

HANDLEIDING

KASPERSKY
INTERNET
SECURITY 2009

Beste gebruiker van Kaspersky Internet Security 2009!

Dank u dat u voor ons product hebt gekozen. We hopen dat deze documentatie u bij uw werk zal helpen en vragen over dit softwareproduct zal beantwoorden.

Belangrijk! Dit document is eigendom van Kaspersky Lab en alle rechten op dit document zijn voorbehouden door de copyrightwetten van de Russische Federatie en internationale verdragen. Onrechtmatige verveelvoudiging en distributie van dit document of delen daarvan resulteren in civiele, administratieve en strafrechtelijke aansprakelijkheid volgens de wetten van de Russische Federatie. Verveelvoudiging en distributie van materialen, inclusief hun vertaling, is alleen toegestaan met schriftelijke toestemming van Kaspersky Lab. Dit document en verwante grafische afbeeldingen mogen uitsluitend voor informatieve, niet-commerciële of persoonlijke doeleinden worden gebruikt.

Dit document mag niet gewijzigd worden zonder voorafgaande kennisgeving. De recentste versie van dit document vindt u op de Kaspersky Lab-website: <http://www.kaspersky.com/docs>. Kaspersky Lab aanvaardt geen enkele aansprakelijkheid voor de inhoud, kwaliteit, relevantie of accuratesse van de materialen die in dit document gebruikt worden en waarvoor de rechten voorbehouden zijn aan derden, en voor de mogelijke schade die met het gebruik van dergelijke documenten in verband gebracht wordt.

Dit document bevat gedeponeerde en niet-gedeponeerde handelsmerken. Alle genoemde handelsmerken zijn het eigendom van hun respectieve eigenaars.

© Kaspersky Lab, 1996-2008

+7 (495) 645-7939,
Tel., fax: +7 (495) 797-8700,
+7 (495) 956-7000

<http://www.kaspersky.com/>
<http://support.kaspersky.com/>

Revisiedatum 4 april 2008

INHOUDSOPGAVE

INLEIDING.....	ERROR! BOOKMARK NOT DEFINED.
Informatie over het programma opvragen.....	6
Informatiebronnen voor eigen research.....	6
Contact opnemen met de verkoopafdeling.....	7
Contact opnemen met de technische support.....	7
Kaspersky Lab-programma's bespreken op het webforum.....	9
Wat is er nieuw in Kaspersky Internet Security 2009.....	9
Beschermingsfacetten van het programma.....	11
Wizards en tools.....	12
Ondersteuningsfuncties.....	13
Heuristische analyse.....	14
Vereisten voor hardware en software.....	15
BEDREIGINGEN VOOR COMPUTERVEILIGHEID.....	17
Bedreigingen: programma's.....	17
Kwaadaardige programma's.....	18
Virussen en wormen.....	18
Trojan programma's.....	22
Kwaadaardige programma's.....	29
Potentieel ongewenste programma's.....	32
Adware.....	33
Pornware.....	33
Andere riskwareprogramma's.....	34
Methoden voor het detecteren van geïnfecteerde, verdachte en potentieel gevaarlijke objecten.....	38
Internetbedreigingen.....	39
Spam of ongevraagde binnenkomende e-mail.....	39
Phishing.....	40
Hackeraanvallen.....	40
Weergave van banners.....	41
HET PROGRAMMA OP DE COMPUTER INSTALLEREN.....	42
Stap 1. Verifiëren of het systeem voldoet aan de installatievereisten.....	43

Stap 2. Naar een nieuwere versie van het programma zoeken	44
Stap 3. Begroetingsvenster van de wizard.....	44
Stap 4. De licentieovereenkomst bekijken	45
Stap 5. Het installatietype selecteren.....	45
Stap 6. De installatiemap selecteren.....	46
Stap 7. Te installeren programmacomponenten selecteren.....	46
Stap 8. Naar andere antivirussoftware zoeken	47
Stap 9. Laatste voorbereiding op de installatie	48
Stap 10. De installatie voltooiën.....	49
PROGRAMMA-INTERFACE	50
Systeemvakpictogram.....	50
Contextmenu.....	51
Hoofdvenster van het programma.....	53
Meldingen	56
Venster voor het configureren van programma-instellingen.....	56
AAN DE SLAG.....	58
Een netwerktype selecteren.....	59
Het programma updaten	60
Beveiligingsanalyse	60
Uw computer scannen op virussen	61
Deelname aan het Kaspersky Security Network.....	62
Beveiligingsbeheer.....	63
Bescherming pauzeren	65
PROGRAMMA-INSTELLINGEN VALIDEREN	67
Het EICAR-testvirus en variaties ervan.....	67
De bescherming van HTTP-verkeer testen.....	71
De bescherming van SMTP-verkeer testen	72
Instellingen van Anti-Virus voor bestanden valideren	73
Instellingen voor virusscantaken valideren	73
Anti-Spam-instellingen valideren.....	74

VERKLARING VOOR GEGEVENSVERZAMELING VAN KASPERSKY SECURITY NETWORK	75
KASPERSKY LAB	82
Andere producten van Kaspersky Lab	83
Contact opnemen.....	94
CRYPTOEX LLC	96
MOZILLA FOUNDATION.....	97
LICENTIEOVEREENKOMST	98

INLEIDING

IN DEZE SECTIE:

Informatie over het programma opvragen	6
Wat is er nieuw in Kaspersky Internet Security 2009.....	9
Beschermingsfacetten van het programma	11
Vereisten voor hardware en software	15

INFORMATIE OVER HET PROGRAMMA OPVRAGEN

U kunt snel antwoord krijgen op vragen over het kopen, installeren of gebruiken van het programma.

Kaspersky Lab heeft allerlei informatiebronnen. Selecteer eenvoudig de bron die u het beste uitkomt, al naar gelang hoe dringend en belangrijk uw vraag is.

INFORMATIEBRONNEN VOOR EIGEN RESEARCH

U kunt het **Help**-systeem gebruiken.

Het Help-systeem bevat informatie over het beheren van computerbescherming: bekijk de beveiligingsstatus, scan verschillende gebieden van de computer en voer andere taken uit.

Klik op de koppeling **Help** in het hoofdvenster van het programma of druk op **<F1>**.

CONTACT OPNEMEN MET DE VERKOOPAFDELING

Met vragen over het selecteren of kopen van het programma of het verlengen van uw gebruiksrecht kunt u terecht bij de specialisten van de verkoopafdeling.

U kunt uw vragen voor de verkoopafdeling naar het volgende e-mailadres sturen: sales@kaspersky.nl.

CONTACT OPNEMEN MET DE TECHNISCHE SUPPORT

Als u het programma al hebt gekocht, kunt u telefonisch of via internet informatie over het programma opvragen bij de technische support.

De specialisten hier beantwoorden vragen over de installatie en het gebruik van het programma, en als uw computer geïnfecteerd is, helpen zij u de gevolgen van malware-activiteiten te elimineren.

Telefonische technische ondersteuning

Als u een probleem hebt waarvoor u dringend hulp nodig hebt, kunt u de technische support bellen op een van de volgende nummers:

Nederland 0900-5284357

België 0902-29005

Onze medewerkers zijn bereikbaar van maandag t/m vrijdag van 09:00 tot 22:00 uur. Kaspersky Lab-gebruikers kunnen rond de klok aanspraak maken op technische ondersteuning in het Russisch of Engels op de volgende nummers:

+7 (495) 797-87-07, +7 (495) 645-79-29 of +7 (495) 956-87-08.

Zij zijn bereikbaar van maandag t/m vrijdag van 10:00 tot 18:30 uur Moskouse tijd (GMT +3). U dient de medewerker van de technische support de activeringscode van het programma of het licentienummer uit het licentiebestand doorgeven.

Raadpleging van de technische ondersteuning via e-mail (alleen voor geregistreerde gebruikers)

U kunt uw vraag naar de specialisten van de technische ondersteuning sturen door een helpdeskwebformulier in te vullen op de technische-ondersteuningswebsite van Kaspersky Lab
<http://support.kaspersky.com/helpdesk.html>.

U kunt vragen stellen in het Russisch, Engels, Duits, Frans of Spaans.

In het e-mailbericht met uw vraag moet u het **klantnummer** vermelden dat u tijdens registratie op de technische-ondersteuningswebsite hebt verkregen, samen met uw **wachtwoord**.

Opmerking

Als u nog niet bent geregistreerd als gebruiker van Kaspersky Lab-programma's, kunt u een registratieformulier invullen op
<https://support.kaspersky.com/nl/PersonalCabinet/Registration/Form/>.

Tijdens de registratie moet u de activeringscode opgeven, of het licentie-nummer (dit nummer maakt deel uit van de naam van het licentiebestand).

Het antwoord op uw vraag wordt verstuurd naar het e-mailadres dat u bij uw vraag hebt opgegeven en naar uw **Persoonlijk Dossier** –
<https://support.kaspersky.com/nl/PersonalCabinet>.

Omschrijf uw probleem zo uitgebreid mogelijk in het webformulier. Geef de volgende informatie op in de verplichte velden:

- **Onderwerp.** De meest gestelde vragen zijn gecategoriseerd op onderwerp, bijvoorbeeld 'Installatie/Verwijderen van het programma' of 'Verwijderen van virussen'. Als u geen toepasselijk onderwerp kunt vinden, selecteert u 'Algemene vraag'.
- **Kaspersky Lab product.**
- **Vraag.** Beschrijf uw probleem zo gedetailleerd mogelijk.
- **Klantnummer en wachtwoord.** Geef het klantnummer en wachtwoord op die u tijdens registratie op de website voor technische ondersteuning zijn toegewezen.
- **E-mailadres.** Geef het e-mailadres op waarnaar de specialisten van de technische support het antwoord op uw vraag moeten sturen.

KASPERSKY LAB-PROGRAMMA'S BESPREKEN OP HET WEBFORUM

Niet-dringende kwesties kunt u bespreken met de Kaspersky Lab-specialisten en andere gebruikers van Kaspersky Lab's antivirusprogramma's op ons webforum op <http://www.kaspersky.nl/forum/>.

Op dit forum kunt u eerder gepubliceerde onderwerpen bekijken, commentaar leveren, nieuwe onderwerpen maken en het zoekprogramma gebruiken.

WAT IS ER NIEUW IN KASPERSKY INTERNET SECURITY 2009

Kaspersky Internet Security 2009 pakt gegevensbeveiliging anders aan. De hoofdfunctie van het programma is de toegangsrechten van het programma tot de systeembronnen te beperken. Zo worden ongewenste acties van verdachte en gevaarlijke programma's voorkomen. De beveiligingsmogelijkheden van het programma voor de vertrouwelijke gegevens van de gebruiker zijn aanzienlijk verbeterd. Het programma bevat nu wizards en tools die de uitvoering van specifieke computerbeveiligingstaken aanzienlijk vereenvoudigen.

Laten we de nieuwe functies van Kaspersky Internet Security 2009 eens nader bekijken:

Nieuwe beveiligingsfuncties

- Kaspersky Internet Security omvat nu de component Application Filtering, evenals Proactive Defense en Firewall, waarmee systeembeveiliging tegen bedreigingen, waaronder bestaande en momenteel onbekende bedreigingen, op een nieuwe, universele manier wordt aangepakt. Kaspersky Internet Security vereist nu aanzienlijk minder gebruikersinvoer dankzij het gebruik van lijsten met vertrouwde programma's ('witte lijst').
- Dankzij het scannen naar en de eliminatie van kwetsbaarheden in besturingssysteem en software wordt een hoog systeembeveiligingsniveau gehandhaafd en wordt voorkomen dat gevaarlijke programma's uw systeem binnendringen.

- Nieuwe wizards Beveiligingsanalyse en Browserconfiguratie vereenvoudigen het scannen naar en de eliminatie van beveiligingsbedreigingen en kwetsbaarheden in de programma's die op uw computer zijn geïnstalleerd, en in de instellingen van het besturingsstelsel en de browser.
- Kaspersky Lab reageert nu sneller op nieuwe bedreigingen dankzij het gebruik van Kaspersky Security Network-technologie, die gegevens verzamelt over de infectie van computers van gebruikers en deze naar de servers van Kaspersky Lab verstuurt.
- Nieuwe gereedschappen (Netwerkbeheer en Netwerkpakketanalyse) vergemakkelijken de verzameling en analyse van informatie over netwerkactiviteiten op uw computer.
- Nieuwe wizard Systeemherstel helpt schade aan het stelsel na malware-aanvallen te verhelpen.

Nieuwe functies voor bescherming van vertrouwelijke gegevens:

- De nieuwe component Programma filteren bewaakt op effectieve wijze de programmatoegang van vertrouwelijke gegevens en de bestanden en mappen van gebruikers.
- Bescherming van vertrouwelijke gegevens die via het toetsenbord worden ingevoerd, wordt verzekerd door de nieuwe tool Virtueel toetsenbord.
- De structuur van Kaspersky Internet Security bevat de wizard voor privacy opschonen, waarmee alle informatie over de acties van een gebruiker die van interesse voor een inbreker kan zijn (lijst met bezochte websites, geopende bestanden, cookies enzovoort), van zijn of haar computer wordt verwijderd.

Nieuwe antispam-functies:

- Efficiëntie van spamfilter door de component Anti-Spam is verbeterd dankzij het gebruik van Recent Terms-servertechnologieën.
- Het gebruik van extensie-plugins voor Microsoft Office Outlook, Microsoft Outlook Express, The Bat! en Thunderbird vereenvoudigt de configuratie van de antispam-instellingen.
- De herziene component Ouderlijk toezicht zorgt voor effectieve beperking van ongewenste toegang tot bepaalde internetbronnen door kinderen.

Nieuwe beveiligingsfuncties voor internetgebruik:

- Beveiliging tegen internetindringers is opgewaardeerd dankzij de uitgebreide databases van phishing-sites.
- Functie voor het scannen van ICQ- en MSN-verkeer is toegevoegd, zodat internetpaggers veilig kunnen worden gebruikt.
- Veilig gebruik van draadloze netwerken wordt gewaarborgd dankzij het scannen van Wi-Fi-verbindingen.

Nieuwe interfacefuncties van programma

- De nieuwe interface van het programma weerspiegelt de brede aanpak van informatiebescherming.
- De dialoogvensters bevatten veel informatie, zodat de gebruiker snel beslissingen kan nemen.
- De functionaliteit van rapport- en statistiek informatie over de werking van het programma is uitgebreid. Het gebruik van filters bij het werken met rapporten biedt een flexibele set-up, wat dit product onmisbaar maakt voor professionals.

BESCHERMINGSFACETTEN VAN HET PROGRAMMA

Kaspersky Internet Security beschermt uw computer tegen bekende en nieuwe bedreigingen, hacker- en inbrekersaanvallen, spam en andere ongewenste gegevens. Elk type bedreiging wordt door een afzonderlijke programma-component verwerkt. Dit maakt het systeem flexibel, met eenvoudige configuratieopties voor alle componenten zodat deze aan de behoeften van de gebruiker of het hele bedrijf kunnen worden aangepast.

Kaspersky Internet Security bevat:

- Controle van programma-activiteiten in het systeem, zodat wordt voorkomen dat programma's gevaarlijke acties uitvoeren.
- Malwarebeveiligingscomponenten voor realtimebeveiliging van alle gegevensoverdrachten en toegangswegen tot uw computer.
- Beveiligingscomponenten voor internetgebruik, zodat uw computer beschermd wordt tegen netwerk- en inbrekersaanvallen die op dit moment bekend zijn.

- Het filteren van ongewenste gegevens bespaart tijd, webverkeer en geld.
- Virusscantaken waarmee u afzonderlijke bestanden, mappen, schijfstations of regio's kunt scannen op virussen, of een volledige computerscan kunt uitvoeren. Scantaken kunnen worden geconfigureerd om kwetsbaarheden te detecteren in de programma's die op de computer zijn geïnstalleerd.
- Updates die de status van interne programmamodules bieden, en ook gebruikt worden voor bedreigingsscans, en detectie van hacker-aanvallen en spamberichten.
- Wizards en tools waarmee u gemakkelijker taken kunt uitvoeren in Kaspersky Internet Security.
- Ondersteuningsfuncties die informatie bieden over het programma en de mogelijkheden ervan uitbreiden.

WIZARDS EN TOOLS

Het verzekeren van computerbeveiliging is een moeilijke taak waarvoor kennis vereist is over de functies van het besturingssysteem, en de methoden die gebruikt worden om zwakke plekken uit te buiten. Bovendien maakt de grote hoeveelheid en verscheidenheid aan informatie over de systeembeveiliging de analyse en verwerking moeilijker.

Kaspersky Internet Security heeft een aantal wizards en tools waarmee specifieke computerbeveiligingstaken gemakkelijker kunnen worden uitgevoerd:

- De wizard Beveiligingsanalyse voert een computerdiagnose uit en zoekt naar kwetsbaarheden in het besturingssysteem en programma's die op de computer zijn geïnstalleerd.
- De wizard Browserconfiguratie analyseert de browserinstellingen van Microsoft Internet Explorer en beoordeelt ze voornamelijk vanuit een beveiligingsoogpunt.
- De wizard Systeemherstel wordt gebruikt om sporen van de malwareobjecten in het systeem te elimineren.
- De wizard voor het opschonen van privacy zoekt naar en elimineert sporen van gebruikersactiviteiten op het systeem en in de instellingen van het besturingssysteem, die kunnen worden gebruikt om informatie over de activiteiten van de gebruiker te verzamelen.

- De herstelschijf is ontworpen om de systeemfunctionaliteit te herstellen na een virusaanval die systeembestanden heeft beschadigd, waardoor u het besturingssysteem niet meer kunt opstarten.
- Netwerkpakketanalyse onderschept netwerkpakketten en geeft hun details weer.
- Network Monitor geeft details over de netwerkactiviteiten op uw computer weer.
- Met het virtuele toetsenbord kunt u verhinderen dat ingetoetste gegevens worden onderschept.

ONDERSTEUNINGSFUNCTIES

Het programma bevat een aantal ondersteuningsfuncties. Ze zijn ontworpen om het programma up-to-date te houden, de mogelijkheden van het programma uit te breiden en om u te helpen bij het gebruik ervan.

Kaspersky Security Network

Kaspersky Security Network – een systeem dat automatische overdracht biedt van rapporten over gedetecteerde en potentiële bedreigingen in de gecentraliseerde database. Deze database verzekert een nog snellere reactie op de meest voorkomende bedreigingen, en stelt gebruikers op de hoogte van virusuitbraken.

Licentie

Wanneer u Kaspersky Internet Security aanschaft, gaat u een licentieovereenkomst aan met Kaspersky Lab die bepaalt hoe u het programma kunt gebruiken, welke toegang u hebt tot de updates van de programma-database en tot de technische ondersteuning gedurende een bepaalde periode. De gebruiksvoorwaarden en andere informatie die noodzakelijk is om alle functies van het programma te kunnen gebruiken, zijn opgenomen in een sleutelbestand.

Met de functie **Licentie** kunt u details oproepen van de licentie die u gebruikt, een nieuwe licentie kopen of uw huidige licentie verlengen.

Ondersteuning

Alle geregistreerde gebruikers van Kaspersky Internet Security kunnen gebruikmaken van onze technische support. Om te weten te komen waar u

precies deze technische ondersteuning kunt verkrijgen, raadpleegt u de functie Ondersteuning.

Via de overeenkomstige links krijgt u toegang tot het gebruikersforum van Kaspersky Lab, kunt u een foutrapport naar de technische support sturen, of kunt u programmafeedback via een speciaal onlineformulier sturen.

U hebt ook toegang tot de online technische support, uw Persoonlijk Dossier en onze werknemers staan uiteraard altijd klaar om u per telefoon te helpen bij het gebruik van Kaspersky Internet Security.

HEURISTISCHE ANALYSE

Heuristiek wordt gebruikt in sommige componenten voor real-time bescherming, zoals Anti-Virus voor bestanden, Anti-Virus voor e-mail en Anti-Virus voor internet, en in virusscans.

U kunt een scan uitvoeren met de handtekeningmethode op basis van een vooraf gemaakte database die een beschrijving van bekende bedreigingen bevat, evenals methoden om deze te behandelen. In dat geval krijgt u een duidelijk antwoord of een gescand object schadelijk is en tot welk type dreiging het behoort. Met de heuristische methode worden geen handtekeningen van schadelijke programmacode gedetecteerd, zoals bij de handtekeningmethode, maar gaat het erom het typische gedrag van bewerkingen te detecteren. Op basis hiervan kan het programma met een bepaalde mate van waarschijnlijkheid conclusies trekken over de aard van een bestand.

Het voordeel van heuristische analyse is dat u de database niet hoeft bij te werken alvorens te scannen. Hierdoor kunnen nieuwe bedreigingen worden gedetecteerd nog voordat virusanalisten deze zijn tegengekomen.

Er zijn echter manieren waarop heuristiek kan worden omzeild. Zo kan een verdedigingsmanoeuvre worden uitgevoerd waarbij de activiteit van een schadelijk programma wordt geblokkeerd zodra een heuristische scan wordt geconstateerd.

Opmerking

Een combinatie van diverse scanmethoden biedt meer bescherming.

In het geval van een potentiële bedreiging emuleert de heuristische analyse objectuitvoering in de beveiligde virtuele omgeving van het programma. Als verdachte activiteit wordt vastgesteld wanneer het object wordt uitgevoerd, wordt het als schadelijk beschouwd en mag het niet op de host worden uitgevoerd, of

verschijnt er een bericht waarin om verdere instructies van de gebruiker wordt gevraagd:

- De nieuwe te scannen dreiging in quarantaine plaatsen en deze later verwerken met bijgewerkte databases.
- Het object verwijderen.
- Overslaan (als u zeker weet dat het object niet schadelijk kan zijn).

