

# KASPERSKY LAB

---



**EASY-TO-USE**  
SYSTEM PROTECTING  
STORED DATA

**ADVANCED**  
TECHNOLOGIES AGAINST  
ALL TYPES OF HACKER  
ATTACKS

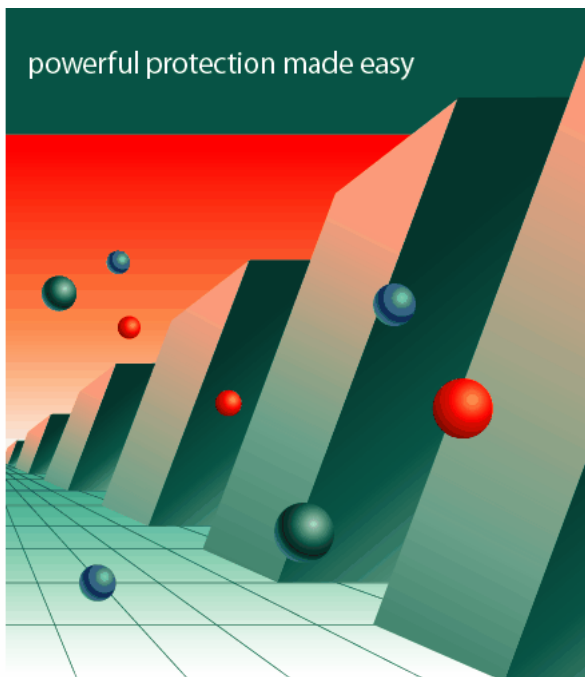
**COMPLETE**  
CONTROL OVER  
INTRUSION ATTEMPTS

**UNIQUE**  
SELF-LEARNING  
ABILITY

**COMPREHENSIVE**  
DATA PACKET  
FILTRATION

**CONTINUOUS**  
CONTROL OVER  
APPLICATION ACTIVITY

**FREE**  
ROUND-THE-CLOCK  
TECHNICAL SUPPORT



# Kaspersky Anti-Hacker

personal  
firewall

[www.kaspersky.com](http://www.kaspersky.com)

**KASPERSKY** 

---

## Kaspersky Anti-Hacker 1.7

MANUALE D'USO

KASPERSKY ANTI-HACKER 1.7

---

# Manuale d'uso

© Kaspersky Lab  
<http://www.kaspersky.com>

Data revisione: novembre 2004

# Sommario

CAPITOLO 1. KASPERSKY ANTI-HACKER.....	6
1.1. Le novità della versione 1.7.....	7
1.2. Kit di distribuzione.....	7
1.2.1. Contratto di licenza .....	8
1.3. Convenzioni.....	8
1.4. Helpdesk per utenti registrati.....	9
CAPITOLO 2. INSTALLAZIONE E DISINSTALLAZIONE DEL SOFTWARE .....	10
2.1. Requisiti hardware e software di sistema .....	10
2.2. Installazione .....	11
2.3. Installazione della chiave di licenza .....	14
2.4. Disinstallazione del programma.....	14
CAPITOLO 3. INIZIARE A LAVORARE .....	16
CAPITOLO 4. PREVENZIONE DEGLI ATTACCHI PROVENIENTI DALL'ESTERNO DURANTE LE SESSIONI DI LAVORO IN INTERNET E LAN...	19
4.1. Principi operativi di Kaspersky Anti-Hacker.....	19
4.2. Livelli di sicurezza.....	20
4.3. Impostazioni raccomandate.....	22
CAPITOLO 5. AVVIO DEL PROGRAMMA.....	26
5.1. Avvio del programma .....	26
5.2. Menu di sistema .....	26
5.3. Finestra principale .....	27
5.3.1. Menu .....	28
5.3.2. Barra degli strumenti.....	31
5.3.3. Area di lavoro.....	32

5.3.4. Barra di stato.....	33
5.4. Menu di scelta rapida delle finestre di dialogo.....	33
5.5. Composizione guidata delle regole.....	33
5.6. Modifica e salvataggio delle impostazioni dell'interfaccia .....	34
5.7. Uscita dal programma .....	36
<b>CAPITOLO 6. ABILITAZIONE DEL SISTEMA DI SICUREZZA E DEFINIZIONE DELLE SUE IMPOSTAZIONI.....</b>	<b>38</b>
6.1. Abilitazione del sistema di sicurezza e selezione del livello di sicurezza .....	38
6.1.1. Abilitazione del sistema di sicurezza.....	38
6.1.2. Selezione del livello di sicurezza .....	41
6.1.3. Avvertimenti sugli eventi di rete.....	42
6.1.4. Finestra Autoistruzione (Livello Medio).....	42
6.1.5. L'avvertimento di sostituzione del modulo eseguibile .....	44
6.2. Risposte del programma agli attacchi.....	45
6.3. Personalizzazione delle regole delle applicazioni .....	47
6.3.1. Gestione dell'elenco di regole .....	47
6.3.2. Aggiunta di una nuova regola per l'applicazione .....	50
6.3.2.1. Fase 1. Personalizzazione della regola .....	50
6.3.2.2. Fase 2. Condizioni delle regole .....	55
6.3.2.3. Fase 3. Azioni supplementari .....	61
6.4. Personalizzazione delle regole di filtraggio pacchetti.....	62
6.4.1. Gestione dell'elenco di regole .....	62
6.4.2. Aggiunta di una nuova regola .....	65
6.4.2.1. Fase 1. Condizioni delle regole .....	65
6.4.2.2. Fase 2. Nome delle regole e azioni supplementari .....	69
6.5. Sistema di rilevamento intrusioni .....	71
6.5.1. Impostazioni del rilevatore intrusioni .....	71
6.5.2. L'elenco degli attacchi rilevabili .....	72
<b>CAPITOLO 7. VISUALIZZAZIONE DEI RISULTATI DELLE PRESTAZIONI.....</b>	<b>75</b>
7.1. Visualizzazione dello stato corrente.....	75

---

7.1.1. Applicazioni attive .....	75
7.1.2. Connessioni stabilite.....	79
7.1.3. Porte aperte .....	82
7.2. Uso dei registri .....	84
7.2.1. Visualizzazione della finestra dei registri .....	85
7.2.2. Il layout della finestra Registri.....	85
7.2.2.1. Menu .....	86
7.2.2.2. Tabella dei rapporti .....	86
7.2.2.3. Schede .....	87
7.2.3. Selezione del registro .....	87
7.2.3.1. Registro di Sicurezza .....	87
7.2.3.2. Attività delle applicazioni.....	88
7.2.3.3. Filtraggio pacchetti .....	89
7.2.4. Definizione delle impostazioni dei registri .....	91
7.2.5. Salvataggio del registro su file.....	92
APPENDICE A. INDICE .....	93
APPENDICE B. DOMANDE FREQUENTI.....	94
APPENDICE C. KASPERSKY LAB.....	95
C.1. Altri prodotti Kaspersky Lab.....	96
C.2. Recapiti .....	99
APPENDICE D. CONTRATTO DI LICENZA.....	100

---

# CAPITOLO 1. KASPERSKY ANTI-HACKER

Kaspersky Anti-Hacker è una firewall personale destinata a garantire la protezione del computer con sistema operativo Windows contro gli accessi non autorizzati e gli attacchi provenienti da Internet o da reti locali adiacenti.

Kaspersky Anti-Hacker svolge le seguenti funzioni:

- Controlla l'attività di rete TCP/IP di tutte le applicazioni eseguite sul computer. In caso di rilevazione di azioni sospette, il programma informa l'utente e, se necessario, blocca l'accesso alla rete da parte di tali applicazioni. Questa misura consente all'utente di conservare dati confidenziali sul proprio computer. Per esempio, se un Troiano tenta di trasmettere dati dal computer, Kaspersky Anti-Hacker impedisce a questa applicazione maligna l'accesso a Internet.
- La tecnologia SmartStealth™ rende difficoltosa la rilevazione del computer dall'esterno. Di conseguenza, gli hacker perdono traccia dell'obiettivo e i loro tentativi di accesso al computer sono destinati a fallire. Ciò consente inoltre di prevenire qualsiasi attacco DoS (Denial of Service), senza peraltro influire minimamente sulla fluidità della navigazione in rete: il programma garantisce infatti la consueta trasparenza e accessibilità ai dati.
- Blocca gli attacchi più comuni alle reti filtrando continuamente il traffico in entrata e in uscita, e informa l'utente ogni volta che tali attacchi si verificano.
- Controlla i tentativi di scansione delle porte (solitamente seguiti da attacchi) e impedisce ogni ulteriore comunicazione con la macchina da cui è partito l'attacco.
- Consente di consultare l'elenco completo delle connessioni stabilite, delle porte aperte e delle applicazioni di rete attive e, se necessario, di interrompere connessioni indesiderate.
- Consente di garantire la massima sicurezza del computer contro gli attacchi esterni senza ricorrere a particolari configurazioni delle impostazioni del programma. Il programma consente una gestione

semplificata offrendo la scelta tra cinque livelli di sicurezza: *Blocca tutto*, *Alto*, *Medio*, *Basso*, *Consenti tutto*. Di default, il programma applica il livello *Medio*, una modalità di apprendimento che configura automaticamente il sistema di sicurezza in base alle risposte dell'utente a eventi di vario tipo.

- Consente di configurare il sistema di sicurezza in maniera flessibile. In particolare, è possibile impostare il programma in modo da operare una distinzione tra operazioni di rete desiderate e indesiderate, configurando in tal modo il Sistema di rilevamento intrusioni.
- Consente di registrare determinati eventi di rete relativi alla sicurezza in vari registri specifici. Se necessario, è possibile definire il livello di dettaglio delle voci di registro.

Il programma può essere utilizzato come prodotto software indipendente o come componente integrato nell'ambito di varie soluzioni **Kaspersky Lab**.



**Attenzione!!! Kaspersky Anti-Hacker non protegge il computer da virus e programmi maligni in grado di distruggere e/o danneggiare i dati. A tal fine, si raccomanda l'installazione di Kaspersky Anti-Virus Personal.**

## 1.1. Le novità della versione 1.7

A differenza della versione 1.5, la nuova versione del programma supporta il funzionamento in Windows XP con la Service Pack 2 installata.

## 1.2. Kit di distribuzione

Il Kit di distribuzione contiene:

- Una busta sigillata contenente il CD di installazione del prodotto
- Questo Manuale d'uso
- Una chiave di licenza allegata al pacchetto di distribuzione o memorizzata in un apposito dischetto
- Il Contratto di licenza



Prima di rompere il sigillo della busta del CD, leggere con attenzione il Contratto di licenza.

## 1.2.1. Contratto di licenza

Il Contratto di licenza (CL) è un accordo con valore legale stipulato tra il cliente (sia esso una persona fisica o una persona giuridica) e il produttore (Kaspersky Lab), che descrive le clausole di utilizzo da parte del cliente del prodotto antivirus acquistato.



Si raccomanda di leggere integralmente le clausole del CL!




Qualora il cliente non accetti tutte le clausole di questo CL, Kaspersky Lab rifiuta di concedere al cliente la licenza del prodotto software, e il cliente è tenuto a restituire il prodotto inutilizzato al proprio rivenditore Kaspersky Anti-Virus per ottenere un rimborso completo, accertandosi che la busta contenente il CD (o i dischetti) sia sigillata.

La rottura del sigillo della busta contenente il CD (o i dischetti) indica l'accettazione di tutte le clausole del CL da parte del cliente.

## 1.3. Convenzioni

In questo manuale abbiamo adottato una serie di convenzioni volte a porre in evidenza le parti più importanti della documentazione. Esse sono illustrate nella tabella sottostante.

Convenzione	Significato
<b>Grassetto</b>	Titoli dei menu, comandi di menu, intestazioni delle finestre, elementi delle finestre di dialogo, ecc.
 <b>Nota.</b>	Informazioni supplementari, note.
 <b>Attenzione!</b>	Informazioni importanti.

Convenzione	Significato
 Per avviare il programma, seguire le seguenti istruzioni: <ol style="list-style-type: none"><li>1. Fase 1.</li><li>2. ...</li></ol>	Istruzioni da eseguire.
 <b>Compito:</b>	Esempio di compito, definito dall'utente, da svolgere con questo programma.
 <b>Soluzione</b>	Soluzione del compito.

## 1.4. Helpdesk per utenti registrati

Kaspersky Lab offre un ampio pacchetto di assistenza che consente ai propri utenti registrati di utilizzare con maggiore efficienza Kaspersky Anti-Hacker.

Registrandosi e sottoscrivendo un abbonamento, si ottiene il diritto ai seguenti servizi per tutta la durata dell'abbonamento:

- Nuove versioni del prodotto software, gratuitamente
- Assistenza telefonica e via e-mail con consulenze sull'installazione, la configurazione e la gestione del prodotto software
- Informazioni sull'uscita di nuovi prodotti Kaspersky Lab e sui nuovi virus informatici (per gli utenti abbonati alla newsletter di Kaspersky Lab)



Kaspersky Lab non fornisce informazioni relative alla gestione e all'uso del sistema operativo e delle tecnologie associate.

---

# CAPITOLO 2. INSTALLAZIONE E DISINSTALLAZIONE DEL SOFTWARE

## 2.1. Requisiti hardware e software di sistema

Per poter eseguire **Kaspersky Anti-Hacker**, è necessario disporre di un sistema che soddisfi i seguenti requisiti hardware e software:

### Requisiti generali:

- Computer con sistema operativo Microsoft Windows 98/ME/NT 4.0/2000/XP installato
- Per effettuare l'installazione in ambiente Microsoft Windows NT 4.0/2000/XP, è necessario disporre dei diritti di amministratore
- Supporto protocollo TCP/IP
- Rete locale (Ethernet) o connessione modem (standard o ADSL)
- Microsoft Internet Explorer 5.0 o successiva)
- Almeno 50 MB di spazio libero su disco per i file del programma e ulteriore spazio per i registri di programma
- **Per l'esecuzione in Windows® 98/Me/NT 4.0, è necessario disporre di:**
  - Processore Intel Pentium® da 133 MHz o più in ambiente Windows 98 o Windows NT 4.0

- Processore Intel Pentium® da 150 MHz o più in ambiente Windows Me
- 32 MB di RAM
- Service Pack v. 6.0 o superiore per Windows NT 4.0 Workstation
- **Per l'esecuzione in ambiente Windows 2000, è necessario disporre di:**
  - Processore Intel Pentium® da 133 MHz o più
  - 64 MB di RAM
- **Per l'esecuzione in Windows XP, è necessario disporre di:**
  - Processore Intel Pentium® da 300 MHz o più
  - 128 MB di RAM

## 2.2. Installazione

Per installare il programma, eseguire il programma Setup.exe dal CD. La procedura di installazione guidata funziona in modalità finestra di dialogo. Ogni finestra di dialogo contiene un certo numero di pulsanti che consentono di gestire l'installazione. I pulsanti principali sono:

- **OK** – per confermare le azioni
- **Annulla** – per annullare una o più azioni
- **Avanti** – per passare alla fase successiva
- **Indietro** – per tornare alla fase precedente



Prima di installare Kaspersky Anti-Hacker chiudere tutte le applicazioni aperte.

## Fase 1. Leggere le informazioni generali

All'avvio del file setup.exe si apre la prima finestra di dialogo contenente informazioni generali sull'esecuzione della procedura di installazione guidata di Kaspersky Anti-Hacker.

Per procedere con l'installazione, fare clic sul pulsante **Avanti>**. Premere **Annulla** se si desidera interrompere l'installazione.

## Fase 2. Leggere il contratto di licenza

La finestra di dialogo successiva della procedura guidata contiene il testo del **Contratto di licenza** tra l'utente e Kaspersky Lab. Leggerlo attentamente e premere **Sì** per accettarne i termini e le condizioni.

## Fase 3. Inserire le informazioni sull'utente

Durante questa fase della procedura guidata, inserire il nome utente e la ragione sociale dell'azienda. Per impostazione predefinita, il programma di installazione guidata utilizza le informazioni memorizzate nel registro del SO. Esse potranno essere modificate successivamente.

Premere **Avanti>** per proseguire.

