fişierul la analiză către laboratorul BitDefender.

Protecția oferită de BitDefender se împarte în două categorii:

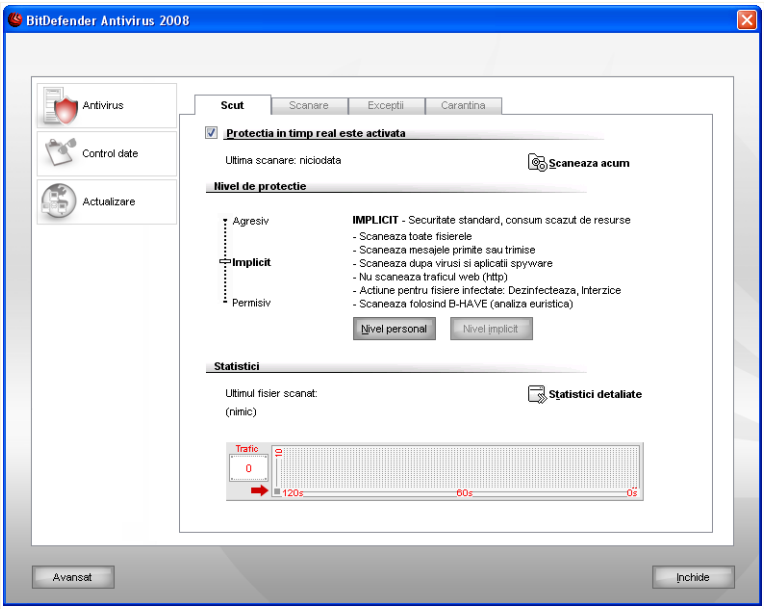
- **Scanarea la acces** - previne pătrunderea în sistemul dumneavoastră a noilor viruşi, aplicații spyware şi a altor programe virale. Această caracteristică se mai numeşte protecție în timp real – fişierele sunt scanate atunci când le utilizați – la acces. BitDefender va scana, de exemplu, un document Word atunci când îl deschideți şi un mesaj e-mail atunci când îl primiți.
- **Scanarea la cerere** - permite detectarea şi ştergerea aplicațiilor malițioase care există deja în sistemul dumneavoastră. Acesta este modul clasic de scanare, inițiată de utilizator – dumneavoastră alegeți partițiile, directoarele sau fişierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere. Sarcinile de scanare permit crearea unor rutine de scanare personalizate şi pot fi programate să ruleze periodic.

Secțiunea **Antivirus** a acestui ghid de utilizare conține următoarele subiecte:

7.1. Scanarea la acces

Scanarea la acces, cunoscută şi sub numele de protecție în timp real, vă protejează calculatorul de toate tipurile de amenințări malițioase scanând toate fişierele accesate, mesajele e-mail şi comunicațiile prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Pentru a configura şi monitoriza protecția în timp real, apăsați pe **Antivirus>Scut** în consola de setări. Va apărea următoarea fereastră:



Protecție în timp real

Important
Pentru a preveni infectarea calculatorului personal cu viruşi, păstrați **Protectia in timp real** activată.

În partea de jos a secțiunii sunt afişate statisticile **Protecției în timp real** privind fişierele şi mesajele e-mail scanate. Apăsați pe **Statistici detaliate** dacă doriți deschiderea unei ferestre cu informații detaliate despre aceste statistici.

Pentru a inița o scanare rapidă a sistemului, apăsați pe **Scanează acum**.

7.1.1. Configurarea nivelului de protecție

Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există trei nivele de protecție:

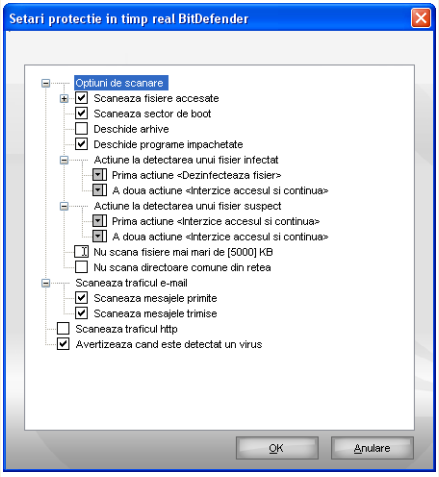
Nivel de protecție	*Descriere*
Permisiv	Acoperă nevoile elementare de securitate. Consumul de resurse este foarte scăzut. Aplicațiile şi mesajele e-mail primite sunt scanate doar împotriva viruşilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Standard	Oferă protecție standard. Consumul de resurse este scăzut. Toate fişierele şi mesajele e-mail sunt scanate împotriva viruşilor şi a aplicațiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.
Agresiv	Oferă protecție avansată. Consumul de resurse este moderat. Toate fişierele şi mesajele e-mail, precum şi traficul web, sunt scanate împotriva viruşilor şi a aplicațiilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică. Acțiunile luate asupra fişierelor infectate sunt următoarele: dezinfectează fişier/interzice accesul.

Pentru a aplica setările implicite ale protecției în timp real, apăsați pe **Nivel implicit**.

7.1.2. Personalizarea nivelului de protecție

Utilizatorii avansați pot folosi şi modifica opțiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fişiere, să caute anumite tipuri de amenințări malițioase sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum şi viteza de reacție a sistemului pe durata scanării.

Puteți personaliza **Protecția în timp real** apăsând pe **Nivel personal**. Va apărea următoarea fereastră:



Setări Scut

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows.

Notă

Apăsați pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Puteți observa că, deşi semnul “+” apare, unele opțiuni de scanare nu pot fi deschise. Motivul este că aceste opțiuni nu au fost selectate încă.Dacă veți selecta aceste opțiuni, ele vor putea fi deschise.

- **Opțiuni de scanare a fişierelor şi a transferurilor P2P** - scanează fişierele accesate şi comunicația prin programe de mesagerie instantă (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). În continuare, selectați tipurile de fişiere care doriți să fie scanate.

Opțiune		*Descriere*
Scanează fişiere accesate	**Scanează toate fisierele**	Vor fi scanate toate fişierele accesate, indiferent de tipul lor.
	Programe	Nu vor fi scanate decât fişierele program, şi anume fişierele cu următoarele extensii: `.exe`;

Opțiune		Descriere
		.bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml şi .nws.
	Extensiile definite de utilizator	Nu vor fi scanate decât fişierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
	Scanează după soft cu risc	Scanează după aplicații care prezintă un potențial risc (riskware). Fişierele detectate vor considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată. Selectați **Nu scana aplicații si programe dialer** dacă doriți să excludeți aceste fişiere de la scanare.
Scanează boot		Scanează sectorul de boot al sistemului.
Deschide arhive		Vor fi scanate şi arhivele accesate. Selectând această opțiune, performanțele calculatorului vor scădea.
Deschide programele împachetate		Programele împachetate accesate vor fi scanate.
Prima acțiune		Selectați din meniu prima acțiune ce va fi luată asupra fişierelor infectate sau suspecte.
	Interzice accesul şi continuă	În caz că un fişier este infectat, accesul la acesta va fi interzis.
	Dezinfectează fişier	Dezinfectează fişierele infectate.
	Şterge fişier	Şterge imediat fişierele infectate, fără niciun avertisment.

Opțiune		Descriere
	Mută fişier în carantină	Mută fişierele infectate în carantină.
A doua acțiune		Selectați din meniu a doua acțiune pentru fişierele infectate sau suspecte, în caz că prima acțiune eşuează.
	Interzice accesul şi continuă	În caz că un fişier este infectat, accesul la acesta va fi interzis.
	Şterge fişier	Şterge imediat fişierele infectate, fără niciun avertisment.
	Mută fişier în carantină	Mută fişierele infectate în carantină.
Nu scana fişiere mai mari de [x] Kb		Introduceți dimensiunea maximă a fişierelor ce vor fi scanate. Dacă dimensiunea este de 0 Kb, toate fişierele vor fi scanate, indiferent de mărimea lor.
Nu scana fişierele din rețea		Dacă această opțiune este activată, BitDefender nu va scana fişierele comune din rețea, permițând accesarea mai rapidă a acestora. Vă recomandăm să activați această opțiune doar dacă rețeaua din care faceți parte este protejată de o soluție antivirus.

- **Scanează traficul e-mail** - scanează traficul e-mail.

  Următoarele opțiuni sunt disponibile:

Opțiune	Descriere
Scanează mesajele primite	Scanează toate mesajele primite.
Scanează mesajele trimise	Scanează toate mesajele trimise.

- **Scanează traficul http** - scanează tot traficul web.
- **Avertizează când este detectat un virus** - afişează o fereastră de avertizare la descoperirea unui virus într-un fişier sau mesaj e-mail.

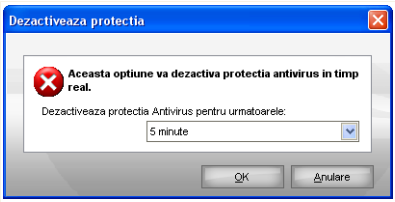
Pentru fişierele infectate fereastra de avertizare va conține calea şi numele virusului, acțiunea luată de BitDefender şi un link către site-ul BitDefender, unde puteți afla mai multe informații despre virus. Pentru mesajele infectate fereastra de avertizare va conține şi informații despre expeditor şi destinatar.

Dacă este detectat un fişier suspect, din fereastra de alertă puteți lansa un program asistent ce vă va ajuta să trimiteți acest fişier Laboratorului BitDefender pentru analiză aprofundată. Pentru a primi informații despre acest fişier introduceți adresa dumneavoastră de e-mail.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

7.1.3. Dezactivarea protecției în timp real

Dacă doriți să dezactivați protecția în timp real, va apărea o fereastră de avertizare.



Dezactivați protecția în timp real

Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată protecția în timp real. Puteți dezactiva protecția în timp real pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

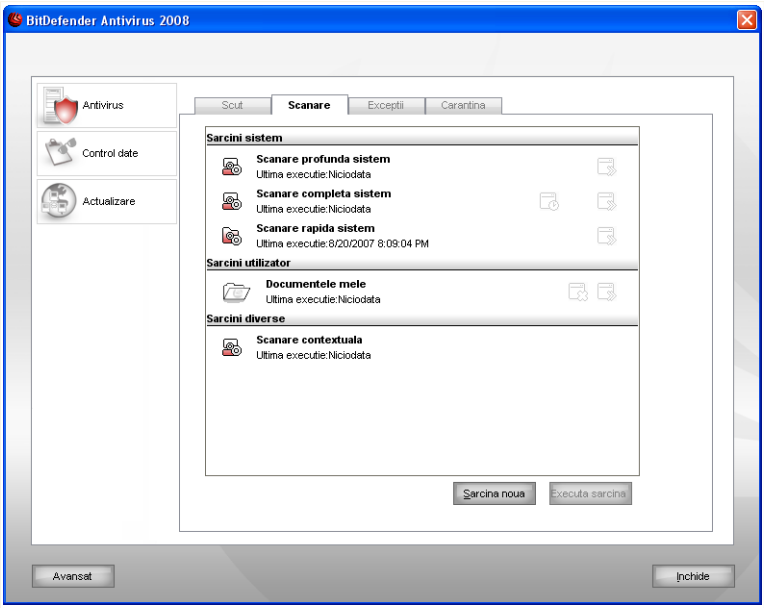
Avertisment
Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați protecția în timp real pentru cât mai puțin timp posibil. Dacă protecția în timp real este dezactivată, nu veți mai fi protejat împotriva amenințărilor malițioase.

7.2. Scanarea la cerere

Principalul obiectiv BitDefender este protejarea calculatorului dumneavoastră de viruşi. Aceasta se face în primul rând nepermițând viruşilor noi să pătrundă în sistem, prin scanarea mesajelor e-mail şi a fişierelor descărcate sau copiate pe calculator.

Există însă riscul ca un virus să fi fost în sistem înainte de instalarea BitDefender. Din acest motiv, este indicat să vă scanați calculatorul de viruşi după instalarea BitDefender. Şi este, de asemenea, recomandat să vă scanați sistemul periodic.

Pentru a configura şi inița scanarea la cerere, apăsați pe **Antivirus>Scanare** în consola de setări. Va apărea următoarea fereastră:



Sarcini de scanare

Scanarea la cerere se bazează pe sarcini de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare şi obiectele care să fie scanate. Puteți scana calculatorul oricând doriți rulând sarcinile de scanare predefinite sau propriile dumneavoastră sarcini de scanare (sarcini definite de utilizator). De asemenea, puteți programa sarcinile să ruleze periodic sau când sistemul nu este utilizat, pentru a nu interfera cu munca dumneavoastră.

7.2.1. Sarcini de scanare

BitDefender este dotat cu o serie de sarcini predefinite, ce acoperă nevoile comune de securitate. Pe lângă acestea, puteți crea propriile dumneavoastră sarcini de scanare personalizate.

Fiecare sarcină are propria fereastră de **Proprietăți** care permite configurarea sarcinii şi examinarea rezultatelor scanării. Pentru mai multe informații, consultați "*Configurarea sarcinilor de scanare*" (p. 46).

Există trei categorii de sarcini de scanare:

- **Sarcini sistem** - conține lista sarcinilor implicite de sistem. Următoarele sarcini sunt disponibile:

Sarcină implicită	*Descriere*
Scanare profundă sistem	Scanează întregul sistem. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanare completă sistem	Scanează întregul sistem, cu excepția arhivelor. În configurația implicită, se scanează după toate tipurile de aplicații malițioase care amenință securitatea sistemului dumneavoastră, cum ar fi viruşii, aplicațiile spyware, aplicațiile adware, aplicațiile ascunse (rootkituri) şi altele.
Scanare rapidă sistem	Scanează directoarele `Windows`, `Program Files` şi `All Users`. În configurația implicită, se scanează după toate tipurile de aplicații malițioase, mai puțin cele ascunse (rootkituri), dar nu sunt scanate memoria, regiştrii şi fişierele cookie.

Notă

Deoarece sarcinile **Scanare profundă sistem** şi **Scanare completă sistem** analizează întregul sistem, scanarea poate lua ceva timp. De aceea, vă recomandăm să rulați aceste sarcini cu prioritate scăzută sau, şi mai bine, atunci când nu utilizați calculatorul.

- **Sarcini utilizator** - conține sarcinile definite de utilizator.

O sarcină denumită `Documentele mele` este furnizată. Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` şi `StartUp`. Astfel, veți asigura siguranța documentelor dumneavostră, un spațiu de lucru sigur şi rularea la pornirea sistemului a unor aplicații necompromise.

- **Sarcini diverse** - conține o listă de sarcini de scanare diverse. Aceste sarcini de scanare se referă la tipuri alternative de scanare ce nu pot fi rulate din această fereastră. Puteți doar să modificați setările acestora şi să examinați rapoartele de scanare.

În partea dreaptă a fiecărei sarcini sunt disponibile trei butoane:

- **Program** - indică faptul că sarcina selectată este planificată să ruleze mai tarziu. Apăsați pe acest buton pentru a deschide fereastra de **Proprietăți** la tabul Planificare, unde puteți vedea şi modifica programul de rulare a sarcinii.
- **Şterge** - şterge sarcina selectată.

> ***Notă***
> Nu este disponibil pentru sarcinile de sistem. Nu puteți şterge o sarcină de sistem.

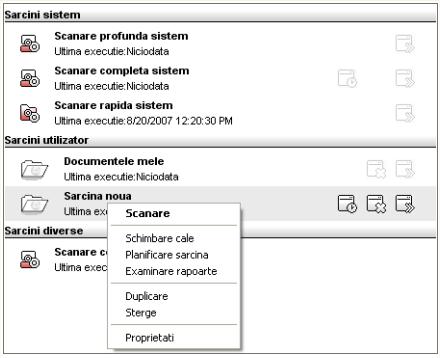
- **Scanare** - execută sarcina selectată, pornind o scanare imediată.

În partea stângă a fiecărei sarcini, puteți vedea butonul **Proprietăți** care vă permite să configurați sarcina şi să vedeți rapoartele de scanare.

7.2.2. Utilizarea meniului contextual

Un meniu contextual este disponibil pentru fiecare sarcină. Faceți clic dreapta pe o sarcină selectată pentru a-l deschide.

Următoarele opțiuni sunt disponibile pe meniul contextual:



Meniu contextual

- **Scanare** - rulează sarcina selectată, lansând o scanare imediată.
- **Schimbare cale** - deschide fereastra de **Proprietăți** la tabul Țintă, unde puteți modifica locațiile de scanare pentru sarcina selectată.