Schakelt **Gebruik heuristische analyse** in om heuristische methoden te gebruiken. Hiertoe zet u de schuifbalk in een van de volgende standen: Oppervlakkig, Gemiddeld of Gedetailleerd. Het detailniveau van de scan biedt een manier om de grondigheid waarmee op nieuwe bedreigingen wordt gescand (en dus de scankwaliteit), af te wegen tegen de belasting van het besturingssysteem en de duur van de scan. Hoe hoger u het heuristische niveau instelt, hoe meer systeembronnen de scan zal gebruiken en hoe langer deze zal duren.

Belangrijk!

Nieuwe bedreigingen die worden gedetecteerd met behulp van heuristische analyse, worden snel geanalyseerd door Kaspersky Lab, en desinfectie-methoden worden toegevoegd aan de uurlijkse database-updates.

Als u uw databases regelmatig bijwerkt, handhaaft u het optimale beschermingsniveau voor uw computer.

VEREISTEN VOOR HARDWARE EN SOFTWARE

Voor normale werking van het programma moet de computer aan de volgende minimale vereisten voldoen:

Algemene vereisten:

- 50 MB vrije ruimte op de harde schijf.
- Cd-rom (voor installatie van het programma vanaf de installatie-cd).
- Een muis.
- Microsoft Internet Explorer 5.5 of hoger (om de databases en softwaremodules van het programma via internet bij te werken).

- Microsoft Windows Installer 2.0.

Microsoft Windows 2000 Professional (SP4 of hoger), Microsoft Windows XP Home Edition (SP2 of hoger), Microsoft Windows XP Professional (SP2 of hoger), Microsoft Windows XP Professional x64 Edition:

- Intel Pentium 300MHz-processor of hoger (of een compatibel equivalent).
- 256 MB vrij RAM.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- Intel Pentium 800 MHz 32-bit (x86)/64-bit (x64) processor of hoger (of een compatibel equivalent).
- 512 MB vrij RAM.

BEDREIGINGEN VOOR COMPUTERVEILIGHEID

Sommige programma's vormen een aanzienlijke bedreiging voor de computerveiligheid. Andere bedreigingen zijn spam, phishing, aanvallen van hackers, adware en banners. Deze bedreigingen houden verband met internetgebruik.

IN DEZE SECTIE:

Bedreigingen: programma's.....	17
Internetbedreigingen.....	39

BEDREIGINGEN: PROGRAMMA'S

Het Kaspersky Lab-programma kan honderdduizenden malwareprogramma's detecteren die zich op uw computer kunnen bevinden. Een aantal van deze programma's vormt een grotere bedreiging voor de computer, terwijl andere alleen gevaarlijk zijn wanneer aan bepaalde voorwaarden wordt voldaan. Na detectie worden malwareprogramma's geclassificeerd en wordt er een gevarenniveau aan toegewezen (hoog of medium).

De virusanalisten van Kaspersky Lab onderscheiden twee hoofdcategorieën: *malwareprogramma's* en *potentieel ongewenste programma's*.

Malwareprogramma's (zie pagina 18) (malware) worden gemaakt om een computer en de computergebruiker schade te berokkenen, bijvoorbeeld door gegevens te stelen, blokkeren, wijzigen of wissen, of door de werking van een computer of computernetwerk te verstoren.

Potentieel ongewenste programma's (zie pagina 32) (PUP's: Potentially Unwanted Programs) zijn in tegenstelling tot malwareprogramma's, niet alleen bedoeld om schade aan te richten.

De Virusencyclopedie (<http://www.viruslist.com/en/viruses/encyclopedia>) bevat een uitgebreide beschrijving van deze programma's.

KWAADAARDIGE PROGRAMMA'S

Kwaadaardige programma's worden specifiek gemaakt om schade aan te richten aan computers en hun gebruikers: ze stelen, blokkeren, wijzigen of wissen informatie, of verstoren de werking van computers of computer-netwerken.

Er zijn drie categorieën malwareprogramma's: *virussen en wormen*, *Trojan programma's* en *malwareprogramma's*.

Virussen en wormen (zie pagina 18) (*Viruses_and_Worms*) kunnen kopieën van zichzelf maken die, op hun beurt, zichzelf kunnen kopiëren. Een aantal van deze programma's wordt buiten medeweten of zonder tussenkomst van de gebruiker uitgevoerd, terwijl andere alleen kunnen worden uitgevoerd als de gebruiker bepaalde handelingen verricht. Deze programma's verrichten hun schadelijke werk terwijl ze worden uitgevoerd.

In tegenstelling tot wormen en virussen kopiëren Trojan programma's (zie pagina 22) (*Trojan_programs*) zichzelf niet. Ze dringen een computer binnen, bijvoorbeeld via e-mail of door middel van een webbrowser wanneer de gebruiker een 'geïnfecteerde' website bezoekt. Deze programma's worden door de gebruiker gestart en verrichten hun schadelijke werk terwijl ze worden uitgevoerd.

Malwareprogramma's (zie pagina 29) (*Malicious_tools*) worden specifiek gemaakt om schade aan te richten. In tegenstelling tot andere malwareprogramma's verrichten ze echter niet direct schadelijke activiteiten terwijl ze worden uitgevoerd. Ze kunnen veilig op de computer van de gebruiker zijn opgeslagen en probleemloos lopen. Dergelijke programma's hebben functies voor het maken van virussen, wormen en Trojan programma's, het uitvoeren van netwerkaanvallen op externe servers, het hacken van computers of andere schadelijke activiteiten.

VIRUSSEN EN WORMEN

Subcategorie: virussen en wormen (*Viruses_and_Worms*)

Ernstniveau: hoog

Klassieke virussen en wormen voeren ongeoorloofde activiteiten op de computer uit en kunnen kopieën van zichzelf maken, die zichzelf op hun beurt ook kunnen kopiëren.

Klassiek virus

Nadat een klassiek virus het systeem is binnengedrongen, infecteert het een bestand en wordt het hierin geactiveerd. Vervolgens voert het virus zijn schadelijke werk uit en plaatst het kopieën van zichzelf in andere bestanden.

Klassieke virussen verspreiden zich alleen op de lokale bronnen van een bepaalde computer: ze kunnen niet onafhankelijk in andere computers binnendringen. Dergelijke virussen kunnen alleen andere computers binnendringen als ze een kopie van zichzelf aan een bestand in een gedeelde map of op een cd toevoegen, of als de gebruiker een e-mailbericht met een geïnfecteerde bijlage doorstuurt.

De programmacode van een klassiek virus kan in verschillende gebieden van een computer, besturingssysteem of programma binnendringen. Al naar gelang de omgeving is er verschil tussen *bestands-*, *opstart-*, *script-* en *macrovirussen*.

Virussen kunnen bestanden op verschillende manieren infecteren. *Over-schrijvende* virussen vervangen de programmacode van het geïnfecteerde bestand door hun eigen programmacode, waarna ze de oorspronkelijke inhoud van dit bestand vernietigen. Het besmette bestand werkt hierna niet meer en kan niet worden gedesinfecteerd. *Parasieten* brengen wijzigingen in bestanden aan, maar de bestanden blijven geheel of gedeeltelijk werkzaam. *Companionvirussen* ofwel partnervirussen brengen geen wijzigingen in bestanden aan maar maken duplicaten van de bestanden. Wanneer zo'n geïnfecteerd bestand wordt geopend, wordt het duplicaat, dat wil zeggen het virus, uitgevoerd. Er zijn ook *linkvirussen* (koppelingsvirussen), OBJ-virussen die *objectmodules infecteren*, virussen die *compilerbibliotheken (LIB) infecteren*, virussen die de *oorspronkelijke tekst van programma's infecteren*, enzovoort.

Worm

Nadat een netwerkworm in het systeem is binnengedrongen, wordt de worm net als het klassieke virus geactiveerd, waarna de schadelijke activiteit van de worm wordt uitgevoerd. De naam 'netwerkworm' houdt verband met het vermogen om van de ene naar de andere computer te kruipen, zonder dat de gebruiker zich hiervan bewust is, om via allerlei informatiekanalen kopieën van zichzelf te versturen.

Het voornaamste verschil tussen de diverse typen wormen is de manier waarop ze zich verspreiden. In de onderstaande tabel wordt de verspreidingsmethode van verschillende typen wormen toegelicht.

Tabel 1. Typen wormen en hun verspreidingsmethoden

TYPE	NAAM	BESCHRIJVING
E-mail-worm	E-mailwormen	<p>E-mailwormen infecteren computers via e-mail.</p> <p>Een geïnfecteerd bericht bevat een bestandsbijlage met een kopie van een worm of een koppeling naar zo'n kopie op een website (bijvoorbeeld een gehackte website of een hackersite). Wanneer u zo'n bijlage opent, wordt de worm geactiveerd. U brengt de worm ook in actie wanneer u op de koppeling klikt en een bestand downloadt en opent. Vervolgens blijft de worm zich vermenigvuldigen door geïnfecteerde berichten naar andere e-mailadressen te sturen.</p>
IM-Worm	IM-wormen	<p>Deze wormen verspreiden zich via IM-programma's (Instant Messaging ofwel expressberichten) zoals ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager of Skype.</p> <p>Dergelijke wormen gebruiken meestal lijsten met contactpersonen om berichten te versturen met een koppeling naar een kopie van de worm op de website. Wanneer een gebruiker zo'n bestand downloadt en opent, wordt de worm geactiveerd.</p>
IRC-Worm	IRC-wormen	<p>Deze wormen dringen computers binnen door middel van IRC (Internet Relay Chat), een systeem waarmee computergebruikers in real-time met elkaar kunnen communiceren via internet.</p> <p>Deze worm publiceert een kopie van de worm of een koppeling naar zo'n kopie in de internetchat. Wanneer een gebruiker zo'n bestand downloadt en opent, wordt de worm geactiveerd.</p>

TYPE	NAAM	BESCHRIJVING
Net-Worm	Netwerkwormen	<p>Deze wormen worden via computernetwerken verspreid.</p> <p>Netwerkwormen vermenigvuldigen zich in tegenstelling tot andere soorten wormen zonder tussenkomst van de gebruiker. Ze zoeken in de LAN's naar computers met programma's die kwetsbaarheden bevatten. Hiertoe verzenden deze wormen een speciaal netwerkpakket (exploit) met hun programmacode of een gedeelte hiervan. Als er zich een computer met een beveiligingsprobleem in het netwerk bevindt, krijgt deze zo'n pakket toegestuurd. Zodra de worm volledig in de computer is binnengedrongen, wordt deze geactiveerd.</p>
P2P-Worm	Bestandsuitwisselingswormen	<p>Bestandsuitwisselingswormen verspreiden zich via peer-to-peer-netwerken voor bestandsuitwisseling zoals Kazaa, Grokster, EDonkey, FastTrack of Gnutella.</p> <p>De wormen infiltreren een bestandsuitwisselingsnetwerk door zichzelf te kopiëren naar de bestandsuitwisselingsmap die zich doorgaans op de computer van de gebruiker bevindt. Er wordt informatie over dit feit weergegeven, waarna de gebruiker het geïnfecteerde bestand in het netwerk op de gebruikelijke manier kan opzoeken, downloaden en openen.</p> <p>Complexere wormen imiteren netwerkprotocollen van een specifiek bestandsuitwisselingsnetwerk: zij geven positieve reacties op zoekopdrachten en stellen hun kopieën voor download beschikbaar.</p>

TYPE	NAAM	BESCHRIJVING
Worm	Andere wormen	<p>Andere netwerkwormen zijn onder andere:</p> <ul style="list-style-type: none"> • Wormen die kopieën van zichzelf verspreiden via netwerkbronnen. Deze wormen gebruiken de functies van het besturingssysteem om beschikbare netwerkmappen te doorlopen, verbinding te maken met computers in het algemene netwerk en te proberen hun schijven te openen voor onbeperkte toegang. Deze wormen verspreiden zich anders dan computernetwerkwormen: de gebruiker moet een bestand met een kopie van de worm openen om de worm te activeren. • Wormen die geen van de hier beschreven verspreidingsmethoden gebruiken (bijvoorbeeld wormen die zich via mobiele telefoons verspreiden).

TROJAN PROGRAMMA'S

Subcategorie: Trojan programma's (Trojan_programs)

Ernstniveau: hoog

In tegenstelling tot wormen en virussen maken Trojan programma's geen kopieën van zichzelf. Ze dringen een computer binnen, bijvoorbeeld via e-mail of door middel van een webbrowser wanneer de gebruiker een 'geïnfecteerde' website bezoekt. Trojan programma's worden gestart door de gebruiker en verrichten hun schadelijke werk terwijl ze worden uitgevoerd.

Het gedrag van verschillende Trojan programma's op de geïnfecteerde computer kan variëren. De hoofdfuncties van Trojan programma's zijn het blokkeren, wijzigen en wissen van gegevens en het verstoren van de werking van computers of computernetwerken. Verder kunnen Trojan programma's bestanden ontvangen en verzenden, deze bestanden uitvoeren, meldingen weergeven, webpagina's openen, programma's downloaden en installeren en de geïnfecteerde computer opnieuw opstarten.

Indringers gebruiken vaak 'sets' van diverse Trojan programma's.

In de onderstaande tabel worden typen Trojan programma's en hun gedrag beschreven.

Tabel 2. Typen Trojan programma's en hun gedrag op de geïnfecteerde computer

TYPE	NAAM	BESCHRIJVING
Trojan-ArcBomb	Trojan programma's - archiefbommen	Archieven; na uitpakken worden de archieven zo groot dat ze de werking van de computer verstoren. Pogingen om zo'n archief uit te pakken kunnen resulteren in tragere werking of blokkering van computer. Bovendien wordt de schijf mogelijk met 'lege' gegevens gevuld. 'Archiefbommen' zijn met name gevaarlijk voor bestands- en e-mailservers. Als op de server een systeem voor automatische verwerking van inkomende gegevens wordt gebruikt, kan zo'n archiefbom de server stoppen.
Backdoor	Trojan programma's voor extern beheer	Deze programma's worden als de gevaarlijkste Trojan programma's beschouwd. Qua functies lijken ze op algemeen verkrijgbare programma's voor extern beheer. Deze programma's installeren zichzelf buiten medeweten van de gebruiker en dragen het externe beheer van de computer aan de indringer over.

TYPE	NAAM	BESCHRIJVING
Trojan programma's	Trojan programma's	<p>De categorie Trojan programma's omvat de volgende schadelijke pro-gramma's:</p> <ul style="list-style-type: none"> • Klassieke Trojan programma's. Deze voeren alleen de hoofdfuncties van Trojan programma's uit: het blokkeren, wijzigen of wissen van gegevens en het verstoren van de werking van computers of computer-netwerken. Deze Trojan pro-gramma's hebben geen van de extra functies die typerend zijn voor de andere soorten Trojan programma's die in deze tabel worden beschreven. • Multifunctionele Trojan pro-gramma's. Deze hebben extra functies die kenmerkend zijn voor verschillende soorten Trojan programma's.
Trojan-Ransom	Trojan programma's die een losgeld eisen	Deze programma's 'gijzelen' informatie op de computer en wijzigen of blokkeren deze informatie, of verstoren de werking van de computer, zodat de gebruiker de gegevens niet kan gebruiken. Vervolgens eist de indringer een losgeld van de computergebruiker in ruil voor een programma dat de normale werking van de computer zal herstellen.
Trojan-Clicker	Trojan-Clickers	<p>Deze programma's openen webpagina's vanaf de computer van de gebruiker. Ze verzenden een opdracht naar de web-browser of vervangen webadressen die in de systeembestanden zijn opgeslagen.</p> <p>Met deze programma's organiseren de indringers netwerkaanvallen en verhogen zij het verkeer naar dergelijke sites om het aantal hits en de weergavefrequentie van banners te vergroten.</p>

TYPE	NAAM	BESCHRIJVING
Trojan-Downloader	Trojan programma's - downloaders	Deze programma's openen de webpagina van de indringer, downloaden andere malwareprogramma's van deze pagina en installeren deze op de computer van de gebruiker. Soms is de naam van het downloadbare malwareprogramma in de downloader zelf opgeslagen. In andere gevallen wordt de naam van het malwareprogramma opgehaald van de webpagina die wordt geopend.
Trojan-Dropper	Trojan programma-droppers	<p>Deze programma's slaan programma's met andere Trojan programma's op de computerschijf op, om ze vervolgens te installeren.</p> <p>Indringers kunnen droppers gebruiken om het volgende te doen:</p> <ul style="list-style-type: none">• Malwareprogramma's installeren buiten medeweten van de gebruiker. Trojan-droppers produceren geen meldingen of alleen valse meldingen, bijvoorbeeld waarschuwingen dat het archief een fout bevat of dat de verkeerde versie van het besturingssysteem wordt gebruikt.• Een ander bekend malwareprogramma beschermen tegen detectie: niet alle antivirusprogramma's kunnen een malwareprogramma in een dropper detecteren.

TYPE	NAAM	BESCHRIJVING
Trojan-Notifier	Trojan programma-notifiers	<p>Deze programma's stellen de indringer op de hoogte dat de geïnfecteerde computer is verbonden, waarna informatie over die computer aan de indringer wordt doorgegeven, waaronder: het IP-adres, het nummer van de geopende poort of het e-mailadres. Ze kunnen op verschillende manieren met de indringer communiceren, bijvoorbeeld via e-mail, via FTP of door de webpagina van de indringer te openen.</p> <p>Notifiers worden vaak in combinatie met andere Trojan programma's gebruikt en delen de indringer mee dat er andere Trojan programma's op de computer van de gebruiker zijn geïnstalleerd.</p>
Trojans-proxy's	Trojan programma-proxy's	Deze programma's stellen de indringer in staat om anoniem webpagina's te openen vanaf de computer van de gebruiker en worden vaak gebruikt voor de verzending van spam.
Trojan-PSW	Trojan programma's die wachtwoorden stelen	<p>Deze programma's maken deel uit van de categorie Password-Staling-Ware en stelen gebruikersaccounts, bijvoorbeeld softwareregistratiegegevens. Ze sporen vertrouwelijke informatie in de systeembestanden en het register op en sturen deze naar hun ontwikkelaar via e-mail of FTP, via de website van de indringer of op een andere manier.</p> <p>Sommige van deze Trojan programma's behoren tot de categorieën die in deze tabel worden beschreven: Trojan-Bankers (programma's die bank-rekeninggegevens stelen), Trojan-IM's (programma's die persoonlijke gegevens van de gebruikers van IM-programma's stelen) en Trojan-GameThieves (programma's die gegevens van de gebruikers van netwerkspelletjes stelen).</p>

TYPE	NAAM	BESCHRIJVING
Trojan-Spy	Trojan spion-programma's	Deze programma's dienen om de gebruiker te bespioneren en verzamelen gegevens over de handelingen die de gebruiker op de computer verricht. Ze onderscheppen bijvoorbeeld gegevens die de gebruiker via het toetsenbord heeft ingevoerd, maken momentopnamen van het scherm en stellen lijsten met actieve programma's samen. Vervolgens worden deze gegevens aan de indringer doorgegeven via e-mail of FTP, via de website van de indringer of op een andere manier.
Trojan-DDoS	Trojan programma's - netwerkaanvallen	Deze programma's verzenden een groot aantal aanvragen vanaf de computer van de gebruiker naar de externe server. De server gebruikt vervolgens alle beschikbare bronnen voor het verwerken van de aanvragen en stopt met werken (Denial-of-Service (DoS)). Deze programma's worden vaak gebruikt om meerdere computers te infecteren teneinde de server vanaf deze computers aan te vallen.
Trojan-IM	Trojan programma's die persoonlijke gegevens van de gebruikers van IM-programma's stelen	Deze programma's stelen nummers en wachtwoorden van de gebruikers van IM-programma's (Instant Messaging ofwel expresberichten) zoals ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager of Skype. Vervolgens worden de gegevens aan de indringer doorgegeven via e-mail of FTP, via de website van de indringer of op een andere manier.

TYPE	NAAM	BESCHRIJVING
Rootkits	Rootkits	Deze programma's verbergen andere malwareprogramma's en hun activiteiten en dragen zodoende bij aan de toename van dergelijke programma's in het systeem. Ze houden bestanden of processen in het geheugen van een geïnfecteerde computer schuil, registreren sleutels die door de malwareprogramma's worden uitgevoerd of verbergen gegevensuitwisseling tussen de programma's die op de computer van de gebruiker zijn geïnstalleerd, en andere computers in het netwerk.
Trojan-SMS	Trojan programma's - sms-berichten	Deze programma's infecteren mobiele telefoons en versturen sms-berichten naar nummers, waarvoor de gebruiker van de geïnfecteerde telefoon moet betalen.
Trojan-GameThieves	Trojan programma's die persoonlijke gegevens van de gebruikers van netwerkspeletjes stelen	Deze programma's stelen gegevens over de gebruikersaccount van de gebruikers van netwerkspeletjes. Vervolgens worden deze gegevens aan de indringer doorgegeven via e-mail of FTP, via de website van de indringer of op een andere manier.
Trojan-Banker	Trojan programma's die bankrekeninggegevens stelen	Deze programma's stelen gegevens over bankrekeningen of elektronische/digitale rekeningen. Vervolgens worden deze gegevens aan de indringer doorgegeven via e-mail of FTP, via de website van de indringer of op een andere manier.
Trojan-Mailfinder	Trojan programma's die e-mailadressen verzamelen	Deze programma's verzamelen e-mailadressen op de computer en spelen deze adressen door aan de indringer via e-mail of FTP, via de website van de indringer of op een andere manier. De indringer kan aan de hand van de verzamelde adressen spam verzenden.