## Fase 4. Installare la chiave di licenza

In questa fase della procedura guidata viene installata la chiave di licenza di Kaspersky Anti-Hacker. La chiave di licenza è la "chiave" personale dell'utente, contenente tutte le informazioni necessarie per il corretto funzionamento del programma, cioè il nome e il numero della licenza e la relativa data di scadenza.



Senza chiave di licenza il programma non funziona.

Specificare il file della chiave di licenza nella finestra di dialogo standard di selezione file e premere il pulsante **Avanti>** per proseguire con l'installazione.

Se in fase di installazione del programma non si dispone della chiave di licenza (per esempio se il prodotto è stato richiesto a Kaspersky Lab tramite Internet ma non è stato ancora ricevuto) è possibile installarla in un secondo momento.

Ricordare che senza chiave di licenza non è possibile eseguire Kaspersky Anti-Hacker.

## **Fase 5. Selezionare la cartella in cui si desidera installare il programma**

In questa fase, Kaspersky Anti-Hacker individua la cartella in cui il programma sarà installato. Il percorso predefinito è **Programmi\Kaspersky Lab\Kaspersky Anti-Hacker**.

Per scegliere un percorso diverso, fare clic su **Sfoggia**, indicare il percorso della cartella nella finestra di dialogo standard di selezione e premere il pulsante **Avanti**>.

Al termine di questa fase, i file di programma di Kaspersky Anti-Hacker saranno copiati nel computer.

## **Fase 6. Copiare i file nel disco fisso**

L'avanzamento della copiatura dei file nel computer viene visualizzato nell'apposita finestra di dialogo.

## **Fase 7. Completare l'installazione**

La finestra di dialogo Installazione completata contiene informazioni sul completamento della procedura di installazione di Kaspersky Anti-Hacker.

Se il completamento della procedura richiede la registrazione di alcuni servizi, il programma propone all'utente di riavviare il computer. Questa operazione è necessaria per completare correttamente l'installazione del prodotto.



*Per completare l'installazione:*

1. Selezionare una delle seguenti opzioni:

- Sì. Riavvia adesso**
- No, non riavviare adesso**

2. Premere il pulsante **Fine**.

## 2.3. Installazione della chiave di licenza

Se durante la procedura di installazione di Kaspersky Anti-Hacker non è stata installata la chiave di licenza, il programma non funziona.

Per poter usare il programma è necessario installare la chiave di licenza.



*Per installare la chiave di licenza, seguire queste istruzioni:*

fare doppio clic sul file corrispondente. Esso verrà installato automaticamente.

OPPURE

copiare il file della chiave di licenza nella cartella **Programmi\File comuni\Kaspersky Lab**.

## 2.4. Disinstallazione del programma



*Per disinstallare Kaspersky Anti-Hacker, seguire queste istruzioni:*

premere il pulsante Start nella barra delle applicazioni di Windows e selezionare **Programmi → Kaspersky Anti-Hacker → Disinstalla Kaspersky Anti-Hacker**.

Così facendo si apre il programma di disinstallazione guidata.

## Fase 1. Prima finestra di dialogo della procedura di disinstallazione guidata

Questa finestra avverte che Kaspersky Anti-Hacker sta per essere rimosso dal computer. Per proseguire premere il pulsante **Avanti**>.

## Fase 2. Disinstallazione del programma dal computer

Questa finestra di dialogo contiene l'indicazione del percorso della cartella da cui viene rimosso il programma. Per disinstallare Kaspersky Anti-Hacker dal computer, premere il pulsante **Rimuovi**. La finestra di dialogo della disinstallazione guidata visualizza il processo di rimozione dei file.

## Fase 3. Completamento della disinstallazione

La finestra di dialogo **Rimozione completa** contiene informazioni sul completamento del processo di disinstallazione di Kaspersky Anti-Hacker. Per completare correttamente il processo è necessario riavviare il computer.



*Per completare la disinstallazione del programma seguire le seguenti istruzioni:*

1. Selezionare una delle opzioni per completare la procedura:

- Sì. Riavvia adesso**
- No, non riavviare adesso**

2. Premere il pulsante **Fine**.




È possibile disinstallare il programma anche dalla finestra di dialogo **Installazione applicazioni** accessibile dal **Pannello di controllo** standard di Windows.

---

## CAPITOLO 3. INIZIARE A LAVORARE

Al termine dell'installazione del programma e dopo aver riavviato il computer, il sistema di sicurezza è attivato. Da questo momento, Kaspersky Anti-Hacker sta monitorando il computer alla ricerca di attacchi provenienti dall'esterno e di tentativi delle applicazioni di interagire attraverso una rete locale o Internet.

Dopo aver attivato il sistema, il lavoro si svolgerà al pari di sempre. Qualora non sia stata stabilita alcuna connessione di rete, il sistema di sicurezza della macchina è indicato solo dall'icona  sulla barra delle applicazioni di Windows. Facendo clic su tale icona, si apre la finestra principale del programma. In questa finestra, è possibile consultare le informazioni relative al livello di sicurezza corrente e modificare tale livello, se necessario (per informazioni dettagliate sulla finestra principale del programma, cfr. paragrafo 5.3 a pag. 27). Di default, è abilitato il livello **Medio**. Questo livello consente di configurare il sistema di sicurezza in maniera interattiva. Nella maggior parte dei casi non è necessario configurare il sistema: le applicazioni di uso frequente sono autorizzate per impostazione predefinita a stabilire connessioni di rete in base alla tipologia cui appartengono. Tuttavia in qualche caso è necessario configurare manualmente il sistema di sicurezza. Esaminiamo l'esempio presentato di seguito.



**Compito:** supponiamo che il computer sia connesso a Internet, e di avviare Microsoft Internet Explorer e inserire l'indirizzo [www.kaspersky.com](http://www.kaspersky.com) nel campo degli indirizzi. Lo schermo visualizza il seguente messaggio: **Crea regola per IEXPLORER.EXE**

Nell'area superiore di questa finestra di dialogo compaiono l'icona dell'applicazione corrispondente, il nome (in questo caso Microsoft Internet Explorer), l'indirizzo del sito, [www.kaspersky.com](http://www.kaspersky.com), e la porta da usare per stabilire la connessione. Per ottenere informazioni più dettagliate su questa applicazione, è sufficiente fare clic sul link sottolineato

La necessaria connessione di rete non sarà stabilita fino a quando non saranno state selezionate le modalità di gestione dell'attività di questa applicazione. A tal fine, è necessario rispondere al messaggio visualizzato.

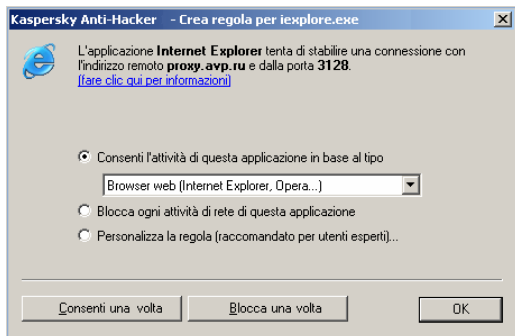


Fig. 1. Finestra di autoistruzione del sistema di sicurezza



Fig. 2. Informazioni sulla connessione da stabilire



Procedura:

1. Selezionare il pulsante **Consenti l'attività di questa applicazione in base al tipo e Web browser (IE, Netscape...)** dall'elenco a tendina.
2. Fare clic su **OK**.

Dopodiché Kaspersky Anti-Hacker consentirà a Microsoft Internet Explorer di stabilire la connessione. Inoltre, all'applicazione sarà consentito di stabilire altre connessioni conformemente al suo tipo.


La finestra di dialogo **Crea regola per IEXPLORER.EXE** prevede tre diverse opzioni:

- **Consenti l'attività di questa applicazione in base al tipo** (l'opzione selezionata nell'esempio precedente) - Consente solo la comunicazione di rete conforme a quanto indicato per la categoria dell'applicazione specificata. Selezionare la categoria desiderata dall'elenco a tendina sotto al pulsante opzione. È possibile consentire qualsiasi attività di questa applicazione selezionando **Consenti tutto** dall'elenco a tendina.

- **Blocca ogni attività di rete di questa applicazione** – Impedisce all'applicazione specificata qualsiasi tipo di attività di rete, inclusa l'operazione descritta.
- **Personalizza la regola** - Consente di specificare le operazioni consentite per questa applicazione. Selezionando questo pulsante opzione e facendo clic su **OK** si apre la finestra di composizione automatica delle regole. Usare la composizione automatica delle regole per definire i requisiti delle operazioni da consentire per questa applicazione (per informazioni più dettagliate sulla composizione automatica delle regole, cfr. paragrafo 6.3.2 a pag. 50).


Se non si è sicuri dell'opzione da selezionare, usare i pulsanti **Consenti una volta** o **Blocca una volta** nella parte inferiore della finestra di dialogo. In seguito si potrà monitorare il comportamento dell'applicazione e decidere quale opzione selezionare.



Chiudendo la finestra di autoistruzione mediante il pulsante  nell'angolo superiore destro, l'operazione in corso sarà immediatamente interrotta.

In questo modo è possibile configurare in maniera interattiva ed appropriata il sistema di sicurezza del computer.



Per consultare l'elenco delle regole definite, selezionare **Regole applicazione** dal menu **Assistenza** oppure premere il pulsante  nella barra degli strumenti della finestra principale.

Si raccomanda di usare il livello **Medio** le prime settimane dopo l'installazione del programma. Ciò consente al programma di configurare automaticamente il sistema di sicurezza in base alle reazioni dell'utente a eventi di rete di vario tipo. Creare le regole consentendo operazioni di rete standard.

Al termine del periodo di autoistruzione, è possibile impostare il programma sul livello **Alto** e garantire il computer contro qualsiasi evento di rete non autorizzato e attacco dall'esterno. Ricordare tuttavia che le applicazioni appena installate sono disabilitate di default dall'accesso a reti locali e/o a Internet. Per istruire il proprio Kaspersky Anti-Hacker in merito alla gestione di queste nuove applicazioni, è necessario ripristinare il livello **Medio** oppure definire manualmente le regole adeguate a queste applicazioni.

---

# CAPITOLO 4. PREVENZIONE DEGLI ATTACCHI PROVENIENTI DALL'ESTERNO DURANTE LE SESSIONI DI LAVORO IN INTERNET E LAN

## 4.1. Principi operativi di Kaspersky Anti-Hacker

Kaspersky Anti-Hacker protegge il computer dagli attacchi di rete e garantisce la sicurezza dei dati confidenziali. A tal fine, Kaspersky Anti-Hacker controlla tutte le operazioni di rete del computer. Esistono due tipi di operazioni di rete:

- Operazioni a livello di applicazione (livello Alto). A questo livello, Kaspersky Anti-Hacker analizza l'attività delle applicazioni di rete, inclusi browser web, programmi di posta elettronica, programmi per il trasferimento di file, ecc.
- Operazioni a livello di pacchetto (livello Basso). A questo livello, Kaspersky Anti-Hacker analizza pacchetti di dati inviati/ricevuti dalla propria scheda di rete o modem.

Si lavora con Kaspersky Anti-Hacker creando speciali regole di filtraggio per operazioni di rete. Parte del filtraggio viene eseguita automaticamente dal Sistema di rilevamento intrusioni, in grado di rilevare scansioni delle porte, attacchi DoS, ecc., e di bloccare quindi l'autore dell'attacco. Inoltre, è possibile definire le proprie regole di filtraggio in modo da rafforzare la protezione della macchina.

Per qualsiasi tipo di operazione di rete, vi sono elenchi separati di regole Kaspersky Anti-Hacker.

- *Regole applicazione.* Da qui è possibile selezionare l'applicazione desiderata e consentire un'attività conforme al tipo di applicazione. È possibile definire qualsiasi numero di regole per ogni applicazione, secondo le esigenze. In caso di rilevazione di una qualsiasi attività di rete non conforme alle condizioni specificate per la regola, il programma informa l'utente e consente di bloccare l'azione non desiderata (se è abilitato il livello **Medio**). Allo scopo di definire la regola più semplice per un'applicazione, è possibile selezionare il tipo dal menu a tendina (per informazioni più dettagliate, cfr. paragrafo 6.3.2.1 a pag. 50). Per definire una regola più complessa, è possibile specificare i servizi e gli indirizzi remoti consentiti per questa applicazione.
- *Regole di filtraggio pacchetti* consentono o impediscono l'invio o la ricezione di pacchetti di rete dalla macchina. Queste regole consultano l'intestazione del pacchetto (il protocollo usato, il numero delle porte, gli indirizzi IP, ecc.), e prendono decisioni in base a questi dati. Esse sono applicate a tutte le applicazioni di rete eseguite sulla macchina. Per esempio, se si crea una regola volta a bloccare un determinato indirizzo IP, qualsiasi comunicazione di rete dirette a tale indirizzo saranno proibite.



Le regole di filtraggio pacchetti hanno una priorità più elevata rispetto alle regole delle applicazioni, esse, cioè, vengono applicate per prime. Per esempio, se si crea una regola volta a bloccare tutti i pacchetti dati in entrata e in uscita, il programma non applicherà alcuna regola per le applicazioni durante il filtraggio dei pacchetti dati.

## 4.2. Livelli di sicurezza

Il programma consente di selezionare uno dei seguenti livelli di sicurezza:

- **Consenti tutto** – disabilita il sistema di sicurezza della macchina. Quando si seleziona questo livello di sicurezza, è consentita qualsiasi attività di rete sulla macchina.
- **Basso** – consente l'attività di rete di tutte le applicazioni ad eccezione di quelle esplicitamente proibite dalle regole per applicazioni definite dall'utente.
- **Medio** – informa l'utente in merito a eventi relativi alle applicazioni e consente di configurare il sistema di sicurezza per una prestazione

ottimale. Se un'applicazione di rete del computer cerca di connettersi alla rete locale o a Internet, viene attivata la modalità di autoistruzione. I dati relativi all'applicazione e all'operazione di rete sono visualizzati sullo schermo. In base a tali dati, il programma invita l'utente a selezionare una delle seguenti azioni: consentire o impedire una volta questo evento, bloccare completamente l'attività di questa applicazione, consentire l'attività dell'applicazione in base al tipo, oppure definire delle impostazioni di comunicazione di rete supplementari. In base alla risposta, il programma crea una regola per l'applicazione che in seguito il programma applicherà automaticamente.

- **Alto** – impedisce l'attività di rete di tutte le applicazioni ad eccezione di quelle esplicitamente consentite dalle regole per applicazioni definite dall'utente. Quando è abilitato questo livello di sicurezza, la finestra di dialogo di autoistruzione del programma non viene visualizzata, e qualsiasi tentativo di stabilire connessioni non definite dalle regole dell'utente è bloccato.



Tutte le applicazioni installate dopo l'attivazione di questo livello di sicurezza vengono disabilitate di default dall'accesso a Internet o alla rete locale.

- **Blocca tutto** – disabilita il computer dall'accesso a Internet o alla rete locale. Questo livello crea una situazione in cui qualsiasi tentativo di stabilire una connessione attraverso Internet o la rete locale viene bloccato se il computer è fisicamente scollegato.

Con il livello **Alto**, **Medio** o **Basso** abilitato, è possibile impostare un'ulteriore strumento per la sicurezza: la modalità **Invisibile** (cfr. paragrafo 5.3.3 a pag. 32). Questa modalità consente solo l'attività di rete avviata dall'utente stesso, proibendo qualsiasi altro tipo di attività (accesso remoto alla macchina, controllo della macchina per mezzo dell'utilità ping, ecc.) se non esplicitamente consentito dalle regole dell'utente.

In realtà, ciò significa che il computer viene reso "invisibile" dall'esterno. Così i pirati informatici perdono traccia dell'obiettivo e i loro tentativi di accesso al computer sono destinati a fallire. Ciò consente inoltre di prevenire attacchi DoS (Denial of Service) di ogni tipo.

Questa modalità tuttavia non influisce minimamente sulla fluidità della navigazione in rete: Kaspersky Anti-Hacker consente l'attività di rete avviata dalla macchina.