Notă
În cazul sarcinilor de sistem, această opțiune este înlocuită cu **Arată locații scanare** deoarece puteți doar vedea locațiile scanate.

- **Planificare sarcină** - deschide fereastra de **Proprietăți** la tabul Planificare, unde puteți programa sarcina selectată.
- **Examinare rapoarte** - deschide fereastra de **Proprietăți** la tabul Rapoarte, unde puteți examina rapoartele generate de fiecare dată când sarcina selectată a rulat.
- **Duplicare** - creează o copie a sarcinii selectate.

Notă
Acest lucru este util în crearea de noi sarcini, deoarece puteți modifica setările duplicatului unei sarcini.

- **Şterge** - şterge sarcina selectată.

Notă
Nu este disponibil pentru sarcinile de sistem. Nu puteți şterge o sarcină de sistem.

- **Proprietăți** - deschide fereastra de **Proprietăți** la tabul Setări, unde puteți modifica setările sarcinii selectate.

Notă
Datorită caracterului special al sarcinilor din categoria **Sarcini diverse**, doar opțiunile **Proprietăți** şi **Examinare rapoarte** sunt disponibile în acest caz.

7.2.3. Crearea sarcinilor de scanare

Pentru a crea o sarcină de scanare, utilizați una dintre următoarele metode:

- Duplicați o sarcină existentă, redenumiți-o şi faceți modificările necesare în fereastra de Proprietăți.
- Apăsați pe **Sarcină nouă** pentru a crea o nouă sarcină şi a o configura.

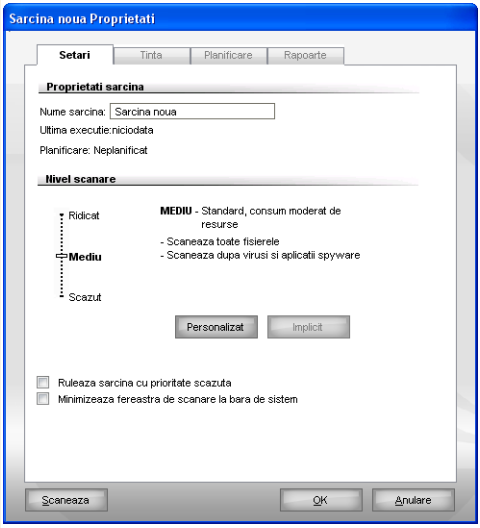
7.2.4. Configurarea sarcinilor de scanare

Fiecare sarcină de scanare are propria fereastră de **Proprietăți**, unde puteți configura opțiunile de scanare, puteți alege obiectele ce vor fi scanate, puteți planifica sarcina sau examina rapoartele. Pentru a accesa această fereastră, apăsați pe butonul **Deschide**, situat în partea dreapta a sarcinii de scanare (sau faceți clic dreapta pe sarcină şi apoi apăsați pe **Deschide**).

Notă
Pentru mai multe informații despre vizualizarea rapoartelor şi tabul **Rapoarte**, consultați "*Examinarea rapoartelor de scanare*" (p. 62).

Configurarea setărilor de scanare

Pentru a configura opțiunile de scanare ale unei anumite sarcini de scanare, faceți clic dreapta pe aceasta şi selectați **Proprietăți**. Va apărea următoarea fereastră:



Descriere generală

Aici puteți vedea informații cu privire la sarcină (nume, când a rulat ultima dată şi programul de rulare) şi puteți configura setările de scanare.

Alegerea nivelului de scanare

Puteți configura uşor setările de scanare alegând nivelul de scanare. Mutați cursorul pentru a seta nivelul de scanare dorit.

Există trei nivele de scanare:

Nivel de protecție	*Descriere*
Scăzut	Oferă o rată de detecție moderată. Consumul de resurse este scăzut. Doar programele sunt scanate împotriva viruşilor. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică.
Mediu	Oferă o rată de detecție bună. Consumul de resurse este moderat.

Nivel de protecție	Descriere
	Toate aplicațiile sunt scanate împotriva viruşilor şi a aplicațiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică.
Ridicat	Oferă o rată de detecție ridicată. Consumul de resurse este şi el ridicat. Toate aplicațiile şi arhivele sunt scanate împotriva viruşilor şi a aplicațiilor spyware. Pe lângă metoda clasică de scanare bazată pe semnături, se mai utilizează şi analiza euristică.

Sunt de asemenea disponibile şi o serie de opțiuni generale privind procesul de scanare:

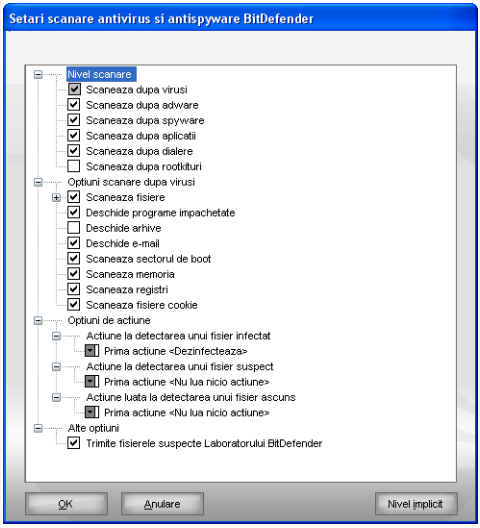
Opțiune	Descriere
Rulează sarcina cu prioritate scăzută	Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va creşte.
Minimizează fereastra de scanare la bara de scanare	Minimizează fereastra de scanare bara de sistem. Faceți dublu-clic pe simbolul BitDefender pentru a o deschide.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina apăsați pe **Scanează**.

Personalizarea nivelului de scanare

Utilizatorii avansați pot folosi şi modifica opțiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fişiere, să caute anumite tipuri de amenințări malițioase sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum şi viteza de reacție a sistemului pe durata scanării.

Apăsați pe **Personalizat** pentru a vă seta propriile opțiuni de scanare. Va apărea o nouă fereastră.



Setări de scanare

Opțiunile de scanare sunt organizate intr-un meniu expandabil similar celor din Windows. Apăsați pe semnul “+” pentru a deschide o opțiune sau pe semnul “-” pentru a închide o opțiune.

Opțiunile de scanare sunt grupate în patru categorii:

- **Nivel scanare**
- **Opțiuni scanare după viruşi**
- **Optiuni de acțiune**
- **Alte opțiuni**

- Specificați tipul de aplicații malițioase după care să scaneze BitDefender, selectând opțiunile adecvate din categoria **Nivel scanare**.

  Următoarele opțiuni sunt disponibile:

Opțiune	*Descriere*
Scanează după viruşi	Scanează după viruşi cunoscuți.

Opțiune	Descriere
	BitDefender detectează, de asemenea, şi corpurile incomplete de viruşi, îndepărtând astfel orice posibilă amenințare ce ar putea afecta securitatea sistemului dumneavostră.
Scanează după adware	Scanează după amenințări adware. Fişierele detectate vor fi considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanează după spyware	Scanează după amenințări spyware cunoscute. Fişierele detectate vor fi considerate ca fiind infectate.
Scanează după aplicații	Scanează aplicații (fişiere `.exe` şi `.dll`).
Scanează după dialere	Scanează după aplicații care apelează numere cu cost ridicat. Fişierele detectate vor fi considerate ca fiind infectate. Programele care includ componente adware se pot opri din funcționare dacă această opțiune este activată.
Scanare după rootkituri	Scanează după obiecte ascunse (fişiere şi procese), cunoscute sub denumirea generică de rootkituri.

- Specificați tipurile de fişiere ce vor fi scanate (arhive, mesaje e-mail şi altele) şi alte opțiuni. Aceasta se face prin selectarea unor opțiuni din categoria **Opțiuni scanare după viruşi**.

  Următoarele opțiuni sunt disponibile:

Opțiune		Descriere
Scanează fişiere	**Scanează toate fisierele**	Vor fi scanate toate fişierele accesate, indiferent de tipul lor.
	Programe	Nu vor fi scanate decât fişierele program, şi anume fişierele cu următoarele extensii: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`;

Opțiune		Descriere
		prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml şi nws.
	Extensiile definite de utilizator	Nu vor fi scanate decât fişierele cu extensiile specificate de utilizator. Aceste extensii trebuie separate prin ";".
Deschide programe impachetate		Scanează programele împachetate.
Deschide arhive		Scanează în interiorul arhivelor.
Deschide e-mail		Scanează în interiorul arhivelor de e-mail.
Scanează sectorul de boot		Scanează sectorul de boot al sistemului.
Scanare memorie		Scanează memoria împotriva viruşilor şi a altor aplicații malițioase.
Scanează regiştri		Scanează intrările din regiştri.
Scanează fişiere cookie		Scanează fişierele cookie.

- Specificați acțiunile ce trebuie aplicate asupra fişierelor infectate, suspecte sau ascunse în categoria **Opțiuni de acțiune**. Puteți specifica o acțiune diferită pentru fiecare categorie.
  - Selectați acțiunea ce trebuie aplicată fişierelor infectate detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Niciuna (înregistrează obiecte)	Nici se va efectua nicio acțiune în legătură cu fişierelor infectate. Aceste fişiere vor apărea în fişierul de raport.
Dezinfectează	Dezinfectează fişierele infectate.
Şterge	Şterge imediat fişierele infectate, fără niciun avertisment.
Mută în carantină	Mută fişierele infectate în carantină.

  - Selectați acțiunea ce trebuie aplicată fişierelor detectate ca fiind infectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Niciuna (înregistrează obiecte)	Nicio acțiune nu va fi aplicată fişierelor suspecte. Aceste fişiere vor apărea în fişierul de raport.
Şterge	Şterge imediat fişierele suspecte, fără niciun avertisment.
Mută în carantină	Mută fişierele suspecte în carantină.

Notă
Fişierele pot fi detectate ca fiind suspecte în urma analizei euristice. Vă recomandăm să trimiteți aceste fişiere Laboratorului BitDefender.

- Selectați acțiunea ce va fi aplicată fişierelor ascunse (rootkituri) detectate. Următoarele opțiuni sunt disponibile:

Acțiune	Descriere
Niciuna (înregistrează obiecte)	Nicio acțiune nu va fi aplicată fişierelor ascunse. Aceste fişiere vor apărea în fişierul de raport.
Mută în carantină	Mută fişierele ascunse în carantină.
Demască	Demască fişierele ascunse astfel încât să le puteți vedea.

Notă
Dacă alegeți să ignorați fişierele detectate sau dacă acțiunea specificată eşuează, va trebui să alegeți o acțiune într-unul dintre paşii programului asistent de scanare.

■ Pentru a fi anunțat să trimiteți fişierele suspecte Laboratorului BitDefender la sfârşitul scanării, bifați **Trimite fişierele suspecte la laboratorul BitDefender** în categoria **Alte opțiuni**.

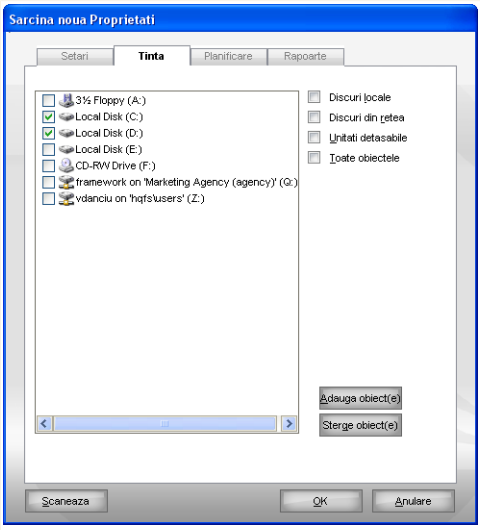
Dacă apăsați pe **Implicit** veți încărca setările standard. Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

Setarea locației de scanare

Notă

Nu puteți modifica ținta de scanare pentru sarcinile din categoria **Sarcini sistem**. Doar puteți vedea obiectele ce vor fi scanate.

Pentru a seta locația de scanare a unei anumite sarcini de scanare, faceți clic dreapta pe sarcină şi selectați **Schimbare cale** (sau **Arată locații scanare** pentru sarcinile de sistem, pentru a vedea ce locații scanează acestea). Va apărea următoarea fereastră:



Locație scanare

Puteți vedea lista partițiilor locale, de rețea şi amovibile (unitatea floppy, CD/DVD), precum şi fişierele şi directoarele adăugate anterior, dacă există. Toate obiectele bifate vor fi scanate atunci când este rulată sarcina.

Secțiunea conține următoarele butoane:

- **Adaugă obiect(e)** - deschide o fereastră de explorare din care puteți selecta fişierele sau directoarele care doriți să fie scanate.

Notă
Puteți folosi drag & drop pentru a adăuga fişiere/directoare în listă.

- **Şterge obiect(e)** - şterge fişierele / directoarele care au fost selectate anterior din lista de obiecte de scanat.

Notă
Numai fişierele / directoarele adăugate de utilizator pot fi şterse, nu şi cele care au fost "văzute" automat de BitDefender.

Pe lângă butoanele explicate mai sus există şi unele opțiuni ce permit selectarea rapidă a locațiilor pentru scanare.

- **Discuri locale** - pentru scanarea partițiilor locale.
- **Discuri din rețea** - pentru scanarea partițiilor din rețea recunoscute.
- **Unități detaşabile** - pentru scanarea unităților mobile de disc (unitățile de CD-ROM şi discheta).
- **Toate obiectele** - pentru scanarea tuturor partițiilor, indiferent dacă sunt locale sau de rețea, precum şi a unităților detaşabile.

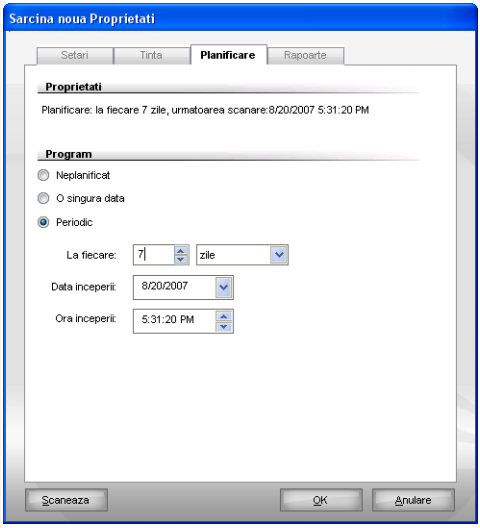
Notă
Dacă doriți să vă scanați tot sistemul, selectați opțiunea **Toate obiectele**.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina apăsați pe **Scanează**.

Programarea sarcinilor de scanare

Pentru sarcini complexe procesul de scanare durează mai mult şi este mai eficient dacă închideți toate programele. Din acest motiv este bine să programați astfel de sarcini să ruleze atunci când nu utilizați sistemul.

Pentru a vedea sau modifica programul de rulare a unei sarcini, faceți clic dreapta pe sarcină şi selectați **Planificare sarcină**. Va apărea următoarea fereastră:



Programator

Puteți vedea programul de rulare al sarcinii, dacă acesta există.

Când planificați o sarcină trebuie să alegeți una dintre următoarele opțiuni:

- **Neplanificat** - sarcina rulează doar atunci când utilizatorul cere acest lucru.
- **O singură dată** - scanarea se face o singură dată, la un anumit moment. Specificați data şi timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.
- **Periodic** - scanarea se realizează periodic, la anumite intervale de timp(ore, zile, săptămâni, luni, ani), începând de la un anumit moment.

  Dacă doriți ca scanarea să se repete la anumite intervale de timp, selectați opțiunea **Periodic** şi introduceți în câmpul de editare **La fiecare** numărul de minute / ore / zile / săptămâni / luni / ani la care doriți să se repete scanarea. De asemenea, trebuie să specificați data şi timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina apăsați pe **Scanează**.

7.2.5. Scanarea obiectelor

Înainte de a începe scanarea, este necesar să vă asigurați că BitDefender este la zi cu semnăturile de aplicații malițioase. Scanarea calculatorului folosind o bază de semnături veche poate împiedica BitDefender să detecteze noi aplicații malițioase descoperite după ultima actualizare efectuată. Pentru a vedea când a fost realizată ultima actualizare, apăsați pe **Actualizare>Actualizare** în consola de setări.

Notă

Pentru ca BitDefender să facă o scanare completă, este necesar să închideți toate programele. Este important să închideți în primul rând clientul de e-mail (i.e. Outlook, Outlook Express sau Eudora).