KWAADAARDIGE PROGRAMMA'S

Subcategorie: kwaadaardige programma's (Malicious_tools)

Ernstniveau: gemiddeld

Deze programma's zijn speciaal ontworpen om schade te berokkenen. In tegenstelling tot andere malwareprogramma's verrichten ze echter niet direct schadelijke activiteiten terwijl ze worden uitgevoerd. Ze kunnen veilig op de computer van de gebruiker zijn opgeslagen en probleemloos lopen. Dergelijke programma's hebben functies voor het maken van virussen, wormen en Trojan programma's, het uitvoeren van netwerkaanvallen op externe servers, het hacken van computers of andere schadelijke activiteiten.

Er zijn uiteenlopende typen malwareprogramma's met verschillende functies. Deze typen worden in de onderstaande tabel beschreven.

Tabel 3. Malwareprogramma's en hun functies

TYPE	NAAM	BESCHRIJVING
Constructor	Constructors	Constructors worden gebruikt om nieuwe virussen, wormen en Trojan pro-gramma's te maken. Sommige constructors hebben een standaard Windows-interface, waarin u kunt selecteren welk type kwaad-aardig programma moet worden gemaakt, welke methode dit programma moet gebruiken om debuggen tegen te gaan, en andere eigenschappen.
Dos	Netwerkaanvallen	Deze programma's verzenden een groot aantal aanvragen vanaf de computer van de gebruiker naar de externe server. De server gebruikt vervolgens alle beschikbare bronnen voor het verwerken van de aanvragen en stopt met werken (Denial-of-Service (DoS)).

TYPE	NAAM	BESCHRIJVING
Exploit	Exploits	<p>Een exploit is een set gegevens die of een stuk programmacode dat de beveiligingsproblemen van een programma uitbuit om een schadelijke activiteit op de computer uit te voeren. Exploits kunnen bijvoorbeeld gegevens in bestanden lezen of ernaar schrijven of geïnfecteerde webpagina's openen.</p> <p>Versillende exploits gebruiken kwetsbaarheden van verschillende programma's of netwerkservices. Een exploit wordt via het netwerk naar meerdere computers overgedragen in de vorm van een netwerkpakket dat naar computers met kwetsbare netwerkservices zoekt. Een exploit in een DOC-bestand gebruikt kwetsbaarheden van tekstverwerkers, en kan door de indringer geprogrammeerde functies uitvoeren wanneer de gebruiker een geïnfecteerd bestand opent. Een exploit in een e-mailbericht zoekt naar kwetsbaarheden in e-mailclientprogramma's; zodra de gebruiker een geïnfecteerd bericht in dit programma opent, kan de kwaadaardige actie worden uitgevoerd.</p> <p>Exploits worden gebruikt om networmen (Net-Worm) te verspreiden. Exploits-Nukers zijn netwerkpakketten die computers buiten werking stellen.</p>
FileCryptor	Bestandscodering	FileCryptors decoderen andere kwaadaardige programma's om deze voor antivirusprogramma's te verbergen.

TYPE	NAAM	BESCHRIJVING
Flooder	Programma's voor het overstromen van netwerken	<p>Deze programma's verzenden een groot aantal berichten via netwerkkanalen. Zo zijn er bijvoorbeeld programma's voor het overstromen van Internet Relay Chat-servers.</p> <p>Programma's die e-mailverkeer en IM- en SMS-kanalen ontregelen, behoren niet tot deze categorie malware. Dergelijke programma's worden geclassificeerd als afzonderlijke typen: Email-Flooder, IM-Flooder en SMS-Flooder (zie hieronder).</p>
HackTool	Hackprogramma's	<p>Hackprogramma's worden gebruikt om computers te hacken waarop ze zijn geïnstalleerd, of om aanvallen op andere computers te plannen (om bijvoorbeeld zonder toestemming andere systeemgebruikers toe te voegen, of de systeemlogboeken te wissen om sporen van hun aanwezigheid in het systeem te verhullen). Tot deze categorie behoort een aantal sniffers die schadelijke functies uitvoeren (bijvoorbeeld het onderscheppen van wachtwoorden). Sniffers zijn programma's waarmee netwerkverkeer kan worden afgeluisterd.</p>
not-virus:Hoax	Hoaxprogramma's	<p>Deze programma's versturen verontwaardigende berichten waarin de gebruiker bijvoorbeeld wordt gewaarschuwd dat een schoon bestand een virus bevat of dat schijfformattering niet zal plaatsvinden.</p>
Spoofers	Spoofers	<p>Deze programma's versturen berichten en netwerkverzoeken met een vals afzendersadres. Indringers gebruiken spoofers om zich bijvoorbeeld als een andere afzender voor te doen.</p>

TYPE	NAAM	BESCHRIJVING
VirTool	Programma's voor het aanpassen van malwareprogramma's	Met deze programma's kunnen andere malwareprogramma's worden gewijzigd om ze te verbergen voor antivirusprogramma's.
Email-Flooder	Programma's voor het versturen van grote hoeveelheden e-mail	Deze programma's overstroomden e-mail-adressen met berichten. Vanwege de vloed van berichten kunnen de gebruikers inkomende niet-spamberichten niet meer bekijken.
IM-Flooder	Programma's voor het overstroomden van IM-programma's	Deze programma's versturen grote hoeveelheden berichten naar de gebruikers van IM-programma's (Instant Messaging ofwel expresberichten) zoals ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager of Skype. Vanwege de vloed van berichten kunnen de gebruikers inkomende niet-spamberichten niet meer bekijken.
SMS-Flooder	Programma's voor het versturen van grote hoeveelheden sms-tekstberichten	Deze programma's versturen grote hoeveelheden sms-berichten naar mobiele telefoons.

POTENTIEEL ONGEWENSTE PROGRAMMA'S

Potentieel ongewenste programma's zijn, in tegenstelling tot malwareprogramma's, niet alleen bedoeld om schade aan te richten. Ze kunnen echter worden gebruikt om de beveiliging van de computer te schenden.

Potentieel ongewenste programma's zijn onder meer adware, pornware en andere *potentieel ongewenste programma's*.

Bij adwareprogramma's (zie pagina 33) krijgen gebruikers reclameboodschappen te zien.

Bij pornwareprogramma's (zie pagina 33) krijgen gebruikers pornografisch materiaal te zien.

Andere riskware (zie pagina 34) – dit zijn meestal handige programma's die door vele computergebruikers worden gebruikt. Als een indringer echter toegang tot deze programma's krijgt of deze op de computer van de gebruiker installeert, kan die indringer de functionaliteit van riskware gebruiken om de beveiliging te schenden.

Potentieel ongewenste programma's worden op een van de volgende manieren geïnstalleerd:

- Door de gebruiker, hetzij afzonderlijk hetzij samen met een ander programma (softwareontwikkelaars nemen bijvoorbeeld adware-programma's op in freeware- of sharewareprogramma's).
- Ze worden ook door indringers geïnstalleerd, die dergelijke programma's bijvoorbeeld opnemen in pakketten met andere malwareprogramma's, en 'kwetsbaarheden' van de webbrowser of Trojan-downloaders en-droppers gebruiken wanneer de gebruiker een 'geïnfecteerde' website bezoekt.

ADWARE

Subcategorie: Adware

Ernstniveau: gemiddeld

Adwareprogramma's hebben ten doel de gebruiker te presenteren met reclamegegevens. Deze programma's geven banners in de interface van andere programma's weer en sturen zoekopdrachten door naar reclamewebsites. Sommige adwareprogramma's verzamelen marketinggegevens over de gebruiker (bijvoorbeeld bezochte sites of uitgevoerde zoekopdrachten) en sturen deze door naar de desbetreffende adwareontwikkelaar. In tegenstelling tot Trojan spionnen vragen deze programma's de gebruiker om toestemming alvorens deze gegevens over te dragen.

PORNWARE

Subcategorie: Pornware

Ernstniveau: gemiddeld

Meestal installeren gebruikers dergelijke programma's zelf om pornografische informatie te zoeken of downloaden.

Deze programma's kunnen ook door indringers op de computer van de gebruiker worden geïnstalleerd om zonder de toestemming van de gebruiker advertenties van commerciële pornografische sites en diensten weer te geven. Voor de installatie van deze programma's wordt gebruikgemaakt van kwetsbaarheden van het besturingssysteem of de webbrowser, Trojan-downloaders en -droppers.

Er wordt onderscheid gemaakt tussen drie typen pornwareprogramma's, gebaseerd op hun functies. Deze typen worden in de onderstaande tabel beschreven.

Tabel 4. Typen pornwareprogramma's en hun functies

TYPE	NAAM	BESCHRIJVING
Porn-Dialer	Auto-inbellers	Deze programma's bellen automatisch pornodiensten (ze slaan de telefoonnummers van dergelijke diensten op). In tegenstelling tot Trojan inbellers stellen ze gebruikers op de hoogte van hun activiteiten.
Porn-Downloader	Programma's voor het downloaden van bestanden van internet	Deze programma's downloaden pornografische informatie naar de computer van de gebruiker. In tegenstelling tot Trojan inbellers stellen ze gebruikers op de hoogte van hun activiteiten.
Porn-Tool	Tools	Dit zijn programma's waarmee pornografie wordt gezocht en weergegeven, bijvoorbeeld speciale browserwerkbalken en videospelers.

ANDERE RISKWAREPROGRAMMA'S

Subcategorie: andere riskwareprogramma's

Ernstniveau: gemiddeld

De meeste riskwareprogramma's zijn handige programma's die algemeen worden gebruikt. Ze omvatten IRC-clients, inbellers, programma's voor

bestandsdownload, controleprogramma's voor systeemactiviteiten, programma's voor het werken met wachtwoorden, en FTP-, HTTP- of Telnet-internet servers.

Als een indringer echter toegang tot deze programma's krijgt of deze op de computer van de gebruiker installeert, kan die indringer riskwarefuncties gebruiken om de beveiliging te schenden.

Andere riskwareprogramma's worden geclassificeerd op basis van hun functies. Deze typen worden in de onderstaande tabel beschreven.

Tabel 5. Andere typen riskware en hun respectieve functies

TYPE	NAAM	BESCHRIJVING
Client-IRC	Internetchat-programma's	Gebruikers installeren deze programma's om te communiceren door middel van IRC (Internet Relay Chat). Indringers gebruiken ze om malwareprogramma's te verspreiden.
Dialer	Programma's voor automatisch inbellen	Deze programma's kunnen 'verborgen' telefoonverbindingen tot stand brengen via de modem.
Downloaders	Downloaders	Deze programma's kunnen heimelijk bestanden van websites downloaden.
Monitor	Monitors	Met deze programma's kunnen computeractiviteiten worden gecontroleerd (hierbij gaat het om activiteiten als programmaprestaties, gegevensuitwisseling met programma's op andere computers enzovoort).
PSWTool	Programma's voor wachtwoordherstel	Deze programma's worden gebruikt om vergeten wachtwoorden weer te geven en te herstellen. De programma's kunnen ook door indringers op de computer worden geïnstalleerd om het wachtwoord van de gebruiker te achterhalen.

TYPE	NAAM	BESCHRIJVING
RemoteAdmin	Programma's voor extern beheer	<p>Deze programma's worden vaak door systeembeheerders gebruikt om de interface van externe computers weer te geven en controle- en beheertaken uit te voeren. De programma's kunnen ook door indringers op de computer worden geïnstalleerd om de computer te controleren en beheren.</p> <p>Riskwareprogramma's voor extern beheer zijn niet hetzelfde als Trojan backdoorprogramma's. Trojan programma's hebben functies waarmee ze zelfstandig in het systeem kunnen infiltreren en zichzelf kunnen installeren. In riskwareprogramma's ontbreekt deze functionaliteit.</p>
Server-FTP	FTP-servers	Deze programma's voeren de functies van FTP-servers uit. Indringers installeren deze programma's op de computers van gebruikers om via het FTP-protocol extern toegang te krijgen.
Server-Proxy	Proxyservers	Deze programma's voeren de functies van proxyservers uit. Indringers installeren ze op de computers van gebruikers om namens hen spam te versturen.
Server-Telnet	Telnet-servers	Deze programma's voeren de functies van Telnet-servers uit. Indringers installeren deze programma's op de computers van gebruikers om via het Telnet-protocol extern toegang te krijgen.

TYPE	NAAM	BESCHRIJVING
Server-Web	Webservers	Deze programma's voeren de functies van webservers uit. Indringers installeren deze programma's op de computers van gebruikers om via het HTTP-protocol extern toegang te krijgen.
RiskTool	Programma's voor de lokale computer	Deze programma's verschaffen gebruikers extra functies op hun eigen computer, bijvoorbeeld om bestanden of vensters van actieve programma's te verbergen en actieve processen te sluiten.
NetTool	Netwerkprogramma's	Wanneer deze programma's op een computer zijn geïnstalleerd, beschikt de gebruiker over extra functies voor het beheren van andere computers in het netwerk (bijvoorbeeld om de computers opnieuw op te starten, geopende poorten te zoeken of programma's uit te voeren die op deze computers zijn geïnstalleerd).
Client-P2P	Peer-to-peer-programma's	Deze programma's worden voor peer-to-peer netwerken gebruikt. Indringers kunnen deze programma's gebruiken om malwareprogramma's te verspreiden.
Client-SMTP	SMTP-clients	Deze programma's versturen e-mailberichten in verborgen modus. Indringers installeren ze op de computers van gebruikers om namens hen spam te versturen.
WebToolbar	Webwerkbalken	Deze programma's voegen hun eigen zoekwerkbalken aan de werkbalken van andere programma's toe.

TYPE	NAAM	BESCHRIJVING
FraudTool	Fraudeprogramma's	Deze programma's doen zich als andere, echte programma's voor. Er zijn bijvoorbeeld frauduleuze anti-virusprogramma's; deze geven berichten weer over detectie van malwareprogramma's, maar vinden of desinfecteren niets.

METHODEN VOOR HET DETECTEREN VAN GEÏNFECTEERDE, VERDACHTE EN POTENTIEEL GEVAARLIJKE OBJECTEN

Het programma van Kaspersky Lab kan malwareprogramma's in objecten op twee manieren detecteren: reactief (met behulp van databases) en proactief (met behulp van heuristische analyse).

Databases zijn bestanden met records op basis waarvan honderdduizenden bekende bedreigingen in de detecteerbare objecten kunnen worden herkend. Deze records bevatten gegevens over de stuurcodesecties van malwareprogramma's, en algoritmen voor het desinfecteren van de objecten waarin deze programma's voorkomen. De virusanalisten van Kaspersky Lab detecteren elke dag honderden nieuwe malwareprogramma's, maken records ter identificatie van deze programma's en nemen deze op in de database-updates.

Als het programma van Kaspersky Lab in een detecteerbaar object codesecties detecteert die volledig overeenkomen met de controlecodesecties van een malwareprogramma (op basis van de informatie in de database), wordt een dergelijk object geïnfecteerd bevonden, en als ze slechts gedeeltelijk overeenkomen (in overeenstemming met een aantal voorwaarden) – wordt het verdacht bevonden.

Met de proactieve detectiemethode kunnen de nieuwste schadelijke programma's worden gedetecteerd, waarvoor nog geen informatie in de database is ingevoerd.

Objecten die nieuwe malwareprogramma's bevatten, worden door het programma van Kaspersky Lab gedetecteerd op basis van hun gedrag. Het zou onjuist zijn om te beweren dat de programmacode van zo'n object geheel of gedeeltelijk overeenkomt met de programmacode van een bekend

malwareprogramma. Wel bevat de programmacode bepaalde opdrachtreeksen die karakteristiek zijn voor malwareprogramma's, bijvoorbeeld voor het openen van of schrijven naar een bestand, of voor het onderscheppen van interrupt-vectoren. Het programma kan bijvoorbeeld vaststellen dat een bestand lijkt te zijn besmet met een onbekend opstartvirus.

Objecten die via de proactieve methode worden gedetecteerd, worden potentieel gevaarlijk genoemd.

INTERNETBEDREIGINGEN

Het programma van Kaspersky Lab gebruikt speciale technologieën om de volgende bedreigingen voor de computerveiligheid te weren:

- Spam of ongevraagde binnenkomende e-mail (zie de sectie Ongevraagde inkomende mail of spam op pagina 39);
- phishing (op pagina 40);
- hackeraanvallen (op pagina 40);
- weergave van banners (op pagina 41);

SPAM OF ONGEVRAAGDE BINNENKOMENDE E-MAIL

Het programma van Kaspersky Lab beschermt gebruikers tegen spam. Spam is ongevraagde binnenkomende e-mail, meestal reclame. Spam vormt een extra belasting voor de kanalen en de e-mailservers van de provider. De ontvanger betaalt voor het verkeer dat door spam wordt gegenereerd en niet-spamberichten worden vertraagd. Spam is daarom in veel landen bij de wet verboden.

Binnenkomende Microsoft Office Outlook-, Microsoft Outlook Express- en The Bat!-berichten worden door het programma van Kaspersky Lab gescand. Als een spambericht wordt gedetecteerd, worden de door u geselecteerde bewerkingen uitgevoerd. Misschien laat u dergelijke berichten bijvoorbeeld in een speciale map plaatsen of verwijderen.

Het Kaspersky Lab-programma detecteert spam met grote precisie, waarbij verschillende spamfiltertechnologieën worden toegepast. Zo wordt spam

gedetecteerd op basis van het adres van de afzender en woorden en woordgroepen in de onderwerpregel van het bericht. Ook grafische spam wordt gedetecteerd, en er wordt een zelflerend algoritme gehanteerd voor de detectie van spam op basis van de berichttekst.

Antispamdatabases bevatten de zwarte en witte lijst van afzenderadressen en lijsten met woorden en woordgroepen die verwant zijn aan diverse spam-categorieën zoals reclame, zorg en welzijn, en gokken.

PHISHING

Phishing is een vorm van internetfraude waarbij wordt 'gevist' naar nummers van creditcards, pincodes en andere persoonlijke gegevens van gebruikers om hun geld afhandig te maken.

Phishing staat vaak in verband met internetbankiers. Indringers maken een exacte kopie van de website van de bank waarop ze het voorzien hebben, en sturen vervolgens berichten naar de klanten van die bank. In deze berichten wordt de klanten namens de bank meegedeeld dat er als gevolg van wijzigingen of storingen in de bankierssoftware gebruikersaccounts verloren zijn gegaan en dat ze hun gegevens op de website van de bank moeten controleren of wijzigen. De gebruiker klikt op de koppeling naar de website die door de indringers is gemaakt en voert zijn of haar persoonlijke gegevens in.

Anti-phishingdatabases bevatten de lijst met URL's van websites die bekend staan als sites die phishingaanvallen lanceren.

Het programma van Kaspersky Lab analyseert binnenkomende Microsoft Office Outlook- en Microsoft Outlook Express-berichten. Als een koppeling wordt gevonden naar een URL die in de databases voorkomt, wordt dit bericht als spam aangemerkt. Als de gebruiker het bericht opent en de koppeling probeert te volgen, wordt deze website door het programma geblokkeerd.

HACKERAANVALLEN

Netwerkaanvallen zijn pogingen om een externe computer binnen te dringen met het doel deze onder controle te krijgen en buiten werking te stellen of toegang te krijgen tot beschermde gegevens.

Netwerkaanvallen worden gelanceerd door indringers (bijvoorbeeld het scannen van poorten of pogingen om wachtwoorden te hacken) of door malware-programma's die namens de gebruiker opdrachten uitvoeren en gegevens naar

hun 'meester' doorspelen of andere functies met betrekking tot netwerkaanvallen uitvoeren. Deze categorie omvat een aantal Trojan programma's, DoS-aanvallen, kwaadaardige scripts en bepaalde typen netwerkwormen.

Netwerkaanvallen worden verspreid in LAN's en algemene netwerken, waarbij gebruik wordt gemaakt van beveiligingsproblemen in de besturingssystemen en programma's. Ze kunnen tijdens het maken van netwerkverbindingen worden overgebracht als afzonderlijke IP-gegevenspakketten.

Het programma van Kaspersky Lab stopt netwerkaanvallen zonder netwerkverbindingen te verbreken. Hierbij worden speciale firewalldatabases gebruikt. Deze databases bevatten records voor IP-gegevenspakketten die kenmerkend zijn voor diverse hackprogramma's. Het programma analyseert netwerkverbindingen en blokkeert de als gevaarlijk aangemerkte IP-pakketten.

WEERGAVE VAN BANNERS

Banners of advertenties die koppelingen naar de website van de adverteerder zijn, worden meestal in de vorm van afbeeldingen weergegeven. De weergave van banners op de website vormt geen bedreiging voor de veiligheid van de computer maar wordt evengoed beschouwd als een verstoring van de normale werking van de computer. Knipperende banners op het scherm verslechteren de werkomstandigheden en verminderen de productiviteit. De gebruiker wordt afgeleid door irrelevante informatie. Het volgen van bannerkoppelingen zorgt voor toename van het internetverkeer.

De weergave van banners in de interfaces wordt door veel organisaties geblokkeerd in het kader van hun beleid voor gegevensbeveiliging.

Het programma van Kaspersky Lab blokkeert banners op basis van de URL van de bijbehorende website. Hiervoor wordt gebruikgemaakt van databases voor bannerblokkering waarin de URL's van binnen- en buitenlandse banner-netwerken zijn opgeslagen. (Deze databases kunnen worden bijgewerkt.) Het programma doorloopt de koppelingen van de website die wordt geladen en vergelijkt deze met de adressen in de databases. Als een koppeling wordt gevonden die overeenkomt met een databaseadres, wordt deze koppeling van de site verwijderd, waarna de pagina verder wordt geladen.