Attenzione! Il sistema di rilevamento intrusioni viene abilitato per tutti i livelli di sicurezza ad eccezione di **Consenti tutto**. Tuttavia, se necessario, è possibile disabilitarlo manualmente (cfr. paragrafo 6.5.1a pag. 71).



## 4.3. Impostazioni raccomandate

Quali componenti di Kaspersky Anti-Hacker si dovrebbero utilizzare e quale livello di sicurezza è opportuno selezionare? La risposta dipende dal compito che si desidera svolgere.



### Compito 1. Come proteggere i propri dati contro attacchi esterni perpetrati tramite Internet?



I due metodi descritti di seguito sono due tra i più usati dai pirati informatici per impadronirsi o danneggiare dati dell'utente tramite Internet: penetrazione in un computer servendosi di errori di software del computer, e infezione di un computer per mezzo di Troiani.

Se si scopre l'esistenza di un errore in uno dei programmi installati sulla propria macchina, creare una regola di blocco per questa applicazione. Si consiglia di creare una regola di blocco complessa (cfr. paragrafo 6.3.2.1a pag. 50) che prenda in considerazione le caratteristiche di questo errore.

Supponiamo che il computer sia stato infettato da un Troiano ricevuto tramite un dischetto o un messaggio di posta elettronica e che il programma maligno cerchi di inviare dei dati tramite Internet. Kaspersky Anti-Hacker garantirà facilmente la sicurezza dei dati bloccando questa operazione (al livello **Alto**), o emettendo un avvertimento adeguato (al livello **Medio**).



**Attenzione!!! Kaspersky Anti-Hacker non protegge il computer da virus e programmi maligni.**

Per esempio, un Cavallo di Troia (Trojan) può usare un programma di posta elettronica standard presente sul computer per inviare dati confidenziali dell'utente. In questo caso, Kaspersky Anti-Hacker non è in grado di impedire l'azione. Inoltre, se il computer è stato infettato da un virus o da un programma maligno, è possibile che i dati vengano semplicemente distrutti e che il computer possa diventare una fonte di infezione. In questo caso, Kaspersky Anti-Hacker può eliminare solo in parte le conseguenze dell'infezione. Per proteggere efficacemente il sistema da virus e programmi maligni, è consigliabile usare il programma antivirus Kaspersky Anti-Virus Personal/Personal anti-virus in combinazione con Kaspersky Anti-Hacker. Si raccomanda di creare delle regole per applicazioni che consentano al computer di avviare attività strettamente in base al tipo. Si raccomanda inoltre di usare l'elenco di regole per applicazioni per assegnare quei tipi di attività alle attività strettamente corrispondenti alle operazioni consentite per tali applicazioni. In tal modo, il rischio di operazioni di rete non autorizzate eseguite sulla macchina sarà ridotto al minimo.



Supponiamo di scoprire che il computer è attaccato costantemente da una macchina remota.

### **Compito 2. Come bloccare questi attacchi da determinati indirizzi Internet?**



Si può proibire al computer di comunicare con tali indirizzi remoti configurando le opportune regole di filtraggio pacchetti. Per esempio, la fig. 3 illustra una regola che blocca la comunicazione con l'indirizzo 111.111.111.111.

Per impedire che si verifichino tali situazioni, è consigliabile tenere abilitato il sistema di rilevamento intrusioni.

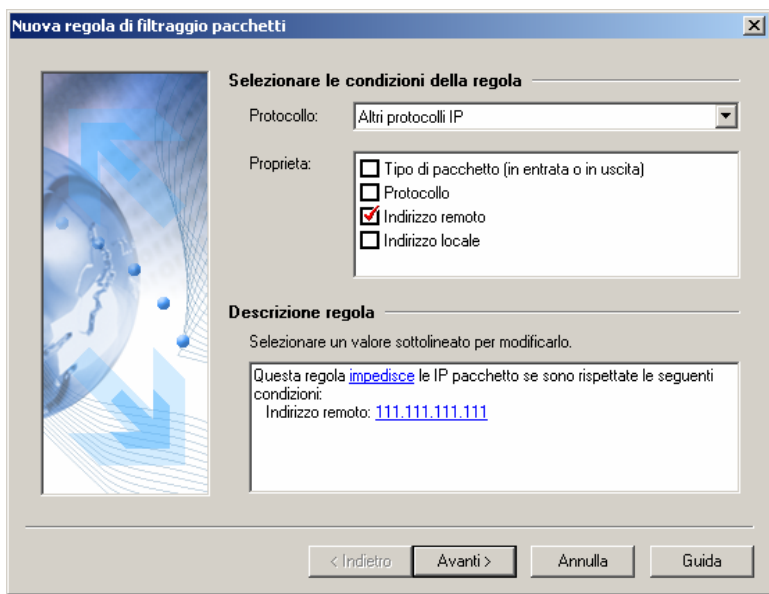


Fig. 3. La regola che blocca la comunicazione con indirizzi non affidabili



Per esempio, si può utilizzare Kaspersky Anti-Hacker per bloccare la visualizzazione di banner sulle pagine web. Per fare questo, creare una regola di filtraggio pacchetti per bloccare la comunicazione con i siti web da cui vengono solitamente caricati i banner (per esempio, [linkexchange.ru](http://linkexchange.ru)).



Supponiamo di temere degli attacchi dalla rete locale o di desiderare di proteggere i propri dati personali dai pirati.

### Compito 3. È necessario monitorare le attività di rete locale



Il computer comunica con una rete locale al livello del sistema operativo, pertanto non è sempre possibile identificare l'applicazione coinvolta. In questo caso è necessario creare un'apposita regola di filtraggio pacchetti per garantire la sicurezza dei propri dati.

Per semplificare la configurazione del sistema di sicurezza, Kaspersky Anti-Hacker preinstalla alcune regole di filtraggio pacchetti che consentono la comunicazione attraverso la rete locale. Di default, la rete locale è consentita. Tuttavia, è possibile ridefinire le regole di filtraggio pacchetti in modo da bloccare completamente l'accesso alla rete locale, o consentirlo solo per determinati computer.

---


# CAPITOLO 5. AVVIO DEL PROGRAMMA

## 5.1. Avvio del programma

Kaspersky Anti-Hacker è avviato automaticamente con il sistema operativo. Se si chiude il programma, è possibile riavviarlo manualmente.



*Per avviare Kaspersky Anti-Hacker, seguire queste istruzioni:*


1. Premere il pulsante **Avvio** nell'angolo inferiore sinistro del desktop di Windows e selezionare **Programmi → Kaspersky Anti-Hacker → Kaspersky → Anti-Hacker**.
2. Fare clic con il pulsante sinistro del mouse sull'icona  nella barra delle applicazioni di Windows, oppure fare clic con il pulsante destro e selezionare **Apri Kaspersky Anti-Hacker** dal menu di scelta rapida del programma.

Si apre la finestra principale di Kaspersky Anti-Hacker (cfr. paragrafo 5.3 a pag. 27).



È inoltre possibile avviare il programma direttamente dalla relativa directory. Per fare questo, aprire la cartella di Kaspersky Anti-Hacker in Windows Explorer (la directory di default del programma è **C:\Programmi\Kaspersky Lab\Kaspersky Anti-Hacker**). Fare doppio clic sul file **KAVPF.exe** incluso in questa directory.

## 5.2. Menu di sistema

Dopo aver avviato il programma, viene visualizzata l'icona  nella barra delle applicazioni di Windows.

Facendo clic con il pulsante destro del mouse su questa icona è possibile visualizzare il menu di scelta rapida (cfr. fig. 4) contenente i seguenti comandi:

Tabella 1

Elemento di menu	Funzione
<b>Apri Kaspersky Anti-Hacker...</b>	Apre la finestra principale dell'applicazione.
<b>Livello di sicurezza</b>	Seleziona un livello di sicurezza: <b>Blocca tutto</b> , <b>Alto</b> , <b>Medio</b> , <b>Basso</b> , <b>Consenti tutto</b> . Per informazioni più dettagliate sui livelli di sicurezza, cfr. paragrafo 4.2 a pag. 20.
<b>Informazioni su Kaspersky Anti-Hacker ...</b>	Apre una finestra di dialogo contenente informazioni sulla versione del programma e sui tasti usati.
<b>Esci</b>	Chiude il programma.

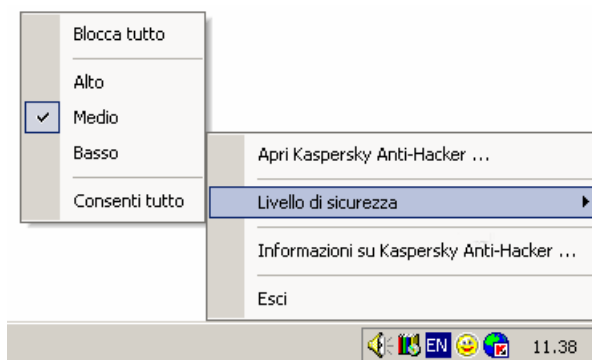


Fig. 4. Menu di scelta rapida

## 5.3. Finestra principale

Dopo l'avvio del programma, viene visualizzata la finestra principale dell'applicazione (cfr. fig. 5). La finestra principale di Kaspersky Anti-Hacker consente di selezionare il livello di sicurezza corrente, di visionare lo stato corrente del sistema di sicurezza, di modificare le impostazioni di filtraggio pacchetti e di consultare/configurare i registri del programma.

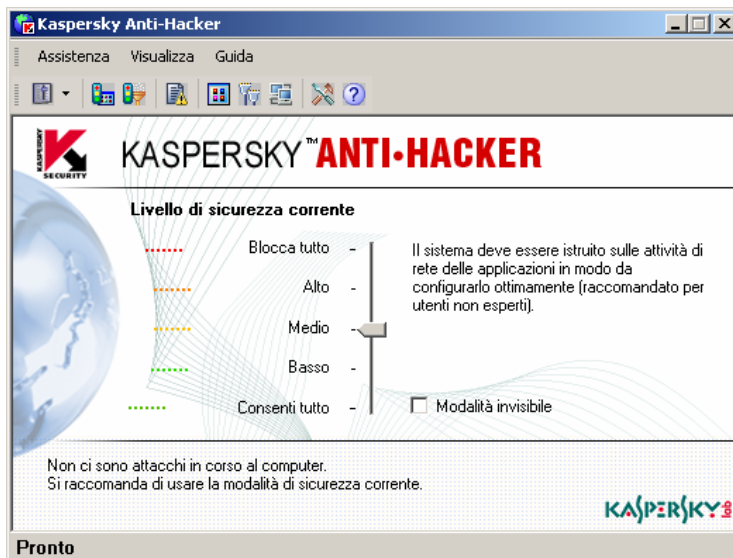


Fig. 5. La finestra principale dell'applicazione di **Kaspersky Anti-Hacker**

La finestra principale di Kaspersky Anti-Hacker contiene i seguenti elementi:

- Menu
- Barra degli strumenti
- Area di lavoro
- Barra di stato

### 5.3.1. Menu

Nella parte superiore della finestra principale si trova una *barra dei menu*. Essa può essere trascinata con il mouse ovunque all'interno o all'esterno della finestra principale.

Alcuni comandi di menu possono inoltre essere attivati mediante gli appositi pulsanti nella barra degli strumenti. Per informazioni più dettagliate sulle funzioni

corrispondenti ai pulsanti della barra degli strumenti e ai comandi di menu, cfr. paragrafo 5.3.2 a pag. 31.

Tabella 2

Menu → comando	Funzione
Assistenza → Regole applicazione	Apre la finestra delle regole dell'applicazione.
Assistenza → Regole filtraggio pacchetti	Apre la finestra delle regole di filtraggio pacchetti.
Assistenza → Livello di sicurezza	<p>Impostazione del livello di sicurezza desiderato:</p> <ul style="list-style-type: none"> <li>• Blocca tutto</li> <li>• Alto</li> <li>• Medio</li> <li>• Basso</li> <li>• Consenti tutto</li> </ul> <p>Inoltre è possibile selezionare il livello di sicurezza desiderato dalle opzioni dell'area di lavoro della finestra. Per informazioni più dettagliate, cfr. paragrafo 4.2 a pag. 20.</p>
Assistenza → Impostazioni	Apre una finestra in cui configurare i propri registri di sicurezza, l'avvio del sistema di sicurezza e le impostazioni di rilevamento attacchi.
Assistenza → Uscita	Chiude il programma.

Menu → comando	Funzione
Visualizza → Barre degli strumenti	Definizione delle opzioni di interfaccia grafica del programma: <ul style="list-style-type: none"> <li>• <b>Barra degli strumenti standard</b> – visualizza/nasconde la barra degli strumenti standard</li> <li>• <b>Personalizza</b> – visualizza una finestra di dialogo in cui è possibile personalizzare l'interfaccia grafica del programma</li> </ul>
Visualizza → Barra di stato	Visualizza / nasconde la barra di stato.
Visualizza → Registri	Apre la finestra registri per: <ul style="list-style-type: none"> <li>• <b>Sicurezza</b></li> <li>• <b>Attività delle applicazioni</b></li> <li>• <b>Filtraggio pacchetti</b></li> </ul>
Visualizza → Mostra	Apre i riquadri di informazioni con i dati di sistema. <ul style="list-style-type: none"> <li>• <b>Applicazioni attive</b> è l'elenco delle applicazioni di rete attive</li> <li>• <b>Porte aperte</b> è l'elenco delle porte aperte della macchina</li> <li>• <b>Connessioni stabilite</b> è l'elenco delle connessioni stabilite</li> </ul>
Guida in linea → Sommario...	Apre gli argomenti della Guida in linea.
Guida in linea → Informazioni su Kaspersky Anti-Hacker...	Apre un riquadro contenente informazioni sul programma e sui tasti usati.
Guida in linea → Kaspersky Anti-Hacker sul Web...	Apre la pagina del sito web ufficiale di Kaspersky Lab




## 5.3.2. Barra degli strumenti







La barra degli strumenti del programma si trova sotto la barra dei menu. Se necessario, è possibile trascinarla con il mouse su qualsiasi posizione all'interno o all'esterno della finestra principale.

La *barra degli strumenti* contiene dei pulsanti, la cui pressione dà inizio a vari comandi. Inoltre è possibile nascondere e visualizzare la barra degli strumenti selezionando il comando **Standard** dal sottomenu **Barra degli strumenti** del menu **Visualizza**.

È possibile aggiungere o eliminare pulsanti dalla barra degli strumenti (cfr. paragrafo 5.6 a pag. 34).

Tabella 3

Pulsante	Menu → Comando	Funzione
	Assistenza → Livello di sicurezza	Impostazione del livello di sicurezza desiderato: <ul style="list-style-type: none"> <li>• Blocca tutto</li> <li>• Alto</li> <li>• Medio</li> <li>• Basso</li> <li>• Consenti tutto</li> </ul> Per informazioni più dettagliate, cfr. paragrafo 4.2 a pag. 20.
	Assistenza → Regole applicazione	Apre la finestra delle regole dell'applicazione.
	Assistenza → Regole di filtraggio pacchetti	Apre la finestra delle regole di filtraggio pacchetti.

Pulsante	Menu → Comando	Funzione
	Visualizza → Registri → Sicurezza	Aprire la finestra dei registri di sicurezza.
	Visualizza → Mostra → Applicazioni attive	Mostra l'elenco delle applicazioni di rete attive.
	Visualizza → Mostra → Porte aperte	Mostra l'elenco delle porte aperte della macchina.
	Visualizza → Mostra → Connessioni stabilite	Mostra l'elenco delle connessioni stabilite.
	Assistenza → Impostazioni	Aprire una finestra in cui configurare i propri registri di sicurezza, l'avvio del sistema di sicurezza e le impostazioni di rilevamento attacchi.
	Guida in linea → Sommario...	Aprire gli argomenti della Guida in linea.

### 5.3.3. Area di lavoro

L'area di lavoro della finestra principale contiene la *scala di sicurezza* e le informazioni relative allo stato corrente del sistema di sicurezza.

La scala di sicurezza consente di selezionare uno dei seguenti livelli di sicurezza:

- **Blocca tutto**
- **Alto**
- **Medio**
- **Basso**
- **Consenti tutto**

È possibile modificare il livello di sicurezza trascinando il cursore lungo la scala. Così facendo, si visualizza una descrizione dettagliata del livello di sicurezza selezionato a destra della nuova posizione del cursore (per informazioni più dettagliate, cfr. paragrafo 4.2 a pag. 20). La nuova modalità è applicata immediatamente.