Metode de scanare

BitDefender oferă patru tipuri de scanare la cerere:

- Scanare imediată - când rulați o sarcină de sistem sau definită de dumneavostră.
- Scanare contextuală - când faceți clic-dreapta pe un fişier sau un director şi selectați opțiunea BitDefender Antivirus 2008.
- Scanare drag&drop - când aduceți un fişier sau director deasupra Barei de scanare.
- Scanare manuală - utilizați scanarea manuală BitDefender pentru a selecta direct fişierele şi directoarele ce trebuie scanate.

Scanare imediată

Pentru a vă scana sistemul sau o parte din el puteți rula sarcinile de scanare predefinite sau propriile sarcini de scanare. Acest tip de scanare este cunoscut drept scanare imediată.

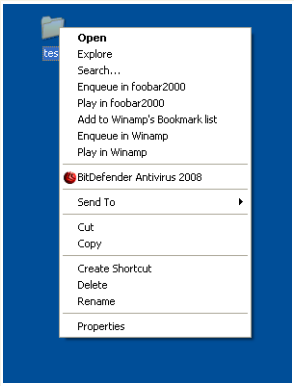
Pentru a rula o sarcină de scanare, utilizați una dintre următoarele metode:

- faceți dublu-clic pe sarcina de scanare dorită din listă.
- apăsați pe butonul **Scanează acum** corespunzător sarcinii.
- selectați sarcina şi apoi apăsați pe **Execută sarcina**.

Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați “*Programul asistent de scanare*” (p. 58).

Scanare contextuală

Pentru a scana un fişier sau un director, fără a mai configura o nouă sarcină de scanare, puteți utiliza meniul contextual. Acest tip de scanare este cunoscut drept scanare contextuală.



Scanare contextuală

Faceți clic-dreapta pe fişierul sau directorul care doriți să fie scanat şi selectați opțiunea **BitDefender Antivirus 2008**.

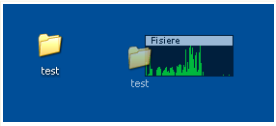
Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 58).

Puteți modifica opțiunile de scanare şi examina fişierele de raport accesând fereastra de **Proprietăți** a sarcinii **Scanare meniu contextual**.

Scanare prin drag&drop

Trageți fişierul sau directorul care doriți să fie scanat peste **Bara de scanare**, ca în imaginile de mai jos.

Trageți fişierul



Lăsați fişierul

Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 58).

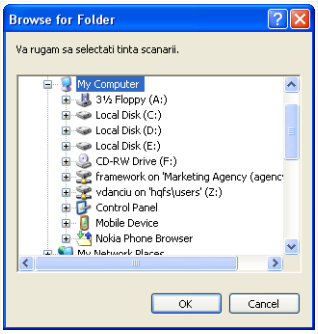
Scanare manuală

Scanarea manuală constă în selectarea directă a obiectului ce trebuie scanat utilizând opțiunea Scanare manuală BitDefender din grupul BitDefender din meniul Start.

Notă
Scanarea manuală este foarte utilă, mai ales că poate fi realizată şi atunci când Windows operează în Safe Mode.

Pentru a selecta obiectul ce trebuie scanat de BitDefender, în meniul Windows Start, urmați calea **Start → Programe → BitDefender 2008 → Scanare manuală BitDefender**.

Va apărea următoarea fereastră:



Scanare manuală

Selectați obiectul care doriți să fie scanat şi apăsați pe **OK**.

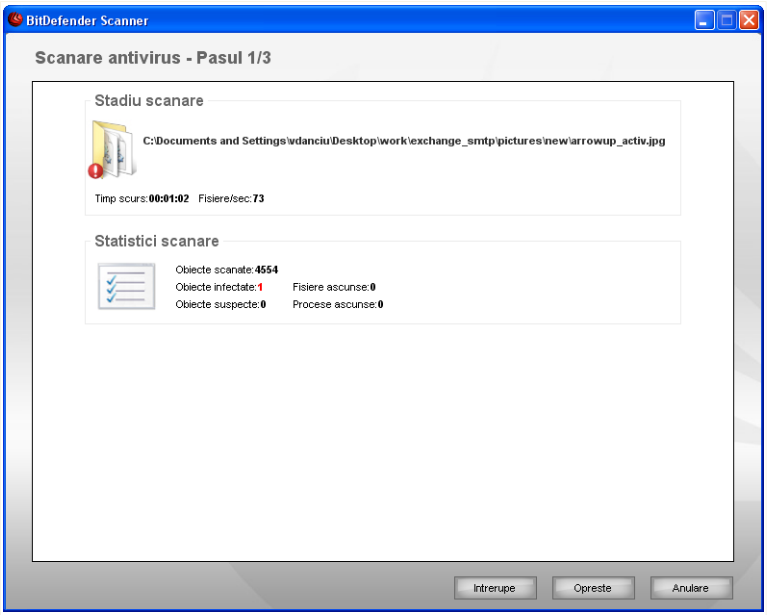
Va apărea programul asistent de scanare şi scanarea va fi inițiată. Pentru mai multe informații, consultați "*Programul asistent de scanare*" (p. 58).

Programul asistent de scanare

Atunci când inițiați un proces de scanare la cerere, va apărea programul asistent de scanare. Urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.



Scanare

Puteți vedea stadiul şi statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse şi altele).

Notã
Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

Pentru a opri temporar procesul de scanare, apăsați pe **Întrerupe**. Va trebui să apăsați pe **Reia** pentru a relua scanarea.

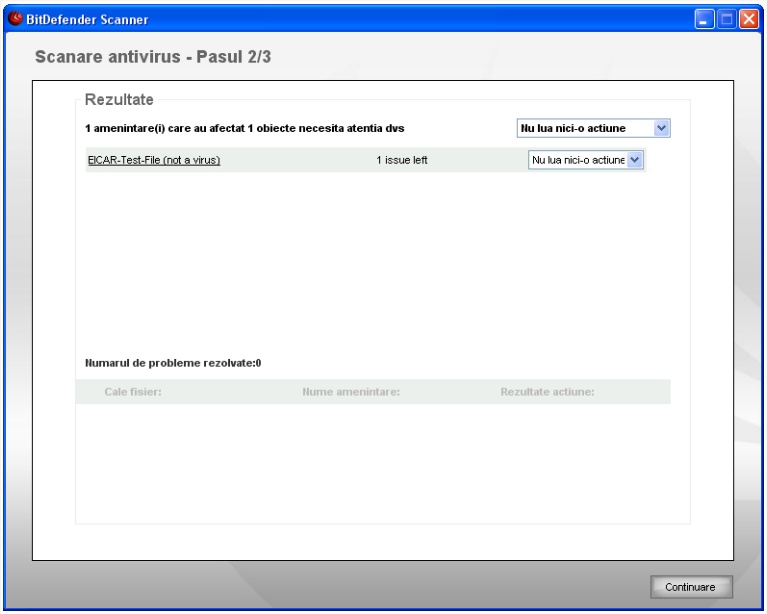
Puteți opri scanarea oricând doriți apăsând pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent.

Notã
Dacă au fost detectate fişiere suspecte în timpul scanării, vi se va cere să le trimiteți laboratorului BitDefender.

Aşteptați ca BitDefender să finalizeze scanarea.

Pasul 2/3 - Selectați acțiunile

După ce scanarea a fost finalizată, va apărea o nouă fereastră, unde puteți vedea rezultatele scanării.



Acțiuni

Puteți vedea numărul problemelor care vă afectează sistemul.

Problemele sunt afişate pe grupuri. Apăsați pe căsuța cu “+” pentru a deschide un grup sau pe căsuța cu “-” pentru a închide un grup.

Puteți alege o acțiune globală care să fie luată asupra fiecărui grup de probleme sau puteți alege acțiuni separate pentru fiecare problemă în parte.

Următoarele opțiuni pot apărea pe meniu:

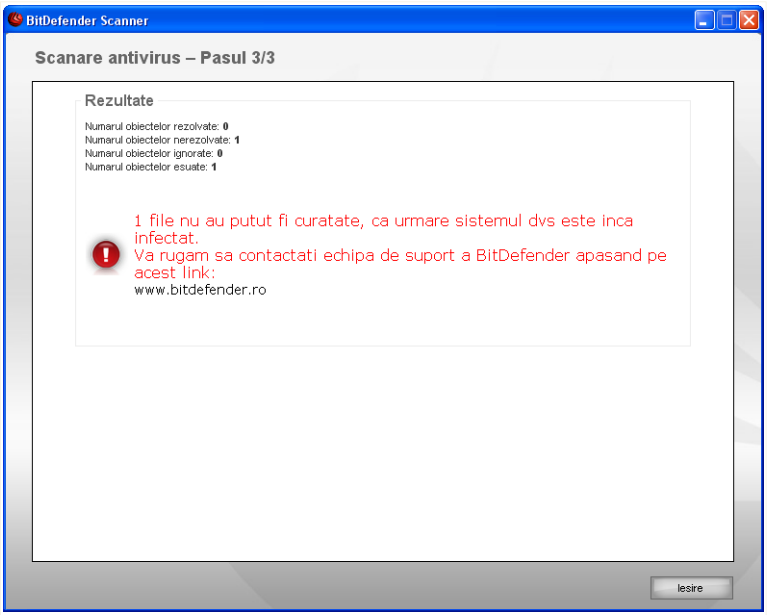
Acțiune	*Descriere*
Nicio acțiune	Nu se va lua nicio acțiune asupra fişierelor detectate.

Acțiune	Descriere
Dezinfectează	Dezinfectează fişierele infectate.
Şterge	Şterge fişierele detectate.
Demască	Face vizibile obiectele ascunse.

Apăsați pe **Repară probleme** pentru a aplica acțiunile specificate.

Pasul 3/3 - Examinați rezultatele

Atunci când BitDefender a remediat toate problemele apărute, rezultatele scanării vor fi afişate într-o nouă fereastră.



Rezumat

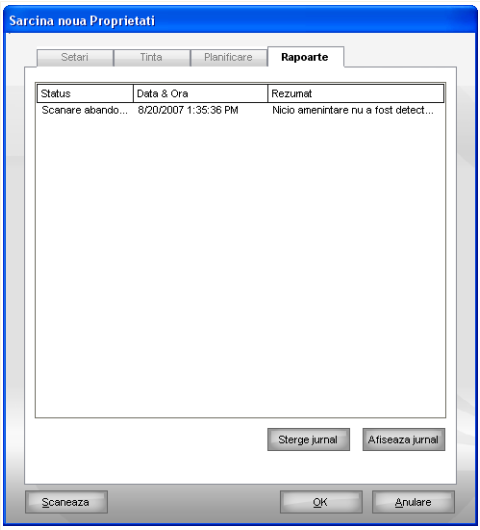
Puteți vedea un rezumat al rezultatelor.

Fişierul de raport este salvat automat în secțiunea Rapoarte din fereastra de **Proprietăți** a sarcinii respective.

Avertisment
Dacă sunt probleme care nu au fost remediate, vă recomandăm să contactaţi echipa de suport a BitDefender pe pagina web www.bitdefender.ro.

7.2.6. Examinarea rapoartelor de scanare

Pentru a examina rezultatele scanării după rularea unei sarcini, faceţi clic dreapta pe sarcină şi selectaţi **Examinare rapoarte**. Va apărea următoarea fereastră:



Rapoarte

Aici puteţi examina rapoartele generate de fiecare dată când sarcina a fost executată. Fiecare fişier conţine informaţii privind rezultatele scanării, data şi timpul la care a fost executată sarcina precum şi un scurt rezumat (scanare finalizată).

Sunt disponibile două butoane:

- **Afişează jurnal** - deschide fişierul de raport selectat.
- **Şterge jurnal** - şterge fişierul de raport selectat.

De asemenea, pentru a deschide sau şterge un fişier de raport, faceţi clic dreapta pe fişier şi selectaţi opţiunea corespunzătoare din meniu.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra. Pentru a executa sarcina apăsați pe **Scanează**.

7.3. Obiecte excluse de la scanare

Este posibil ca uneori să fie nevoie să excludeți unele fişiere de la scanare. De exemplu, puteți exclude un fişier de test EICAR de la scanarea la acces sau fişiere `.avi` de la scanarea la cerere.

BitDefender permite excluderea obiectelor atât de la scanarea la acces, cât şi de la scanarea la cerere. Această caracteristică este menită să reducă timpul de scanare şi să evite orice fel de interferență cu munca dumneavostră.

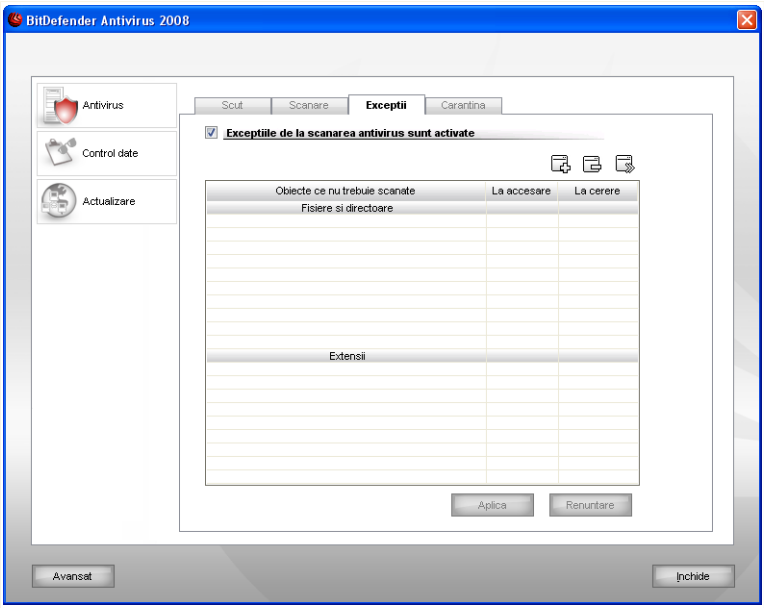
Pot fi excluse de la scanare două tipuri de obiecte:

- **Căi** - fişierul sau directorul (incluzând toate obiectele conținute) indicat de o cale specificată va fi exclus de la scanare.
- **Extensii** - toate fişierele având o extensie specificată vor fi excluse de la scanare.

Notă

Obiectele excluse de la scanarea la acces nu vor fi scanate, indiferent dacă acestea sunt accesate de către dumneavoastră sau de către o aplicație.

Pentru a vedea şi gestiona obiectele excluse de la scanare, apăsați pe **Antivirus>Excepții** în consola de setări. Va apărea următoarea fereastră:



Excepții

Puteți vedea obiectele (fişiere, directoare, extensii) care sunt excluse de la scanare. Pentru fiecare obiect, puteți vedea dacă este exclus de la scanarea la acces, de la scanarea la cerere sau de la ambele.

Notã
Excepțiile specificate aici NU se vor aplica scanării contextuale.

Pentru a şterge un obiect din listă, selectați-l şi apăsați pe butonul **Şterge**.

Pentru a edita un obiect din listă, selectați-l şi apăsați pe butonul **Editează**. Va apărea o nouă fereastră unde puteți schimba extensia sau calea care va fi exclusă, precum şi tipul de scanare de la care acestea să fie excluse. Faceți modificările necesare şi apoi apăsați pe **OK**.

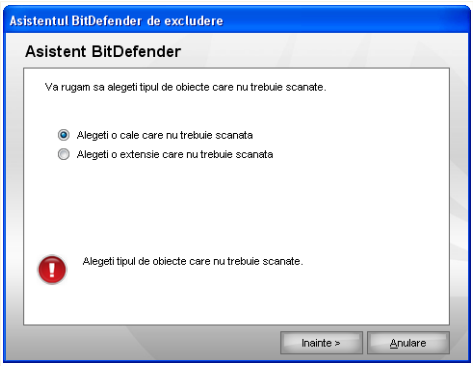
Notã
De asemenea, puteți face clic dreapta pe un obiect şi utiliza opțiunile meniului contextual pentru a-l edita sau şterge.

Puteți face clic pe **Revino** pentru a reveni asupra schimbărilor făcute în tabelul de reguli, cu condiția să nu le fi salvat anterior apăsând pe **Aplică**.

7.3.1. Excluderea căilor de la scanare

Pentru a exclude căi de la scanare, apăsați pe butonul **Adaugă**. Veți fi ghidat pe parcursul procesului de excludere a căilor de la scanare de către programul asistent de configurare care va apărea.