HET PROGRAMMA OP DE COMPUTER INSTALLEREN

Het programma wordt in de interactieve modus op de computer geïnstalleerd met behulp van de instellingenwizard van het programma.

Belangrijk!

Het is raadzaam alle actieve programma's te sluiten voordat u de installatie voortzet.

Voer het distributiebbestand uit (het bestand met de extensie *.exe) om het programma op uw computer te installeren.

Opmerking

Installatie van het programma via het installatiebestand dat van het internet wordt gedownload, is precies hetzelfde als installatie vanaf de cd.

Hierna zoekt de instellingenwizard het installatiepakket van het programma (het bestand met de extensie *.msi), en als dit bestand wordt gevonden, zoekt de wizard naar een nieuwere versie op de internetserver van Kaspersky Lab. Is het bestand voor het installatiepakket niet gevonden, dan kunt u het downloaden. Zodra het bestand is gedownload, wordt de programma-installatie gestart. Als u de download annuleert, wordt de programma-installatie in normale modus hervat.

Het installatieprogramma wordt als wizard geïmplementeerd. Elk venster bevat een set knoppen voor het installatieproces. Hieronder staat een korte beschrijving van hun functies:

- **Volgende** – hiermee accepteert u de actie en gaat u naar de volgende stap van het installatieproces.
- **Vorige** – hiermee gaat u terug naar de vorige stap van het installatieproces.
- **Annuleren** – hiermee annuleert u de installatie.
- **Voltooien** – hiermee voltooit u de installatie.

Hieronder wordt elke stap van de pakketinstallatie uitvoerig besproken.

IN DEZE SECTIE:

Stap 1. Verifiëren of het systeem voldoet aan de installatievereisten.....	43
Stap 2. Naar een nieuwere versie van het programma zoeken	44
Stap 3. Begroetingsvenster van de wizard	44
Stap 4. De licentieovereenkomst bekijken.....	45
Stap 5. Het installatietype selecteren	45
Stap 6. De installatiemap selecteren	46
Stap 7. Te installeren programmacomponenten selecteren	46
Stap 8. Naar andere antivirussoftware zoeken.....	47
Stap 9. Laatste voorbereiding op de installatie.....	48
Stap 10. De installatie voltooien	49

STAP 1. VERIFIËREN OF HET SYSTEEM VOLDOET AAN DE INSTALLATIEVEREISTEN

Voordat u het programma op uw computer installeert, controleert de wizard de compatibiliteit van het besturingssysteem en de geïnstalleerde servicepacks tegen de software-installatievereisten (zie de sectie *Systeemvereisten voor hardware en software* op pagina 15). De wizard controleert ook of de vereiste programma's op uw computer zijn geïnstalleerd en of u de juiste rechten hebt om software erop te installeren.

Als er niet aan alle vereisten wordt voldaan, verschijnt er een overeenkomstige melding op het scherm. Het is raadzaam om de vereiste updates via de service **Windows Update** te installeren, evenals de vereiste programma's voordat u het programma van Kaspersky Lab installeert.

STAP 2. NAAR EEN NIEUWERE VERSIE VAN HET PROGRAMMA ZOEKEN

Tijdens deze stap roept de wizard de updateservers van Kaspersky Lab op om te controleren of er een nieuwere versie bestaat van het programma dat wordt geïnstalleerd.

Als er op de updateservers van Kaspersky Lab geen nieuwere versie wordt gedetecteerd, wordt de instellingenwizard gestart om de huidige versie te installeren.

Als er een nieuwere versie van het programma op de servers wordt gevonden, dan kunt u het downloaden. Als u de download annuleert, wordt de instellingenwizard gestart om de huidige versie te installeren. Als u besluit een nieuwere versie te installeren, worden de installatiebestanden naar uw computer gedownload en wordt de instellingenwizard automatisch gestart om de nieuwere versie te installeren. Voor meer informatie over de installatie van een nieuwere versie raadpleegt u de documentatie van de overeenkomstige programmaversie.

STAP 3. BEGROETINGSVENSTER VAN DE WIZARD

Als uw systeem aan alle vereisten voldoet (zie de sectie *Systeemvereisten voor hardware en software* op pagina 15), of als er op de updateservers van Kaspersky Lab geen nieuwere versie van het programma is gevonden, of als u de installatie van een dergelijke nieuwere versie hebt geannuleerd, wordt de instellingenwizard gestart om de huidige versie van het programma te installeren. Op het scherm verschijnt dan het eerste dialoogvenster van de instellingenwizard met informatie over het starten van de programma-installatie op uw computer.

Klik op de knop **Volgende** om de installatie voort te zetten. Klik op de knop **Annuleren** om de installatie te beëindigen.

STAP 4. DE LICENTIEOVEREENKOMST BEKIJKEN

Het volgende dialoogvenster van de wizard bevat de licentieovereenkomst tussen u en Kaspersky Lab. Lees deze aandachtig door, en als u akkoord gaat met alle voorwaarden en bepalingen van de overeenkomst, selecteert u **Ik ga akkoord met de inhoud van de licentieovereenkomst** en klikt u op de knop **Volgende**. De installatie wordt voortgezet.

Klik op de knop **Annuleren** om de installatie te beëindigen.

STAP 5. HET INSTALLATIETYPE SELECTEREN

Tijdens deze stap kunt u het gewenste installatietype selecteren:

- **Snelle installatie.** Als u deze optie selecteert, wordt het gehele programma op uw computer geïnstalleerd met de beveiligingsinstellingen die door Kaspersky Lab-experts worden aanbevolen. Wanneer de installatie is voltooid, wordt de wizard voor programma-installatie gestart.
- **Aangepaste installatie** In dit geval kunt u selecteren welke programmacomponenten u op uw computer wilt installeren, opgeven in welke map het programma moet worden geïnstalleerd (zie de sectie Stap 6. De installatiemap selecteren op pagina 46), het programma activeren en het met een speciale wizard configureren.

Als u de eerste optie selecteert, gaat de wizard voor programma-installatie direct naar stap 8 (zie de sectie Stap 8. Naar andere antivirusprogramma's zoeken op pagina 47). Selecteert u de tweede optie, dan moet u bij elke stap van de installatie gegevens invoeren of bevestigen.

STAP 6. DE INSTALLATIEMAP SELECTEREN

Opmerking

Deze stap van de installatiewizard wordt alleen uitgevoerd als u de optie Aangepaste installatie hebt geselecteerd (zie de sectie Stap 5. Het installatietype selecteren op pagina 45).

Tijdens deze stap kunt u opgeven in welke map op uw computer het programma moet worden geïnstalleerd. Het standaardpad is:

- <Schijf> \ Programmabestanden \ Kaspersky Lab \ Kaspersky Internet Security 2009 – voor 32-bits systemen.
- <Schijf> \ Programmabestanden (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009 – voor 64-bits systemen.

U kunt een andere map opgeven door op de knop **Bladeren** te klikken en een map in het standaarddialoogvenster voor mapselectie te kiezen, of het pad ernaar in het toepasselijke veld in te voeren.

Belangrijk!

Let er bij het handmatig invoeren van het volledige pad naar de installatiemap op dat het niet meer dan 200 tekens lang mag zijn en geen speciale tekens mag bevatten.

Klik op de knop **Volgende** om de installatie voort te zetten.

STAP 7. TE INSTALLEREN PROGRAMMACOMPONENTEN SELECTEREN

Opmerking Deze stap van de installatiewizard wordt alleen uitgevoerd als u de optie Aangepaste installatie hebt geselecteerd (zie de sectie Stap 5. Het installatietype selecteren op pagina 45).

Bij een aangepaste installatie moet u selecteren welke programmacomponenten u op uw computer wilt installeren. Standaard zijn alle programmacomponenten voor installatie geselecteerd: beschermings-, scan- en updatecomponenten.

Aan de hand van korte informatie over elke component kunt u beslissen welke componenten u niet wilt installeren. Hiervoor selecteert u de component in de lijst, en leest u de bijbehorende informatie in het veld eronder. De informatie omvat een korte beschrijving van de component, en hoeveel vrije hardeschijfruimte voor de installatie is vereist.

Als u de installatie van een onderdeel wilt annuleren, opent u het contextmenu door op het pictogram naast de naam van het onderdeel te klikken, en selecteert u vervolgens het item **Onderdeel zal niet beschikbaar zijn**. Let erop dat als u de installatie van een component annuleert, u niet beschermd bent tegen een aantal gevaarlijke programma's.

Voor selectie van een component die u wilt installeren, opent u het contextmenu door op het pictogram naast de naam van de component te klikken. Selecteer vervolgens **Component wordt geïnstalleerd op de harde schijf**.

Wanneer u de gewenste componenten voor installatie hebt geselecteerd, klikt u op de knop **Volgende**. Klik op de knop **Verwijder** om terug te gaan naar de lijst met componenten die standaard worden geïnstalleerd.

STAP 8. NAAR ANDERE ANTIVIRUSSOFTWARE ZOEKEN

Tijdens deze stap zoekt de wizard naar andere antivirusprogramma's, waaronder Kaspersky Lab-programma's, die misschien conflicteren met het programma dat wordt geïnstalleerd.

Als dergelijke programma's op uw computer worden gedetecteerd, wordt de lijst van die programma's op het scherm weergegeven. U krijgt de optie ze te verwijderen voordat u de installatie voortzet.

Via de knoppen onder de lijst met gedetecteerde antivirusprogramma's kunt u kiezen of u ze automatisch of handmatig wilt verwijderen.

Als de lijst met gedetecteerde antivirusprogramma's het programma Kaspersky Lab 7.0 bevat, slaat u het sleutelbestand op dat voor dit programma wordt gebruikt, wanneer u het programma verwijdert. U kunt dit sleutelbestand voor de nieuwe versie van het programma gebruiken. Het is ook raadzaam objecten in quarantaine en back-upobjecten op te slaan; deze objecten worden automatisch

naar de quarantaine van de nieuwe versie verplaatst, en u kunt ze na de installatie beheren.

Bij automatische verwijdering van versie 7.0 wordt informatie over de activering ervan door het programma opgeslagen, en vervolgens tijdens de installatie van versie 2009 gebruikt.

Belangrijk!

Het programma ondersteunt sleutelbestanden voor versie 6.0 en 7.0. Sleutels die door programmaversie 5.0 worden gebruikt, worden niet ondersteund.

Klik op de knop **Volgende** om de installatie voort te zetten.

STAP 9. LAATSTE VOORBEREIDING OP DE INSTALLATIE

Tijdens deze stap kunt u de laatste voorbereidingen treffen voor de installatie op uw computer.

Het is raadzaam het vakje **Zelfbescherming inschakelen voor het installeren** geselecteerd te laten tijdens de oorspronkelijke installatie. Als de optie voor modulebeveiliging is ingeschakeld en er tijdens de installatie een fout optreedt, kan de installatie correct worden teruggedraaid. Wanneer u de installatie opnieuw uitvoert, is het raadzaam dit vakje uit te schakelen.

Opmerking

Bij een externe installatie van het programma via **Remote Desktop** is het raadzaam het vakje **Zelfbescherming inschakelen voor het installeren** uit te schakelen. Is dit vakje geselecteerd, dan wordt de installatie misschien incorrect of helemaal niet uitgevoerd.

Klik op de knop **Volgende** om de installatie voort te zetten. Er worden dan installatiebestanden naar uw computer gekopieerd.

Belangrijk!

Tijdens het installatieproces wordt de huidige netwerkverbinding verbroken als het programmapakket componenten bevat voor het onderscheppen van netwerkverkeer. De meeste verbroken verbindingen worden na een tijdje weer hersteld.

STAP 10. DE INSTALLATIE VOLTOOIEN

Het venster **Installatie voltooid** bevat informatie over het voltooiën van de programma-installatie op uw computer.

Als u de computer opnieuw moet starten om de installatie correct te kunnen voltooiën, wordt er een overeenkomstige melding op het scherm weergegeven. Nadat het systeem opnieuw is gestart, wordt de instellingenwizard automatisch gestart.

Als het niet nodig is het systeem opnieuw te starten om de installatie te kunnen voltooiën, klikt u op de knop **Volgende** om de wizard voor programma-configuratie te starten.

PROGRAMMA-INTERFACE

Het programma heeft een vrij eenvoudige en gebruiksvriendelijke interface. In deze sectie wordt uitgebreid ingegaan op de basisonderdelen van de interface.

Behalve de hoofdinterface zijn er plug-ins voor Microsoft Office Outlook (virusscans en spamverwerking), Microsoft Outlook Express (Windows Mail), The Bat! (virusscans en spamverwerking), Microsoft Internet Explorer en Microsoft Windows Verkenner. De plug-ins breiden de functionaliteit van de bovengenoemde programma's uit door de gebruiker in staat te stellen de componenten Anti-Virus voor e-mail en Anti-Spam via de interface te beheren en configureren.



IN DEZE SECTIE:

Systeemvakpictogram	50
Contextmenu	51
Hoofdvenster van het programma	53
Meldingen	56
Venster voor het configureren van programma-instellingen	56

SYSTEEMVAKPICTOGRAM

Direct na de installatie van het programma wordt het programmapictogram weergegeven in het systeemvak van Microsoft Windows.

Dit pictogram geeft aan dat het programma wordt uitgevoerd. Het geeft de beschermingsstatus weer en toont een aantal basisfuncties die het programma uitvoert.

Als het pictogram actief is  (gekleurd), wordt de volledige bescherming of een aantal van de componenten uitgevoerd. Als het pictogram inactief is  (zwart-wit), zijn alle beschermingscomponenten uitgeschakeld.

Het programmapictogram verandert afhankelijk van de bewerking die wordt uitgevoerd:



– e-mails worden gescand.



– scripts worden gescand.



– bestanden worden gescand - scan van een bestand dat wordt geopend, opgeslagen of uitgevoerd (door uzelf of door een programma), is in voortgang.



– databases en programmamodules worden bijgewerkt.



– computer moet opnieuw worden gestart om updates toe te passen.




– er is een fout opgetreden in een component van Kaspersky Internet Security.

Het pictogram geeft u ook toegang tot de basisonderdelen van de interface: het contextmenu (zie de sectie Contextmenu op pagina 51) en het hoofdvenster (zie de sectie Hoofdprogrammavenster op pagina 53).

U opent het contextmenu door met de rechtermuisknop op het programmapictogram te klikken.

U opent het hoofdvenster van het programma door op het programmapictogram te dubbelklikken. Het hoofdvenster wordt altijd met de sectie **Bescherming** geopend.

Als er nieuws beschikbaar is van Kaspersky Lab, verschijnt dit pictogram in het systeemvak van de taakbalk . Dubbelklik op het pictogram om het nieuws te bekijken in het venster dat wordt geopend.

CONTEXTMENU

Vanuit het contextmenu kunt u primaire beschermingstaken uitvoeren.

Het programmamenu bevat de volgende opties:

- **Scan mijn computer** - hiermee start u een volledige scan van de computer op gevaarlijke objecten. Alle schijven, met inbegrip van de verwisselbare opslagmedia, worden gescand.

- **Virusscan** - Selecteer objecten en start een virusscan. De lijst bevat standaard een aantal objecten, zoals de map **Mijn documenten** en postvakken. U kunt deze lijst aanvullen door te scannen objecten te selecteren en een virusscan starten.
- **Update** - hiermee start u de programmamodule en database-updates en installeert u updates op uw computer.
- **Netwerkbeheer** – bekijk de lijst met tot stand gebrachte netwerkverbindingen, open poorten en verkeer.
- **Blokkeer netwerkverkeer** – Blokkeer tijdelijk alle netwerkverbindingen van de computer. Als u de computer in staat wilt stellen met het netwerk te communiceren, selecteert u dit item opnieuw in het contextmenu.
- **Virtueel toetsenbord** - hiermee schakelt u naar het virtuele toetsenbord.
- **Activeren** - Hiermee activeert u het programma. Als u de status van een geregistreerd gebruiker wilt verkrijgen, moet u uw programma activeren. Deze menuoptie is alleen beschikbaar als het programma niet actief is.
- **Instellingen** - hiermee bekijkt en configureert u de programma-instellingen.
- **Kaspersky Internet Security** - hiermee opent u het hoofdvenster (zie de sectie Hoofdprogrammavenster op pagina 53).
- **Bescherming pauzeren/hervatten** - hiermee schakelt u de realtime-beveiligingscomponenten tijdelijk uit of in. Deze menuoptie heeft geen invloed op programma-updates of virusscantaken.
- **Over** - hiermee geeft u een venster weer met informatie over het programma.

- **Sluiten** - hiermee sluit u het programma (wanneer deze optie is geselecteerd, wordt het programma uit het RAM van de computer gehaald).



Afbeelding 1: Contextmenu

Als u het contextmenu opent terwijl een virusscantaak wordt uitgevoerd, worden de naam en voortgangsstatus (percentage voltooid) van deze taak weergegeven in het contextmenu. Wanneer u de taak selecteert, kunt u naar het hoofdvenster gaan waar een rapport over de huidige resultaten van de uitvoering wordt weergegeven.

HOOFDVENSTER VAN HET PROGRAMMA

Het hoofdvenster bestaat uit drie delen.

- Het bovenste gedeelte van het venster geeft de huidige beveiligingsstatus van uw computer aan.

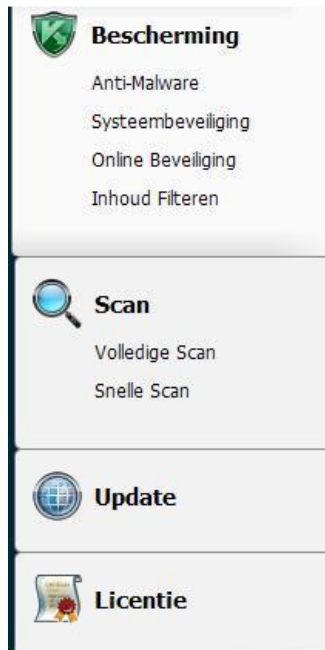


Afbeelding 2: Huidige status van de computerbeveiliging

Er zijn drie beveiligingsstatussen mogelijk, die alledrie met een bepaalde kleur worden aangeduid, vergelijkbaar met verkeerslichten. Groen betekent dat de bescherming van uw computer op het juiste niveau is, geel en rood waarschuwen over de aanwezigheid van een aantal beveiligingsbedreigingen in de instellingenconfiguratie of de uitvoering van het programma. Behalve malwareprogramma's omvatten bedreigingen bijvoorbeeld ook verouderde programmadatabases, een aantal uitgeschakelde beschermingscomponenten, of selectie van minimale programma-instellingen.

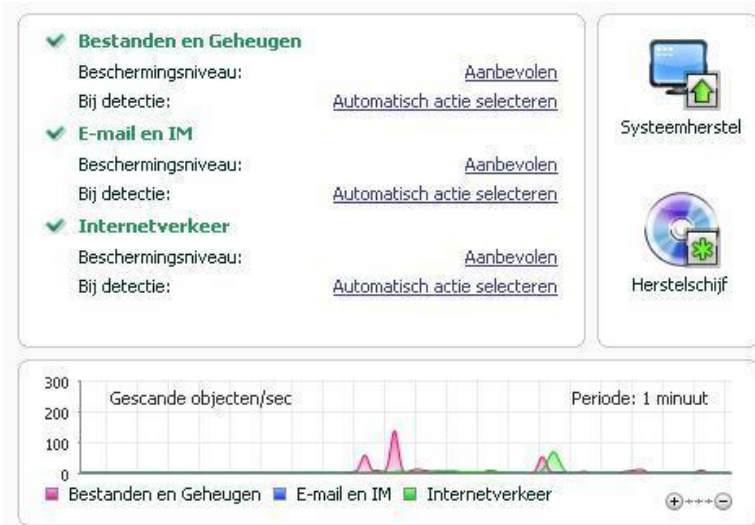
De beveiligingsbedreigingen moeten worden geëlimineerd zodra ze zich voordoen. Gebruik de koppeling **Nu repareren** (zie bovenstaande afbeelding) voor uitgebreide informatie over deze bedreigingen en hoe u ze snel kunt elimineren.

- Het linkerdeel van het venster - de navigatiebalk - wordt gebruikt om snel te schakelen tussen programmafuncties, antivirusscans, updatetaken, enzovoort.



Afbeelding 3: Navigatiebalk

- Het rechterdeel bevat informatie over de programmafunctie die in het linkerdeel is geselecteerd en wordt gebruikt om instellingen voor deze functie te configureren. Verder bevat dit gedeelte tools voor het uitvoeren van virusscantaken, het downloaden van updates, enzovoort.



Afbeelding 4: Informatief gedeelte van het hoofdvenster

U kunt ook de volgende knoppen gebruiken:

- **Instellingen** - hiermee schakelt u naar de programma-instellingen.
- **Help** - hiermee schakelt u naar het Help-systeem van het programma.
- **Gedetecteerd** - hiermee schakelt u naar de lijst met schadelijke objecten die zijn gedetecteerd als gevolg van de uitvoering van een component of een voltooide antivirusscan, en kunt u de gedetailleerde statistieken van de uitvoeringsresultaten van het programma bekijken.
- **Rapporten** - hiermee schakelt u naar de lijst met gebeurtenissen die plaatsvonden tijdens de uitvoering van het programma.
- **Ondersteuning** - hiermee opent u het venster met informatie over het systeem en koppelingen naar de informatiebronnen van Kaspersky Lab (technische-ondersteuningswebsite, forum).

Opmerking

U kunt de weergave van het programma veranderen door uw eigen afbeeldingen en kleurenschema's te creëren en te gebruiken.