Con i livelli **Alto**, **Medio** or **Basso** abilitati, è possibile impostare lo strumento di sicurezza supplementare, la **modalità invisibile** (cfr. paragrafo 4.2 a pag. 20).

Sotto la scala vi sono dati sull'ultimo attacco informatico rilevato dal programma. Le varie informazioni comprendono la data e l'ora dell'attacco, il tipo di attacco e l'indirizzo del computer di provenienza.

### 5.3.4. Barra di stato

Nella parte inferiore della finestra principale si trova una *barra di stato*. Essa visualizza suggerimenti per l'utente sull'uso dell'elemento della finestra principale correntemente selezionato. Inoltre è possibile nascondere e visualizzare la barra selezionando il comando **Barra di stato** dal menu **Visualizza**.

## 5.4. Menu di scelta rapida delle finestre di dialogo

I *menu di scelta rapida* nelle finestre di dialogo del programma consentono di attivare comandi applicabili a una particolare finestra di dialogo.



*Per visualizzare il menu contestuale della finestra di dialogo, fare clic con il pulsante destro del mouse al suo interno.*

## 5.5. Composizione guidata delle regole

La funzione di composizione guidata del programma che consente di creare/modificare regole dell'utente contiene numerose finestre di dialogo. Ogni finestra di dialogo contiene una serie di pulsanti che consentono all'utente di gestire il processo della creazione/modifica delle regole. Questi pulsanti sono:

- **Fine** – applica le impostazioni definite e crea la regola.
- **Annulla** – annulla la procedura.
- **Avanti >** – passa alla finestra successiva dell'applicazione.
- **< Indietro** – torna alla finestra precedente dell'applicazione.
- **Guida** – visualizza gli argomenti della Guida.

## 5.6. Modifica e salvataggio delle impostazioni dell'interfaccia



*Per modificare le impostazioni dell'interfaccia, selezionare **Personalizza** dal sottomenu **Barre degli strumenti** del menu **Visualizza**.*

Si apre la finestra di dialogo **Personalizza** (cfr. fig. 6).

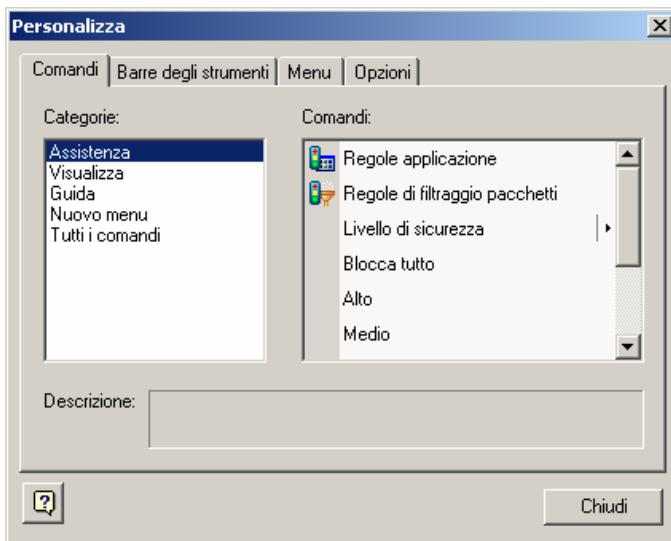


Fig. 6. La finestra di dialogo **Personalizza**

Durante la modifica dell'interfaccia, è consigliabile organizzare lo schermo in modo che la finestra di dialogo **Personalizza** non si sovrapponga alla barra dei menu della finestra principale e alla barra degli strumenti.

È possibile utilizzare la pagina **Comandi** per modificare il layout del menu della finestra principale e della barra degli strumenti.

Per aggiungere nuovi comandi è necessario trascinare i comandi desiderati dall'elenco alla barra dei menu o alla barra degli strumenti.

Per eliminare un comando dalla barra dei menu o dalla barra degli strumenti è necessario trascinarlo fuori dalla finestra principale.

Le pagine **Barre degli strumenti** e **Menu** consentono di ripristinare l'aspetto originale delle barre degli strumenti e dei menu.

La pagina **Impostazioni** consente di abilitare/disabilitare i suggerimenti a video relativi ai pulsanti della barra degli strumenti, di selezionarne le dimensioni e definire il layout della barra dei menu.

Se necessario, è possibile modificare le intestazioni dei pulsanti e dei comandi di menu e visualizzare i pulsanti della barra degli strumenti come immagini o come testo.



*Per modificare tali intestazioni e/o altre proprietà di un comando o di un pulsante, seguire queste istruzioni:*

1. Visualizzare la finestra di dialogo **Personalizza** e selezionare il comando o pulsante desiderato all'interno della finestra principale.
2. Fare clic con il pulsante destro del mouse. Selezionare il comando desiderato dal menu contestuale:
  - **Cancella** – rimuove il comando di menu o pulsante selezionato.
  - **Aspetto del pulsante** – consente di modificare l'intestazione. Si apre una finestra di dialogo con lo stesso nome. Modificare l'intestazione del pulsante/comando di menu nel campo **Testo del pulsante** (cfr. fig. 7). Fare clic su **OK**.
  - **Solo immagine** – visualizza come immagine il comando di menu/pulsante selezionato.


- **Solo testo** – visualizza come testo il comando di menu/pulsante selezionato.
- **Bitmap e testo** – visualizza come immagine integrata da testo il comando di menu/pulsante selezionato.
- **Inizio gruppo** – inserisce un separatore prima del comando di menu/pulsante selezionato.



Fig. 7. Modifica delle proprietà dei comandi

Le nuove impostazioni dell'interfaccia sono salvate automaticamente e subito applicate. Queste modifiche saranno mantenute durante tutte le sessioni successive del programma.

## 5.7. Uscita dal programma

Per chiudere il programma dalla memoria del computer, selezionare **Esci** dal menu di scelta rapida o dal menu **Assistenza** della finestra principale dell'applicazione. Inoltre è possibile chiudere la finestra principale facendo clic sul pulsante  nell'angolo superiore destro della finestra stessa.




Tuttavia, la chiusura della finestra principale del programma non scarica il programma dalla memoria del computer se la casella di controllo **Riduci ad icona la finestra principale del programma nella barra delle applicazioni alla chiusura** è selezionata. Di default, questa casella è selezionata, ma se necessario è possibile deselegzionarla (cfr. paragrafo 6.1.1 a pag. 38). Posizionando l'icona nella barra delle applicazioni di Windows, il programma indica che è caricato nella memoria del computer.

---

# CAPITOLO 6. ABILITAZIONE DEL SISTEMA DI SICUREZZA E DEFINIZIONE DELLE SUE IMPOSTAZIONI

## 6.1. Abilitazione del sistema di sicurezza e selezione del livello di sicurezza

### 6.1.1. Abilitazione del sistema di sicurezza

Il sistema di sicurezza viene attivato non appena si installa Kaspersky Anti-Hacker sul computer e si riavvia il sistema operativo. Dopo aver avviato il programma, viene visualizzata l'icona  nella barra delle applicazioni di Windows. Di default, il programma implementa il livello **Medio** e se un'applicazione di rete del computer cerca di connettersi a una rete locale o a Internet, viene attivata la modalità di autoistruzione. I dati relativi all'applicazione e all'operazione di rete sono visualizzati sullo schermo. In base a tali dati, il programma invita l'utente a selezionare una delle seguenti azioni: consentire o impedire una volta questo evento, bloccare completamente l'attività di questa applicazione, consentire l'attività dell'applicazione in base al tipo, oppure definire una regola complessa per questo evento. In base alla risposta, il programma crea una regola per l'applicazione che in seguito applicherà automaticamente.

Kaspersky Anti-Hacker inizia a proteggere il computer dopo la connessione da parte dell'utente. Tuttavia, è possibile impostare il programma in modo da abilitare la sicurezza con l'avvio stesso del sistema operativo Windows.



Per abilitare/disabilitare l'esecuzione automatica di Kaspersky Anti-Hacker all'avvio del sistema operativo, seguire queste istruzioni:

1. Selezionare **Impostazioni** dal menu **Assistenza**.
2. Nella pagina **Generali** della finestra di dialogo **Impostazioni** (cfr. fig. 8), selezionare la casella di controllo  **Lancia il sistema di sicurezza all'avvio del sistema operativo**. In tal caso, il programma viene avviato con le impostazioni dell'utente immediatamente dopo l'avvio del sistema operativo, ma i registri sono disabilitati. Se il programma implementa il livello **Medio**, tutte le comunicazioni di rete saranno automaticamente consentite fino all'accesso al sistema operativo perché la finestra di autoistruzione non può essere visualizzata in mancanza di un utente nel sistema. Ai livelli **Basso** o **Consenti tutto**, il programma consente comunicazioni di rete ignote per il periodo di tempo corrente, mentre agli altri livelli di sicurezza tutte le comunicazioni di rete ignote sono bloccate.



Supponiamo che il computer sia collegato a una rete locale e che il programma sia stato abilitato in modo da lanciare il sistema di sicurezza all'avvio del sistema operativo. Supponiamo inoltre che l'utente abbia scelto di bloccare tutto il traffico di rete selezionando il livello di sicurezza **Blocca tutto**, oppure creando una regola di filtraggio pacchetti appropriata a qualsiasi livello di sicurezza (ad eccezione di **Consenti tutto**). In questo caso, sarà necessario attendere più a lungo del solito prima di accedere al sistema, e dopo l'accesso l'utente scoprirà che la rete locale non è disponibile.

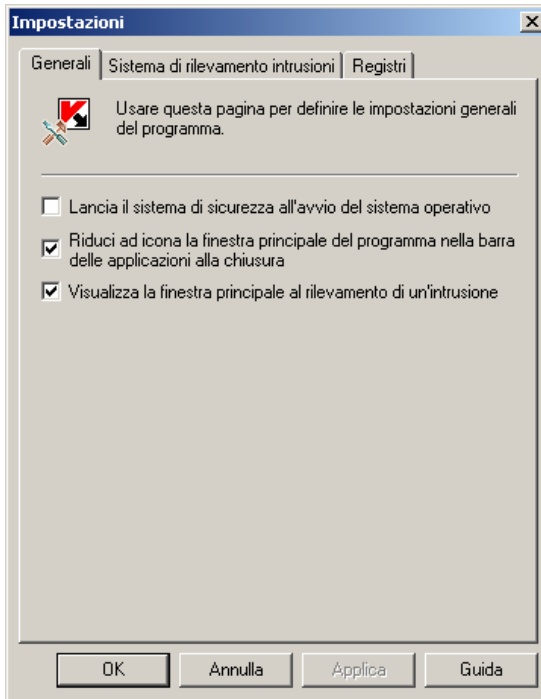




Fig. 8. La finestra di dialogo **Impostazioni**

È possibile modificare l'assegnazione del pulsante  nell'angolo superiore destro della finestra principale. Di default, questo pulsante riduce la finestra principale a icona nella barra delle applicazioni di Windows mentre il programma resta nella memoria del computer.



*Per modificare l'assegnazione del pulsante  in modo che scarichi il programma dalla memoria del computer alla chiusura della finestra principale, seguire queste istruzioni:*

1. Selezionare **Impostazioni** dal menu **Assistenza**.
2. Nella pagina **Generali** della finestra di dialogo **Impostazioni** (cfr. fig. 8) deselezionare la casella di controllo  **Riduci a icona la finestra principale del programma nella barra delle applicazione alla chiusura**.

Di default, se il programma rileva un attacco alla macchina, viene visualizzata la finestra principale con il messaggio corrispondente.



Per disabilitare la visualizzazione della finestra principale ogni volta che viene rilevata un'intrusione, seguire queste istruzioni:

1. Selezionare **Impostazioni** dal menu **Assistenza**.
2. Nella pagina **Generali** della finestra di dialogo **Impostazioni** (cfr. fig. 8) deselezionare la casella di controllo  **Visualizza la finestra principale al rilevamento di un'intrusione**.

## 6.1.2. Selezione del livello di sicurezza

È possibile modificare il livello di sicurezza trascinando il cursore lungo la scala di sicurezza all'interno della finestra principale del programma oppure selezionando il comando **Livello di sicurezza** dal menu **Assistenza**. In alternativa, è possibile selezionare il comando appropriato dal menu di sistema.

Il programma consente di passare a uno dei seguenti livelli di sicurezza:

- **Blocca tutto**;
- **Alto**;
- **Medio**;
- **Basso**;
- **Consenti tutto**.

Con i livelli **Alto**, **Medio** o **Basso** abilitati, è possibile abilitare uno strumento di sicurezza supplementare selezionando la casella di controllo  **modalità invisibile**.



I livelli di sicurezza vengono applicati non appena l'utente li ha selezionati.

Per informazioni più dettagliate sui livelli di sicurezza disponibili, cfr. paragrafo 4.2 a pag. 20.

### 6.1.3. Avvertimenti sugli eventi di rete

Se è stata creata una regola selezionando la casella di controllo  **Visualizza avvertimento** (cfr. paragrafi 6.3.2.3 a pag. 61 e 6.4.2.2 a pag. 69), quando il programma applica questa regola viene visualizzato il messaggio corrispondente (cfr. fig. 9).

Per un esempio di tale messaggio, che appare dopo l'applicazione di una regola di filtraggio pacchetti, cfr. fig. 9. Il messaggio indica i relativi indirizzi locale e remoto e le porte usate.

È possibile consultare la regola di filtraggio pacchetti corrispondente facendo clic sul collegamento ipertestuale.

Inoltre è possibile disabilitare qualsiasi avvertimento successivo per questo evento selezionando la casella di controllo  **Non visualizzare questo avvertimento**.

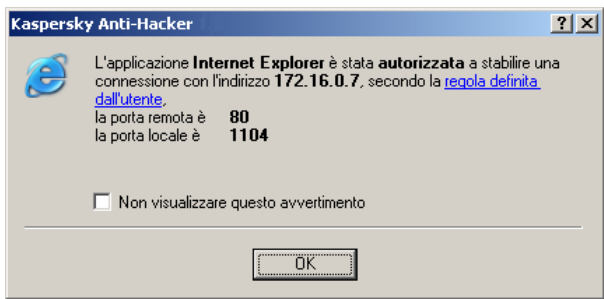


Fig. 9. Un esempio di avvertimento su un evento



Durante la creazione di una regola, è possibile selezionare la casella di controllo  **Registra evento** per registrare l'evento corrispondente.

### 6.1.4. Finestra Autoistruzione (Livello Medio)

Il programma visualizza la finestra di autoistruzione (cfr. fig. 10) quando rileva un evento ignoto durante l'esecuzione con il livello **Medio** selezionato.

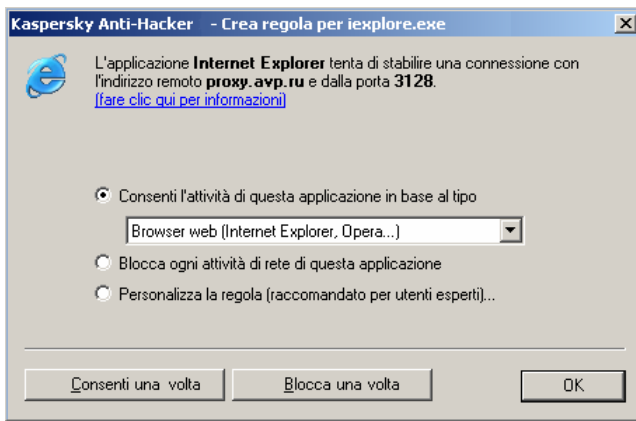



Fig. 10. Un esempio di finestra di autoistruzione

Nella parte superiore di questo riquadro sono visibili il nome dell'applicazione che richiede la connessione con una macchina remota, l'indirizzo della macchina remota e il numero delle porte. Se necessario, è possibile visualizzare ulteriori dati sulla connessione richiesta facendo clic sul collegamento ipertestuale [... informazioni](#).