Pasul 1/3 - Selectați tipul obiectului

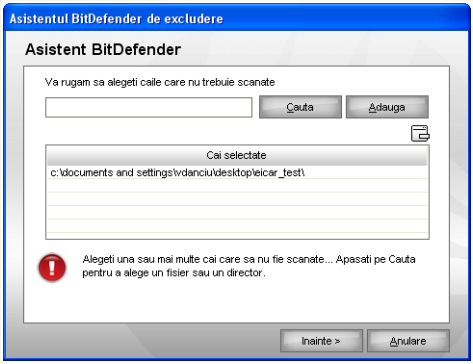


Tip obiect

Selectați opțiunea de excludere a unei căi de la scanare.

Apăsați pe **Înainte**.

Pasul 2/3 - Specificați căile excluse



Căi excluse

Pentru a preciza căile ce vor fi excluse de la scanare, utilizați una dintre următoarele metode:

- Apăsați pe **Caută**, selectați fișierul sau directorul care doriți să fie exclus de la scanare şi apăsați pe **Adaugă**.
- Introduceți calea care doriți să fie exclusă de la scanare şi apăsați pe **Adaugă**.

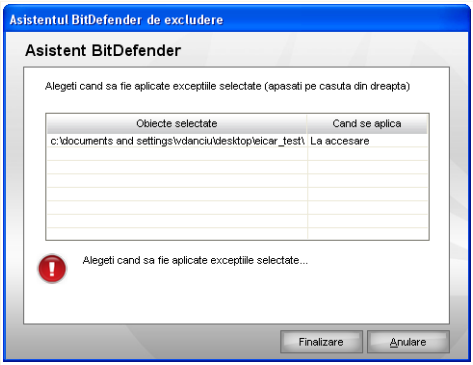
> ***Notă***
> Un mesaj de eroare va apărea dacă nu există calea furnizată. Apăsați pe **OK** şi verificați validitatea căii.

Căile vor apărea în tabel pe măsură ce le adăugați. Puteți adăuga oricâte căi doriți.

Pentru a şterge un obiect din listă, selectați-l şi apăsați pe butonul **Şterge**.

Apăsați pe **Înainte**.

Pasul 3/3 - Selectați tipul de scanare



Tip scanare

Puteți vedea un tabel conținând căile ce vor fi excluse de la scanare şi tipul de scanare de la care acestea sunt excluse.

Implicit, căile selectate sunt excluse atât de la scanarea la acces cât şi de la scanarea la cerere. Pentru a alege când să fie aplicată excepția, apăsați pe coloana din dreapta şi selectați opțiunea dorită din listă.

Apăsați pe **Finalizare**.

Apăsați pe **Aplică** pentru a salva modificările.

7.3.2. Excluderea extensiilor de la scanare

Pentru a exclude extensii de la scanare, apăsați pe butonul **Adaugă**. Veți fi ghidat pe parcursul procesului de excludere a extensiilor de la scanare de către programul asistent de configurare care va apărea.

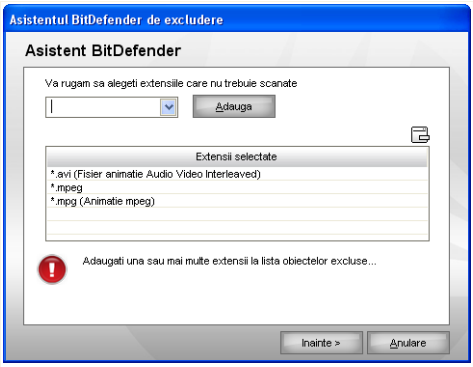
Pasul 1/3 - Selectați tipul obiectului

Tip obiect

Selectați opțiunea de excludere a unei extensii de la scanare.

Apăsați pe **Înainte**.

Pasul 2/3 - Specificați extensiile excluse



Extensii excluse

Pentru a specifica extensiile ce vor fi excluse de la scanare, utilizați una dintre următoarele metode:

- Selectați din meniu extensia care doriți să fie exclusă de la scanare şi apăsați pe **Adaugă**.

Notă
Meniul conține lista tuturor extensiilor înregistrate pe sistemul dumneavoastră. Atunci când selectați o extensie, îi puteți vedea descrierea, dacă aceasta există.

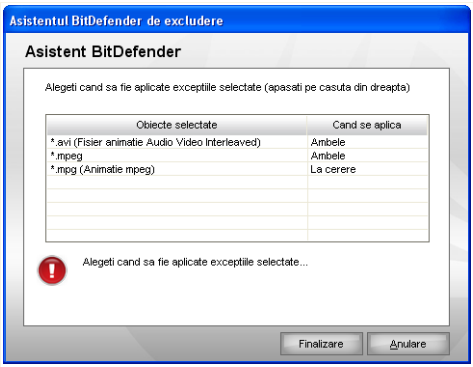
- Introduceți extensia care doriți să fie exclusă de la scanare şi apăsați pe **Adaugă**.

Extensiile vor apărea în tabel pe măsură ce le adăugați. Puteți adăuga oricâte extensii doriți.

Pentru a şterge un obiect din listă, selectați-l şi apăsați pe butonul **Şterge**.

Apăsați pe **Înainte**.

Pasul 3/3 - Selectați tipul de scanare



Tip scanare

Puteți vedea un tabel conținând extensiile excluse de la scanare şi tipul de scanare de la care acestea sunt excluse.

Implicit, extensiile selectate sunt excluse atât de la scanarea la acces cât şi de la scanarea la cerere. Pentru a schimba când să fie aplicată excepția, apăsați pe coloana din dreapta şi selectați opțiunea dorită din listă.

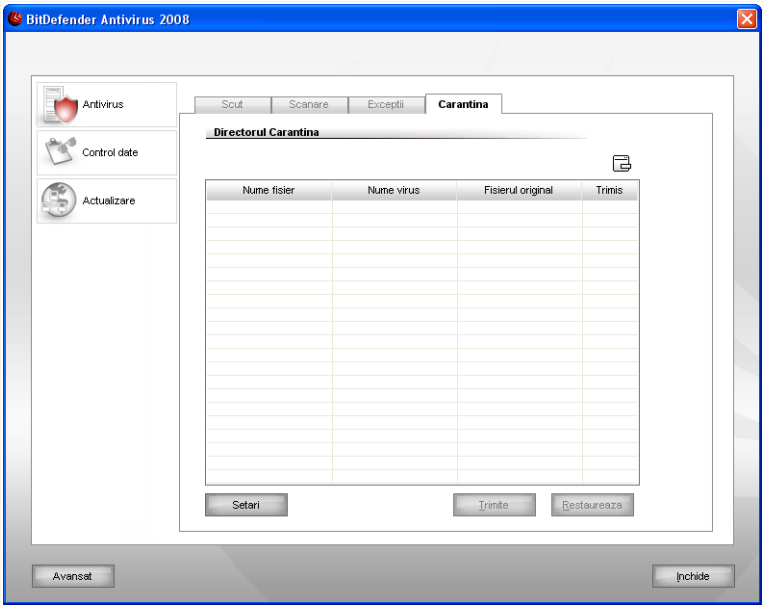
Apăsați pe **Finalizare**.

Apăsați pe **Aplică** pentru a salva modificările.

7.4. Zona de carantină

BitDefender permite izolarea fişierelor infectate sau suspecte într-o zonă sigură, numită carantină. Izolând aceste fişiere în carantină, riscul răspândirii infecției dispare, iar în plus, aveți posibilitatea să trimiteți aceste fişiere Laboratorului BitDefender pentru analiză aprofundată.

Pentru a vedea şi gestiona fişierele din carantină şi pentru a configura setările carantinei, apăsați pe **Antivirus>Carantină** în consola de setări.



Carantină

7.4.1. Gestionarea fişierelor din carantină

După cum puteți observa, secțiunea **Carantină** conține o listă cu toate fişierele care au fost izolate până acum. Fiecărui fişier i se poate afla numele, dimensiunea, data izolării şi data trimiterii.

Notă
Atunci când sunt în carantină viruşii sunt inofensivi, pentru că nu pot fi executaţi sau citiţi.

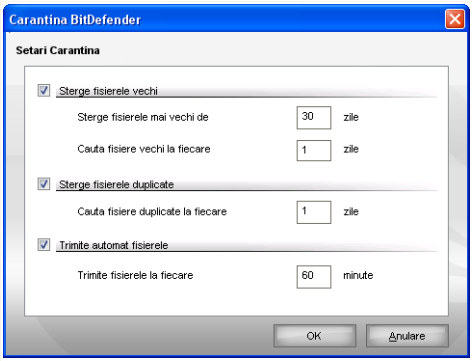
Pentru a şterge un fişier selectat din carantină apăsaţi pe butonul **Şterge**. Dacă doriţi să mutaţi fişierul selectat la locaţia originală apăsaţi pe **Restaurează**.

Puteţi trimite fişierele selectate la Laboratorul BitDefender pentru o analiză detaliată apăsând pe **Trimite**.

Meniul contextual. Un meniu contextual este disponibil, permiţând gestionarea rapidă a fişierelor din carantină. Aceleaşi opţiuni ca cele amintite anterior sunt disponibile. De asemenea, puteţi selecta **Actualizează** pentru a actualiza carantina.

7.4.2. Configurarea setărilor carantinei

Pentru a configura setările carantinei, apăsaţi pe **Setări**. Va apărea o nouă fereastră.



Setări Carantină

Utilizând setările carantinei, puteţi seta BitDefender să execute automat următoarele acţiuni:

Şterge fişierele vechi. Pentru a şterge automat fişierele vechi din carantină, bifaţi opţiunea corespunzătoare. Trebuie să specificaţi numărul de zile după care fişierele din carantină ar trebui şterse şi frecvenţa cu care BitDefender să caute fişiere vechi.

Notă
Implicit, BitDefender va căuta fişiere vechi în fiecare zi şi va şterge fişierele mai vechi de 10 zile.

Şterge fişierele duplicat. Pentru a şterge automat fişierele duplicat din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați numărul de zile dintre două căutări consecutive de fişiere duplicat.

Notă
Implicit, BitDefender va căuta fişiere duplicat în carantină în fiecare zi.

Trimite automat fişierele. Pentru a trimite automat fişierele din carantină, bifați opțiunea corespunzătoare. Trebuie să specificați frecvența cu care să fie trimise fişierele.

Notă
Implicit, BitDefender va trimite automat fişierele din carantină la fiecare 60 minute.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

8. Control date

BitDefender monitorizează zeci de potențiale puncte sensibile ale sistemului dumneavoastră de operare, acolo unde pot acționa aplicațiile spyware, şi verifică orice schimbare apărută. Acest modul blochează în mod eficient caii troieni şi alte instrumente instalate de hackeri, care încearcă să vă dezvăluie identitatea şi să trimită informațiile personale, cum ar fi seria cărții de credit,din computerul dumneavoastră, către hacker.

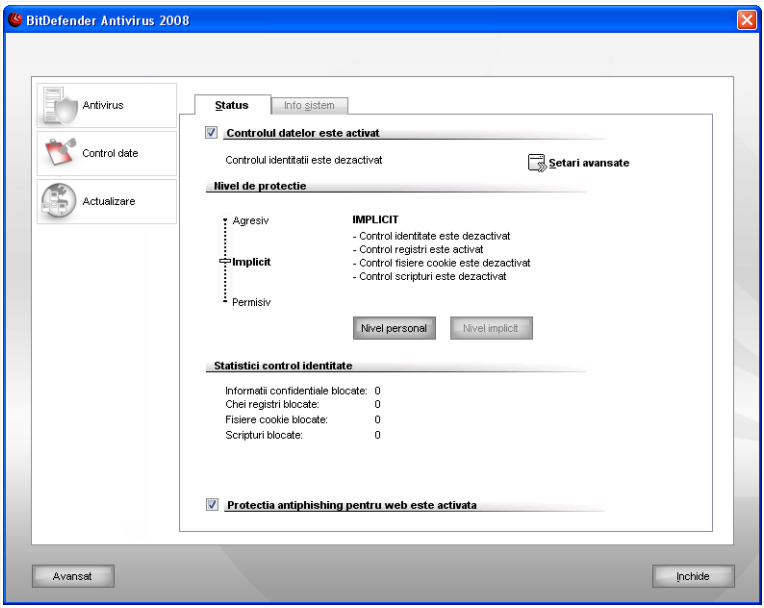
De asemenea, BitDefender scanează paginile web pe care le vizitați şi vă avertizează dacă sunt detectate amenințări phishing.

Secțiunea **Control date** a acestui ghid de utilizare conține următoarele subiecte:

- Status Control date
- Setări avansate - Control identitate
- Setări avansate - Control regiştri
- Setări avansate - Control cookie
- Setări avansate - Control scripturi
- Informații sistem
- Bara de comenzi antiphishing

8.1. Status Control date

Pentru a configura Controlul datelor şi a vedea informații legate de activitatea sa, apăsați pe **Control date** în consola de setări. Va apărea următoarea fereastră:



Status Control date

8.1.1. Control date

Important
Pentru a preveni infecțiile cu aplicații spyware mențineți activat **Controlul datelor**.

Controlul datelor vă protejează calculatorul prin intermediul a cinci controale:

- Controlul identității - vă protejează datele confidențiale filtrând traficul HTTP(la ieşire) şi SMTP potrivit regulilor create de dumneavoastră în secțiunea Identitate.
- Controlul regiştrilor - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.
- Controlul fişierelor cookie - vă cere permisiunea de fiecare dată când un site încearcă să seteze un cookie.
- Controlul scripturilor - vă cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ.

Pentru a configura setările pentru aceste controale apăsați pe Setări avansate.

În partea de jos a acestei secțiuni, puteți vedea **statisticile Controlului datelor**.

Configurarea nivelului de protecție

Puteți alege nivelul de protecție adecvat nevoilor dumneavoastră de securitate. Mutați cursorul pentru a seta nivelul de protecție dorit.

Există trei nivele de protecție:

Nivel de protecție	*Descriere*
Permisiv	Doar **Controlul regiştrilor** este activat.
Standard	**Controlul regiştrilor** şi **Controlul identității** sunt activate.
Agresiv	**Controlul regiştrilor**, **Controlul identității** şi **Controlul scripturilor** sunt activate.

Puteți personaliza nivelul de protecție apăsând pe **Nivel personal**. În fereastra care va apărea, selectați controalele Antispyware pe care doriți să le activați şi apăsați pe **OK**.

Apăsați pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

8.1.2. Protecție antiphishing

Phishingul reprezintă o activitate criminală pe Internet care foloseşte tehnici de inginerie socială pentru a înşela oamenii în scopul obținerii de informații personale.

De cele mai multe ori, încercările de phishing se manifestă prin trimiterea în masă de mesaje e-mail ce pretind, în mod fals, a proveni de la companii recunoscute. Aceste mesaje contrafăcute sunt trimise în speranța că cel puțin o parte dintre cei care primesc mesajul şi corespund profilului persoanei țintă a phishingului vor fi convinse să divulge informații private.

De obicei, un mesaj phishing prezintă o problemă legată de contul dumneavostră online. Conținutul acestuia încearcă să vă convingă să apăsați pe un link furnizat în mesaj pentru a accesa o pagină web presupusă a fi legitimă (în realitate, o pagină contrafăcută) unde sunt cerute informații private. Vi se poate cere, de exemplu, să confirmați informații referitoare la contul dumneavoastră, cum ar fi numele de utilizator şi parola, şi să furnizați numărul contului dumneavoastră bancar (IBAN) sau PIN-ul cardului. Uneori, pentru a fi şi mai convingător, mesajul poate pretinde că v-a fost suspendat contul sau că acesta va fi suspendat dacă nu utilizați linkul furnizat.

De asemenea, phishingul utilizează şi aplicaţii spyware, cum ar fi troieni ce reţin parole, pentru a fura informaţii legate de conturi direct de pe calculatorul dumneavoastră.

Principalele ţinte ale phishingului sunt clienţii serviciilor de plată online, cum ar fi eBay şi PayPal, precum şi băncile care oferă servicii online. Recent, şi utilizatorii de pagini web tip reţea socială au devenit o ţintă a phishingului, scopul fiind acela de a obţine informaţii personale de identificare utilizate mai apoi pentru furtul identităţii.