MELDINGEN

Als er zich tijdens het gebruik van het programma gebeurtenissen voordoen, worden boven het programmapictogram in de Microsoft Windows-taakbalk speciale schermmeldingen in de vorm van pop-upberichten weergegeven.

Afhankelijk van hoe kritiek de gebeurtenis is voor de veiligheid van uw computer, kunt u de volgende soorten meldingen ontvangen:

- **Alarm.** Er heeft een kritieke gebeurtenis plaatsgevonden; er is bijvoorbeeld een virus of gevaarlijke activiteit op uw systeem gedetecteerd. U moet direct beslissen hoe hierop moet worden gereageerd. Dit type meldingen is rood.
- **Belangrijk!** Er heeft zich een potentieel gevaarlijke gebeurtenis voorgedaan. Er zijn bijvoorbeeld potentieel geïnfecteerde bestanden of verdachte activiteiten op uw systeem gedetecteerd. U moet bepalen hoe ernstig deze gebeurtenis naar uw mening is, en het programma dienovereenkomstig laten reageren. Dit type meldingen is geel.
- **Opmerking:** Deze melding informeert u over gebeurtenissen die niet kritiek zijn. Dit soort meldingen heeft bijvoorbeeld betrekking op de uitvoering van de component **Inhoud filteren**. Informatiemeldingen zijn groen.

VENSTER VOOR HET CONFIGUREREN VAN PROGRAMMA-INSTELLINGEN

Het venster met programma-instellingen kan worden geopend via het hoofdvenster (zie de sectie Hoofdprogrammavenster op pagina 53) of via het contextmenu (zie de sectie Contextmenu op pagina 51) van het programma. Als u dit venster wilt oproepen, klikt u op de koppeling **Instellingen** in het bovenste gedeelte van het hoofdvenster, of selecteert u een toepasselijke optie in het contextmenu.

Het instellingenvenster bestaat uit twee delen:

- Via het linkerdeel kunt u toegang krijgen tot de programma-componenten, virusscantaken, updatetaken enzovoort.
- Het rechterdeel van het venster bevat een gedetailleerde lijst met instellingen voor het item (bijvoorbeeld een component of taak) dat in het linkerdeel is geselecteerd.

AAN DE SLAG

Met Kaspersky Internet Security wilde Kaspersky Lab vooral optimale configuratie voor alle programmaopties bieden. Zo kan iedereen, met of zonder computerkennis, zijn of haar computer snel beveiligen, onmiddellijk na installatie zonder uren aan de instellingen te hoeven besteden.

Voor het gemak van de gebruiker hebben we de voorbereidende configuratiestappen gecombineerd in de Instellingenwizard, die van start gaat zodra het programma geïnstalleerd is. Wanneer u de instructies van de wizard volgt, kunt u het programma activeren, de instellingen voor updates configureren, de toegang tot het programma beperken met behulp van een wachtwoord, en andere instellingen uitvoeren.

Uw computer kan met malware geïnfecteerd worden, voordat het programma geïnstalleerd wordt. Voer een computerscan uit om malwareprogramma's te detecteren (zie de sectie De computer op antivirus scannen op pagina 61).

Als gevolg van de malwarewerking en systeemuitval kunnen de instellingen van uw computer beschadigd zijn. Voer de wizard Beveiligingsanalyse uit om de zwakke punten van de geïnstalleerde software en fouten in de systeeminstellingen te detecteren.

De databases die standaard meegeleverd worden in het databasepakket, kunnen verouderd zijn. Start de programma-update (als dit nog niet via de instellingenwizard of automatisch onmiddellijk na de installatie is gebeurd).

De component Anti-Spam die in de programmastructuur opgenomen is, gebruikt een zelflerend algoritme om ongewenste berichten te detecteren. Start de wizard Anti-Spam training om de component zodanig te configureren dat deze met uw correspondentie kan werken.

Nadat de hierboven beschreven acties voltooid zijn, is het programma gebruiksklaar. Via de wizard Beveiligingsbeheer kunt u het beschermingsniveau van uw computer beoordelen (zie de sectie Beveiligingsbeheer op pagina 63).

IN DEZE SECTIE:

Een netwerktype selecteren	59
Het programma updaten.....	60
Beveiligingsanalyse	60
Uw computer scannen op virussen.....	61
Deelname aan het Kaspersky Security Network.....	62
Beveiligingsbeheer	63
Bescherming pauzeren.....	65

EEN NETWERKTYPE SELECTEREN

Na installatie van het programma analyseert de component Firewall de actieve netwerkverbindingen op uw computer. Elke netwerkverbinding krijgt een status toegewezen die de toegestane netwerkactiviteiten bepaalt.

Als u de interactieve modus van Kaspersky Internet Security hebt geselecteerd, wordt er een melding weergegeven telkens wanneer er een netwerkverbinding tot stand is gebracht. In het meldingsvenster kunt u de status voor nieuwe netwerken selecteren:

- Openbaar netwerk - voor netwerkverbindingen met deze status is toegang tot uw computer van buitenaf niet toegestaan. Voor deze netwerken is toegang tot openbare mappen en printers toegestaan. Deze status kan het beste aan het internetnetwerk worden toegewezen.
- Lokaal netwerk - voor de netwerkverbindingen met deze status is toegang tot openbare mappen en netwerkprinters toegestaan. Het is raadzaam deze status aan beschermde lokale netwerken toe te wijzen, zoals een bedrijfsnetwerk.
- Vertrouwd netwerk - voor netwerkverbindingen met deze status zijn alle activiteiten toegestaan. Het is raadzaam deze status alleen aan absoluut beveiligde zones toe te wijzen.

Voor elke netwerkstatus levert Kaspersky Internet Security de set regels waarmee de netwerkactiviteiten beheerd kunnen worden. U kunt de opgegeven netwerkstatus later wijzigen wanneer deze voor het eerst gedetecteerd wordt.

HET PROGRAMMA UPDATEN

Belangrijk!

U hebt een internetverbinding nodig om Kaspersky Internet Security te kunnen updaten.

Kaspersky Internet Security bevat databases die definities van bedreigingen bevat, voorbeelden van uitdrukkingen die kenmerkend zijn voor spam, en beschrijvingen van netwerkaanvallen. Het kan echter zijn dat de databases verouderd zijn wanneer het programma geïnstalleerd wordt, aangezien Kaspersky Lab databases en programmamodules regelmatig bijwerkt.

U kunt de updatemodus selecteren wanneer u de wizard voor de programma-instellingen uitvoert. Kaspersky Internet Security controleert standaard automatisch voor updates op de servers van Kaspersky Lab. Als de server een nieuwe set updates heeft, worden deze door Kaspersky Internet Security gedownload en in stille modus geïnstalleerd.

Het is raadzaam Kaspersky Anti-Virus onmiddellijk na de installatie te updaten om de bescherming van uw computer up-to-date te houden.

- ▶ Kaspersky Internet Security handmatig updaten:
 1. Open het hoofdvenster van het programma.
 2. Selecteer de sectie **Update** aan de linkerkant.
 3. Klik op de knop **Update**.

Kaspersky Internet Security wordt nu bijgewerkt. Alle details van het proces worden in een speciaal venster weergegeven.

BEVEILIGINGSANALYSE

Als gevolg van ongewenste activiteiten op uw computer die het gevolg kunnen zijn van systeemuitval of de activiteiten van malware, kunnen de instellingen van

uw besturingssysteem beschadigd raken. Verder kunnen programma's die op uw computer geïnstalleerd zijn, zwakke plekken hebben die door indringers worden gebruikt om schade aan uw computer toe te brengen.

Als u dergelijke beveiligingsproblemen wilt detecteren en elimineren, is het raadzaam de wizard Beveiligingsanalyse te starten nadat u het programma hebt geïnstalleerd. Deze wizard zoekt naar kwetsbaarheden in de geïnstalleerde programma's en naar afwijkende en beschadigde instellingen van het besturingssysteem en de browser.

- ▶ De wizard starten:
 1. Open het hoofdvenster van het programma.
 2. In het linkerdeel van het venster selecteert u **Systeembeveiliging**.
 3. Start de taak **Beveiligingsanalyse**.

UW COMPUTER SCANNEN OP VIRUSSEN

Aangezien ontwikkelaars van malware hun uiterste best doen om de activiteiten van hun programma's te verbergen, merkt u het misschien niet als er malwareprogramma's op uw computer staan.

Wanneer het programma op uw computer is geïnstalleerd, wordt automatisch de taak **Snelle scan** op uw computer uitgevoerd. Hiermee worden schadelijke programma's in objecten die bij het starten van het systeem zijn geladen, opgezocht en geneutraliseerd.

Kaspersky Lab raadt ook aan de taak **Volledige scan** uit te voeren.

- ▶ U start/stopt een virusscantaak als volgt:
 1. Open het hoofdvenster van het programma.
 2. In het linkerdeel van het venster selecteert u de sectie **Scannen (Volledige scan, Snelle scan)**.
 3. Klik op **Start scannen** om van start te gaan. Als u de taak wilt stoppen, klikt u op **Stop scannen** terwijl de taak wordt uitgevoerd.

DEELNAME AAN HET KASPERSKY SECURITY NETWORK

Elke dag steken overal ter wereld legio nieuwe bedreigingen de kop op. Kaspersky Lab biedt u toegang tot de Kaspersky Security Network-service, waarmee gemakkelijker statistieken over nieuwe typen bedreigingen en hun bron kunnen worden verzameld, en een eliminatiemethode kan worden ontwikkeld.

Bij gebruik van Kaspersky Security Network worden de volgende gegevens naar Kaspersky Lab verzonden:

- De unieke ID die door het programma aan uw computer is toegewezen. Deze ID geeft de hardware-instellingen van uw computer en bevat geen informatie.
- Informatie over bedreigingen die door de programmacomponenten zijn gedetecteerd. De structuur en inhoud van de informatie zijn afhankelijk van het type bedreiging dat is gedetecteerd.
- Systeeminformatie: versie van besturingssysteem, geïnstalleerde servicepakketten, downloadbare services en stuurprogramma's, browser- en mailclientversies, browserextensies, aantal geïnstalleerde Kaspersky Lab-programma's.

Kaspersky Security Network verzamelt ook extra statistieken met informatie over:

- uitvoerbare bestanden en ondertekende programma's die op uw computer zijn gedownload.
- programma's die op uw computer worden uitgevoerd.

De statistieken worden verstuurd wanneer de programma-update voltooid is.

Belangrijk!

Kaspersky Lab garandeert dat er geen persoonlijke gegevens van gebruikers binnen het Kaspersky Security Network worden verzameld en gedistribueerd.

► *De instellingen configureren voor het verzenden van statistieken:*

1. Open het instellingenvenster van het programma.
2. Selecteer de sectie **Feedback** aan de linkerkant.

3. Schakel het vakje **Ik stem toe te participeren in het Kaspersky Security Network** in om uw deelname aan het netwerk te bevestigen. Schakel het vakje **Ik stem toe om uitgebreide statistieken te versturen binnen het kader van Kaspersky Security Network** in om uw toestemming te bevestigen.

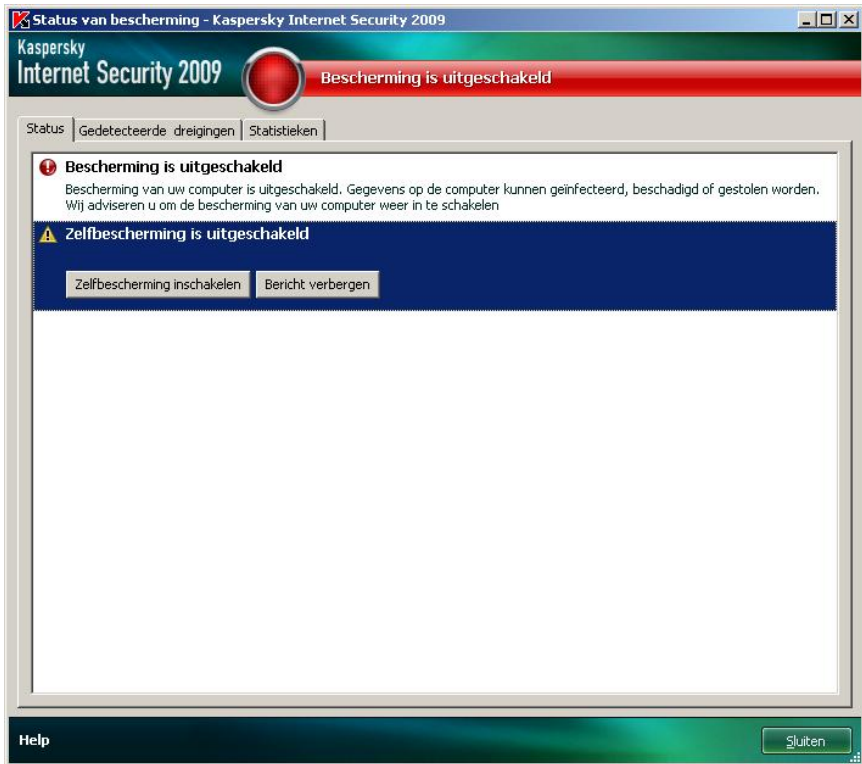
BEVEILIGINGSBEHEER

Problemen in de beveiliging van uw computer worden weergegeven in het hoofdvenster van het programma. U kunt de status van de computerbeveiliging aflezen aan de kleur van het beveiligingsstatuspictogram en het deelvenster waarin dit pictogram zich bevindt. In geval van problemen in het beschermingssysteem raden wij aan deze onmiddellijk te verhelpen.



Afbeelding 5: Huidige status van de computerbeveiliging

In het venster **Beveiligingsproblemen oplossen** (zie onderstaande afbeelding) dat u oproept via de koppeling **Nu repareren**, kunt u een lijst met opgetreden problemen zien, evenals hun beschrijving en mogelijke oplossingen.



Afbeelding 6: Beveiligingsproblemen oplossen

U kunt de lijst met bestaande problemen weergeven. Problemen worden weergegeven naar gelang van hun urgentie: eerst de meest kritieke problemen, dat wil zeggen de problemen met het rode statuspictogram, dan de minder belangrijke problemen, gemarkeerd met het gele statuspictogram, en ten slotte de informatieve berichten. Voor elk probleem wordt een gedetailleerde beschrijving gegeven en de volgende bewerkingen zijn beschikbaar:

- *Dreiging onmiddellijk verwijderen.* Met behulp van de toepasselijke knoppen kunt u het probleem verhelpen (raadzaam).
- *Uitschakelen van dreiging uitstellen.* Als het probleem om een of andere reden niet direct kan worden verholpen, kunt u ervoor kiezen dit later te doen. Klik hiervoor op de knop **Verberg dit bericht**.

Deze optie is niet beschikbaar voor ernstige problemen, bijvoorbeeld problemen met betrekking tot schadelijke objecten die niet zijn gedesinfecteerd, crashes van een of meer componenten, of beschadiging van de programmabestanden.

Als u de verborgen berichten opnieuw in de algemene lijst wilt weergeven, schakelt u het vakje **Toon verborgen berichten** in.

BESCHERMING PAUZEREN

Het pauzeren van realtime-bescherming betekent het tijdelijk uitschakelen van alle beschermingscomponenten.

- ▶ De bescherming van uw computer pauzeren:
 1. Selecteer de optie **Bescherming pauzeren** in het contextmenu van het programma (zie de sectie Contextmenu op pagina 51).
 2. In het venster **Bescherming pauzeren** dat wordt geopend, selecteert u de tijdsperiode waarna de bescherming weer ingeschakeld moet worden:
 - **Na <tijdsinterval>** - de bescherming wordt ingeschakeld nadat het opgegeven tijdsinterval is verstreken. Selecteer de waarde voor het tijdsinterval in het vervolgkeuzemenu.
 - **Na herstarten** – bescherming wordt ingeschakeld nadat het systeem opnieuw is gestart (mits de modus voor programmastart bij het opstarten van de computer is ingeschakeld).
 - **Handmatig** – bescherming kan alleen handmatig worden ingeschakeld. Als u bescherming wilt inschakelen, selecteert u **Bescherming hervatten** in het contextmenu van het programma.

Wanneer u de bescherming tijdelijk uitschakelt, worden alle beschermingscomponenten gepauzeerd. Dit wordt aangegeven door:

- Inactieve (grijze) benamingen van de uitgeschakelde componenten in de sectie **Bescherming** van het hoofdvenster.
- Inactief (grijs) programmapictogram (zie de sectie Pictogram in systeemvak op pagina 50) in het systeemvenster.
- Het rode statuspictogram en het rode hoofdvenster van het programma.

Als er actieve netwerkverbindingen zijn op het moment dat de bescherming wordt gepauzeerd, wordt er een bericht weergegeven dat deze verbindingen worden verbroken.

PROGRAMMA-INSTELLINGEN VALIDEREN

Nadat het programma is geïnstalleerd en geconfigureerd, kunt u controleren of de installatie en configuratie correct zijn uitgevoerd aan de hand van een testvirus en variaties daarvan. Er wordt een aparte test uitgevoerd voor alle beschermingscomponenten/-protocollen.

IN DEZE SECTIE:

Het EICAR-testvirus en variaties ervan	67
De bescherming van HTTP-verkeer testen	71
De bescherming van SMTP-verkeer testen	72
Instellingen van Anti-Virus voor bestanden valideren	73
Instellingen voor virusscantaken valideren	73
Anti-Spam-instellingen valideren	74

HET EICAR-TESTVIRUS EN VARIATIES ERVAN

Dit testvirus is speciaal ontwikkeld door EICAR  (The European Institute for Computer Antivirus Research) voor het testen van antivirusproducten.

Het testvirus IS GEEN VIRUS en bevat geen programmacode die schadelijk is voor uw computer. De meeste antivirusprogramma's zullen het echter als een virus identificeren.

Belangrijk!

Gebruik nooit echte virussen om de functionaliteit van een antivirusprogramma te testen.

U kunt het testvirus downloaden van de officiële EICAR-website:
http://www.eicar.org/anti_virus_test_file.htm.

Opmerking

Voordat u het bestand downloadt, moet u de antivirusbeveiliging uitschakelen, omdat het programma het bestand *anti_virus_test_file.htm* anders zal identificeren en verwerken als geïnfecteerd object dat via HTTP-protocol is overgedragen.

Vergeet niet de antivirusbescherming na het downloaden van het testvirus onmiddellijk weer in te schakelen.

Het programma identificeert de bestanden die van de **EICAR**-site zijn gedownload, als geïnfecteerd object met een virus dat **niet kan worden schoongemaakt**, en voert acties uit die voor een dergelijk object zijn opgegeven.

U kunt ook variaties van het standaardtestvirus gebruiken om de werking van het programma te controleren. Hiervoor wijzigt u de inhoud van het standaardvirus door er een van de voorvoegsels aan toe te voegen (zie de onderstaande tabel). Als u varianten van het testvirus wilt maken, kunt u een willekeurige tekst- of hypertexteditor gebruiken, zoals **Microsoft Kladblok** en **UltraEdit32**.

Belangrijk!

U kunt de werking van het antivirusprogramma alleen met het aangepaste EICAR-virus testen als uw antivirusdatabases voor het laatst zijn bijgewerkt op of na 24 oktober 2003 (cumulatieve updates tot en met oktober 2003).

De eerste kolom bevat de voorvoegsels die moeten worden toegevoegd aan het begin van de string voor een standaardtestvirus. In de tweede kolom worden alle mogelijke waarden van de status weergegeven die het antivirusprogramma op basis van de scanresultaten aan het object toewijst. De derde kolom geeft informatie over de manier waarop objecten met de desbetreffende status door het programma worden verwerkt. Welke bewerkingen op de objecten worden uitgevoerd, is afhankelijk van de programma-instellingen.

Nadat u het voorvoegsel aan het testvirus hebt toegevoegd, slaat u het nieuwe bestand onder een andere naam op, bijvoorbeeld *ecar_dele.com*. Geef alle gewijzigde 'virussen' een gelijksoortige naam.

1.

tabel 6. Variaties van het testvirus

Voorvoegsel	Objectstatus	Informatie over objectverwerking
Geen voorvoegsel, standaard-testvirus	Geïnfecteerd. Geïnfecteerd object bevat code van een bekend virus. Desinfectie is onmogelijk.	Het object wordt door het programma aangemerkt als niet-desinfecteerbaar. Pogingen om het object te desinfecteren resulteren in een foutmelding. De bewerking die voor niet-desinfecteerbare objecten is ingesteld, wordt toegepast.
CORR-	Beschadigd.	Het object is toegankelijk maar kan niet door het programma worden gescand omdat het beschadigd is (de bestandsstructuur is bijvoorbeeld beschadigd of het bestandsformaat is ongeldig). Informatie over de objectverwerking kunt u vinden in het rapport over de programmawerking.
WARN-	Verdacht. Verdacht object bevat code van een onbekend virus. Desinfectie is onmogelijk.	Het object is als verdacht aangeduid door de heuristische analyzer. Op het moment van detectie bevatten de Anti-Virus-databases geen omschrijving van de procedure voor behandeling van dit object. U ontvangt een melding wanneer een dergelijk object wordt gedetecteerd.