È possibile consentire o bloccare questa operazione specifica facendo clic rispettivamente sui pulsanti **Consenti una volta** o **Blocca una volta**.



Chiudendo la finestra di autoistruzione per mezzo del pulsante  nell'angolo superiore destro, l'operazione in corso sarà immediatamente interrotta.

Per definire una regola in grado di gestire successivamente eventi iniziati da questa applicazione, selezionare una delle azioni elencate di seguito e fare clic sul pulsante **OK**. Dopodiché, la nuova regola sarà aggiunta all'elenco delle regole per applicazioni.

- **Consenti l'attività dell'applicazione in base al tipo** – consente solo la comunicazione di rete conforme a quanto indicato per il tipo di applicazione specificato. Selezionare il tipo desiderato dall'elenco a tendina sotto il pulsante dell'opzione (per informazioni più dettagliate cfr. paragrafo 6.3.2.1 a pag. 50).
- **Disabilita tutte le attività dell'applicazione** – Impedisce all'applicazione specificata qualsiasi tipo di attività di rete, inclusa l'operazione descritta.

- **Personalizza la regola ...** – Consente di specificare le operazioni consentite per questa applicazione. Selezionando questo pulsante opzione e facendo clic su **OK**, si apre la finestra di composizione guidata regole (per informazioni più dettagliate sulla composizione guidata cfr. paragrafo 6.3.2 a pag. 50).



Se la regola creata non corrisponde all'evento descritto, viene visualizzato il messaggio appropriato (cfr. fig. 11). Quindi è possibile premere il pulsante **Sì** per aggiungere la regola creata all'elenco, oppure il pulsante **No** se la regola è stata creata per errore. In entrambi i casi, un messaggio invita a selezionare un'altra opzione dall'elenco della finestra di autoistruzione.

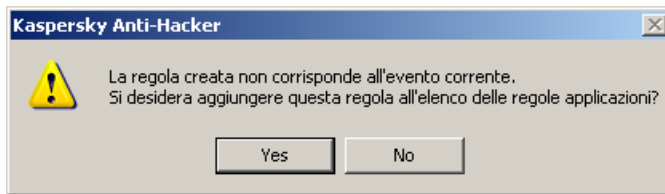


Fig. 11. La regola creata non corrisponde all'evento corrente



Se diversi programmi del computer tentano entro breve di eseguire operazioni di rete non descritte dalle regole dell'utente, sarà creata una *coda di richieste* per la creazione di regole. Tali richieste saranno visualizzate successivamente all'interno della finestra di autoistruzione: innanzitutto sarà necessario definire la risposta del programma alle azioni della prima applicazione di rete, quindi della seconda, ecc. Tutti i programmi di questa coda restano in attesa della reazione dell'utente.

## 6.1.5. L'avvertimento di sostituzione del modulo eseguibile

Kaspersky Anti-Hacker protegge le applicazioni di rete contro qualsiasi tentativo non autorizzato di sostituire i file eseguibili originali. Se Kaspersky Anti-Hacker rileva una tale sostituzione, il programma visualizza il messaggio di avvertimento appropriato (cfr. figura 12).

È possibile selezionare una delle seguenti opzioni:

- **Blocca qualsiasi attività di rete di questa applicazione** – qualsiasi ulteriore operazione di rete di questa applicazione sarà proibita: la regola di blocco corrispondente sarà aggiunta all'inizio dell'elenco di

regole dell'applicazione e tutte le altre regole di questo elenco saranno disabilitate. È consigliabile avviare il programma antivirus per verificare che l'applicazione non sia infetta, oppure ripristinare l'applicazione dall'archivio, o reinstallarla. Fatto questo, eliminare la regola di blocco dall'elenco delle regole dell'applicazione e abilitare tutte le altre regole dell'elenco. Se Kaspersky Anti-Hacker visualizza di nuovo il messaggio "modulo eseguibile sostituito", selezionare l'opzione sottostante.

- **So che il file è stato modificato e continuo a ritenere sicura questa applicazione** – tutte le regole dell'utente correntemente disponibili per questa applicazione saranno valide anche per il file modificato.

Fare clic su **OK**.

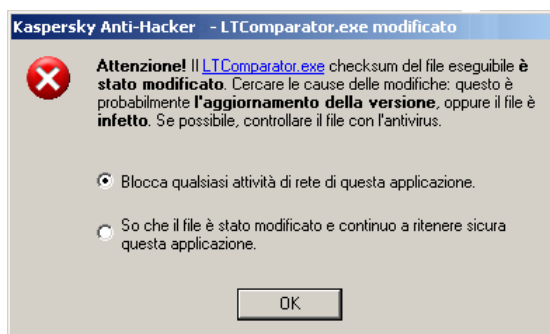


Fig. 12. L'avvertimento di sostituzione del modulo eseguibile

## 6.2. Risposte del programma agli attacchi

Se il sistema di sicurezza rileva un attacco ai danni della macchina, viene visualizzata la finestra principale del programma (a meno che non sia stata deselezionata la casella di controllo  **Visualizza la finestra principale al rilevamento di un'intrusione** - cfr. paragrafo 6.1.1 a pag. 38). In tal caso, leggere attentamente i dati relativi all'attacco nella parte inferiore dell'area di lavoro della finestra; il programma visualizza la data, l'ora e il tipo di attacco (cfr. fig. 15).

Questo attacco sarà bloccato. Il programma bloccherà anche la macchina da cui è partito l'attacco per il periodo di tempo definito dalle impostazioni (cfr. Paragrafo 6.5 a pag. 71).

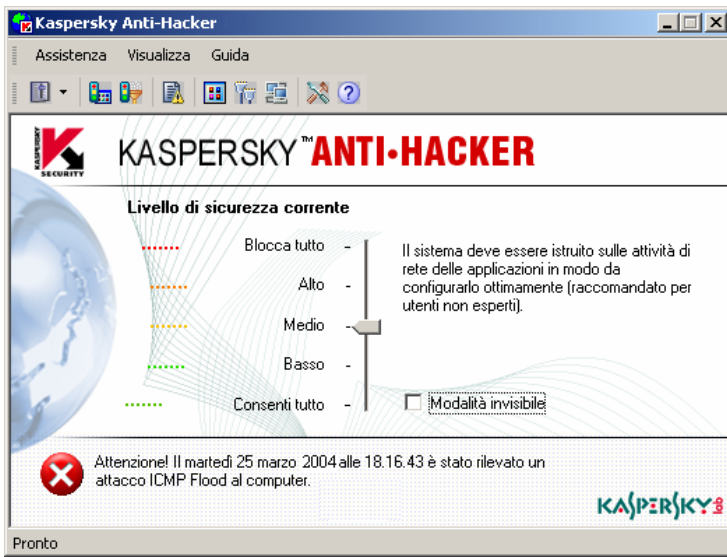


Fig. 13. Messaggio relativo alla rilevazione di un attacco

Supponiamo di scoprire che il computer è attaccato costantemente da una macchina remota. Si può proibire al computer di comunicare con tali indirizzi remoti configurando le opportune regole di filtraggio pacchetti (cfr. paragrafo 6.4 a pag. 62).

Se gli attacchi provenienti da un determinato indirizzo remoto sono frequenti, è consigliabile attivare il livello di sicurezza **Blocca tutto** e rivolgersi al proprio amministratore di sistema o provider.

## 6.3. Personalizzazione delle regole delle applicazioni

### 6.3.1. Gestione dell'elenco di regole



Per visualizzare l'elenco delle regole applicazione sullo schermo,

Selezionare **Regole applicazione** dal menu **Assistenza**.

Si apre la finestra di dialogo **Regole applicazione** (cfr. fig. 14).

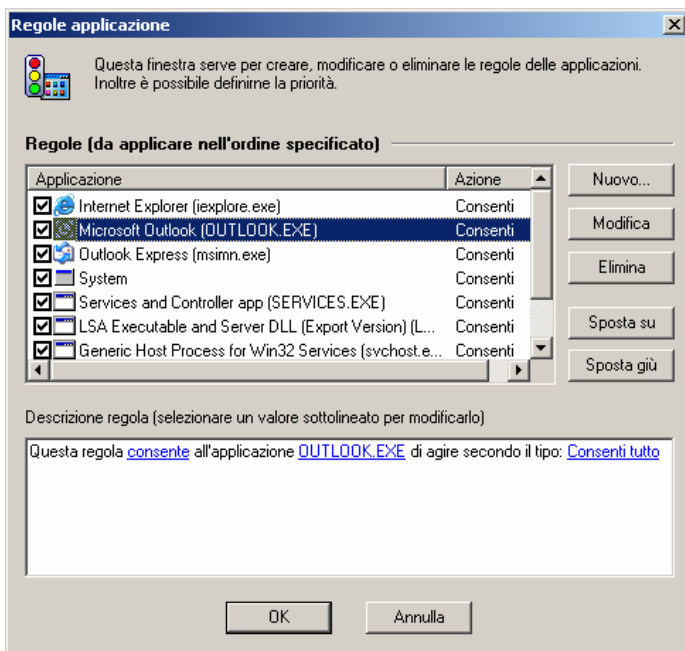


Fig. 14. La finestra di dialogo **Regole applicazione**

Nella sezione superiore della finestra di dialogo è visualizzato l'elenco delle regole per applicazioni. La colonna **Applicazione** contiene le icone delle

applicazioni, i loro nomi e le caselle di controllo che consentono di abilitare/disabilitare queste regole. La colonna **Azione** contiene i dati relativi all'azione eseguita dalla regola corrispondente: **Consenti**, per le regole che consentono alcuni eventi, e **Blocca**, per le regole che bloccano alcuni eventi.

Le regole sono elencate in base alla loro priorità. La regola nella parte superiore dell'elenco viene applicata per prima, e solo in seguito il programma applicherà la seconda regola, ecc. Se un'applicazione cerca di eseguire qualche operazione di rete, il programma confronta questa attività a fronte dell'elenco di regole, esaminandolo dalla prima all'ultima voce fino a trovare la regola corrispondente a questa operazione o fino ad esaminare l'intero elenco. Se la regola corrispondente non viene trovata, viene applicata l'azione di default (cfr. paragrafo 4.2 a pag. 20). In tal modo, se si desidera bloccare solo alcune operazioni per un'applicazione, è necessario creare due regole per tale applicazione: la prima regola deve consentire le operazioni desiderate per questa applicazione, mentre la seconda regola deve bloccare tutte le operazioni di tale applicazione. Inoltre, la prima regola deve essere collocata al di sopra della seconda nell'elenco delle regole. Così facendo, l'applicazione cercherà di eseguire un'operazione consentita e Kaspersky Anti-Hacker effettuerà una ricerca nell'elenco delle regole, individuando la regola che consente l'operazione. Se l'operazione non è desiderata, Kaspersky Anti-Hacker applicherà la seconda regola bloccando tutte le operazioni di questa applicazione.

Per esempio, come risulta anche dalla fig. 14, la terza regola dell'applicazione impedisce a MS Internet Explorer di accedere a Internet, ma la seconda regola consente a questo programma di comunicare attraverso Internet utilizzando il protocollo HTTP. Poiché la seconda regola ha una priorità maggiore rispetto alla terza, MS Internet Explorer è autorizzato a comunicare con server remoti HTTP (ma solo con quelli).

Vengono applicate solo le regole le cui caselle sono state selezionate. Per esempio, nella fig. 14 le caselle della quarta e della quinta regola sono disabilitate.



*Per abilitare/disabilitare una regola di un'applicazione,*

Selezionare/deselezionare la casella di controllo corrispondente nell'elenco delle regole per applicazioni.

A destra dell'elenco di regole si trovano i seguenti pulsanti:

- **Nuovo...** – consente di creare una nuova regola. Premendo questo pulsante, si apre la finestra di Composizione guidata regole per applicazioni.

- **Modifica** – consente di modificare la regola selezionata. Premendo questo pulsante, si apre la finestra di Composizione guidata regole per applicazioni.
- **Elimina** – rimuove la regola selezionata dall'elenco.
- **Sposta su** – sposta la regola selezionata sulla riga superiore, ovvero ne aumenta il livello di priorità.
- **Sposta giù** – sposta la regola selezionata sulla riga inferiore, ovvero ne riduce il livello di priorità.

Per modificare una regola selezionata dall'elenco, è anche possibile premere il tasto **<INVIO>** oppure fare doppio clic su di essa. Per rimuovere dall'elenco la regola selezionata, premere il tasto **<CANC>**, e per aggiungere una nuova regola, premere il tasto **<INS>**.

Inoltre è possibile modificare l'elenco dal menu contestuale, che contiene i seguenti comandi:

- **Modifica...** – consente di modificare la regola selezionata.
- **Elimina** – rimuove la regola selezionata dall'elenco.
- **Replica la regola** – crea una copia della regola selezionata. La copia creata è collocata subito sotto la regola selezionata.

Sotto la lista, la sezione **Descrizione regola** visualizza i dati relativi alla regola selezionata dall'elenco nel frame superiore. La stessa sezione si trova nei riquadri della Composizione guidata regola, pertanto avremo occasione di descrivere questo frame con maggior dettaglio.

La descrizione delle regole contiene del testo di colore nero non modificabile, e del testo di colore blu non sostituibile con i valori appropriati. Se un'impostazione è scritta in grassetto, ciò significa che il suo valore è di importanza cruciale ai fini di questa regola.



*Per inserire o modificare il valore richiesto nella descrizione della regola,*

1. Fare clic sul collegamento sottolineato corrispondente nel frame **Descrizione regola**.
2. Selezionare il valore desiderato nella finestra di dialogo visualizzata (per informazioni più dettagliate cfr. paragrafi successivi).

Nella sezione inferiore della finestra di dialogo **Regole applicazione** vi sono i seguenti pulsanti:

- **OK** – chiude la finestra di dialogo e salva le modifiche apportate.
- **Annulla** – chiude la finestra di dialogo senza salvare le modifiche.



Tutte le modifiche apportate all'elenco sono applicate subito dopo il salvataggio.

## 6.3.2. Aggiunta di una nuova regola per l'applicazione



Per lanciare la finestra di *Composizione guidata delle regole per applicazioni*:

Premere il pulsante **Nuovo...** nella finestra di dialogo **Regole applicazione** (cfr. fig. 14).

### 6.3.2.1. Fase 1. Personalizzazione della regola

All'avvio della procedura di composizione guidata, si apre una finestra di dialogo simile a quella illustrata nella fig. 15.

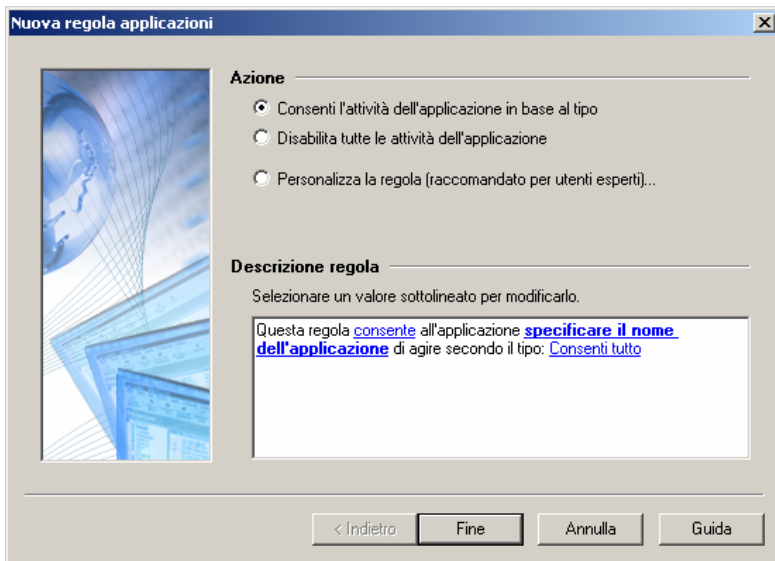


Fig. 15. La prima finestra di dialogo della procedura di composizione guidata regole per applicazioni

L'elenco delle opzioni **Azione** consente di selezionare una delle tre opzioni seguenti:

Azione	Descrizione regola
<ul style="list-style-type: none"> <li>• <b>Consenti l'attività dell'applicazione in base al tipo</b></li> </ul>	Questa regola <a href="#">consente</a> all'applicazione <a href="#">EXPLORE.EXE</a> di agire secondo il tipo: <a href="#">Browser web (Internet Explorer, Opera...)</a>
<ul style="list-style-type: none"> <li>• <b>Disabilita tutte le attività dell'applicazione</b></li> </ul>	Questa regola <a href="#">impedisce</a> all'applicazione <a href="#">EXPLORE.EXE</a> da qualsiasi attività di rete
<ul style="list-style-type: none"> <li>• <b>Personalizza la regola</b></li> </ul>	Questa regola <a href="#">consente</a> all'applicazione <a href="#">EXPLORE.EXE</a> di <a href="#">stabilire connessioni</a> con computer remoto mediante protocollo TCP



Selezionando **Personalizza la regola**, il riquadro successivo della Composizione guidata può richiedere di definire alcune impostazioni supplementari.