Pentru a fi protejat împotriva tentativelor de phishing atunci când navigaţi pe Internet, menţineţi **Protecţia antiphishing** activată. Astfel, BitDefender va scana fiecare pagină web înainte de a o accesa şi vă va alerta de existenţa oricărei ameninţări phishing. O listă albă de pagini web care nu vor fi scanate de BitDefender poate fi configurată.

Pentru o administrare facilă a protecţiei antiphishing şi a listei albe, utilizaţi bara de comenzi antiphishing a BitDefender, integrată în Internet Explorer. Pentru mai multe informaţii, consultaţi "*Bara de comenzi antiphishing*" (p. 92).

8.2. Setări avansate - Control identitate

Păstrarea datelor confidenţiale în siguranţă este o problemă importantă ce ne preocupă pe toţi. Furtul de date a ţinut pasul cu dezvoltarea comunicaţiilor pe Internet şi se foloseşte de noi metode de a păcăli oamenii să cedeze informaţiile private.

Fie că este vorba de adresa e-mail sau de numărul cărţii de credit, dacă acestea ajung în mâinile unor persoane nepotrivite vă pot aduce daune: puteţi să vă treziţi că aveţi contul de mail plin de spam sau să constataţi cu surprindere că aveţi contul bancar golit.

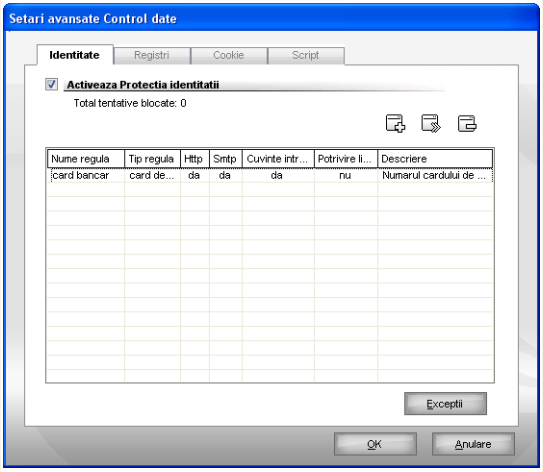
Controlul identităţii vă ajută să păstraţi informaţiile confidenţiale în siguranţă. Acesta scanează traficul HTTP sau SMTP, sau pe amândouă, în căutare de şiruri de caractere definite de dumneavoastră. Dacă este găsită o concordanţă, site-ul sau mesajul respectiv este blocat.

Este oferit suport pentru mai mulţi utilizatori, astfel încât niciun alt utilizator al sistemului nu poate vedea regulile pe care le-aţi configurat.

Regulile privind confidenţialitatea pot fi configurate în secţiunea **Identitate**. Pentru a accesa această secţiune, deschideţi fereastra **Setări avansate Control date** şi apăsaţi pe tabul **Identitate**.

Notă

Pentru a deschide fereastra **Setări avansate Control date**, apăsaţi pe **Control date>Status** în consola de setări şi apoi pe **Setări avansate**.



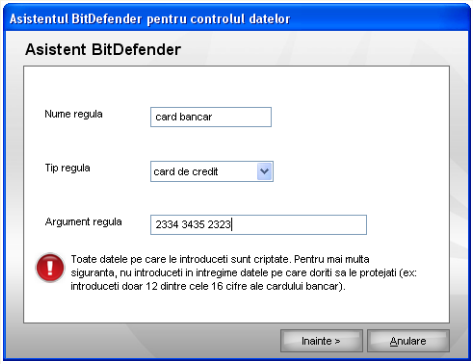
Control identitate

8.2.1. Crearea regulilor de identitate

Regulile trebuie introduse manual (apăsaţi pe butonul **Adaugă** şi alegeţi parametrii regulei). Va apărea asistentul de configurare.

Asistentul de configurare este o procedură constituită din trei paşi.

Pasul 1/3 - Furnizați tipul şi argumentul regulei



Furnizați tipul şi argumentul regulei

Introduceți numele regulei în câmpul editabil.

Trebuie setați parametrii următori:

- **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
- **Argument regulă** - introduceți argumentul regulei.

Notă

Dacă introduceți mai puțin de trei caractere, vi se va cere confirmarea acțiunii. Vă recomandăm să introduceți cel puțin trei caractere pentru a evita blocarea greşită a mesajelor şi a paginilor web.

Tot ceea ce introduceți este criptat. Pentru mai multă siguranță, nu introduceți întreaga dată pe care vreți să o protejați ci doar o parte a acesteia.

Apăsați pe **Înainte**.

Pasul 2/3 - Selectați traficul

Selectați traficul

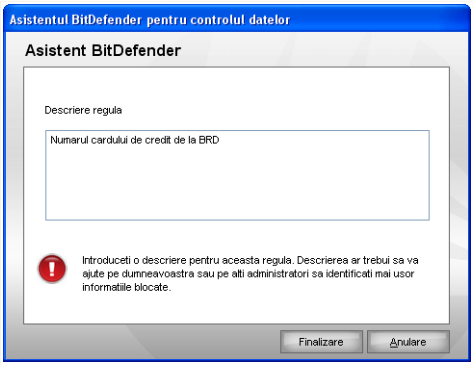
Selectați tipul de trafic care doriți să fie scanat de BitDefender. Următoarele opțiuni sunt disponibile:

- **Scanează HTTP** - scanează traficul HTTP (web) şi blochează la ieşire toate datele ce corespund unei reguli.
- **Scanează SMTP** - scanează traficul SMTP (mail) şi blochează la ieşire toate mesajele e-mail ce corespund unei reguli.

Puteți alege să aplicați regula doar dacă argumentul regulei apare ca şir independent sau ținând cont de majuscule şi minuscule.

Apăsați pe **Înainte**.

Pasul 3/3 - Descrieți regula



Descrieți regula

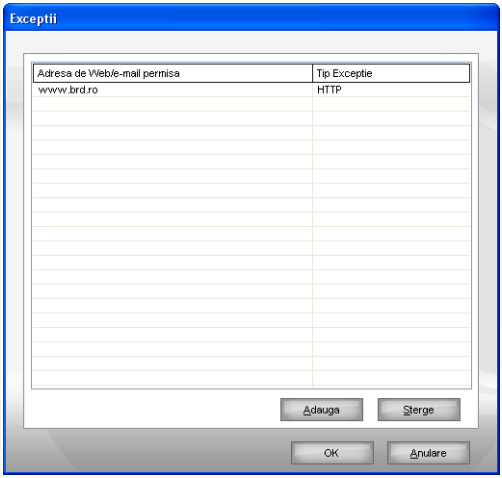
Introduceți o scurtă descriere a regulei în câmpul editabil.

Apăsați pe **Finalizare**.

8.2.2. Specificarea excepțiilor

În unele cazuri, este nevoie să definiți excepții la anumite reguli de identitate. Considerați cazul în care creați o regulă de identitate care împiedică trimiterea numărului cărții dumneavoastră de credit prin HTTP (pe web). De fiecare dată când acesta este trimis pe o pagină web de pe contul dumneavoastră de utilizator, pagina respectivă este blocată. Dacă doriți, de exemplu, să cumpărați o pereche de adidaşi prin intermediul unui magazin online (care ştiți că este securizat), va trebui să specificați o excepție de la regula respectivă.

Pentru a deschide fereastra unde puteți gestiona excepțiile, apăsați pe **Excepții**.



Excepții

Pentru a adăuga o excepție, urmați aceşti paşi:

1. Apăsați pe **Adaugă** pentru a adăuga o nouă înregistrare în listă.
2. Faceți dublu-clic pe **Specificați adresa permisă** şi furnizați adresa web sau adresa de mail pe care doriți să o adăugați ca excepție.
3. Faceți dublu-clic pe **Alegeți tipul** şi alegeți din meniu opțiunea corespunzătoare tipului de adresă furnizată anterior.
   - Dacă ați specificat o adresă web, selectați **HTTP**.
   - Dacă ați specificat o adresă de mail, selectați **SMTP**.

Pentru a şterge o excepție din listă, selectați-o şi apăsați pe **Şterge**.

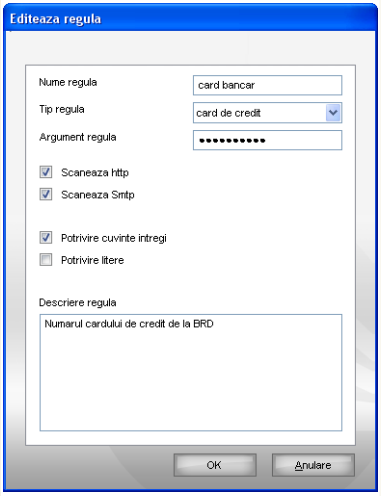
Apăsați pe **OK** pentru a salva modificările.

8.2.3. Administrarea regulilor

Puteți vedea regulile listate în tabel.

Pentru a şterge o regulă, selectați-o şi apăsați pe butonul **Şterge**. Pentru a dezactiva o regulă temporar, fără a o şterge, debifați căsuța corespunzătoare.

Pentru a modifica atributele unei reguli, selectați-o şi apăsați pe butonul **Editează** sau faceți dublu-clic pe ea. Va apărea o nouă fereastră.



Editează regula

Aici puteți modifica numele, descrierea şi parametrii regulei (tip, argument şi trafic). Apăsați pe **OK** pentru a salva modificările.

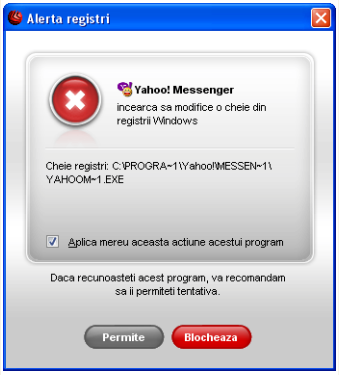
Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

8.3. Setări avansate - Control regiştri

Una dintre părțile importante ale sistemului de operare Windows sunt **regiştrii**. Aici îşi păstrează Windows configurația şi setările, programele instalate, informații despre utilizator şi alte date.

Tot în **regiştri** sunt definite programele care sunt lansate la pornirea Windows. Viruşii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul îşi reporneşte calculatorul.

Controlul Regiştrilor supraveghează regiştrii Windows – în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiştri astfel încât să fie lansat la pornirea Windows.



Alertă regiştri

Puteți interzice această modificare apăsând pe **Nu** sau puteți să o permiteți apăsând pe **Da**.

Dacă doriți ca BitDefender să rețină răspunsul dumneavoastră, selectați opțiunea **Aplică mereu această acțiune acestui program**. Astfel, va fi creată o regulă şi aceeaşi acțiune va fi aplicată de fiecare dată când acest program încearcă să modifice o cheie de regiştri pentru a fi executat la pornirea Windowsului.

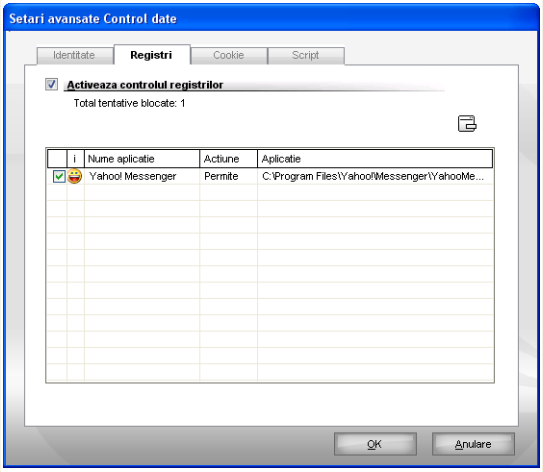
Notă

BitDefender vă va alerta atunci când instalați programe pentru care este necesară lansarea la pornirea Windows. În cele mai multe cazuri, aceste programe sunt de încredere.

Fiecare regulă care a fost creată poate fi accesată în secțiunea **Regiştri** pentru modificări ulterioare. Pentru a accesa această secțiune, deschideți fereastra **Setări avansate Control date** şi apăsați pe tabul **Regiştri**.

Notă

Pentru a deschide fereastra **Setări avansate Control date**, apăsați pe **Control date>Status** în consola de setări şi apoi pe **Setări avansate**.



Control regiştri

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a şterge o regulă, selectați-o şi apăsați pe butonul **Şterge**. Pentru a dezactiva temporar o regulă, fără a o şterge, debifați căsuța corespunzătoare.

Pentru a schimba acțiunea regulei, faceți dublu-clic pe câmpul acțiunii şi selectați opțiunea corespunzătoare din meniu.

Apăsați pe **OK** pentru a închide fereastra.

8.4. Setări avansate - Control cookie

Fişierele cookie sunt foarte comune pe Internet. Ele sunt fişiere mici salvate pe calculatorul dumneavoastră. Paginile web creează aceste fişiere pentru a vă monitoriza activitatea pe Internet şi a salva informații specifice despre dumneavoastră.

În general, fişierele cookie vă fac viața mai uşoară. De exemplu ele ajută site-urile să vă rețină numele şi preferințele, pentru a nu trebui să le introduceți la fiecare vizită.

Dar ele pot fi folosite şi pentru a vă compromite intimitatea, urmărindu-vă obiceiurile de navigare pe Internet.

Aici vă ajută **Controlul fişierelor cookie**. Când este activat, **Controlul fişierelor cookie** vă va cere permisiunea de fiecare dată când un site încearcă să seteze un cookie:

Alertă cookie

Puteți vedea numele aplicației care încearcă să trimită fişierul cookie.

Selectați opțiunea **Reține acest răspuns** şi apăsați pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Data viitoare când vă veți conecta la acelaşi site nu veți mai fi notificat.

Aceasta vă va ajuta să alegeți paginile web în care aveți încredere şi pe cele în care nu aveți.

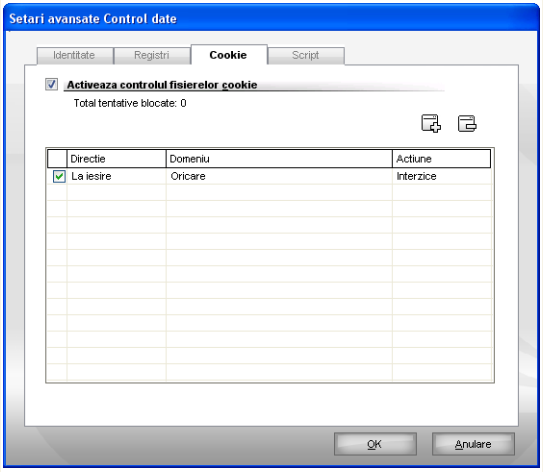
Notă

Din cauza numărului mare de fişiere cookie de pe Internet, **Controlul fişierelor cookie** poate fi la început. Inițial, vă va pune foarte multe întrebări despre pagini web care încearcă să seteze cookie-uri pe calculatorul dumneavoastră. După ce adăugați paginile web pe care le folosiți frecvent în lista de reguli, navigarea va deveni la fel de uşoară ca la început.

Fiecare regulă care a fost creată poate fi accesată în secțiunea **Cookie** pentru modificări ulterioare. Pentru a accesa această secțiune, deschideți fereastra **Setări avansate Control date** şi apăsați pe tabul **Cookie**.

Notă

Pentru a deschide fereastra **Setări avansate Control date**, apăsați pe **Control date>Status** în consola de setări şi apoi pe **Setări avansate**.



Control cookie

Puteți vedea listate în tabel regulile create până în momentul de față.

Important
Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

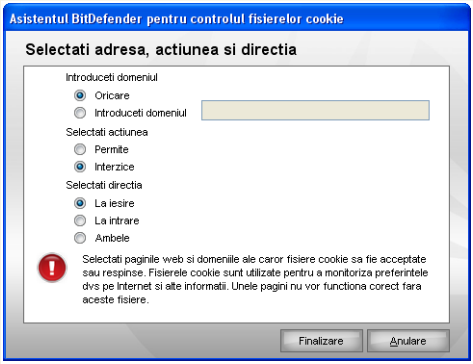
Pentru a şterge o regulă, selectați-o şi apăsați pe butonul **Şterge**. Pentru a modifica parametrii unei reguli, faceți dublu-clic pe câmpul corespunzător şi faceți modificările dorite. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Regulile pot fi introduse automat (prin fereastra de alertă) sau manual (apăsați pe butonul **Adaugă** şi selectați parametrii regulei). Va apărea asistentul de configurare.

8.4.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită dintr-un singur pas.