Voorvoegsel	Objectstatus	Informatie over objectverwerking
SUSP-	<p>Verdacht. Verdacht object bevat gewijzigde code van een bekend virus. Desinfectie is onmogelijk.</p>	<p>Het programma heeft gedetecteerd dat een sectie van de programmacode van het object overeenkomt met een sectie van de programmacode van een bekend virus. Op het moment van detectie bevatten de Anti-Virus-databases geen omschrijving van de procedure voor behandeling van dit object. U ontvangt een melding wanneer een dergelijk object wordt gedetecteerd.</p>
ERRO-	<p>Scanfout:</p>	<p>Er is een fout opgetreden tijdens het scannen van een object. Het object kan niet door het programma worden geopend: de integriteit van het object is geschonden (bijvoorbeeld een archief met meerdere volumes zonder einde van archief) of er is geen verbinding met het object (als het gescande object zich op een netwerkstation bevindt). Informatie over de objectverwerking kunt u vinden in het rapport over de programmawerking.</p>
CURE-	<p>Geïnfecteerd. Geïnfecteerd object bevat code van een bekend virus. Desinfecteerbaar.</p>	<p>Het object bevat een virus dat onschadelijk kan worden gemaakt. Het programma maakt het object schoon. De tekst van het virus wordt vervangen met het woord CURE. U ontvangt een melding wanneer een dergelijk object wordt gedetecteerd.</p>

Voorvoegsel	Objectstatus	Informatie over objectverwerking
DELE-	Geïnficeerd. Geïnficeerd object bevat code van een bekend virus. Desinfectie is onmogelijk.	Het object wordt door het programma aangemerkt als niet-desinfecteerbaar. Pogingen om het object te desinfecteren resulteren in een foutmelding. De bewerking die voor niet-desinfecteerbare objecten is ingesteld, wordt toegepast. U ontvangt een melding wanneer een dergelijk object wordt gedetecteerd.

DE BESCHERMING VAN HTTP-VERKEER TESTEN

- ▶ Het kan gebeuren dat de gegevensstroom die via het HTTP-protocol wordt overgebracht, virussen bevat. U controleert als volgt of dergelijke virussen worden gedetecteerd:

Download het testvirus op de officiële EICAR-website:
http://www.eicar.org/anti_virus_test_file.htm.

Wanneer u probeert het testvirus te downloaden, wordt dit object door Kaspersky Internet Security gedetecteerd en aangemerkt als een geïnficeerd object dat niet kan worden gedesinfecteerd. Vervolgens wordt de bewerking uitgevoerd die in de HTTP-verkeersinstellingen voor dit objecttype is opgegeven. Wanneer u het testvirus probeert te downloaden, wordt de verbinding met de website standaard verbroken en ziet u een browserbericht met de mededeling dat dit object is besmet met het EICAR-virustestbestand.

DE BESCHERMING VAN SMTP- VERKEER TESTEN

Als u virussen wilt detecteren in de gegevensstromen die via het SMTP-protocol worden overgebracht, gebruikt u een e-mailsysteem waarin gegevensverkeer door middel van dit protocol wordt geregeld.

Opmerking

Het is raadzaam te testen hoe Kaspersky Internet Security inkomende en uitgaande e-mailberichten verwerkt, inclusief de tekst van het bericht en de bijlagen. Als u wilt testen of virussen in de berichttekst worden gedetecteerd, kopieert u de tekst van het standaardtestvirus of van het aangepaste testvirus naar de berichttekst.

► Dit doet u als volgt:

1. Maak een bericht in de indeling Tekst zonder opmaak met een e-mailprogramma dat op uw computer is geïnstalleerd.

Opmerking

Een bericht met een testvirus wordt niet gescand als het in RTF- of HTML-indeling is gemaakt.

2. Kopieer de tekst van het aangepaste of standaardvirus naar het begin van het bericht of voeg een bestand met het testvirus als bijlage toe aan het bericht.
3. Verzend het bericht naar de beheerder.
4. Lees het bericht dat op dit adres binnenkomt.

Het object wordt door het programma gedetecteerd en als geïnfecteerd aangemerkt, waarna de bewerking wordt uitgevoerd die in de SMTP-verkeersinstellingen voor dit objecttype is geselecteerd. Standaard wordt de verzending van een bericht met een geïnfecteerd object geblokkeerd.

INSTELLINGEN VAN ANTI-VIRUS VOOR BESTANDEN VALIDEREN

- ▶ Als u wilt controleren of Anti-Virus voor bestanden correct is geconfigureerd, gaat u als volgt te werk:
 1. Maak een map op een schijf, kopieer het testvirus dat van de officiële website van de organisatie is gedownload (http://www.eicar.org/anti_virus_test_file.htm), evenals de varianten van het testvirus die u hebt gemaakt.
 2. Sta toe dat alle gebeurtenissen worden gerapporteerd, zodat het rapportbestand gegevens opneemt over beschadigde objecten en objecten die niet werden gescand vanwege fouten.
 3. Voer het testvirus of een variatie hiervan uit.

De aanroep van het bestand wordt geblokkeerd, het bestand wordt gescand en de ingestelde bewerking wordt uitgevoerd. Wanneer u verschillende acties voor toepassing op het gedetecteerde object selecteert, kunt u een volledige controle op de werking van de component uitvoeren.

U kunt informatie over de resultaten van Anti-Virus voor bestanden bekijken in het rapport over de werking van de component.

INSTELLINGEN VOOR VIRUSSCANTAKEN VALIDEREN

- ▶ Als u wilt controleren of virusscantaken correct zijn geconfigureerd, gaat u als volgt te werk:
 1. Maak een map op een schijf, kopieer het testvirus dat van de officiële website van de organisatie is gedownload (http://www.eicar.org/anti_virus_test_file.htm), evenals de varianten van het testvirus die u hebt gemaakt.
 2. Maak een nieuwe virusscantaak en selecteer de map met de set testvirussen als het te scannen object.

3. Sta toe dat alle gebeurtenissen worden gerapporteerd, zodat het rapportbestand gegevens opneemt over beschadigde objecten en objecten die niet werden gescand vanwege fouten.
4. Voer de virusscantaak uit.

Terwijl de scantaak loopt en verdachte of geïnfecteerde objecten worden gedetecteerd, worden de acties uitgevoerd die in de taakinstellingen zijn opgegeven. Wanneer u verschillende acties voor toepassing op het gedetecteerde object selecteert, kunt u een volledige controle op de werking van de component uitvoeren.

U kunt uitgebreide informatie over de resultaten van de taak bekijken in het rapport over de werking van de component.

ANTI-SPAM-INSTELLINGEN VALIDEREN

U kunt de anti-spambescherming testen met een testbericht dat als SPAM is aangeduid.

De tekst van het testbericht moet de volgende regel bevatten:

```
Spam is bad do not send it
```

Nadat dit bericht op de doelcomputer is ontvangen, wordt het door het programma gescand, wordt de spamstatus eraan toegewezen en wordt de actie uitgevoerd die voor dit objecttype is opgegeven.

VERKLARING VOOR GEGEVENSVERZAMELING VAN KASPERSKY SECURITY NETWORK

INLEIDING

LEES DIT DOCUMENT ZORGVULDIG. HET BEVAT BELANGRIJKE INFORMATIE WAARVAN U OP DE HOOGTE MOET ZIJN VOORDAT U VERDERGAAT MET HET GEBRUIK VAN ONZE SERVICES OF SOFTWARE. ALS U GEBRUIK BLIJFT MAKEN VAN DE SOFTWARE EN SERVICES VAN KASPERSKY LAB, WORDT U GEACHT AKKOORD TE ZIJN GEGAAN MET DEZE VERKLARING voor gegevensverzameling van KASPERSKY LAB. We behouden ons het recht voor deze Verklaring voor gegevensverzameling te allen tijde te wijzigen door de wijzigingen op deze pagina te publiceren. Controleer de revisiedatum hieronder om vast te stellen of het beleid is gewijzigd sinds u het voor het laatst hebt ingezien. Als u na publicatie van de bijgewerkte Verklaring voor gegevensverzameling een gedeelte van Kaspersky Labs-services blijft gebruiken, geeft u aan in te stemmen met de wijzigingen.

Kaspersky Lab en zijn dochterondernemingen (hierna samen aangeduid als '**Kaspersky Lab**') hebben deze Verklaring voor gegevensverzameling samengesteld om u te informeren over hun werkwijze voor de verzameling en verspreiding van gegevens voor Kaspersky Anti-Virus en Kaspersky Internet Security.

Bericht van Kaspersky Lab

Kaspersky Lab legt zich erop toe alle klanten superieure service te verlenen en zal zijn uiterste best doen om uw privacy betreffende Gegevensverzameling te waarborgen. We begrijpen dat u misschien vragen hebt over de wijze waarop Kaspersky Security Network informatie en gegevens verzamelt en gebruikt, en hebben deze verklaring opgesteld om u in te lichten over de principes van Gegevensverzameling waaraan Kaspersky Security Network onderworpen is (de '**Verklaring voor gegevensverzameling**' of '**Verklaring**').

Deze Verklaring voor gegevensverzameling bevat vele algemene en technische details over de stappen die we ondernemen om uw privacy betreffende Gegevensverzameling te waarborgen. We hebben deze Verklaring voor

gegevensverzameling ingedeeld op belangrijke processen en gebieden, zodat u de informatie die het interessantst voor u is, snel kunt bekijken. Kortom: we streven er in al onze bezigheden naar om aan uw behoeften en verwachtingen te voldoen, ook wat betreft de bescherming van uw Gegevensverzameling.

De gegevens en informatie worden door Kaspersky Lab verzameld, en als u nadat u deze Verklaring voor gegevensverzameling hebt gelezen, vragen hebt of u zorgen maakt over de Gegevensverzameling, kunt u een e-mail naar support@kaspersky.com sturen.

Wat is Kaspersky Security Network?

Dankzij de Kaspersky Security Network-service wordt identificatie voor gebruikers van Kaspersky Lab-beveiligingsproducten over de hele wereld vergemakkelijkt, en kan er sneller bescherming worden geboden tegen nieuwe beveiligingsrisico's die hun computer aanvallen. Kaspersky Security Network verzamelt geselecteerde beveiligings- en programmeergegevens over potentiële beveiligingsrisico's die uw computer aanvallen, en verzendt die gegevens voor analyse naar Kaspersky Lab om nieuwe bedreigingen en hun bronnen te identificeren, en de gebruikersbeveiliging en productfunctionaliteit te verbeteren. **Dergelijke informatie bevat geen persoonlijk identificeerbare informatie over de gebruiker, en wordt alleen door Kaspersky Lab gebruikt om zijn beveiligingsproducten te verbeteren en oplossingen tegen kwaadaardige bedreigingen en virussen verder te ontwikkelen. Mochten er per ongeluk persoonlijke gegevens van de gebruiker worden verzonden, dan zal Kaspersky Lab deze in overeenstemming met deze Verklaring voor gegevensverzameling bewaren en beschermen.**

Door deel te nemen aan Kaspersky Security Network, leveren u en de andere gebruikers van Kaspersky Lab-beveiligingsproducten over de hele wereld een aanzienlijke bijdrage aan een veiligere internetomgeving.

Wettelijke kwesties

Kaspersky Security Network kan onderworpen zijn aan de wetten van verscheidene rechtsgebieden, omdat zijn services in verschillende rechtsgebieden kunnen worden gebruikt, met inbegrip van de Verenigde Staten van Amerika. Kaspersky Lab zal persoonlijk identificeerbare informatie zonder uw toestemming bekendmaken wanneer dit door de wet wordt vereist, of als we reden hebben te geloven dat een dergelijke actie noodzakelijk is om een onderzoek in te stellen naar schadelijke activiteiten of om de gasten, bezoekers, partners of het eigendom van Kaspersky Lab of anderen te beschermen tegen schadelijke activiteiten. Zoals hierboven wordt vermeld, kunnen wetten betreffende gegevens en informatie die door Kaspersky Security Network zijn verzameld, per land verschillen. Bepaalde persoonlijk identificeerbare informatie die in de Europese Unie en haar lidstaten wordt verzameld, is bijvoorbeeld onderworpen aan de Europese richtlijnen voor persoonlijke gegevens, privacy en

elektronische communicatie, inclusief maar niet beperkt tot richtlijn 2002/58/EC van het Europese parlement en de Raad van 12 juli 2002 inzake de verwerking van persoonlijke gegevens en de bescherming van Privacy in de sector elektronische communicatie en richtlijn 95/46/EC van het Europese parlement en de Raad van 24 oktober 1995 betreffende de bescherming van individuen in verband met de verwerking van persoonlijke gegevens en betreffende het vrije verkeer van die gegevens en de daaropvolgende wetgeving die in de Europese lidstaten werd aangenomen, het Besluit 497/2001/EC van de Europese commissie aangaande standaard contractuele clausules (persoonlijke gegevens die aan derde landen worden verzonden) en de daaropvolgende wetgeving die in de Europese lidstaten werd aangenomen.

Kaspersky Security Network zal de betreffende gebruikers wanneer de bovengenoemde informatie wordt verzameld, naar behoren inlichten over het op enige wijze delen van dergelijke informatie die hoofdzakelijk voor de bedrijfsontwikkeling zal worden gebruikt, en zal deze internetgebruikers online een opt-inoptie (in de Europese lidstaten en andere landen waar de opt-inprocedure verplicht is) of een opt-outoptie (voor alle andere landen) bieden, zodat zij al dan niet toestemming kunnen verlenen voor het commerciële gebruik van deze gegevens en/of voor de verzending van deze gegevens aan derden.

Kaspersky Lab moet op verzoek van gerechtelijke of ordehandhavingsautoriteiten wellicht bepaalde persoonlijk identificeerbare informatie aan toepasselijke overheidsinstanties verstrekken. Wij zullen deze informatie, indien door gerechtelijke of ordehandhavingsautoriteiten verzocht, na ontvangst van de juiste documentatie verstrekken. Kaspersky Lab mag zoals wettelijk is toegestaan, ook informatie verstrekken aan de ordehandhavingsautoriteiten om zijn eigendom en de gezondheid en veiligheid van individuen te beschermen.

Er zullen verklaringen aan de lidstaatautoriteiten ter bescherming van persoonlijke gegevens worden afgelegd in overeenstemming met de van kracht zijnde wetgeving in de betreffende Europese lidstaat. Informatie over dergelijke verklaringen is beschikbaar op Kaspersky Security Network-services.

VERZAMELDE INFORMATIE

Gegevens die we verzamelen

De Kaspersky Security Network-service verzamelt en verzendt basisgegevens en uitgebreide gegevens naar Kaspersky Lab over potentiële beveiligingsrisico's die uw computer aanvallen. De verzamelde gegevens omvatten:

Basisgegevens

- informatie over de hardware en software van uw computer, waaronder het besturingssysteem en de geïnstalleerde servicepacks, kernel-objecten, stuurprogramma's, services, Internet Explorer-uitbreidingen,

printeruitbreidingen, Windows Explorer-uitbreidingen, gedownloade programmabestanden, actieve set-upelementen, applets in het Configuratiescherm, host- en registerrecords, IP-adressen, browsertypen, e-mailclients en het versienummer van het Kaspersky Lab-product, die gewoonlijk niet persoonlijk identificeerbaar is;

- een unieke ID die door het product van Kaspersky Lab wordt gegenereerd om individuele apparaten te identificeren zonder dat de gebruiker wordt geïdentificeerd en die geen persoonlijke informatie bevat.
- informatie over de status van de antivirusbescherming op uw computer, en de gegevens in bestanden of activiteiten die vermoedelijk malware zijn (bijv. virusnaam, datum/tijd van detectie, namen/paden en grootte van geïnfecteerde bestanden, IP-adres en poort van netwerkaanval, naam van het programma dat vermoedelijk malware is). De verzamelde gegevens waarnaar hierboven wordt verwezen, bevatten geen persoonlijk identificeerbare informatie.

Uitgebreide gegevens

- informatie over digitaal ondertekende programma's die door de gebruiker zijn gedownload (URL, bestandsformaat, naam van ondertekenaar);
- informatie over uitvoerbare programma's (grootte, kenmerken, aanmaakdatum, informatie over PE-koppen, regio, naam, locatie en gebruikt compressieprogramma).

De verzending en opslag van gegevens beveiligen

Kaspersky Lab legt zich erop toe de veiligheid van verzamelde informatie te garanderen. De verzamelde informatie wordt op computerservers met beperkte en bewaakte toegang opgeslagen. Kaspersky Lab gebruikt beveiligde gegevensnetwerken die door industriestandaard firewall- en wachtwoord-beschermingsystemen worden beveiligd. Kaspersky Lab benut een groot aantal beveiligingstechnologieën en -procedures om de verzamelde informatie te beschermen tegen bedreigingen zoals onbevoegde toegang, bekendmaking of onbevoegd gebruik. Ons beveiligingsbeleid wordt waar vereist periodiek herzien en verbeterd, en alleen bevoegde individuen hebben toegang tot de gegevens die we verzamelen. Kaspersky Lab onderneemt stappen om ervoor te zorgen dat uw informatie op veilige wijze en volgens deze Verklaring wordt behandeld. Helaas kan van geen enkele gegevensverzending worden gegarandeerd dat deze veilig is. Dientengevolge kunnen we, hoewel we er naar streven uw gegevens te beschermen, geen garantie bieden voor de veiligheid van de gegevens die u naar ons verzendt via onze producten of services, inclusief maar niet beperkt tot Kaspersky Security Network, en u gebruikt al deze services op eigen risico.

De verzamelde gegevens kunnen naar de servers van Kaspersky Lab worden overgedragen, en Kaspersky Lab heeft de nodige voorzorgsmaatregelen getroffen om te verzekeren dat de verzamelde informatie, als deze wordt overgedragen, zo goed mogelijk is beveiligd. We behandelen de gegevens die we verzamelen als vertrouwelijke informatie; deze zijn dienovereenkomstig onderworpen aan onze beveiligingsprocedures en ons bedrijfsbeleid betreffende de bescherming en het gebruik van vertrouwelijke informatie. Wanneer de verzamelde gegevens door Kaspersky Lab zijn ontvangen, worden ze zoals gebruikelijk is in deze industrie op een server met fysieke en elektronische beveiligingsfuncties opgeslagen. Hierbij wordt onder meer gebruik gemaakt van aanmeldings-/wachtwoordprocedures en elektronische firewalls die zijn ontworpen om onbevoegde toegang van buiten Kaspersky Lab te blokkeren. Gegevens die door Kaspersky Security Network worden verzameld en in deze Verklaring worden behandeld, worden verwerkt en opgeslagen in de Verenigde Staten en mogelijk in andere rechtsgebieden en andere landen waar Kaspersky Lab zaken doet. Alle werknemers van Kaspersky Lab zijn op de hoogte van ons beveiligingsbeleid. Uw gegevens zijn alleen toegankelijk voor werknemers die deze nodig hebben om hun werk te kunnen verrichten. De opgeslagen gegevens zijn op geen enkele wijze aan persoonlijk identificeerbare informatie gekoppeld. Kaspersky Lab combineert de gegevens die door Kaspersky Security Network zijn opgeslagen, niet met gegevens, adressenlijsten of abonnementsinformatie die voor promotionele of andere doeleinden door Kaspersky Lab zijn verzameld.

HET GEBRUIK VAN DE VERZAMELDE GEGEVENS

Het gebruik van uw persoonlijke gegevens

Kaspersky Lab verzamelt de gegevens om de bron van mogelijke beveiligingsrisico's te analyseren en identificeren, en om het vermogen van Kaspersky Lab-producten te verbeteren om kwaadaardig gedrag, frauduleuze websites, crimeware en andere soorten internetbeveiligingsbedreigingen te detecteren, zodat in de toekomst het best mogelijke beschermingsniveau aan de klanten van Kaspersky Lab kan worden geboden.

Informatie aan derden bekendmaken

Kaspersky Lab mag de verzamelde informatie bekendmaken indien dit door een ordehandhavingsautoriteit wordt vereist, zoals wettelijk vereist of toegestaan of als gevolg van een dagvaarding of ander wettelijk proces, of als wij reden hebben te geloven dat wij hiertoe verplicht zijn om te voldoen aan toepasbare wetgeving, voorschriften of dagvaardingen, of ander wettelijk proces of afdwingbaar overheidsverzoek. Kaspersky Lab mag persoonlijk identificeerbare informatie ook bekendmaken wanneer we reden hebben om te geloven dat het bekendmaken van deze informatie noodzakelijk is om iemand te identificeren, contact op te nemen met iemand of om iemand rechtelijk te vervolgen die deze Verklaring of de voorwaarden in de overeenkomsten met het Bedrijf mogelijk schendt, of om de veiligheid van onze gebruikers en het publiek te beschermen

of onder vertrouwelijkheids- en licentieovereenkomsten met bepaalde derde partijen die ons helpen bij de ontwikkeling, het gebruik en beheer van het Kaspersky Security Network. Kaspersky Lab mag bepaalde informatie delen met onderzoeksorganisaties en andere leveranciers van beveiligingssoftware om kennis, detectie en preventie van internetbeveiligingsrisico's te stimuleren. Kaspersky Lab mag ook gebruikmaken van statistieken die zijn afgeleid van de verzamelde informatie om rapporten over de trends in beveiligingsrisico's bij te houden en te publiceren.

Beschikbare mogelijkheden

Deelname aan Kaspersky Security Network is optioneel. U kunt de Kaspersky Security Network-service op elk moment activeren of deactiveren door naar de feedbackinstellingen onder de optiepagina van uw Kaspersky Lab-product te gaan. Als u er echter voor kiest de verzochte informatie of gegevens niet te verstrekken, kunnen we bepaalde services die afhankelijk zijn van de verzameling van deze gegevens, misschien niet aan u aanbieden.

Zodra de serviceperiode van uw Kaspersky Lab-product verloopt, blijven sommige functies van de Kaspersky Lab-software misschien werken, maar wordt er niet langer automatisch informatie naar Kaspersky Lab verstuurd.