- Tipo di applicazione Internet (client o server)
- Protocollo
- Indirizzo remoto
- Porta remota
- Porta locale



*Per creare una regola che consenta l'attività dell'applicazione in base al tipo:*

1. Selezionare il pulsante **Consenti l'attività dell'applicazione in base al tipo** dall'elenco delle opzioni nella sezione **Azione**.
2. Fare clic sul collegamento ipertestuale [specificare il nome dell'applicazione](#) nella sezione **Descrizione regola**. Specificare il nome dell'applicazione desiderata nella finestra di dialogo **Seleziona applicazione**.
3. Definire il tipo di applicazione facendo clic sul collegamento ipertestuale appropriato nella sezione **Descrizione regola**. Il valore di default è [Consenti tutto](#), che non limita in nessun modo i diritti dell'applicazione. Per modificarlo, fare clic su di esso e selezionare un nuovo valore

dall'elenco a discesa all'interno della finestra di dialogo **Specificare il tipo di applicazione** (cfr. fig. 16). Quindi fare clic su **OK**.

- Browser Web – browser Internet, Netscape Navigator ecc. È consentita la comunicazione tramite i protocolli HTTP, HTTPS, FTP e server proxy.
- Trasferimento file – per Reget, Gozilla, ecc. È consentita la comunicazione tramite i protocolli HTTP, HTTPS, FTP, TFTP e server proxy standard.
- Posta - per MS Outlook, MS Outlook Express, the Bat e altri programmi di posta elettronica. È consentita la comunicazione tramite i protocolli SMTP, NNTP, POP3 e IMAP4.
- News - per Forte Agent e altri programmi di news. È consentita la comunicazione tramite i protocolli SMTP e NNTP.
- Instant messaging - per ICQ, AIM e altri programmi di chat. È consentita la comunicazione tramite server proxy standard e collegamenti diretti computer-computer.
- Internet Relay Chat – per mIRC e programmi simili. Sono consentiti l'autenticazione standard utente per reti IRC e l'accesso a porte server IRC.
- Business Conferences - per MS NetMeeting e programmi simili. È consentita la comunicazione tramite i protocolli HTTP e HTTPS, nonché tramite server proxy standard. Il tipo supporta inoltre la comunicazione all'interno della rete locale (LDAP e altre).
- Remote Management - per Telnet, ecc. È consentita la comunicazione tramite i protocolli Telnet e SSH.
- Time Synchronization - per Timehook e programmi simili. È consentita la connessione con server time e daytime.

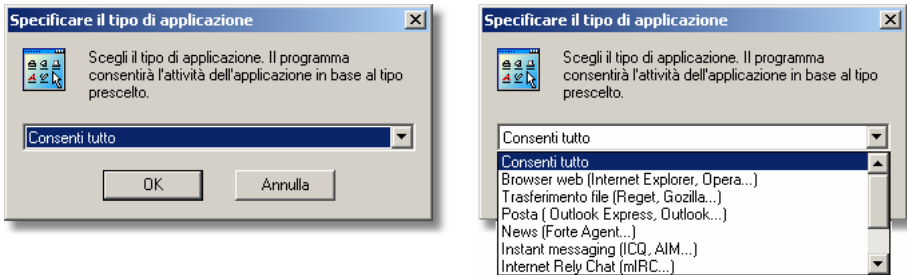


Fig. 16. Selezione del tipo di applicazione



*Per impedire all'applicazione ogni comunicazione di rete,*

1. Selezionare **Disabilita tutte le attività dell'applicazione** dall'elenco delle opzioni nella sezione **Azione**.
2. Fare clic sul collegamento ipertestuale [specificare il nome dell'applicazione](#) nella sezione **Descrizione regola**. Specificare il nome dell'applicazione desiderata nella finestra di dialogo **Seleziona applicazione**.

Se le impostazioni sopra descritte non consentono di creare la regola desiderata (per esempio, se si desidera consentire la comunicazione a un certo indirizzo IP), è possibile configurare una regola più complessa.



*Per configurare una regola più complessa, seguire queste istruzioni:*

1. Selezionare **Personalizza la regola** dall'elenco delle opzioni nella sezione **Azione**.
2. Fare clic sul collegamento ipertestuale [specificare il nome dell'applicazione](#) nella sezione **Descrizione regola**. Specificare il nome dell'applicazione desiderata nella finestra di dialogo **Seleziona applicazione**.
3. Fare clic sul collegamento ipertestuale [Consenti tutto](#) nella sezione **Descrizione regola**. Selezionare l'azione desiderata dal seguente elenco di opzioni nella finestra di dialogo **Specificare l'azione** (cfr. fig. 17) e fare clic su **OK**:

- **Blocca tutto**

- **Consenti tutto**

4. Selezionare l'attività dell'applicazione da monitorare e da regolare per mezzo di questa regola; attuazione (default) o ricezione della connessione. Per modificare l'attività di default, fare clic sul collegamento ipertestuale [attuazione connessioni](#) nella sezione **Descrizione regola**. Selezionare l'opzione **Ricezione di connessione di rete in entrata da una macchina remota in corso** nella finestra di dialogo **Selezionare il tipo di attività dell'applicazione** (cfr. fig. 18) e fare clic su **OK**.

Conclusa la fase di selezione delle opzioni nella prima finestra della Composizione guidata, fare clic su **Avanti >**.

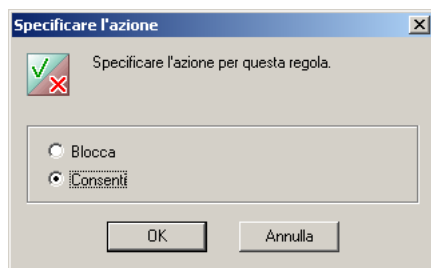


Fig. 17. Selezione dell'azione

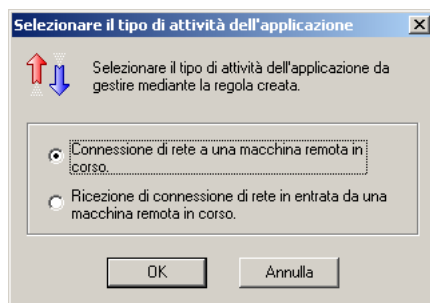


Fig. 18. Selezione del tipo di attività dell'applicazione



Se si fa clic su **Avanti >** senza selezionare un'applicazione, viene visualizzato un messaggio che invita a selezionare un'applicazione.

### 6.3.2.2. Fase 2. Condizioni delle regole

La finestra di Composizione guidata regole è visualizzata solo se nella prima finestra è stato selezionato il pulsante con l'opzione **Personalizza la regola**.

In questa finestra è possibile specificare il protocollo, l'indirizzo della macchina remota e le porte.

**Il protocollo:** un elenco a tendina in questa finestra di dialogo contiene i seguenti protocolli predefiniti e i numeri di porta corrispondenti:


- HTTP
- IMAP


- SMTP
- NNTP
- POP3
- DNS


Se si desidera definire il numero di un'altra porta, selezionare uno dei seguenti elementi da questo elenco a tendina:

- **Altro protocollo basato su TCP** – per servizi basati sul protocollo TCP
- **Altro protocollo basato su UDP** – per servizi basati sul protocollo UDP

L'elenco delle **Impostazioni** contiene impostazioni supplementari e il suo contenuto dipende completamente dal protocollo selezionato dall'elenco a discesa di cui sopra.

 **Indirizzo remoto** – l'indirizzo del computer remoto coinvolto nella comunicazione. Per definire l'indirizzo, fare clic sul collegamento ipertestuale corrispondente [specificare l'indirizzo](#) nella sezione **Descrizione regola**. Per specificare più di un indirizzo, tenere premuto il tasto **<CTRL>** e fare clic sul collegamento ipertestuale. Per informazioni più dettagliate, cfr. Paragrafo 6.3.2.2.2 a pag. 60.

 **Porta remota** – il numero della porta remota. Per specificare la porta, fare clic sul collegamento ipertestuale corrispondente [specificare la porta](#) nella sezione **Descrizione regola**. Per specificare più di una porta, tenere premuto il tasto **<CTRL>** e fare clic sul collegamento ipertestuale. Per i dati specifici vedere il numero. Per specificare la porta fare clic sul collegamento ipertestuale corrispondente [specificare la porta](#), paragrafo 6.3.2.2.2 a pag. 60.

 **Porta locale** – la porta locale nella sezione **Descrizione regola**. Per specificare più di una porta, tenere premuto il tasto **<CTRL>** e fare clic sul collegamento ipertestuale. Per i dati specifici vedere il numero. Per specificare la porta fare clic sul collegamento ipertestuale corrispondente [specificare la porta](#), paragrafo 6.3.2.2.2 a pag. 60.

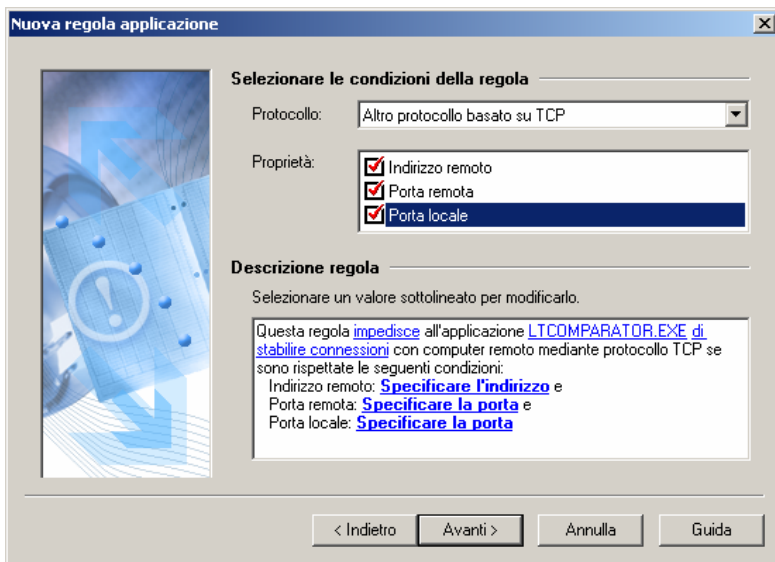


Fig. 19. Definizione delle condizioni delle regole

### 6.3.2.2.1. Definizione dell'indirizzo o dell'intervallo di indirizzi

Per definire gli indirizzi desiderati, è necessario utilizzare due finestre di dialogo.

La finestra di dialogo **Specificare l'indirizzo o l'intervallo di indirizzi** (cfr. fig. 20) viene visualizzata sullo schermo tenendo premuto il tasto <CTRL> e facendo clic sul collegamento ipertestuale [specificare l'indirizzo](#) nella seconda finestra della composizione guidata delle regole.

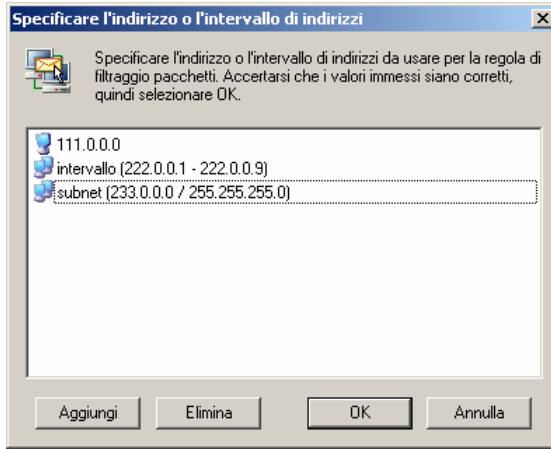


Fig. 20. La finestra di dialogo **Specificare l'indirizzo o l'intervallo di indirizzi**

Da qui è possibile utilizzare i pulsanti **Aggiungi** ed **Elimina** per aggiungere il numero desiderato di indirizzi di computer, intervalli di indirizzi e indirizzi di subnet. Al termine della configurazione dell'elenco di indirizzi, fare clic su **OK** e tornare alla finestra di Composizione guidata regole.

Premendo **Aggiungi** nella finestra di dialogo **Specificare l'indirizzo o l'intervallo di indirizzi**, si apre la finestra di dialogo **Specificare l'indirizzo** (cfr. fig. 21). La stessa finestra di dialogo viene visualizzata sullo schermo facendo clic sul collegamento ipertestuale [Specificare l'indirizzo](#) nella seconda finestra della Composizione guidata delle regole senza tenere premuto il tasto **<CTRL>**.

La finestra di dialogo **Specificare l'indirizzo** consente di specificare l'indirizzo, l'intervallo di indirizzi o l'indirizzo di subnet da usare per la propria regola (cfr. fig. 21).

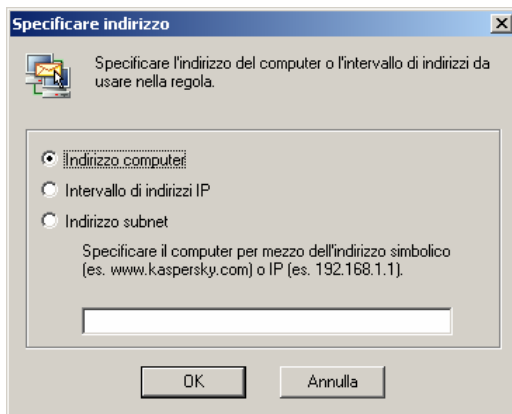


Fig. 21. Inserimento dell'indirizzo del computer nella finestra di dialogo **Specificare l'indirizzo**

Da qui è possibile selezionare una delle seguenti opzioni:

- **Indirizzo computer** - consente di specificare il computer per mezzo dell'indirizzo simbolico (per esempio [www.kaspersky.com](http://www.kaspersky.com)) o dell'indirizzo IP (per esempio 192.168.1.1).
- **Intervallo di indirizzi IP** - consente di specificare l'intervallo di indirizzi utilizzando i campi **Inizia da:** e **Finisce per:** (cfr. fig. 22).
- **Indirizzo subnet** - consente di specificare l'indirizzo di subnet nel campo **Indirizzo subnet:** e/o la maschera subnet nel campo **Maschera subnet:** (cfr. fig. 23).

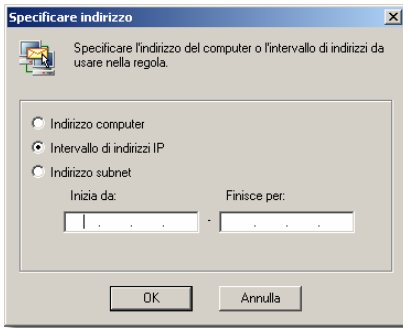


Fig. 22. Indicazione dell'intervallo di indirizzi IP

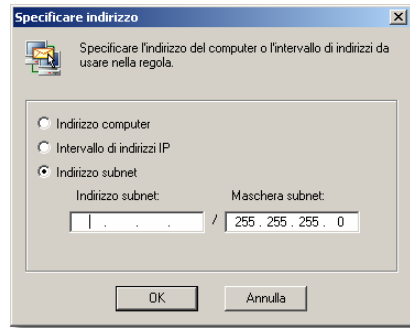


Fig. 23. Indicazione dell'indirizzo subnet

Una volta specificato l'indirizzo desiderato, fare clic su **OK**.

### 6.3.2.2.2. Definizione della porta o dell'intervallo di porte

Per definire le porte desiderate sono necessarie due finestre di dialogo.