Pasul 1/1 - Selectați adresa, acțiunea şi direcția



Selectați adresa, acțiunea şi direcția

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Fişierele cookie de la domeniul respectiv vor fi acceptate.
Interzice	Fişierele cookie de la domeniul respectiv vor fi blocate.

- **Direcție** - selectați direcția traficului.

Tip	Descriere
La ieşire	Regula se aplică fişierelor cookie trimise.
La intrare	Regula se aplică fişierelor cookie recepționate.
Ambele	Regula se va aplica în ambele direcții.

Apăsați pe **Finalizare**.

Notă
Puteți accepta fişiere cookie fără a le returna: setați acțiunea **Interzice** şi direcția **La ieşire**.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

8.5. Setări avansate - Control scripturi

Scripturile şi alte coduri cum ar fi elementele ActiveX şi Applet-urile Java, care sunt folosite pentru a crea pagini web, pot fi programate astfel încât să aibă efecte dăunătoare. Elemente de tipul ActiveX, de exemplu, pot avea în întregime acces la datele dumneavoastră şi le pot citi sau şterge de pe calculatorul dumneavoastră, pot captura parole şi intercepta mesaje cât timp sunteți conectați la Internet. Este recomandat să acceptați conținutul activ doar de la paginile web pe care le cunoaşteți foarte bine şi care sunt de încredere.

BitDefender vă permite să alegeți să permiteți sau să blocați execuția acestor elemente.

Având **Controlul scripturilor** activat, veți monitoriza adresele web în care aveți încredere şi pe cele în care nu aveți. BitDefender vă va cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ:

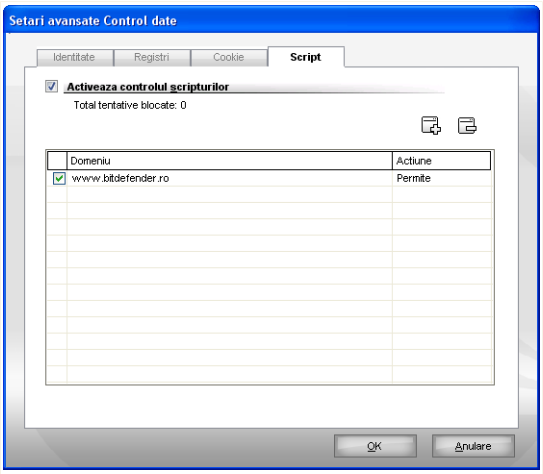
Alertă script

Puteți vedea numele resursei.

Selectați opțiunea **Reține acest răspuns** şi apăsați pe **Da** sau **Nu** şi o regulă va fi creată, aplicată şi afişată în lista de reguli. Nu veți mai fi notificați data viitoare când acelaşi domeniu încearcă să va trimită conținut activ.

Fiecare regulă care a fost creată poate fi accesată în secțiunea **Script** pentru modificări ulterioare. Pentru a accesa această secțiune, deschideți fereastra **Setări avansate Control date** şi apăsați pe tabul **Script**.

Notă
Pentru a deschide fereastra **Setări avansate Control date**, apăsați pe **Control date>Status** în consola de setări şi apoi pe **Setări avansate**.



Control scripturi

Puteți vedea listate în tabel regulile create până în momentul de față.

Important
Regulile sunt listate în ordinea priorității începând de sus, adică prima regulă are cea mai mare prioritate. Mutați regulile în sus sau în jos pentru a le schimba prioritatea.

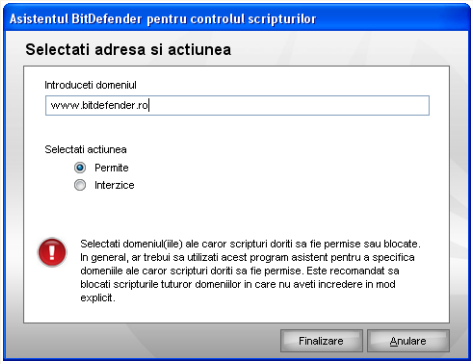
Pentru a şterge o regulă, selectați-o şi apăsați pe butonul **Şterge**. Pentru a modifica parametrii unei reguli, faceți dublu-clic pe câmpul corespunzător şi faceți modificările dorite. Pentru a dezactiva temporar o regulă fără a o şterge, deselectați căsuța corespunzătoare.

Regulile pot fi introduse automat (prin fereastra de alertă) sau manual (apăsați pe butonul **Adaugă** şi selectați parametrii regulei). Va apărea asistentul de configurare.

8.5.1. Asistentul de configurare

Asistentul de configurare este o procedură constituită dintr-un singur pas.

Pasul 1/1 - Selectați adresa şi acțiunea



Selectați adresa şi acțiunea

Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Rularea scripturilor este permisă.
Interzice	Rularea scripturilor este interzisă.

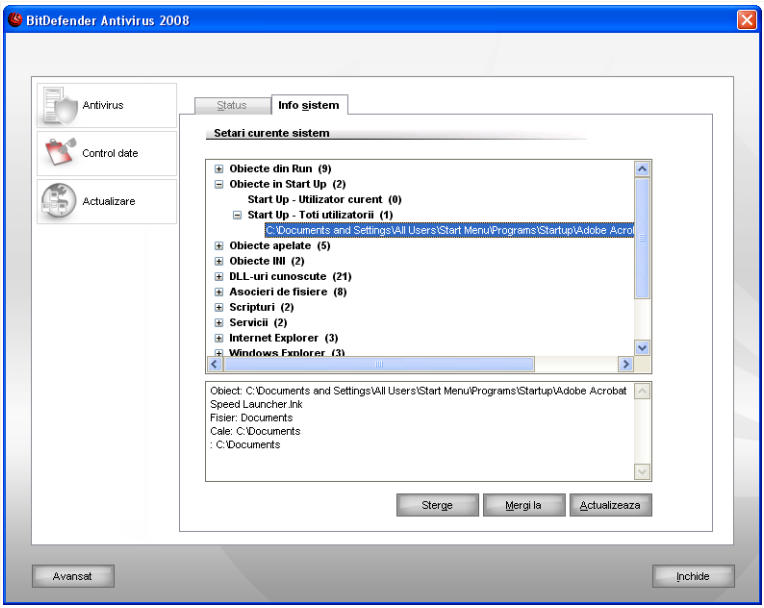
Apăsați pe **Finalizare**.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

8.6. Informații sistem

BitDefender vă permite să vedeți, dintr-un singur loc, toate setările de sistem şi aplicațiile înregistrate să ruleze la pornirea sistemului. Astfel, puteți monitoriza activitatea sistemului şi a aplicațiilor instalate pe acesta şi identifica posibile infecții ale sistemului.

Pentru a obține informații legate de sistem, apăsați pe **Control date>Info sistem** în consola de setări. Va apărea următoarea fereastră:



Informații sistem

Lista conține toate obiectele încărcate la pornirea sistemului precum şi obiectele încărcate de diverse aplicații.

Sunt disponibile trei butoane:

- **Şterge** - şterge obiectul selectat. Trebuie să apăsați pe **Da** pentru a confirma alegerea făcută.

> ***Notă***
> Dacă doriți să nu mai fiți avertizat să confirmați alegerea făcută în timpul sesiunii curente, bifați **Nu mă mai avertiza în sesiunea curentă**.

- **Mergi la** - deschide o fereastră unde obiectul selectat este plasat (de exemplu, **Regiştrii**).
- **Actualizează** - redeschide secțiunea **Info sistem**.

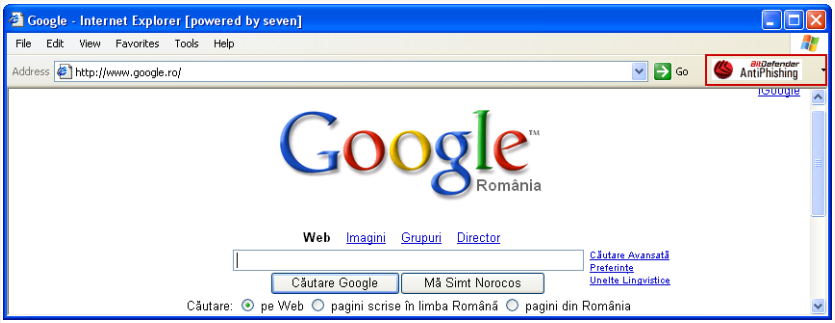
8.7. Bara de comenzi antiphishing

BitDefender vă protejează împotriva tentativelor de phishing atunci când navigați pe Internet. Acesta scanează paginile web accesate şi vă alertează dacă sunt amenințări phishing. O listă albă de pagini web care nu vor fi scanate de BitDefender poate fi configurată.

Puteți gestiona facil şi eficient protecția antiphishing şi lista albă, utilizând bara de comenzi antiphishing a BitDefender integrată în Internet Explorer.

Bara de comenzi antiphishing, reprezentată prin **iconița BitDefender**, este localizată în partea superioară a Internet Explorer. Apăsați pe ea pentru a deschide meniul barei de instrumente.

Notă
Dacă nu puteți vedea bara de instrumente, deschideți meniul **View**, mergeți cu cursorul pe **Toolbars** şi bifați **BitDefender Toolbar**.



Bara de comenzi antiphishing

Următoarele comenzi sunt disponibile pe meniul barei de instrumente:

- **Activează / Dezactivează** - activează / dezactivează bara de comenzi antiphishing a BitDefender.

Notă
Dacă alegeți să dezactivați bara de comenzi antiphishing, nu veți mai fi protejat împotriva tentativelor de phishing.

- **Setări** - deschide o fereastră în care puteți specifica setările barei de comenzi antiphishing.

  Următoarele opțiuni sunt disponibile:
  - **Activează scanarea** - activează scanarea antiphishing.
  - **Întreabă înainte de a adăuga în lista albă** - vă avertizează înainte de a adăuga o pagină web în lista albă.
- **Adaugă la lista albă** - adaugă pagina web curentă în lista albă.

  Notă
  Adăugarea unei pagini web în lista albă înseamnă că BitDefender nu o va mai scana după amenințări phishing. Vă recomandăm să adăugați în lista albă doar paginile web în care aveți deplină încredere.

- **Vizualizează lista albă** - deschide lista albă.

  Puteți vedea lista tuturor paginilor web care nu sunt verificate de motoarele antiphishing ale BitDefender.

  Dacă doriți să ştergeți o pagină web din lista albă, astfel încât să fiți avertizat în legătură cu orice amenințare phishing existentă pe pagina respectivă, apăsați pe butonul **Şterge** corespunzător paginii.

  Puteți adăuga paginile web în care aveți deplină încredere la lista albă pentru a nu mai fi scanate de motoarele antiphishing. Pentru a adăuga o pagină web la lista albă, introduceți adresa acesteia în câmpul corespunzător şi apăsați pe **Adaugă**.
- **Ajutor** - deschide documentația electronică.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender şi unde să apelați pentru ajutor în cazul unei probleme.

9. Actualizare

În fiecare zi sunt descoperite şi identificate noi aplicaţii malițioase. De aceea, este foarte importantă actualizarea BitDefender cu ultimele semnături de aplicaţii malițioase.

Dacă sunteţi conectat la Internet, prin bandă largă sau ADSL, BitDefender se ocupă singur de actualizări. Implicit, BitDefender caută actualizări când deschideţi calculatorul şi apoi la fiecare **oră**.

Dacă o actualizare este disponibilă, în funcţie de opţiunile setate în secţiunea Setări actualizare automată, vi se va cere să confirmaţi actualizarea sau aceasta va fi realizată automat.

Procesul de actualizare este realizat progresiv, ceea ce inseamna ca fisierele care trebuie actualizate sunt inlocuite unul cate unul. Astfel, procesul de actualizare nu va afecta funcţionarea produsului şi, în acelaşi timp, orice vulnerabilitate va fi exclusă.

Actualizările sunt de mai multe tipuri:

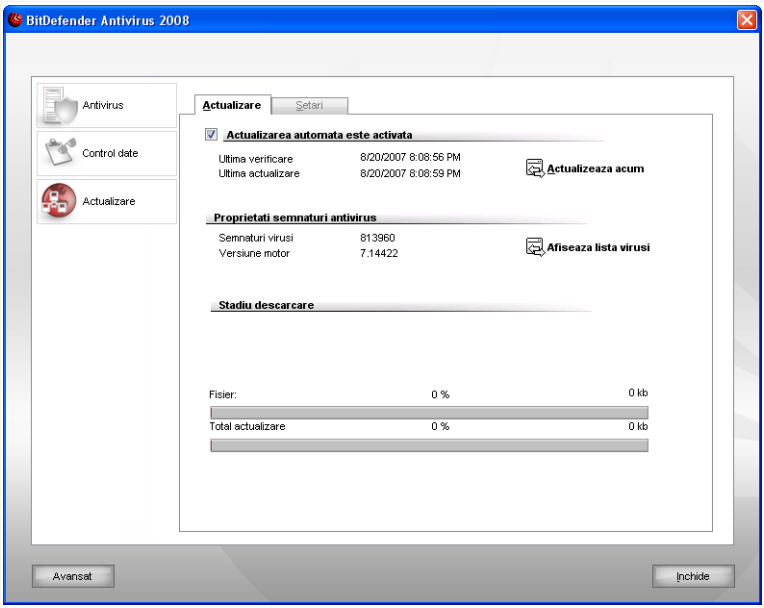
- **Actualizări pentru motoarele Antivirus** - pentru că tot timpul apar noi ameninţări, fişierele ce conţin semnăturile de viruşi trebuie actualizate pentru a asigura protecţie permanentă, la zi, împotriva acestora. Acest tip de actualizare se mai numeşte **Actualizare definiţii viruşi**.
- **Actualizări ale motoarelor Antispam** - se vor adăuga noi reguli filtrelor euristic şi URL şi noi imagini filtrului de imagine. Astfel, eficienţa motorului Antispam va creşte. Acest tip de actualizare se mai numeşte **Actaulizare Antispam**.
- **Actualizări ale motoarelor antispyware** - se vor adăuga noi semnături de spyware la baza de date. Acest tip de actualizare se mai numeşte **Actualizare Antispyware**.
- **Actualizare de produs** - la lansarea unei noi versiuni de produs, noi caracteristici şi tehnici de scanare sunt introduse pentru a îmbunătăţi performanţele produsului. Acest tip de actualizare se mai numeşte **Upgrade Produs**.

Secţiunea **Actualizare** a acestui ghid de utilizare conţine următoarele subiecte:

- Actualizare automată
- Setări actualizare

9.1. Actualizarea Automată

Pentru a vedea informaţii referitoare la actualizare şi iniţia actualizări automate, apăsaţi pe **Actualizare>Actualizare** în consola de setări. Va apărea următoarea fereastră:



Actualizarea Automată

Aici puteți vedea când au fost realizate ultima căutare de actualizări şi ultima actualizare, precum şi informații despre ultima actualizare realizată (dacă a fost reuşită sau dacă au apărut erori). De asemenea, sunt afişate informații despre versiunea curentă a motorului de scanare şi numărul de semnături.

Puteți obține semnăturile aplicațiilor malițioase deținute de produsul dumneavoastră BitDefender apăsând pe **Afişează listă viruşi**. Un fişier HTML care conține toate semnăturile disponibile va fi creat şi deschis într-un browser. Puteți căuta prin baza de date după o anumită semnătură sau puteți face clic pe **Lista de viruşi BitDefender** pentru a accesa baza de semnături online a BitDefender.

Dacă deschideți această secțiune în timpul unei actualizări, puteți vedea stadiul acesteia.

Important
Pentru a fi protejat împotriva celor mai noi amenințări, mențineți **Actualizarea automată** activată.

9.1.1. Cererea unei actualizări

Actualizarea automată poate fi realizată oricând apăsând pe **Actualizează acum**. Acest tip de actualizare este cunoscut şi ca **Actualizare la cererea utilizatorului**.

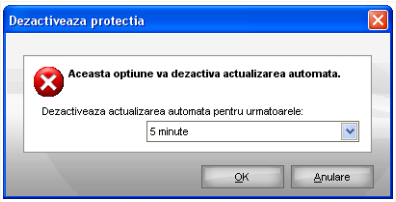
Modulul **Actualizare** se va conecta la serverul de actualizare BitDefender şi va verifica dacă sunt disponibile noi semnături. Dacă sunt detectate noi semnături, în funcție de opțiunile setate în secțiunea Setări actualizare la cerere, vi se va cere să confirmați actualizarea sau aceasta va fi realizată automat.