We behouden ons ook het recht voor om af en toe waarschuwingsberichten te sturen om gebruikers in te lichten over specifieke wijzigingen die invloed hebben op hun vermogen om de services te gebruiken waarvoor zij zich eerder hebben aangemeld. We behouden ons ook het recht voor contact met u op te nemen als dit vereist is voor een gerechtelijke actie of als toepasselijke licenties, garanties en inkoopovereenkomsten zijn geschonden.

Kaspersky Lab behoudt zich deze rechten voor omdat wij menen dat het in een beperkt aantal gevallen noodzakelijk is contact met u op te nemen betreffende wettelijke aangelegenheden of zaken die voor u van belang zijn. Deze rechten staan ons niet toe contact met u op te nemen om nieuwe of bestaande services bij u te promoten als u ons hebt gevraagd dit niet te doen, en dergelijke berichten worden slechts sporadisch verzonden.

GEGEVENSVERZAMELING – GERELATEERDE VRAGEN EN KLACHTEN

Kaspersky Lab neemt en behandelt de vragen van gebruikers over Gegevensverzameling bijzonder serieus. Als u denkt dat uw informatie of gegevens niet volgens deze Verklaring worden behandeld of als u andere gerelateerde vragen of klachten hebt, kunt u Kaspersky Lab e-mailen op: support@kaspersky.com.

Maak uw vraag zo gedetailleerd mogelijk. We zullen uw vraag of klacht zo spoedig mogelijk behandelen.

Het verstrekken van informatie is vrijwillig. In de sectie **Feedback** op de pagina **Instellingen** van elk toepasselijk Kaspersky-product vindt u een optie waarmee u gegevensverzameling op elk moment kunt uitschakelen.

Copyright © 2008 Kaspersky Lab. Alle rechten voorbehouden.

KASPERSKY LAB

Kaspersky Lab is opgericht in 1997 en is een algemeen erkend leider op het gebied van informatiebeveiligingstechnologieën geworden. Het bedrijf produceert een breed scala aan gegevensbeveiligingssoftware en levert hoogpresterende antivirus-, antisпам- en anti-inbraaksystemen.

Kaspersky Lab is een internationale onderneming met hoofdkantoor in Rusland en vertegenwoordigingen in het Verenigd Koninkrijk, Frankrijk, Duitsland, Japan, de Benelux, China, Polen, Roemenië en de Verenigde Staten (Californië). Onlangs is in Frankrijk een nieuw kantoor gevestigd: het European Anti-Virus Research Centre. Het partnernetwerk van Kaspersky Lab omvat wereldwijd meer dan 500 bedrijven.

Kaspersky Lab heeft nu meer dan 450 specialisten in dienst, van wie er 10 een MBA-graad (Master of Business Administration) en 16 een doctoraat bezitten. Seniordeskundigen zijn lid van CARO (Computer Anti-Virus Researchers Organization).

Onze meest waardevolle bedrijfsmiddelen zijn de unieke kennis en know-how die onze specialisten de afgelopen veertien jaar hebben vergaard gedurende de niet aflatende strijd tegen computervirussen. Dankzij een grondige analyse van computervirusactiviteiten kunnen zij de trends in de ontwikkeling van malware voorspellen en onze gebruikers tijdig voorzien van beveiliging tegen nieuwe typen aanvallen. Weerstand tegen toekomstige aanvallen is de grondslag van alle Kaspersky Lab-producten. De producten van het bedrijf blijven altijd een stapje voor op die van andere producenten bij het leveren van antivirusbescherming aan onze klanten.

Jaren van hard werken hebben het bedrijf tot één van de toonaangevende ontwikkelaars van antivirussoftware gemaakt. Kaspersky Lab ontwikkelde als een van de eerste bedrijven van zijn soort de meest hoogstaande standaarden voor antivirusbescherming. Het paradepaardje van de onderneming, Kaspersky Anti-Virus, biedt bescherming op alle niveaus voor alle segmenten van een netwerk, zoals werkstations, bestandsservers, e-mailsystemen, firewalls, internetgateways en PDA's. De handige en gebruiksvriendelijke beheertools garanderen optimale automatisering van de antivirusbescherming van computers en bedrijfsnetwerken. Vele bekende producenten gebruiken de Kaspersky Anti-Virus-kernel: zoals Nokia ICG (VS), F-Secure (Finland), Aladdin (Israël), Sybari (VS), G Data (Duitsland), Deerfield (VS), Alt-N (VS), Microworld (India) en BorderWare (Canada).

De klanten van Kaspersky Lab profiteren van een gevarieerd aanbod extra diensten die niet alleen een stabiele werking van de producten van de

onderneming verzekeren, maar ook tegemoetkomen aan specifieke vereisten van het bedrijfsleven. Wij ontwerpen, implementeren en ondersteunen complexe antivirussystemen voor ondernemingen. De antivirusdatabase van Kaspersky Lab wordt elk uur bijgewerkt. Het bedrijf biedt zijn klanten 24 uur per dag technische ondersteuning in een aantal talen.

IN DEZE SECTIE:

Andere producten van Kaspersky Lab.....	83
Contact opnemen	94

ANDERE PRODUCTEN VAN KASPERSKY LAB

Kaspersky Lab's News Agent

Het programma News Agent wordt gebruikt voor een snelle levering van het nieuws, mededelingen over 'virusomstandigheden' en de recentste gebeurtenissen van Kaspersky Lab. Het programma leest op gezette tijden de lijst met beschikbare nieuwskanalen en de hierin vermelde informatie van Kaspersky Labs nieuwsserver.

Daarnaast kunt u met de News Agent:

- in het systeemvenster de 'virusomstandigheden' weergeven;
- een abonnement nemen op de nieuwskanalen van Kaspersky Labs of dit opzeggen;
- op elk kanaal waarop u bent geabonneerd, met een bepaalde regelmaat nieuws ontvangen; bovendien kunt u aangeven dat u wilt worden ingelicht over nieuw ongelezen nieuws;
- nieuws op de kanalen bekijken waarop u bent geabonneerd;
- de lijst met kanalen en hun status bekijken;
- gedetailleerd nieuws in een webbrowserspagina openen.

De News Agent wordt onder Microsoft Windows uitgevoerd en kan als een zelfstandig programma worden gebruikt of in de geïntegreerde oplossingen van Kaspersky Lab worden opgenomen.

Kaspersky® Online Scanner

Dit programma is een gratis service die aan de bezoekers van de bedrijfswebsite wordt aangeboden. Zij kunnen hiermee online op efficiënte wijze antivirusscans op hun computer uitvoeren. Kaspersky OnLine Scanner kan in de webbrowser worden uitgevoerd. Zo kunnen gebruikers snel antwoord ontvangen op hun vragen over malware-infecties. De gebruiker kan tijdens een scan:

- archieven en e-maildatabases van de scan uitsluiten;
- standaard of uitgebreide databases selecteren om voor de scan te gebruiken;
- resultaten van de scan in txt- of html-indeling opslaan.

Kaspersky® OnLine Scanner Pro

Dit programma is een abonnementservice die aan de bezoekers van de bedrijfswebsite wordt aangeboden. Zij kunnen hiermee online op efficiënte wijze antivirusscans op hun computer uitvoeren en geïnfecteerde bestanden schoonmaken. Kaspersky OnLine Scanner Pro kan direct in de webbrowser worden uitgevoerd. De gebruiker kan tijdens een scan:

- archieven en e-maildatabases van de scan uitsluiten;
- standaard of uitgebreide databases selecteren om voor de scan te gebruiken;
- gedetecteerde geïnfecteerde objecten schoonmaken;
- resultaten van de scan in txt- of html-indeling opslaan.

Kaspersky Anti-Virus® Mobile

Kaspersky Anti-Virus Mobile biedt antivirusbescherming voor mobiele apparaten waarop Symbian OS- en Microsoft Windows Mobile-besturingssystemen draaien. Met het programma kan een complexe antivirusscan worden uitgevoerd, met inbegrip van:

- een scan op verzoek van het geheugen van een mobiel apparaat, geheugenkaarten, individuele mappen of bestanden. Zodra er een geïnfecteerd object wordt gedetecteerd, wordt het in quarantaine geplaatst of verwijderd;

- realtime-bescherming: alle inkomende of gewijzigde objecten worden gescand, evenals bestanden wanneer wordt geprobeerd ze te openen;
- bescherming tegen sms- en mms-spam.

Kaspersky Anti-Virus for File Servers

Dit softwareproduct verzekert betrouwbare bescherming van bestandssystemen op servers die onder het besturingssysteem Microsoft Windows, Novell NetWare of Linux worden uitgevoerd, tegen alle typen malware. In het softwareproduct zijn de volgende programma's van Kaspersky Lab opgenomen:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Voordelen en functionele capaciteiten:

- *realtime-bescherming voor bestandssystemen op servers*: alle bestanden op de server worden gescand bij een poging om ze te openen of op de server op te slaan.
- *voorkoming van virusuitbraken*;
- *scan op verzoek* van het complete bestandssysteem of van de afzonderlijke bestanden en mappen;
- *het gebruik van de optimaliseringstechnologieën* bij het scannen van objecten in het bestandssysteem op de server;
- *herstel van het systeem na de infectie*;
- *schaalbaarheid van het softwareproduct* voor overeenstemming met de beschikbare systeembronnen;
- *handhaving van de gelijkmatige verdeling van het systeem*;
- *aanmaak van de lijst met vertrouwde processen* waarvan de activiteiten op de server niet door dit product worden bewaakt;
- *extern beheer* van de software, inclusief gecentraliseerde installatie, configuratie en beheer;

- *opslag van reservekopieën van geïnfekteerde en verwijderde objecten voor het geval ze moeten worden hersteld;*
- *isolatie van verdachte objecten in de speciale opslagplaats;*
- *meldingen over gebeurtenissen die plaatsvinden tijdens het gebruik van de software en naar de systeembeheerder worden verzonden;*
- *bijhouden van gedetailleerde rapporten;*
- *automatische bijwerking van databases van de software.*

Kaspersky Open Space Security

Kaspersky Open Space Security is een softwareproduct dat een volledig nieuwe benadering heeft ten opzichte van de beveiliging van moderne bedrijfsnetwerken van elke omvang en biedt gecentraliseerde bescherming van informatiesystemen en ondersteuning voor afgelegen kantoor sites en mobiele gebruikers.

Dit softwareproduct omvat vier programma's:

- Kaspersky Open Space Security.
- Kaspersky Business Space Security.
- Kaspersky Enterprise Space Security.
- Kaspersky Total Space Security.

Hieronder vindt u een gedetailleerde beschrijving van elk product.

Kaspersky Work Space Security is een product dat is ontworpen om aan werkposten binnen en buiten het bedrijfsnetwerk gecentraliseerde bescherming te bieden tegen alle moderne internetbedreigingen: virussen, spyware, hackeraanvallen en spam.

Voordelen en functionele capaciteiten:

- *uitgebreide bescherming tegen virussen, hackeraanvallen en spam;*
- *proactieve bescherming tegen nieuwe malwareprogramma's die nog niet aan de databases zijn toegevoegd;*
- *persoonlijke firewall met het systeem voor de detectie van indringers en het voorkomen van netwerkaanvallen;*

- *terugdraaifunctie in geval er schadelijke wijzigingen in het systeem zijn aangebracht;*
- *bescherming tegen phishing-aanvallen en spam;*
- *dynamische nieuwe toewijzing van bronnen tijdens de volledige systeemscaan;*
- *extern beheer van de software, inclusief gecentraliseerde installatie, configuratie en beheer;*
- *ondersteuning van Cisco® NAC (Network Admission Control);*
- *real-time scannen van e-mail en internetverkeer;*
- *blokkeert pop-upvensters en advertentiebalken op het internet;*
- *veilig werken op elk type netwerk, inclusief Wi-Fi;*
- *gereedschappen voor het aanmaken van herstelschijven, zodat het systeem na een virusaanval kan worden hersteld;*
- *ontwikkeld systeem met rapporten over de beschermings-status;*
- *automatische bijwerking van databases;*
- *volledige ondersteuning voor 64-bits besturingssystemen;*
- *optimalisering van de laptopsoftware (Intel® Centrino® Duo-technologie voor mobiele pc);*
- *vermogen om het schoonmaken op afstand uit te voeren (Intel® Active Management-technologie, component van Intel® vPro™).*

Kaspersky Business Space Security biedt optimale bescherming voor informatiebronnen tegen moderne internetbedreigingen. Kaspersky Business Space Security beschermt werkposten en bestandsservers tegen alle soorten virussen, Trojan programma's en wormen. Zo voorkomt u virusuitbraken, zijn uw gegevens beveiligd, en hebben gebruikers bovendien onmiddellijk toegang tot netwerkbronnen.

Voordelen en functionele capaciteiten:

- *beheer op afstand van de software, inclusief gecentraliseerde installatie, configuratie en beheer;*
- *ondersteuning van Cisco® NAC (Network Admission Control);*
- *bescherming van werkposten en bestandsservers tegen alle soorten internetbedreigingen;*
- *het gebruik van de iSwift-technologie om te voorkomen dat scans steeds opnieuw moeten worden uitgevoerd in het netwerk;*
- *verdeling van de belasting over de processors van de server;*
- *isolatie van verdachte objecten in de speciale opslagplaats;*
- *terugdraaifunctie in geval er schadelijke wijzigingen in het systeem zijn aangebracht;*
- *schaalbaarheid van het softwareproduct voor overeenstemming met de beschikbare systeembronnen;*
- *proactieve bescherming van werkstations tegen nieuwe malwareprogramma's die nog niet aan de databases zijn toegevoegd;*
- *real-time scannen van e-mail en internetverkeer;*
- *persoonlijke firewall met het systeem voor de detectie van indringers en het voorkomen van netwerkaanvallen;*
- *bescherming van gebruik in draadloze Wi-Fi-netwerken;*
- *zelfbeschermingstechnologie van het antivirus tegen malware;*
- *isolatie van verdachte objecten in de speciale opslagplaats;*
- *automatische bijwerking van databases.*

Kaspersky Enterprise Space Security

Dit softwareproduct omvat componenten voor de bescherming van werkposten en samenwerkingsservers tegen alle soorten moderne internetbedreigingen, verwijdert virussen uit de e-mailstromen, beveiligd

gegevens en zorgt ervoor dat gebruikers onmiddellijk toegang hebben tot netwerkbronnen.

Voordelen en functionele capaciteiten:

- *bescherming van werkposten en bestandsservers tegen virussen, Trojan programma's en wormen;*
- *bescherming van de mailservers Sendmail, Qmail, Postfix en Exim;*
- *scannen van alle berichten op de Microsoft Exchange Server, inclusief de gedeelde mappen;*
- *verwerking van berichten, databases en andere objecten van Lotus Domino-servers;*
- *bescherming tegen phishing-aanvallen en spam;*
- *voorkomt massamailings en virusuitbraken;*
- *schaalbaarheid van het softwareproduct voor overeenstemming met de beschikbare systeembronnen;*
- *beheer op afstand van de software, inclusief gecentraliseerde installatie, configuratie en beheer;*
- *ondersteuning van Cisco® NAC (Network Admission Control);*
- *proactieve bescherming van werkstations tegen nieuwe malwareprogramma's die nog niet aan de databases zijn toegevoegd;*
- *persoonlijke firewall met het systeem voor de detectie van indringers en het voorkomen van netwerkaanvallen;*
- *veilig werken in draadloze Wi-Fi-netwerken;*
- *real-time scannen van internetverkeer;*
- *terugdraaifunctie in geval er schadelijke wijzigingen in het systeem zijn aangebracht;*
- *dynamische nieuwe toewijzing van bronnen tijdens de volledige systeemscaan;*

- *isolatie van verdachte objecten in de speciale opslagplaats;*
- *ontwikkeld systeem met rapporten over de beschermingsstatus van het systeem;*
- *automatische bijwerking van databases.*

Kaspersky Total Space Security

Deze oplossing controleert alle inkomende en uitgaande gegevensstromen (e-mail, internetverkeer en alle interacties op het netwerk). Het product omvat componenten die worden gebruikt om werkposten en mobiele apparaten te beschermen, biedt onmiddellijke en veilige toegang tot bedrijfsgegevens en het internet, en garandeert veilige communicatie via e-mail.

Voordelen en functionele capaciteiten:

- *uitgebreide bescherming tegen virussen, hackeraanvallen en spam op alle niveaus van het bedrijfsnetwerk; van werkposten tot gateways;*
- *proactieve bescherming van werkstations tegen nieuwe malwareprogramma's die nog niet aan de databases zijn toegevoegd;*
- *bescherming van mailservers en gedeelde servers;*
- *realtime scannen van inkomend LAN-webverkeer (HTTP/FTP);*
- *schaalbaarheid van het softwareproduct voor overeenstemming met de beschikbare systeembronnen;*
- *blokkeert toegang vanuit geïnfecteerde werkposten;*
- *voorkoming van virusuitbraken;*
- *gecentraliseerde rapporten over de beschermingsstatus;*
- *extern beheer van de software, inclusief gecentraliseerde installatie, configuratie en beheer;*
- *ondersteuning van Cisco® NAC (Network Admission Control);*
- *ondersteuning voor proxyservers van hardware;*

- *filtert internetverkeer op basis van de lijst met vertrouwde servers, objecttypen en gebruikersgroepen;*
- *het gebruik van de iSwift-technologie om te voorkomen dat scans steeds opnieuw moeten worden uitgevoerd in het netwerk;*
- *dynamische nieuwe toewijzing van bronnen tijdens de volledige systeemscaan;*
- *persoonlijke firewall met het systeem voor de detectie van indringers en het voorkomen van netwerkaanvallen;*
- *veilig werken op elk type netwerk, inclusief Wi-Fi;*
- *bescherming tegen phishing-aanvallen en spam;*
- *vermogen om het schoonmaken op afstand uit te voeren (Intel® Active Management-technologie, component van Intel® vPro™);*
- *terugdraaifunctie in geval er schadelijke wijzigingen in het systeem zijn aangebracht;*
- *zelfbeschermingstechnologie van het antivirus tegen malware;*
- *volledige ondersteuning voor 64-bits besturingssystemen;*
- *automatische bijwerking van databases.*

Kaspersky Security for Mail Servers

Softwareproduct voor bescherming van mailservers en gedeelde servers tegen malwareprogramma's en spam. Het product bestaat uit programma's voor de bescherming van alle populaire mailservers: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix en Exim, en biedt u bovendien de mogelijkheid een toegewezen mailgateway in te stellen. Deze oplossing omvat:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus voor Lotus Notes/Domino.
- Kaspersky Anti-Virus voor Microsoft Exchange.

- Kaspersky Anti-Virus® voor Linux Mail Server

Dit programma doet het volgende:

- *betrouwbare bescherming tegen malware en potentieel gevaarlijke programma's;*
- *filtert spam;*
- *scant inkomende en uitgaande e-mailberichten en bijlagen;*
- *antivirusscan van alle berichten op de Microsoft Exchange Server, inclusief de gedeelde mappen;*
- *scan van berichten, databases en andere objecten van Lotus Domino-servers;*
- *filtert berichten op bijlagetype;*
- *isolatie van verdachte objecten in de speciale opslagplaats;*
- *handig systeem voor het beheer van het softwareproduct;*
- *voorkoming van virusuitbraken;*
- *bewaakt de beschermingsstatus van het systeem aan de hand van meldingen;*
- *systeem met rapporten over het gebruik van het programma;*
- *schaalbaarheid van het softwareproduct voor overeenstemming met de beschikbare systeembronnen;*
- *automatische bijwerking van databases.*

Kaspersky Security voor Gateways

Dit softwareproduct biedt alle werknemers van het bedrijf veilige toegang tot het internet door malware en riskware automatisch te verwijderen uit de gegevensstroom die via HTTP/FTP-protocollen door het netwerk wordt ontvangen. Deze oplossing omvat:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus voor Proxy Server.
- Kaspersky Anti-Virus voor Microsoft ISA Server.
- Kaspersky Anti-Virus voor Check Point FireWall-1.

Dit programma doet het volgende:

- *betrouwbare bescherming tegen malware en potentieel gevaarlijke programma's;*
- *real-time scannen van internetverkeer (HTTP/FTP);*
- *filtert internetverkeer op basis van de lijst met vertrouwde servers, objecttypen en gebruikersgroepen;*
- *isolatie van verdachte objecten in de speciale opslagplaats;*
- *handig controlesysteem;*
- *systeem met rapporten over het gebruik van het programma;*
- *ondersteuning voor proxy servers van hardware;*
- *schaalbaarheid van het softwareproduct voor overeenstemming met de beschikbare systeembronnen;*
- *automatische bijwerking van databases.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam is het eerste Russische softwarepakket dat bescherming biedt tegen spam voor kleine en middelgrote ondernemingen. Dit product combineert revolutionaire technologieën voor de linguïstische analyse van teksten, alle moderne methoden voor het filteren van e-mail (inclusief DNS zwarte lijsten en formele kenmerken van berichten) en een unieke reeks services waarmee de gebruiker tot 95 procent van het ongewenste verkeer kan detecteren en elimineren.

Kaspersky Anti-Spam is een filter dat ingesteld is bij de 'ingang' van het bedrijfsnetwerk en dat de inkomende stroom berichten op spam scant. Het is compatibel met alle mailsystemen die in het netwerk van de client worden gebruikt, en kan op de bestaande mailserver of op een toegewezen server worden geïnstalleerd.

Het programma is bijzonder efficiënt wegens de dagelijkse automatische update van de database voor inhoudsfiltering, waarbij voorbeelden worden geleverd door de specialisten van het linguïstische lab. Er worden elke 20 minuten updates uitgebracht.

Kaspersky Anti-Virus® voor MIMESweeper

Kaspersky Anti-Virus® voor MIMESweeper biedt een scan van hoge snelheid van het verkeer voor servers die gebruikmaken van Clearswift MIMESweeper

voor SMTP, Clearswift MIMESweeper voor Exchange, of Clearswift MIMESweeper voor Web.