Per visualizzare la finestra di dialogo **Specificare porta o intervallo porte** (cfr. fig. 24) tenere premuto il tasto **<CTRL>** e fare clic sul collegamento ipertestuale [specificare la porta](#) nella seconda finestra di Composizione guidata regole.

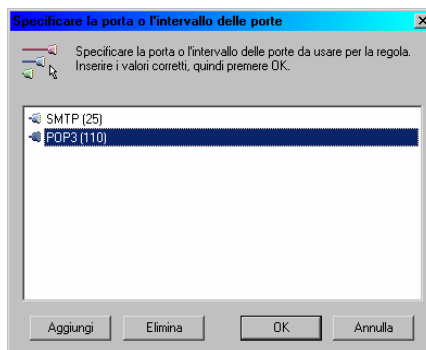


Fig. 24. La finestra di dialogo **Specificare porta o intervallo porte**

Da qui è possibile utilizzare i pulsanti **Aggiungi** e **Rimuovi** per aggiungere i numeri corrispondenti alle porte e agli intervalli porte desiderati. Una volta completata la configurazione dell'elenco delle porte, premere il pulsante **OK** e tornare alla finestra di composizione guidata delle regole.

Il pulsante **Aggiungi** nella finestra di dialogo **Specificare porta o intervallo porte**, determina la visualizzazione della finestra di dialogo **Porta** (cfr. fig. 21). La stessa finestra di dialogo viene visualizzata facendo clic sul collegamento ipertestuale [specificare la porta](#) nella seconda finestra di composizione automatica delle regola senza tenere premuto il tasto **<CTRL>**.

La finestra di dialogo **Porta** consente di specificare la porta o le porte da utilizzare per la regola (cfr. fig. 25).

Da qui è possibile selezionare una delle seguenti opzioni:

- **Specificare il numero della porta** – consente di selezionare uno dei valori predefiniti dall'elenco a discesa o di inserire il numero della porta dalla tastiera.
- **Specificare l'intervallo delle porte** – consente di specificare l'intervallo di porte desiderato inserendo la porta iniziale nel primo campo di testo e la porta finale nel secondo (cfr. fig. 26).

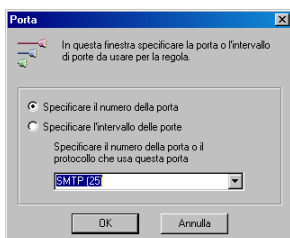


Fig. 25. La finestra di dialogo **Porta**

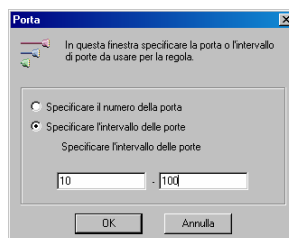


Fig. 26. Definizione dell'intervallo delle porte

Una volta specificate le porte desiderate, fare clic su **OK**.

### 6.3.2.3. Fase 3. Azioni supplementari

Fra le azioni supplementari, è possibile selezionare la casella di controllo  **Registra evento**, che abilita la registrazione degli eventi rilevati, e  **Visualizza avvertimento**, che abilita la visualizzazione di messaggi sull'evento rilevato (cfr. fig. 27).

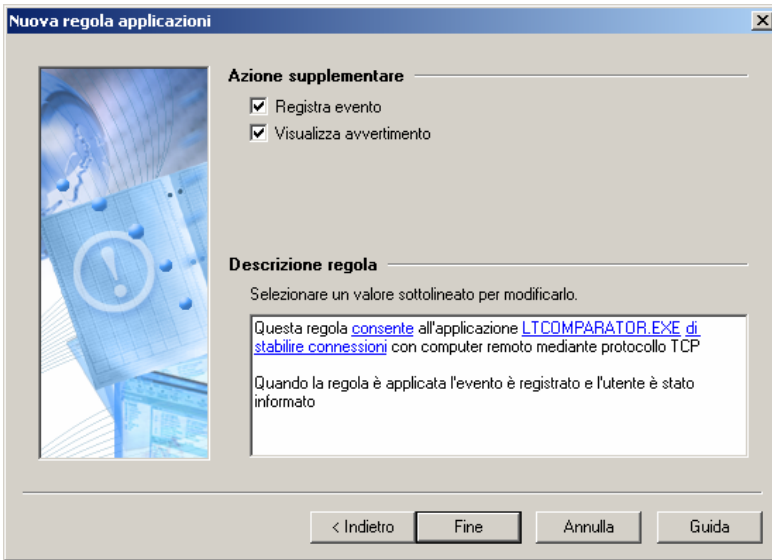


Fig. 27. Azioni supplementari per la regola

## 6.4. Personalizzazione delle regole di filtraggio pacchetti

### 6.4.1. Gestione dell'elenco di regole

La gestione dell'elenco delle regole di filtraggio pacchetti è simile per molti aspetti alla gestione dell'elenco delle regole per applicazioni.



*Per visualizzare l'elenco delle regole di filtraggio pacchetti sullo schermo,*

selezionare **Regole di filtraggio pacchetti** dal menu **Assistenza**.

Si apre la finestra di dialogo **Regole di filtraggio pacchetti** (cfr. fig. 28).

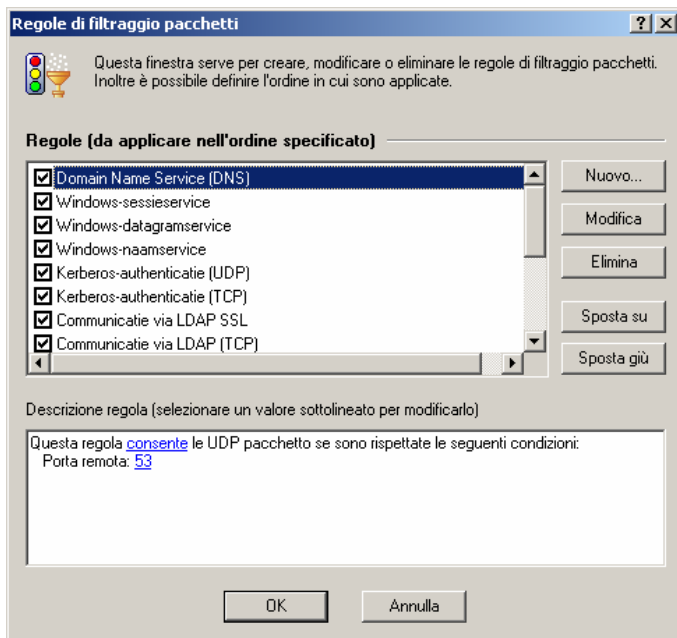


Fig. 28. La finestra di dialogo **Regole di filtraggio pacchetti**

Nella sezione superiore della finestra di dialogo è visualizzato l'elenco delle regole di filtraggio pacchetti. Le caselle di controllo a destra di ogni regola consentono di abilitare/disabilitare queste regole.

Le regole sono elencate in base alla priorità; la regola posta alla prima posizione dell'elenco viene applicata per prima, poi il programma applica la seconda, ecc. Vengono applicate solo le regole la cui casella di controllo è stata selezionata.



*Per abilitare/disabilitare una regola di filtraggio pacchetti,*

selezionare/deselezionare la casella di controllo corrispondente nell'elenco delle regole di filtraggio pacchetti.

A destra dell'elenco di regole si trovano i seguenti pulsanti:

- **Nuovo...** - consente di creare una nuova regola. Premendo questo pulsante, si apre la finestra di Composizione guidata regole filtraggio pacchetti.

- **Modifica** - consente di modificare la regola selezionata. Premendo questo pulsante, si apre la finestra di composizione guidata regole filtraggio pacchetti.
- **Elimina** – rimuove la regola selezionata dall'elenco.
- **Sposta su** – sposta la regola selezionata sulla riga superiore, ovvero ne aumenta il livello di priorità.
- **Sposta giù** – sposta la regola selezionata sulla riga inferiore, ovvero ne riduce il livello di priorità.

Per modificare una regola selezionata dall'elenco, è anche possibile premere il tasto **<INVIO>** oppure fare doppio clic su di essa. Per rimuovere dall'elenco la regola selezionata, premere il tasto **<CANC>**. Per aggiungere una nuova regola all'elenco premere **<INS>**.

Inoltre è possibile modificare l'elenco dal menu contestuale, che contiene i seguenti comandi:

- **Modifica** - consente di modificare la regola selezionata.
- **Elimina** – rimuove la regola selezionata dall'elenco.
- **Replica la regola** – crea una copia della regola selezionata. La copia è collocata subito sotto la regola selezionata.

Sotto la lista, la sezione **Descrizione regola** visualizza i dati relativi alla regola selezionata dall'elenco nel frame superiore. La stessa sezione si trova nei riquadri della composizione guidata regola, pertanto avremo occasione di descrivere questo frame con maggior dettaglio.

La descrizione delle regole contiene del testo di colore nero non modificabile, e del testo di colore blu non sostituibile con i valori appropriati. Se un'impostazione è scritta in grassetto, ciò significa che il suo valore è di importanza cruciale ai fini di questa regola.



*Per inserire o modificare il valore richiesto nella descrizione della regola,*

1. Fare clic sul collegamento sottolineato corrispondente nella sezione **Descrizione regola**.

2. Selezionare il valore desiderato nella finestra di dialogo visualizzata (per informazioni più dettagliate cfr. paragrafi successivi).

Nella sezione inferiore della finestra di dialogo **Regole filtraggio pacchetti** vi sono i seguenti pulsanti:

- **OK** – chiude la finestra di dialogo e salva le modifiche apportate.
- **Annulla** – chiude la finestra di dialogo senza salvare le modifiche.



Tutte le modifiche apportate all'elenco sono applicate subito dopo il salvataggio.

Le regole di filtraggio pacchetti hanno un livello di priorità maggiore rispetto alle regole per applicazioni e vengono pertanto eseguite per prime.

## 6.4.2. Aggiunta di una nuova regola

La Composizione guidata delle regole di filtraggio pacchetti è simile per molti aspetti a quella delle regole per applicazioni. Tuttavia, contiene solo due finestre.

### 6.4.2.1. Fase 1. Condizioni delle regole

La prima finestra della Composizione guidata consente di specificare:

- Il protocollo usato (TCP, UDP, ICMP, altri protocolli IP)
- L'indirizzo di destinazione del pacchetto
- La direzione del traffico (in uscita, in entrata)
- Le impostazioni dipendenti dai protocolli (le porte per i protocolli TCP e UDP, i tipi di messaggio per il protocollo ICMP, il numero di protocollo degli altri protocolli IP)
- L'azione (consenti/blocca)

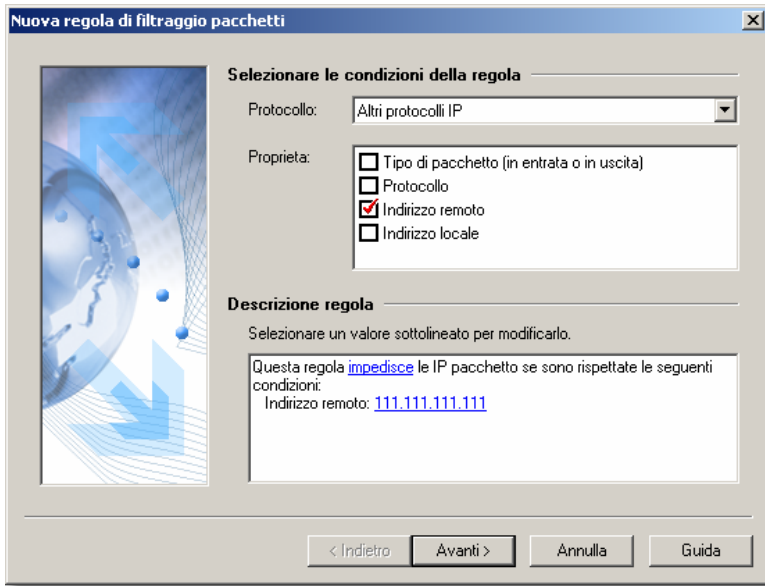


Fig. 29. La prima finestra di Composizione guidata delle regole di filtraggio pacchetti



*Per configurare una regola di filtraggio pacchetti, seguire queste istruzioni:*

1. Selezionare il protocollo da filtrare nell'elenco a tendina Protocollo. I valori disponibili sono TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) e Altri protocolli IP. Il valore di default è TCP.
2. Selezionare le seguenti caselle di controllo nella sezione Proprietà:



**Tipo di pacchetto** (in entrata o in uscita) – relativo alla direzione del traffico. Di default, la casella di controllo è deselezionata, consentendo di filtrare sia il traffico in entrata che quello in uscita. Se si desidera controllare solo il traffico in entrata o quello in uscita, selezionare questa casella di controllo e specificare il tipo di pacchetto desiderato nella sezione **Descrizione regola**. Per inserire il valore desiderato, fare clic sul collegamento ipertestuale del [tipo di pacchetto](#) e selezionare l'opzione desiderata nella finestra di dialogo Specificare la direzione del pacchetto, quindi fare clic sul pulsante OK.

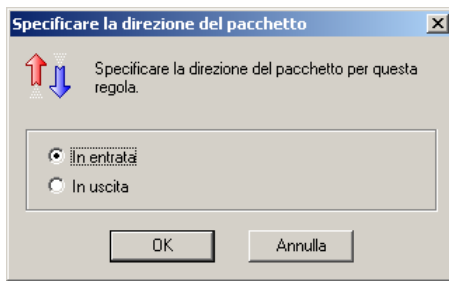


Fig. 30. La finestra di dialogo **Specificare la direzione del pacchetto**

3. Alcune caselle di controllo nella sezione **Proprietà** dipendono dal protocollo.
  - Per i protocolli **TCP** e **UDP** è necessario specificare la porta remota e la porta locale.
  - Per il protocollo ICMP è necessario specificare il **tipo di messaggio ICMP**.
  - Per altri tipi di protocollo basati su IP è possibile specificare il **protocollo**.

**Indirizzo remoto** – l'indirizzo della macchina remota (per tutti i protocolli).

**Indirizzo locale** – l'indirizzo della macchina locale (per tutti i protocolli).

Per definire l'indirizzo (locale o remoto), fare clic sul collegamento ipertestuale corrispondente [specificare l'indirizzo](#) nella sezione **Descrizione regola**. Per specificare più di un indirizzo, tenere premuto il tasto <CTRL> e fare clic sul collegamento ipertestuale. Per informazioni più dettagliate, cfr. paragrafo 6.3.2.2.1 a pag. 57.

**Porta remota** – il numero della porta remota (per i protocolli TCP e UDP).

**Porta locale** – il numero della porta locale (per i protocolli TCP e UDP).

Per specificare la porta (locale o remota), fare clic sul collegamento ipertestuale corrispondente [specificare la porta](#) nella sezione

**Descrizione regola.** Per informazioni più dettagliate, cfr. il numero. Per specificare la porta fare clic sul collegamento ipertestuale corrispondente [specificare la porta](#), cfr. paragrafo 6.3.2.2.2 a pag. 60.



**Tipo di messaggio ICMP** - il tipo di messaggio ICMP (solo per il protocollo ICMP). Per specificare il tipo di messaggio, fare clic sul collegamento ipertestuale corrispondente [Specificare il tipo di messaggio ICMP](#) nella sezione **Descrizione regola** e selezionare il valore desiderato nell'elenco a tendina della finestra di dialogo **Specificare il tipo di messaggio ICMP** (cfr. fig. 31), quindi fare clic sul pulsante **OK**.

- Richiesta di eco
- Risposta di eco
- Individua percorso? (eccedenza TTL)
- Rete non raggiungibile
- Host non raggiungibile
- Protocollo non raggiungibile
- Porta non raggiungibile
- Reindirizza per l'host
- Reindirizza per la rete
- Reindirizza per TOS e rete
- Reindirizza per TOS e host



Fig. 31. La finestra di dialogo **Specificare il tipo di messaggio ICMP**



**Protocollo** – il nome o numero del protocollo (solo per protocolli IP). Se questa casella di controllo viene lasciata deselezionata, il programma gestisce tutti i protocolli IP. Per specificare il nome o il numero di protocollo desiderato, fare clic sul collegamento ipertestuale [specificare protocollo](#) nella sezione **Descrizione regola** e selezionare il valore desiderato nell'elenco a discesa della finestra di dialogo **Specificare il protocollo** (cfr. fig. 32). Premere quindi il pulsante **OK**. Nell'elenco dei protocolli disponibili di seguito, i numeri di protocollo sono indicati fra parentesi.