Important
Poate fi necesar ca după realizarea unei actualizări să reporniți calculatorul. Este recomandat să faceți acest lucru cât mai repede posibil.

Notă
Dacă vă conectați la Internet prin dial-up, este o idee bună să faceți un obicei din a actualiza BitDefender manual.

9.1.2. Dezactivarea actualizării automate

Dacă doriți să dezactivați actualizarea automată, va apărea o fereastră de avertizare.



Dezactivează actualizarea automată

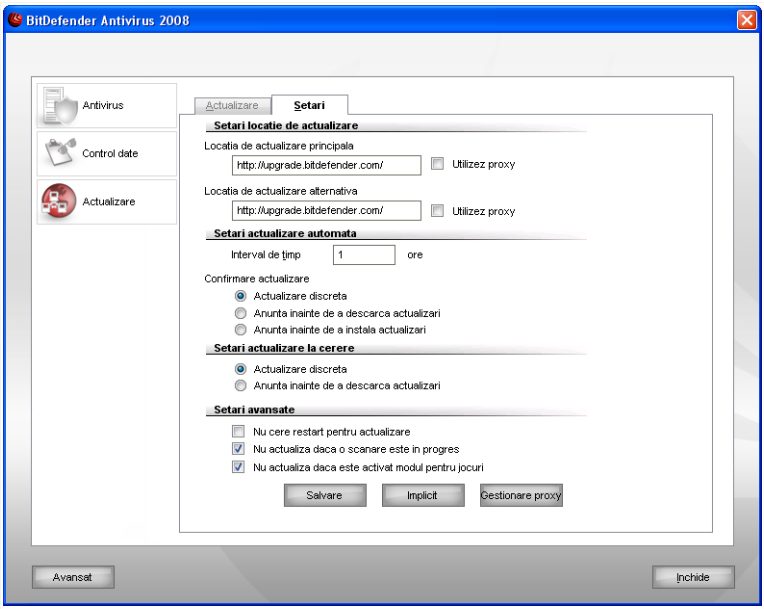
Va trebui să confirmați acțiunea selectând din meniu intervalul de timp pentru care să fie dezactivată actualizarea automată. Puteți dezactiva actualizarea automată pentru 5, 15 sau 30 minute, pentru o oră, permanent sau doar până la repornirea sistemului.

Avertisment
Aceasta este o problemă majoră de securitate. Vă recomandăm să dezactivați actualizarea automată pentru cât mai puțin timp posibil. Dacă nu este actualizat în mod regulat, BitDefender nu va putea să vă protejeze împotriva ultimelor amenințări apărute.

9.2. Setări actualizare

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy. Implicit, BitDefender va căuta actualizări la fiecare oră, pe Internet, şi va instala actualizările disponibile fără a vă mai avertiza.

Pentru a configura setările de actualizare şi a gestiona setările de proxy, apăsați pe **Actualizare>Setări** în consola de setări. Va apărea următoarea fereastră:



Setări actualizare

Setările de actualizare sunt grupate în patru categorii (**Setări locație de actualizare**, **Setări actualizare automată**, **Setări actualizare la cerere** şi **Setări avansate**). Fiecare categorie va fi descrisă separat.

9.2.1. Configurarea locațiilor de actualizare

Pentru a seta locațiile de actualizare, utilizați opțiunile din categoria **Setări locație de actualizare**.

Notă
Configurați aceste setări doar dacă sunteți conectat la o rețea locală care stochează local semnături BitDefender de aplicații malițioase sau dacă vă conectați la Internet printr-un server proxy.

Pentru o actualizare mai sigură şi mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** şi o **Locație de actualizare alternativă**. Implicit, acestea sunt setate la fel: `http://upgrade.bitdefender.com`.

Pentru a modifica una dintre locațiile de actualizare, introduceți adresa URL a serverului local în câmpul **URL** corespunzător locației pe care doriți să o modificați.

Notă
Vă recomandăm să setați ca locație principală de actualizare serverul local şi să lăsați neschimbată adresa locației de actualizare alternative, ca o măsură de siguranță în caz că serverul local devine indisponibil.

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, bifați **Utilizez proxy** şi apoi apăsați pe **Gestionare proxy** pentru a configura setările proxy.

Notă
Pentru mai multe informații, consultați "*Administrarea proxy-urilor*" (p. 100).

9.2.2. Configurarea actualizării automate

Pentru a configura procesul de actualizare realizat automat de BitDefeneder, utilizați opțiunile din categoria **Setări actualizare automată**.

Puteți specifica numărul de ore dintre două căutări consecutive după actualizări în câmpul **Interval de timp**. Implicit, intervalul de timp dintre actualizări este de o oră.

Pentru a specifica modul în care să fie realizată actualizarea automată, selectați una dintre următoarele opțiuni:

- **Actualizare discretă** - BitDefender descarcă şi realizează actualizarea automat.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.

Notă
Veți fi anunțat înainte de a descărca actualizări chiar dacă opriți centrul de securitate.

- **Anunță înainte de a instala actualizări** - de fiecare dată când o actualizare a fost descărcată, veți fi anunțat înainte de a o instala.

Notă
Veți fi anunțat înainte de instalarea actualizărilor chiar dacă opriți centrul de securitate.

9.2.3. Configurarea actualizării manuale

Pentru a specifica cum să fie realizată actualizarea manuală (actualizarea la cererea utilizatorului), selectați una dintre opțiunile din categoria **Setări actualizare manuală**:

- **Actualizare discretă** - actualizarea manuală va fi realizată automat în fundal, fără intervenția utilizatorului.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.

Notă
Veți fi anunțat înainte de a descărca actualizări chiar dacă opriți centrul de securitate.

9.2.4. Configurarea setărilor avansate

Pentru ca procesul de actualizare al BitDefender să nu vă afecteze munca, configurați opțiunile din categoria **Setări avansate**:

- **Nu cere restart pentru actualizare** - Dacă o actualizare necesită repornirea sistemului, produsul işi va continua funcționarea folosind fişierele vechi până când utilizatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului şi astfel actualizarea BitDefender nu va interfera cu activitatea utilizatorului.
- **Nu actualiza dacă o scanare este în progres** - BitDefender nu se va actualiza dacă o scanare este în desfăşurare. Astfel, procesul de actualizare BitDefender nu va interfera cu sarcinile de scanare.

Notă
Dacă BitDefender este actualizat în timpul unei scanări, procesul de scanare va fi anulat.

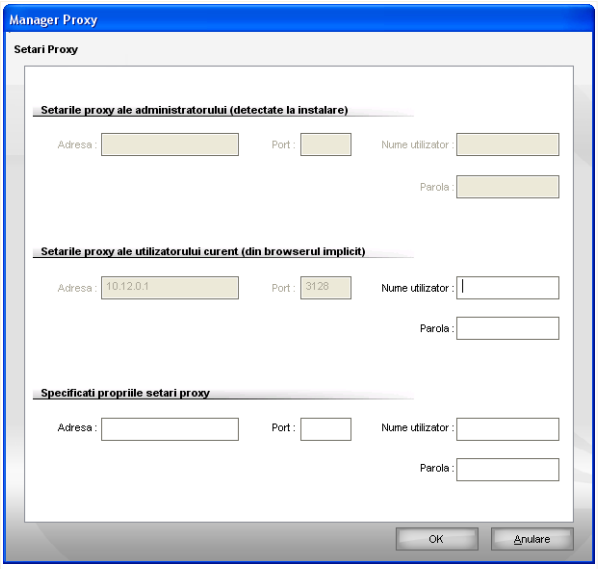
- **Nu actualiza dacă este activat modul pentru jocuri** - BitDefender nu se va actualiza dacă funcționează în modul pentru jocuri. Astfel, puteți minimiza influența produsului asupra performanțelor sistemului în timpul jocului.

9.2.5. Administrarea proxy-urilor

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, trebuie să specificați setările proxy pentru ca BitDefender să se poată actualiza. Altfel, BitDefender va utiliza setările proxy ale administratorului care a instalat produsul sau ale browserului implicit al utilizatorului curent, dacă acestea există.

Notă
Setările proxy pot fi configurate doar de utilizatori cu drepturi administrative pe calculator sau de către utilizatori care cunosc parola produsului.

Pentru a gestiona setările proxy, apăsați pe **Gestionare proxy**. Va apărea o nouă fereastră.



Fereastra de gestionare a setărilor proxy

Există trei seturi de setări proxy:

- **Setările proxy ale administratorului (detectate la instalare)** - setări proxy detectate pe contul administratorului în timpul instalării şi care pot fi configurate doar dacă sunteți logat pe acel cont. Dacă serverul proxy necesită un nume de utilizator şi o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.
- **Setările proxy ale utilizatorului curent (din browserul implicit)** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy necesită un nume de utilizator şi o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.

Notă

Browserele web suportate sunt Internet Explorer, Mozilla Firefox şi Opera. Dacă utilizați un alt browser în mod implicit, BitDefender nu va putea obține setările proxy ale utilizatorului curent.

- **Specificați propriile setări proxy** - setări proxy pe care le puteți configura dacă sunteți logat ca administrator.

  Următoarele setări trebuie specificate:
  - **Adresă** - introduceți adresa IP a serverului proxy.
  - **Port** - introduceți portul folosit BitDefender pentru a se conecta la serverul proxy.
  - **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
  - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.

Atunci când BitDefender va încerca să se conecteze la Internet, va fi încercat pe rând fiecare set de setări proxy, până când se va reuşi conexiunea.

Mai întâi, va fi utilizat setul conținând propriile dumneavoastre setări proxy pentru conectarea la Internet. Dacă acesta nu merge, vor fi încercate în continuare setările proxy detectate la instalare. În sfârşit, dacă nici acestea nu sunt bune, vor fi extrase setările proxy ale utilizatorului curent din browserul implicit şi vor fi folosite pentru conectarea la Internet.

Apăsați pe **OK** pentru a salva modificările şi închide fereastra.

Apăsați pe **Salvare** pentru a salva modificările sau pe **Implicit** pentru a încărca setările standard.

BitDefender Rescue CD

10. Descriere generală

BitDefender Antivirus 2008 este furnizat cu un CD de boot (BitDefender Rescue CD) capabil a scana şi dezinfecta tot calculatorul fără a fi necesară pornirea sistemului de operare.

Este indicat să utilizaţi BitDefender Rescue CD oricând sistemul dumneavoastră de operare nu funcţionează corect din cauza infecţiei cu viruşi. Aceasta se întâmplă în general când nu folosiţi un produs antivirus.

Actualizarea definiţiilor de viruşi se face automat, fără intervenţia utilizatorului de fiecare dată când este pornit BitDefender Rescue CD.

BitDefender Rescue CD este o distribuţie Knoppix adaptată de BitDefender, care integrează cea mai recentă soluţie de securitate BitDefender pentru Linux într-un CD GNU/Linux Knoppix Live, oferind un antivirus pentru desktop care este capabil să scaneze şi să dezinfecteze hard discurile existente (incluzând partiţiile Windows NTFS). De asemenea, BitDefender Rescue CD poate fi utilizat pentru a restaura datele dumneavoastră importante atunci când nu puteţi porni Windowsul.

10.1. Cerinţe de sistem

Înainte de a porni BitDefender Rescue CD, trebuie să vă asiguraţi că sistemul dumneavoastră îndeplineşte următoarele cerinţe.

Tip procesor

Procesor compatibil cu x86, minimum 166 MHz, dar nu aşteptaţi performanţe ridicate în acest caz. Un procesor de generaţie i686, la 800MHz, constituie o alegere mai bună.

Memorie RAM

Minimum 512 MB memorie RAM (1 GB recomandat)

CD-ROM

BitDefender Rescue CD rulează de pe un CD-ROM, de aceea sunt necesare un CD-ROM şi un BIOS capabil să-l pornească.

Conexiune Internet

Deşi BitDefender Rescue CD va rula fără conexiune Internet, procedurile de actualizare vor necesita un link HTTP activ, chiar şi printr-un server proxy. De aceea, pentru o protecţie actualizată, conexiunea Internet este o CERINŢĂ.

Rezoluție grafică
Placă video standard compatibilă SVGA.

10.2. Soft inclus

BitDefender Rescue CD include următoarele pachete soft.

Xedit
Acesta este un editor text de fişiere.

Vim
Acesta este un editor text de fişiere avansat, oferind evidențierea sintaxei, o interfață grafică şi multe altele. Pentru mai multe informații, consultați pagina web a Vim.

Xcalc
Acesta este un calculator.

RoxFiler
RoxFiler este manager de fişiere grafic, rapid şi avansat.

Pentru mai multe informații, consultați pagina web a RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) este un manager de fişiere în mod text.

Pentru mai multe informații, consultați pagina web a MC.

Pstree
Pstree afişează procesele care rulează.

Top
Top afişează sarcinile Linux.

Xkill
Xkill opreşte un program care rulează în X.

Partition Image
Partition Image vă ajută să salvați partiții în format EXT2, Reiserfs, NTFS, HPFS, FAT16 şi FAT32 într-un fişier imagine. Acest program poate fi util în scopuri de backup.

Pentru mai multe informații, consultați pagina web a Partimage.

GtkRecover
GtkRecover este o versiune GTK a programului de recuperare de consolă. Vă ajută să recuperați un fişier.

Pentru mai multe informații, consultați pagina web a GtkRecover.

ChkRootKit

ChkRootKit este un utilitar care vă ajută să vă scanați calculatorul după rootkituri.

Pentru mai multe informații, consultați pagina web a ChkRootKit.

Nessus Network Scanner

Nessus este un scaner de securitate remote pentru Linux, Solaris, FreeBSD şi Mac OS X.

Pentru mai multe informații, consultați pagina web a Nessus.

Iptraf

Iptraf este un soft de monitorizare de rețea.

Pentru mai multe informații, consultați pagina web a Iptraf.

Iftop

Iptraf afişează consumul de lățime de bandă pe o interfață.

Pentru mai multe informații, consultați pagina web a Iftop.

MTR

MTR este un utilitar de analiză de rețea.

Pentru mai multe informații, consultați pagina web a MTR.

PPPStatus

PPPStatus afişează statistici referitoare la traficul TCP/IP la intrare şi la ieşire.

Pentru mai multe informații, consultați pagina web a PPPStatus.

Wavemon

Wavemon este o aplicație de monitorizare a dispozitivelor de rețea wireless.

Pentru mai multe informații, consultați pagina web a Wavemon.

USBView

USBView afişează informații despre dispozitivele conectate la magistrala USB.

Pentru mai multe informații, consultați pagina web a USBView.

Pppconfig

Pppconfig vă ajută să configurați automat o conexiune ppp prin dial-up.

DSL/PPPoe

DSL/PPPoe configurează o conexiune PPPoE (ADSL).

I810rotate

I810rotate activează ieşirea video pe hardware i810 utilizând i810switch(1).

Pentru mai multe informații, consultați pagina web a I810rotate.

Mutt

Mutt este un client de mail MIME avansat, cu interfață text.

Pentru mai multe informații, consultați pagina web a Mutt.

Mozilla Firefox

Mozilla Firefox este un browser web foarte popular.

Pentru mai multe informații, consultați pagina web a Mozilla Firefox.

Elinks

Elinks un browser web în mod text.

Pentru mai multe informații, consultați pagina web a Elinks.

11. Instrucțiuni BitDefender Rescue CD

Acest capitol conține informații despre pornirea şi oprirea BitDefender Rescue CD, scanarea calculatorului dumneavoastră după aplicații malițioase precum şi salvarea datelor de pe un PC cu Windows compromis pe un dispozitiv mobil. Totuşi, utilizând aplicațiile software care sunt oferite pe CD, puteți executa numeroase alte sarcini, descrierea acestora fiind departe de scopul acestui manual de utilizare.

11.1. Pornirea BitDefender Rescue CD

Pentru a porni cd-ul, setați BIOS-ul calculatorului dumneavoastră să demareze de pe cd, aşezați cd-ul în drive şi reporniți calculatorul. Asigurați-vă că poate fi pornit calculatorul dumneavoastră de pe cd.

Aşteptați până apare următorul ecran şi urmați instrucțiunile pentru a porni BitDefender Rescue CD.

Ecran la pornirea sistemului

La pornirea sistemului, se face automat actualizarea semnăturilor de viruşi. Procesul poate lua ceva timp.

La finalizarea procesului de pornire veți vedea următorul desktop. Acum puteți începe să utilizați BitDefender Rescue CD.