Het programma wordt als invoegtoepassing (uitbreidingsmodule) geïmplementeerd, en voert een realtime-antivirusscan uit en verwerkt inkomende en uitgaande e-mailberichten.

CONTACT OPNEMEN

Als u vragen hebt, kunt u rechtstreeks contact opnemen met Kaspersky Lab of met een van onze dealers. U kunt telefonisch of per e-mail advies ontvangen. U krijgt uitgebreid antwoord op alle vragen.

Adres:	Hambakenwetering 10. 5231 DC 's-Hertogenbosch
Tel., Fax:	+31 (0)73 6154860 +31 (0)73 6154869
24/7 ondersteuning in noodgevallen	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Ondersteuning voor gebruikers van bedrijfsproducten:	http://support.kaspersky.com/nl/helpdesk.html
Ondersteuning voor zakelijke gebruikers:	contactgegevens worden verstrekt nadat u een bedrijfssoftwareproduct hebt gekocht, afhankelijk van uw ondersteuningspakket.
Webforum van Kaspersky Lab:	http://www.kaspersky.nl/forum
Anti-Virus Lab:	newvirus@kaspersky.com (alleen voor het verzenden van nieuwe virussen naar archieven)
Groep voor het ontwikkelen van gebruikersdocumentatie	docfeedback@kaspersky.com (alleen voor het verzenden van feedback over documentatie en Help-systeem)

Verkoopafdeling:	sales@kaspersky.nl
Algemene informatie:	info@kaspersky.nl
WWW:	http://www.kaspersky.nl http://www.viruslist.com

CRYPTOEX LLC

Voor het maken en controleren van de digitale handtekening maakt Kaspersky Anti-Virus gebruik van Crypto C, een bibliotheek van gegevens-beveiligingssoftware die is ontwikkeld door CryptoEx LLC.

Crypto Ex is houder van een licentie voor het ontwikkelen, vervaardigen en verspreiden van complexe versleutelingssystemen ter beveiliging van gegevens die geen staatsgeheim vormen. Deze licentie is toegekend door de federale inlichtingendienst FAPSI (FSB ofwel Staatsveiligheidsdienst).

Library Crypto C is ontworpen voor gebruik in systemen voor complexe bescherming van vertrouwelijke informatie (klasse KS1) en krijgt het FSB-certificaat No. SF/114-0901 d.d. 1 juli 2006.

Modules van deze bibliotheek gebruiken versleuteling en ontsleuteling van gegevenspakketten en/of gegevensstromen met vaste grootte op basis van een cryptografisch algoritme (GOST 28147-89). Verder worden in deze modules elektronische digitale handtekeningen gegenereerd en gecontroleerd op basis van algoritmen (GOST R 34.10-94 en GOST 34.10-2001) en de hash-functie (GOST 34.11-94), en wordt sleutelgegevens gegenereerd met een programma dat pseudowillekeurige getallen produceert. CryptoEx LLC heeft daarnaast een systeem voor generatie van sleutelgegevens en simulatievectoren geïmplementeerd (GOST 28147-89).

Bibliotheekmodules zijn geïmplementeerd met de programmeertaal C (overeenkomstig de ANSI C-standaard) en kunnen als statisch en dynamisch geladen programmacode in programma's worden geïntegreerd. Deze modules kunnen worden uitgevoerd op de platformen x86, x86-64 en Ultra SPARC II, en op platforms die hiermee compatibel zijn.

Bibliotheekmodules kunnen naar de volgende besturingssystemen worden gemigreerd: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris voor Ultra SPARC II).

Bedrijfswebsite van CryptoEx LLC: <http://www.cryptoex.ru>

E-mail: info@cryptoex.ru

MOZILLA FOUNDATION

De bibliotheek **Gecko SDK ver. 1.8** werd gebruikt voor de ontwikkeling van de programmacomponenten.

Deze software wordt gebruikt in overeenstemming met de voorwaarden en bepalingen van de MPL 1.1-licentie van de Public Mozilla Foundation <http://www.mozilla.org/MPL>.

Voor meer informatie over de bibliotheek Gecko SDK gaat u naar: http://developer.mozilla.org/en/docs/Gecko_SDK.

© Mozilla Foundation

Website Mozilla Foundation: <http://www.mozilla.org>.

LICENTIEOVEREENKOMST

Standaardlicentieovereenkomst voor Eindgebruikers

MEDEDELING AAN ALLE GEBRUIKERS: LEES DE VOLGENDE WETTELIJKE OVEREENKOMST ('OVEREENKOMST') VOOR DE LICENTIE VAN KASPERSKY INTERNET SECURITY ('SOFTWARE') GEPRODUCEERD DOOR KASPERSKY LAB ('KASPERSKY LAB') ZORGVULDIG DOOR.

ALS U DEZE SOFTWARE VIA HET INTERNET HEBT AANGESCHAFT DOOR OP DE KNOP AKKOORD TE KLIKKEN, STEM T U (ALS INDIVIDU OF AFZONDERLIJKE ENTITEIT) ERMEE IN GEBONDEN TE ZIJN DOOR EN EEN PARTIJ TE WORDEN BIJ DEZE OVEREENKOMST. ALS U NIET AKKOORD GAAT MET ALLE BEPALINGEN VAN DEZE OVEREENKOMST, KLIKT U OP DE KNOP DIE AANGEEFT DAT U NIET AKKOORD GAAT MET DEZE OVEREENKOMST EN INSTALLEERT U DE SOFTWARE NIET.

ALS U DEZE SOFTWARE OP EEN FYSIEK MEDIUM HEBT AANGESCHAFT, STEM T U (ALS INDIVIDU OF AFZONDERLIJKE ENTITEIT) DOOR HET BREKEN VAN HET ZEGEL VAN DE CD-VERPAKKING, ERMEE IN DAT U GEBONDEN BENT DOOR DEZE OVEREENKOMST. ALS U NIET AKKOORD GAAT MET ALLE BEPALINGEN VAN DEZE OVEREENKOMST, OPEN DAN DE CD-VERPAKKING NIET EN DOWNLOAD, INSTALLEER OF GEBRUIK DEZE SOFTWARE NIET.

IN OVEREENSTEMMING MET DE WETGEVING INZAKE SOFTWARE VAN KASPERSKY BESTEMD VOOR INDIVIDUELE GEBRUIKERS EN ONLINE AANGESCHAFT VAN DE INTERNETSITE VAN KASPERSKY LAB OF PARTNERS HIERVAN, HEBBEN KLANTEN EEN PERIODE VAN VEERTIEN (14) WERKDAGEN VOLGEND OP DE DAG VAN LEVERING VAN HET PRODUCT OM DIT AAN DE HANDELAAR TERUG TE GEVEN TER OMRUILING OF TERUGBETALING, OP VOORWAARDE DAT DE SOFTWARE NIET IS GEOPEND.

WAT BETREFT DE SOFTWARE VAN KASPERSKY BESTEMD VOOR INDIVIDUELE GEBRUIKERS DIE NIET ONLINE WERD AANGESCHAFT OP HET INTERNET, WORDT DEZE SOFTWARE NIET TERUGGENOMEN NOCH OMGERUID BEHALVE INDIEN DE PARTNER DIE HET PRODUCT VERKOOPT, DIT ANDERS BESLIST. IN DAT GEVAL WORDT KASPERSKY LAB NIET GEHOUDEN DOOR DE BEPALINGEN VAN DE PARTNER.

HET RECHT OP RETOURNERING EN RESTITUTIE HEEFT ENKEL BETREKKING OP DE OORSPRONKELIJKE AANKOPER.

Alle verwijzingen naar 'Software' in dit document worden geacht tevens de activeringscode voor de software die u van Kaspersky Lab ontvangt als onderdeel van Kaspersky Internet Security 2009, te omvatten.

1. *Licentieverlening.* Mits betaling van de toepasselijke licentievergoedingen en behoudens de bepalingen en voorwaarden van deze Overeenkomst, verleent Kaspersky Lab u hierbij het niet-exclusieve en niet-overdraagbare recht om één kopie van de vermelde versie van de Software en de bijbehorende documentatie (de 'Documentatie') te gebruiken voor de duur van deze Overeenkomst, enkel voor uw eigen interne bedrijfsdoeleinden. U mag één kopie van de Software installeren op één computer.

1.1 *Gebruik.* De licentie van de Software geldt voor één enkel product; de Software mag niet op meer dan één computer of door meer dan één gebruiker tegelijk worden gebruikt, behalve op de wijze omschreven in deze Sectie.

1.1.1 De Software is 'in gebruik' op een computer als deze wordt geladen in het tijdelijke geheugen (d.w.z. RAM of random-access geheugen) of wordt geïnstalleerd in het permanente geheugen (d.w.z. harde schijf, cd-rom of ander opslagmedium) van die computer. Conform deze licentie bent u slechts geautoriseerd om zoveel back-upkopieën van de Software te maken als nodig is voor het rechtmatig gebruik ervan en uitsluitend voor back-updoeleinden, mits al deze kopieën alle eigendomsvermeldingen van de Software bevatten. U bent verplicht het aantal en de locatie van alle kopieën van de Software en Documentatie bij te houden en alle redelijke voorzorgsmaatregelen te nemen om de Software tegen ongeautoriseerd kopiëren of gebruik te beschermen.

1.1.2 De Software beveiligd uw computer tegen virussen en netwerkaanvallen waarvan de definities zijn opgenomen in de databases met definities van dreigingen en netwerkaanvallen, die beschikbaar zijn op de Kaspersky Lab update-servers.

1.1.3 Als u de computer waarop de Software is geïnstalleerd, verkoopt, zorgt u ervoor dat alle kopieën van de Software op voorhand worden verwijderd.

1.1.4 Het is u niet toegestaan ook maar een deel van deze Software te decompileren, aan reverse engineering te onderwerpen, te disassembleren of anderszins trachten de broncode van de Software te achterhalen, noch is het toegelaten dit een derde partij toe te staan. De interface-informatie die nodig is voor de interoperabiliteit van de Software met onafhankelijk aangemaakte computerprogramma's wordt door Kaspersky Lab tegen betaling van de redelijke kosten en uitgaven voor het verkrijgen en leveren van dergelijke informatie voorzien. Als Kaspersky Lab u meedeelt dat het niet de intentie heeft dergelijke informatie beschikbaar te stellen om welke reden dan ook, met inbegrip (zonder beperking) van kosten, zal het u toegestaan zijn de stappen ter interoperabiliteit te ondernemen, op voorwaarde dat u de Software enkel onderwerpt aan reverse engineering of decompilatie in de mate die bij wet is toegestaan.

1.1.5 Het is u niet toegestaan foutverbeteringen aan te brengen aan de Software of deze te bewerken, aan te passen of te vertalen, noch is het toegestaan afgeleide werken van de Software te maken, of een derde partij toe te staan deze te kopiëren (anders dan uitdrukkelijk toegestaan in dit schrijven).

1.1.6 Het is niet toegestaan de Software aan een derde te verhuren, leasen of uit te lenen, noch mag u uw licentierechten aan een derde overdragen of deze een sublicentie verlenen.

1.1.7 Het is niet toegestaan de activatiecode of het licentiesleutelbestand aan derden over te dragen of derden toegang te verschaffen tot de activatiecode of de licentiesleutel. De activatiecode en de licentiesleutel zijn vertrouwelijke gegevens.

1.1.8 Kaspersky Lab mag de gebruiker vragen de meest recente versie van de Software te installeren (de meest recente versie en het meest recente onderhoudspakket).

1.1.9 U mag deze Software niet gebruiken in automatische, semi-automatische of handmatige tools die ontworpen zijn om virusdefinities, virusdetectieroutines of andere gegevens of code voor het detecteren van kwaadaardige code of gegevens, aan te maken.

1.1.10 U hebt het recht om Kaspersky Lab informatie te bieden over potentiële bedreigingen en kwetsbaarheden van uw computer. Meer informatie staat in de Verklaring voor gegevensverzameling. De verzamelde informatie wordt in algemene vorm gebruikt en heeft alleen tot doel de producten van Kaspersky Lab te verbeteren.

1.1.11 Voor de doelen die in clause 1.1.10 worden vermeld, verzamelt de Software automatisch informatie over controlesommen van bestanden, die op een computer worden uitgevoerd, en verzendt de Software deze naar Kaspersky Lab.

2. *Ondersteuning*¹.

¹ Als u gebruikmaakt van demosoftware, hebt u geen recht op de Technische Ondersteuning aangegeven in Clause 2 van deze Licentieovereenkomst voor Eindgebruikers, noch hebt u het recht de kopie in uw bezit te verkopen aan andere partijen.

U bent bevoegd de software te gebruiken voor demodoelinden gedurende de periode die in het licentiesleutelbestand wordt aangegeven en ingaat op het moment van activering (deze periode wordt weergegeven in het venster Service van de gebruikersinterface van de software).

(i) Kaspersky Lab zal u ondersteuningsdiensten aanbieden ('Ondersteuningsdiensten') zoals hieronder omschreven gedurende een termijn die wordt bepaald in het Licentiesleutelbestand en aangegeven in het venster Service en die ingaat op het moment van activering na:

- (a) betaling van de op dat moment geldende bijdrage, en;
- (b) het correct en volledig invullen van het Inschrijvingsformulier voor de Ondersteuningsdiensten dat u samen met deze Overeenkomst is bezorgd of beschikbaar is op de website van Kaspersky Lab, waarop u de activeringscode moet invoeren die u ook door Kaspersky Lab samen met deze Overeenkomst bezorgd zal zijn. Kaspersky Lab heeft de absolute vrijheid te oordelen of u al dan niet aan deze voorwaarde hebt voldaan voor het ter beschikking stellen van Ondersteuningsdiensten.

Ondersteuningsdiensten zullen beschikbaar zijn na activering van de Software. De technische ondersteuning van Kaspersky Lab is ook bevoegd om van u een aanvullende registratie te verzoeken teneinde de gebruiker te identificeren voor het bezorgen van Ondersteuningsdiensten.

Tot aan de activering van de Software en/of het ontvangen van de Eindgebruiker-identificatie (klant-ID), verleent de technische ondersteuning alleen hulp bij het activeren van de Software en het registreren van de Eindgebruiker.

(ii) Ondersteuningsdiensten zullen ophouden behalve indien zij jaarlijks worden vernieuwd door betaling van de op dat moment geldende jaarlijkse bijdrage en door een nieuwe succesvolle voltooiing van het Inschrijvingsformulier voor de Ondersteuningsdiensten.

(iii) 'Ondersteuningsdiensten' betekent:

- (a) Regelmatige updates van de antivirusdatabase;
- (b) Updates van database met netwerkaanvallen;
- (c) Updates van anti-spam database;
- (d) Gratis software-updates, met inbegrip van versie-upgrades;
- (e) Technische ondersteuning via internet en telefoonlijn door Verkoper en/of Wederverkoper;
- (f) Updates van virusdetectie en desinfectie in 24 uur.

- (iv) Ondersteuningsdiensten worden aangeboden enkel en alleen als u de meest recente versie van de Software geïnstalleerd hebt op uw computer (met inbegrip van de onderhoudspakketten) zoals beschikbaar op de officiële Kaspersky Lab-website (www.kaspersky.com).

3. *Eigendomsrechten.* De Software is auteursrechtelijk beschermd. Kaspersky Lab en zijn leveranciers bezitten en behouden alle rechten, aanspraken en belangen van en op de Software, inclusief alle auteursrechten, octrooirechten, handelsmerken en andere intellectuele eigendomsrechten. Door uw bezit, installatie of gebruik van de Software wordt geen enkele aanspraak op intellectuele eigendom van de Software aan u overgedragen en u krijgt uitsluitend rechten met betrekking tot de Software zoals uitdrukkelijk in deze Overeenkomst uiteengezet.

4. *Vertrouwelijkheid.* U stemt ermee in dat de Software en Documentatie, inclusief het specifieke ontwerp en de structuur van afzonderlijke programma's, vertrouwelijke eigendomsinformatie van Kaspersky Lab vormen. U mag dergelijke vertrouwelijke informatie niet openbaar maken, overdragen of anderszins op welke manier dan ook aan derden ter beschikking stellen zonder voorafgaande schriftelijke toestemming van Kaspersky Lab. U neemt redelijke veiligheidsmaatregelen om dergelijke vertrouwelijke informatie te beschermen, en zonder beperking van het voorgaande zult u de grootste moeite doen de veiligheid van de activeringscode te bewaren.

5. *Beperkte garantie.*

- (i) Kaspersky Lab geeft de garantie dat de Software aangekocht op een fysiek medium, gedurende een periode van zes (6) maanden na de eerste download of installatie, wezenlijk functioneert in overeenstemming met de functionaliteit omschreven in de Documentatie, mits de Software op de correcte manier en volgens de aanwijzingen in de Documentatie wordt gebruikt.
- (ii) U draagt alle verantwoordelijkheid voor het uitkiezen van deze Software om aan uw eisen te voldoen. Kaspersky Lab staat er niet garant voor dat de Software en/of de Documentatie voor deze vereisten geschikt is noch dat alle gebruik vrij is van fouten of onderbrekingen.
- (iii) Kaspersky Lab geeft geen garantie dat deze Software alle bekende virussen en spamberichten identificeert, noch dat de Software niet af en toe verkeerdelijk een virus meldt in een onderdeel dat niet door dat virus is geïnfecteerd.
- (iv) Uw enig verhaal en de volledige aansprakelijkheid van Kaspersky Lab voor schending van de garantie uit paragraaf (i) zal, naar keuze van Kaspersky Lab, het herstellen, vervangen of terugbetalen van de Software zijn, als dit werd gerapporteerd aan Kaspersky Lab of zijn

aangestelde tijdens de garantieperiode. U zult alle informatie die op redelijke wijze noodzakelijk kan zijn om de Leverancier bij te staan in het oplossen van het defecte item, ter beschikking stellen.

- (v) De in (i) vermelde garantie is niet van toepassing indien (a) wijzigingen aan deze Software zijn aangebracht door u of door uw toedoen zonder de instemming van Kaspersky Lab, indien u (b) de Software gebruikt op een wijze waarvoor deze niet is bestemd, of (c) de Software gebruikt anders dan is toegestaan krachtens deze Overeenkomst.
- (vi) De waarborgen en voorwaarden uiteengezet in deze Overeenkomst vervangen alle andere voorwaarden, waarborgen of andere bepalingen betreffende de levering of bedoelde levering, het uitblijven van leveren of de vertraging in levering van de Software of de Documentatie, die zonder dit lid (vi) van kracht zouden zijn tussen Kaspersky Lab en u of die anderszins opgenomen of geïntegreerd zouden worden in deze Overeenkomst of een ander ondergeschikt contract, hetzij krachtens statuut, gewoonterecht of anderszins, deze worden hierbij allen uitgesloten (inclusief, zonder beperking, stilzwijgende voorwaarden, waarborgen of andere bepalingen betreffende toereikende kwaliteit, doelgeschiktheid of het hanteren van redelijke bekwaamheid en zorgvuldigheid).

6. *Beperkte aansprakelijkheid.*

- (i) Niets in deze Overeenkomst zal de aansprakelijkheid van Kaspersky Lab uitsluiten of beperken voor (a) de onrechtmatige daad van bedrog, (b) de dood of lichamelijk letsel veroorzaakt door de schending van een gewoonterechtelijke verplichting van zorgvuldigheid of een onachtzame schending van een bepaling van deze Overeenkomst, of (c) elke andere aansprakelijkheid die niet kan worden uitgesloten bij wet.
- (ii) Behoudens paragraaf (i) hierboven, draagt Kaspersky Lab geen aansprakelijkheid (zij het in contract, onrechtmatige daad, restitutie of anderszins) voor de volgende verliezen of schade (ongeacht of deze verliezen of schade voorzien, te voorzien, bekend of anderszins waren):
 - (a) Gederfde inkomsten;
 - (b) Gederfde werkelijke of verwachte winst (waaronder gederfde winst op contracten);
 - (c) Verlies van het gebruik van geld;
 - (d) Verlies van verwachte besparingen;
 - (e) Verlies van handel;
 - (f) Verlies van mogelijkheden;
 - (g) Verlies van goodwill;
 - (h) Verlies van reputatie;

- (i) Schade aan, verlies of verminking van gegevens, of:
- (j) Elke andere vorm van indirecte of gevolgschade of verlies door welke oorzaak ook (waaronder, om twijfel te voorkomen, de gevallen waarin dergelijk verlies of schade valt onder de bepalingen van paragrafen (ii), (a) tot (ii), (i).
- (iii) Behoudens lid (i) hierboven, zal de aansprakelijkheid van Kaspersky Lab (zij het in contract, onrechtmatige daad, restitutie of anderszins) die voortkomt of in verband staat met de levering van de Software, in geen enkele omstandigheid meer bedragen dan de som gelijk aan het bedrag dat door u werd betaald voor de Software.

7. Deze Overeenkomst bevat de volledige verstandhouding tussen de partijen met betrekking tot het hierin behandelde onderwerp en krijgt voorrang op alle en andere voorafgaande afspraken, garanties en toezeggingen tussen u en Kaspersky Lab, hetzij mondeling of schriftelijk, die werden toegezegd of mogelijk zijn gesuggereerd in wat geschreven of gezegd is in onderhandelingen tussen ons of onze vertegenwoordigers voorafgaand aan deze Overeenkomst. Alle eerdere overeenkomsten tussen de partijen die betrekking hebben op de behandelde onderwerpen zullen ophouden van kracht te zijn vanaf de Datum waarop deze Overeenkomst ingaat. ➡