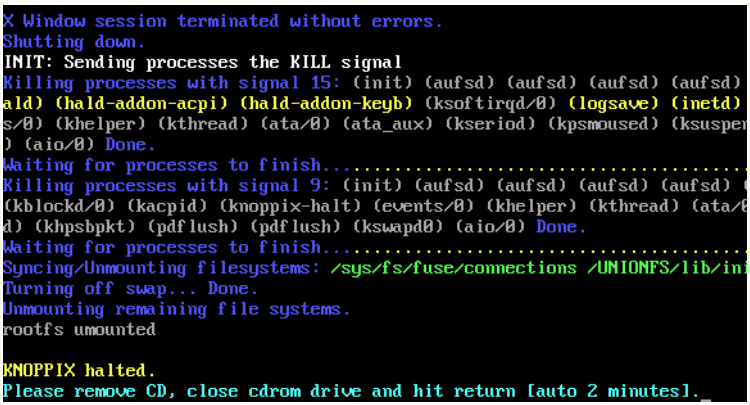
Desktopul

11.2. Oprirea BitDefender Rescue CD

Puteți închide calculatorul fără griji selectând **Închide** din meniul contextual BitDefender Rescue CD (faceți clic-dreapta pentru a-l deschide) sau introducând comanda **halt** într-un terminal.

Alegeți "EXIT"

Atunci când BitDefender Rescue CD a terminat de închis cu succes toate problemele va apărea un ecran ca cel din imagine. Puteți scoate cd-ul pentru a porni sistemul direct de pe hard drive. Acum puteți opri sau reporni calculatorul.



Aşteptați acest mesaj înainte de oprire

11.3. Cum realizez o scanare antivirus?

După ce sistemul a fost pornit, va apărea un program asistent care vă permite să vă scanați complet calculatorul. Trebuie doar să apăsați pe butonul **Start**.

Notă
Dacă rezoluția ecranului nu este suficient de mare, vi se va cere să porniți scanarea în mod text.

Urmați programul asistent în trei paşi pentru a realiza procesul de scanare.

1. Puteți vedea stadiul şi statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse şi altele).

   Notă
   Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

2. Puteți vedea numărul problemelor care vă afectează sistemul.

Problemele sunt afişate pe grupuri. Apăsaţi pe căsuţa cu “+” pentru a deschide un grup sau pe căsuţa cu “-” pentru a închide un grup.

Puteţi alege o acţiune globală care să fie luată asupra fiecărui grup de probleme sau puteţi alege acţiuni separate pentru fiecare problemă în parte.

3. Puteţi vedea un rezumat al rezultatelor.

Dacă doriţi să scanaţi doar un anumit director, procedaţi în felul următor:

Navigaţi printre fişiere, faceţi clic-dreapta pe fişierul sau directorul dorit şi selectaţi **Send to**. Apoi alegeţi **BitDefender Scanner**.

Sau puteţi iniţializa următoarea comandă de la un terminal. **BitDefender Antivirus Scanner** va începe cu fişierul sau directorul selectat ca locaţie implicită de scanare.

```
# bdscan /path/to/scan/
```

11.4. Cum îmi salvez datele?

Să presupunem că nu puteţi porni calculatorul dumneavoastră, cu Windows instalat, din cauza unor probleme necunoscute. În acelaşi timp, trebuie neapărat să accesaţi date importante de pe calculatorul dumneavoastră. Aici este util BitDefender Rescue CD.

Pentru a salva datele dumneavoastră de pe calculator pe un dispozitiv mobil, cum ar fi un stick de memorie USB, urmaţi aceşti paşi:

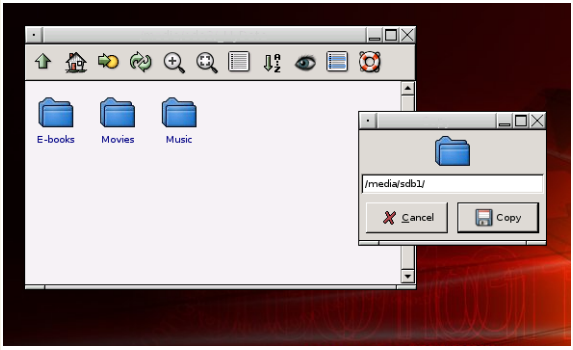
1. Introduceţi CD-ul cu BitDefender Rescue CD în unitatea CD-ROM, stickul de memorie în USB şi apoi reporniţi calculatorul.
2. Aşteptaţi până ce BitDefender Rescue CD porneşte calculatorul. Va apărea următoarea fereastră:

Ecran desktop

3. Faceți dublu-clic pe partiția unde se află datele pe care vreți să le salvați (de exemplu, `[sda3]`).

> ***Notă***
> Atunci când lucrați cu BitDefender Rescue CD, veți avea de-a face cu nume de partiții de tip Linux. Aşadar, `[sda1]` va corespunde probabil partiției `(C:)` din Windows, `[sda3]` partiției `(F:)` şi `[sdb1]` stickului de memorie.

4. Căutați printre directoare şi alegeți-l pe cel dorit. De exemplu, `MyData` care conține subdirectoarele `Movies`, `Music` şi `E-books`.
5. Faceți clic-dreapta pe directorul dorit şi selectați **Copiază**. Va apărea următoarea fereastră.



Salvarea datelor

6. Introduceți `/media/sdb1/` în căsuța de text corespunzătoare şi apăsați pe **Copiază**.

Obținere ajutor

12. Suport

BitDefender se străduieşte să ofere clienţilor săi un nivel cât mai ridicat în ceea ce priveşte rapiditatea şi calitatea suportului tehnic. Centrul de suport (cu care puteţi lua legătura prin adresa indicată mai jos) este actualizat continuu. Aici vă sunt oferite răspunsurile la întrebările dumneavoastră în cel mai scurt timp.

La BitDefender, preocuparea pentru economisirea timpului şi banilor clienţilor prin oferirea celor mai avansate produse la preţuri rezonabile a fost dintotdeauna o prioritate. Mai mult, considerăm că o afacere de succes se bazează pe o bună comunicare şi dedicare în suportul acordat clienţilor.

Sunteţi binevenit oricând să cereţi ajutor la suport@bitdefender.ro. Pentru un răspuns prompt, includeţi în e-mail cât mai multe detalii despre produsul BitDefender pe care-l deţineţi, despre sistemul dumneavoastră şi descrieţi cât mai exact problema.

12.1. BitDefender Knowledge Base

BitDefender Knowledge Base este o bază online de informaţii despre produsele BitDefender. Stochează, într-un format accesibil, rapoarte ale echipelor de suport şi dezvoltare cu privire la rezultatele suportului tehnic continuu şi ale activităţilor de eliminare a bug-urilor BitDefender împreună cu articole mai generale despre prevenţia viruşilor, administrarea soluţiilor BitDefender şi explicaţii detaliate, şi multe alte articole.

BitDefender Knowledge Base este pusă la dispoziţia publicului. Această multitudine de informaţii reprezintă încă o cale de a oferi clienţilor BitDefender asistenţa tehnică de care au nevoie. Toate cererile valide de informaţii sau rapoarte despre bug-uri venind de la clienţii BitDefender ajung în cele din urmă în BitDefender Knowledge Base, ca rapoarte asupra eliminării bug-urilor, fişe de lucru sau articole informative pentru a suplimenta fişierele de suport ale produsului.

BitDefender Knowledge Base este disponibilă oricând la adresa http://kb.bitdefender.com.

12.2. Solicitarea ajutorului

12.2.1. Mergeţi la serviciul Web Self

Aveţi o întrebare? Experţii noştri în securitate vă stau la dispoziţie non-stop, oferindu-vă ajutor gratuit prin telefon, email sau chat.

Utilizați linkurile de mai jos:

Engleză

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

Germană

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

Franceză

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

Română

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

Spaniolă

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

12.2.2. Deschideți o cerere de ajutor

Dacă doriți să faceți o cerere de ajutor şi să primiți ajutor prin email, utilizați unul dintre linkurile următoare:

Engleză: http://www.bitdefender.com/site/Main/contact/1/
Germană: http://www.bitdefender.de/site/Main/contact/1/
Franceză: http://www.bitdefender.fr/site/Main/contact/1/
Română: http://www.bitdefender.ro/site/Main/contact/1/
Spaniolă: http://www.bitdefender.es/site/Main/contact/1/

12.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câştigat o reputație indisputabilă în depăşirea aşteptărilor clienților şi partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

12.3.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Suport tehnic: suport@bitdefender.ro
Documentație: documentation@bitdefender.com
Programe de Parteneriat: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Relații Media: pr@bitdefender.com
Cariere: jobs@bitdefender.com
Subscrieri viruşi: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Site produs: http://www.bitdefender.ro
Arhive ftp ale produsului: ftp://ftp.bitdefender.com/pub
Distribuitori locali: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

12.3.2. Filiale

Sucursalele BitDefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce priveşte problemele comerciale cât şi pe cele generale. Adresele lor precum şi modul în care pot fi contactate sunt date mai jos.

Germany

BitDefender GmbH
Sediul pentru Europa de Vest
Karlsdorferstrasse 56
88069 Tettnang
Germany
Tel: +49 7542 9444 60
Fax: +49 7542 9444 99
Email: info@bitdefender.com
Vânzări: sales@bitdefender.ro
Pagină web: http://www.bitdefender.com
Suport tehnic: support@bitdefender.com

Marea Britanie şi Irlanda

One Victoria Square
Birmingham

B1 1BD
Telefon: +44 207 153 9959
Fax: +44 845 130 5069
Email: info@bitdefender.com
Vânzări: sales@bitdefender.ro
Pagină web: http://www.bitdefender.co.uk
Suport tehnic: suport@bitdefender.ro

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender-es.com
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Suport tehnic: suport@bitdefender.ro
Servicii clienți: 954-776-6262
Pagină web: http://www.bitdefender.com

Romania

BITDEFENDER
Str. Fabrica de Glucoză nr. 5
Bucureşti
Suport tehnic: suport@bitdefender.ro
Vânzări: sales@bitdefender.ro
Telefon: +40 21 4085600
Fax: +40 21 2330763
Site produs: http://www.bitdefender.ro

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe şi sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca nişte aplicaţii şi nu ca nişte simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane şi să interacţioneze şi în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securităţii; experţii în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Adware

Aplicaţia adware este adesea combinată cu o aplicaţie gazdă care este oferită gratuit dacă utilizatorul acceptă aplicaţia adware. Deoarece aplicaţiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licenţiere care explică scopul aplicaţiei, nu este comisă nicio infracţiune.

Totuşi, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanţele sistemului. De asemenea, informaţiile pe care unele dintre aceste aplicaţii le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licenţiere.

Arhivă

Un disc, o casetă sau un director care conţine fişiere de rezervă.

Un fişier care conţine unul sau mai multe fişiere într-un format comprimat.

Backdoor

Reprezintă o gaură de securitate realizată în mod deliberat. Motivaţia acestor "găuri" nu este întotdeauna maliţioasă: unele sisteme de operare, de exemplu, sunt puse în circulaţie cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanţă produsului din partea vânzătorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului şi altele). În cazul discurilor de startup, sectorul de boot conţine un program care încarcă sistemul de operare.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus

de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza şi încărca pagini de Web. Două din cele mai populare browsere sunt Mozilla Firefox şi Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afişa atât grafice cât şi text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet şi animație.

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Cookie

Un cookie reprezintă un set de date pe care un server Web îl transmite către un browser atunci când utilizatorul vizitează prima oară site-ul şi care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca şi browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fişier text în directoarele de sistem ale browserelor Netscape şi Explorer;nu toate browserele suportă cookie. Fişierele cookie stochează informații cum ar fi numele utilizatorului şi parola, cât şi ce părți din site au fost vizitate. Browserul împarte fiecare cookie doar cu server-ul care l-a generat, celelalte servere le pot citi doar pe cele generate de ele. Unele fişiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi şterse automat după o anumită perioadă de timp.

Drive de disc

Este un dispozitiv care citeşte date de pe un disc şi scrie date pe un disc.

Un drive de hard disc citeşte / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

Download

Reprezintă copierea (de obicei a unui întreg fişier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fişier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi şi la copierea unui fişier de pe un server de rețea pe un calculator din rețea.

E-mail

Se referă la poşta electronică. Acesta este un serviciu care transmite mesaje prin intermediul reţelei locale sau globale.

Evenimente

O acţiune sau întâmplare detectată de un program. Evenimentele pot fi acţiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Fals pozitiv

Apare atunci când un analizator detectează un fişier ca fiind infectat când de fapt acesta nu este infectat.

Extensie de fişier

Reprezintă porţiunea dintr-un nume de fişier ce urmează după caracterul punct, şi care indică tipul de date pe care le stochează fişierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fişiere. De obicei aceasta este formată din una până la trei caractere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "txt" pentru fişierele text oarecare, "c" pentru fişierele sursă scrise în limbajul C, etc.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruşi noi. Această metodă de scanare nu se bazează pe semnături de viruşi cunoscuţi. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuşi ocazional poate raporta un cod suspicios în programe normale, generând aşa-numitul "fals pozitiv".

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât şi reasamblarea pachetelor IP.

Applet-uri Java

Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului şi mărimea acestuia. Când este accesată o pagină web, browser-ul descarcă applet-ul de pe un server şi îl rulează pe maşina utilizatorului (clientul). Applet-urile diferă de aplicaţii prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deşi pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricţionate de domeniul de care aparţin în ceea ce priveşte scrierea şi citirea datelor.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word şi Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente şi execută aceste macro-uri de fiecare dată când este deschis documentul.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți şi să recepționați mesaje.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri şi pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături specifice de viruşi. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus şi din acest motiv nu generează fals pozitiv.

Programe împachetate

Reprezintă un fişier în format comprimat. Multe din sistemele de operare şi aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fişier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fişier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuşi, un program care împachetează fişiere va înlocui caracterele de spațiu printr-un caracter reprezentând spațiu, urmat de un număr care reprezintă numărul de spații care este înlocuit. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Cale

Reprezintă direcția exactă către un fişier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fişierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole şi numere de card de credit, de asigurări sociale şi de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals şi folosit pentru a fura informațiile despre utilizator.

Virus polimorf

Reprezintă un virus care îşi schimbă forma cu fiecare fişier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruşi sunt greu de identificat.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor şi tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului şi a altor dispozitive periferice.

În rețelele TCP / IP şi UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Fişier de raport

Reprezintă un fişier care listează acțiunile care au avut loc. BitDefender menține un fişier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fişierelor, numărul de arhive şi fişiere scanate, câte fişiere infectate şi suspecte au fost găsite.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX şi se referea la unelte recompilate ce furnizau intruşilor drepturi administrative, permițându-le să îşi ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fişiere, loginuri şi jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele şi chiar unele aplicații ascunde fişiere critice utilizând rootkituri. Totuşi, ele sunt folosite în general

pentru a ascunde aplicații malițioase sau prezența intruşilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea şi integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fişiere şi jurnale şi evita detecția.

Script

Un alt termen pentru fişiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Spam

Termen ce acoperă întreagă gamă a mesajelor electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără ştirea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuşi, trebuie ştiut că majoritatea aplicațiilor de tip shareware şi freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet şi transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail şi chiar parole şi numere de carduri de credit.

Asemănarea dintre spyware şi un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obişnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fişiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică şi intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât şi a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie şi resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente din startup

Orice fişier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, şi nu direct fişierul.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în taskbar-ul de Windows (situat lângă ceas) şi conține iconițe pentru accesul rapid la aplicații sistem cum ar fi cele legate de fax, imprimantă, modem, volum,

şi altele. Executați dublu-clic cu mouse-ul pe o iconiță pentru a vizualiza şi accesa elementele.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet şi care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware şi sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât şi convenții folosite în conectarea rețelelor şi rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruşi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină viruşii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruşi pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă duşmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul oraşului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraş şi să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiaşi produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

BitDefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără ştirea dumneavoastră şi rulează independent de voința dumneavoastră. Cea mai mare parte a viruşilor se pot şi înmulți. Toți viruşii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar şi un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus şi mai periculos este acela care este capabil să se răspândească în rețea şi poate să treacă de sistemele de securitate.

Semnătură de virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția şi eliminarea virusului.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândeşte. Nu se poate ataşa la alte programe.