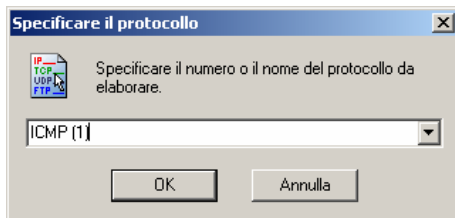


Fig. 32. La finestra di dialogo **Specificare il protocollo**

- IGMP, RGMP(2)
- GGP(3)
- IP in encapsulation IP (4)
- TCP(6)
- IGRP(9)
- UDP(17)
- GRE(47)
- ESP(50)
- AH(51)
- IP con crittografia (53)

4. Specificare l'azione da applicare ai pacchetti che soddisfano le condizioni sopra definite – blocca o consenti. Di default, è selezionata l'opzione **Blocca**. Per modificare il valore, fare clic sul collegamento ipertestuale corrispondente nella sezione **Descrizione regola** e selezionare il valore desiderato nella finestra di dialogo **Specificare l'azione**, quindi fare clic su **OK** (cfr. fig. 33).

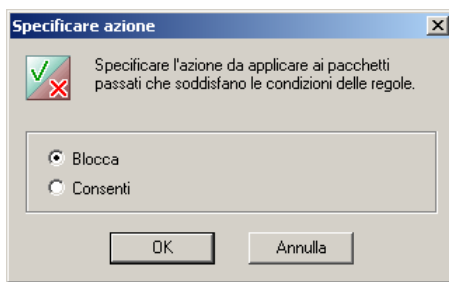


Fig. 33. La finestra di dialogo **Specificare l'azione**

#### 6.4.2.2. Fase 2. Nome delle regole e azioni supplementari

È necessario specificare il nome della regola di filtraggio pacchetti nel campo di testo **Nome della regola** della seconda finestra della composizione guidata. Di default, il programma suggerisce un nome esclusivo, come **Regola di filtraggio pacchetti #<numero di sequenza della regola>**. Tuttavia, è consigliabile

specificare un nome dotato di significato che faciliti in futuro l'individuazione della regola desiderata all'interno dell'elenco.

È inoltre possibile abilitare azioni supplementari per la regola. La composizione guidata contiene le due seguenti caselle di controllo: **Registra evento** – se selezionata, vengono registrati gli eventi rilevati, e **Visualizza avvertimento** – se selezionata, visualizza un messaggio sull'evento rilevato (cfr. fig. 9).

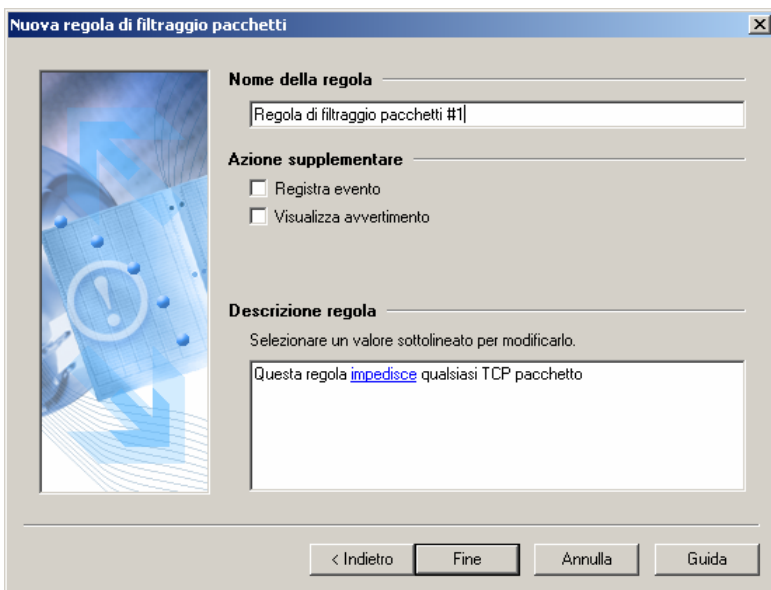


Fig. 34. Definizione del nome della regola e azioni supplementari

## 6.5. Sistema di rilevamento intrusioni

### 6.5.1. Impostazioni del rilevatore intrusioni



*Per visualizzare le impostazioni intrusioni,*

selezionare Impostazioni dal menu **Assistenza** e portarsi sulla pagina **Sistema di rilevamento intrusioni** (cfr. fig. 35).

È consigliabile tenere sempre selezionata la casella di controllo  **Abilita sistema di rilevamento intrusioni** nella pagina **Sistema di rilevamento intrusioni**. Questa casella di controllo consente di abilitare/disabilitare il rilevamento delle intrusioni esterne nella macchina.

Sotto questa casella di controllo si trova la casella di selezione **Periodo di arresto attacco (min.)** che consente di definire il periodo durante il quale la macchina di provenienza dell'attacco dovrà restare bloccata quando viene rilevato un indirizzo remoto. Questa impostazione viene applicata a tutti i tipi di attacco.



Modificando il parametro **Periodo di arresto attacco**, esso sarà applicato a tutti i nuovi attacchi subito dopo aver premuto il pulsante **OK** nella finestra Impostazioni. Per quanto riguarda i computer che sono stati bloccati a causa di attacchi precedenti, il loro periodo di blocco non subirà variazioni.

L'insieme di campi collocati alla base della pagina dipende dal tipo di attacco selezionato dall'elenco a tendina **Tipo di attacco**.

Selezionare la casella di controllo **Abilita rilevamento di questo attacco** se si desidera che il programma rilevi il tipo di attacco selezionato. Sotto la casella di controllo vi sono informazioni sui tipi di attacco, che possono tornare utili in caso di incertezza sull'opzione da usare.

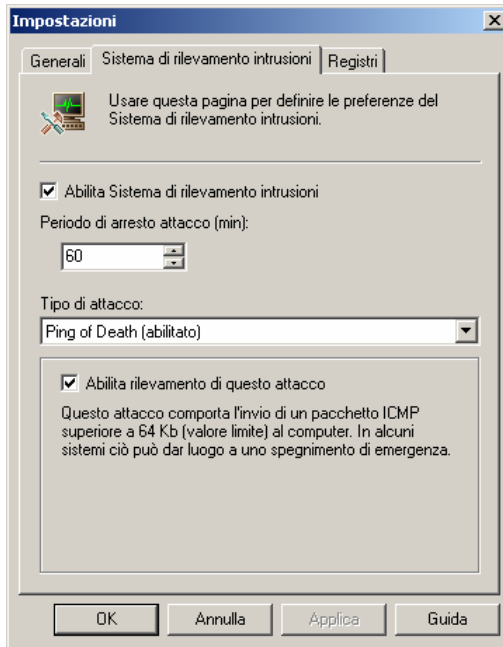


Fig. 35. La pagina **Sistema di rilevamento intrusioni** della finestra di dialogo **Impostazioni**

## 6.5.2. L'elenco degli attacchi rilevabili

Kaspersky Anti-Hacker è in grado di rilevare gli attacchi DoS più comuni (*Ridondanza SYN*, *Ridondanza UDP*, *Ridondanza ICMP*), il *Ping of death*, e gli attacchi *Land*, *Helkern*, *SmbDie* e *Lovesan*, e di rilevare inoltre le operazioni di scansione delle porte, che sono solitamente seguite da un attacco più potente:

- L'attacco **"Ping of death"** comporta l'invio di un pacchetto ICMP superiore a 64 Kb (valore limite) al computer attaccato. Ciò può determinare l'arresto d'emergenza di alcuni sistemi operativi.
- L'attacco **"Land"** comporta la trasmissione di una richiesta di autoconnessione (quando a un computer viene richiesto di connettersi con se stesso) al computer attaccato. Ciò determina un circolo vizioso in quanto il computer cerca di connettersi con se stesso. Di conseguenza, il

carico della CPU e le probabilità di arresto di emergenza aumentano drasticamente.

- L'*attacco "Scanning TCP ports"* comporta il rilevamento di porte TCP aperte sul computer. Questo tipo di attacco viene usato per cercare i punti deboli di un computer ed è generalmente seguito da attacchi più pericolosi. È possibile definire le seguenti impostazioni per questo tipo di attacco: **Cont. porte:** - il numero di porte che la macchina remota cerca di aprire, e **Ora (sec):** - il tempo necessario.
- L'*attacco "Scanning UDP ports"* comporta il rilevamento di porte UDP aperte sul computer. L'attacco viene rilevato dalla quantità di pacchetti UDP inviati a varie porte del computer in un determinato periodo di tempo. Questo tipo di attacco viene usato per cercare i punti deboli di un computer ed è generalmente seguito da attacchi più pericolosi. È possibile definire le seguenti impostazioni per questo tipo di attacco: **Cont. porte:** - il numero di porte che la macchina remota cerca di aprire, **Ora (sec):** - il tempo necessario.
- L'*attacco "Ridondanza SYN"* comporta l'invio di una falsa richiesta di connessione al computer attaccato. Il sistema riserva determinate risorse per ogni richiesta di connessione. Di conseguenza, il computer non risponde alle richieste di connessione da altre provenienze. È possibile definire le seguenti impostazioni per questo tipo di attacco: **Cont. connessioni:** - il numero di connessioni che la macchina remota cerca di stabilire, e **Ora (sec):** - il tempo necessario.
- L'*attacco "Ridondanza UDP"* comporta l'invio di speciali pacchetti UDP al computer attaccato. Questi pacchetti vengono trasmessi senza fine tra le macchine coinvolte. Di conseguenza, questo attacco consuma risorse ingenti e sovraccarica il canale di comunicazione. È possibile definire le seguenti impostazioni per questo tipo di attacco: **Cont. pacchetti UDP:** - il numero di pacchetti UDP in entrata, e **Ora (sec):** - il tempo necessario.
- L'*attacco "Ridondanza ICMP"* comporta l'invio di speciali pacchetti ICMP al computer attaccato. Ciò determina un incremento del carico della CPU del computer attaccato che risponde ad ogni pacchetto. È possibile definire le seguenti impostazioni per questo tipo di attacco: **Cont. pacchetti ICMP:** - il numero di pacchetti ICMP in entrata, e **Ora (sec):** - il tempo necessario.
- L'*attacco "Helkern"* comporta l'invio di speciali pacchetti UDP (in grado di eseguire codici maligni) al computer attaccato. Questo attacco determina un rallentamento della connessione Internet.

- L'attacco "**SmbDie**" comporta il tentativo di stabilire una connessione SMB; se l'attacco ha esito positivo, viene inviato al computer attaccato uno speciale pacchetto che provoca la ridondanza del buffer. In conseguenza di ciò, l'utente deve riavviare il sistema operativo. I sistemi operativi Windows 2k/XP/NT sono esposti a questo tipo di attacco.
- L'attacco "**Lovesan**" prende di mira i punti vulnerabili del servizio DCOM RPC dei sistemi operativi Windows NT 4.0/NT 4.0 Terminal Services Edition/2000/XP/Server (tm) 2003. Una volta rilevata la vulnerabilità, il worm, costituito da un malware che consente al mittente di effettuare qualsiasi manipolazione, viene scaricato sul computer attaccato.

---

# CAPITOLO 7. VISUALIZZAZIONI E DEI RISULTATI DELLE PRESTAZIONI

## 7.1. Visualizzazione dello stato corrente


Le prestazioni di tutte le applicazioni di rete in esecuzione sul computer vengono costantemente monitorate e registrate da Kaspersky Anti-Hacker. È possibile consultare le seguenti statistiche dell'attività di rete:

- **Applicazioni attive.** Le operazioni di rete sono classificate sulla base delle applicazioni coinvolte. Per ogni applicazione presente sul computer è possibile consultare l'elenco delle porte e delle connessioni da essa gestite.
- **Connessioni stabilite.** Visualizza tutte le connessioni in entrata e in uscita, gli indirizzi dei computer remoti e il numero delle porte.
- **Porte aperte.** Visualizza tutte le porte aperte del computer.

### 7.1.1. Applicazioni attive



*Per consultare l'elenco delle applicazioni di rete correntemente attive,*

selezionare **Applicazioni attive** dal sottomenu **Mostra** del menu **Visualizza** (cfr. fig. 36). Inoltre è possibile premere il pulsante  nella barra degli strumenti.

Si apre la finestra di dialogo **Applicazioni attive di rete**.

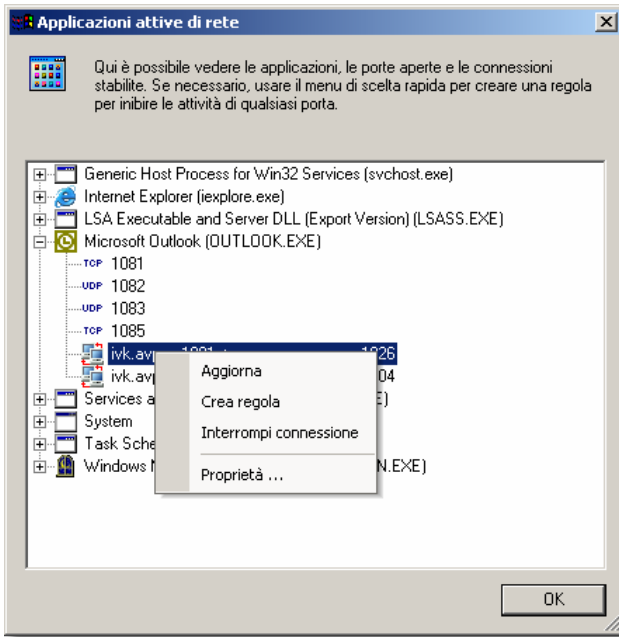




Fig. 36. La finestra di dialogo **Applicazioni attive di rete**

Questa finestra di dialogo consente di consultare l'elenco delle applicazioni di rete attive e delle risorse di rete utilizzate. I nomi delle applicazioni sono elencati in ordine alfabetico, agevolando la ricerca nell'elenco. A sinistra del nome di ogni applicazione dell'elenco si trova l'icona dell'applicazione.

Espandendo ogni applicazione, è possibile visualizzare l'elenco delle porte aperte corrispondenti sul computer e le connessioni stabilite da questa applicazione. Gli indicatori sono i seguenti:

- Le porte aperte sono indicate dall'icona **TCP** o **UDP**, in base al tipo di porta aperta. A destra di ogni porta è indicato il numero corrispondente.
- Le connessioni stabilite sono indicate con l'icona  se stabilite dal proprio computer, o dall'icona  se ricevute dall'esterno. Le impostazioni delle connessioni sono descritte a destra dell'icona: <indirizzo di provenienza>:<porta di provenienza> → <indirizzo di destinazione>:<porta di destinazione>

L'elenco delle applicazioni di rete attive viene aggiornato automaticamente due volte al secondo.

L'elenco è dotato di un menu contestuale che contiene i seguenti comandi:

- **Aggiorna** – aggiorna l'elenco delle applicazioni attive su richiesta dell'utente.
- **Crea regola** - consente di creare una regola per una porta o connessione selezionata. Il programma avvia la composizione guidata delle regole per applicazioni, quindi inserisce automaticamente i dati relativi alla porta o connessione selezionata negli appositi campi.
- **Interrompi connessione** – interrompe la connessione selezionata (questo comando è disponibile solo è stata selezionata una connessione dall'elenco).



**Attenzione!** Se si interrompe forzatamente una connessione, l'applicazione relativa potrà funzionare in maniera non corretta.

- **Proprietà** – visualizza maggiori dati sull'elemento selezionato nell'elenco, cioè l'applicazione (cfr. fig. 37), la connessione (cfr. fig. 39) o la porta (cfr. fig. 41).



L'elenco può contenere più di una stringa per la stessa applicazione. Ciò significa che è in esecuzione più di una copia dell'applicazione. Espandendo i giunti delle copie dell'applicazione, si visualizzano diversi elenchi di porte aperte e di connessioni stabilite.

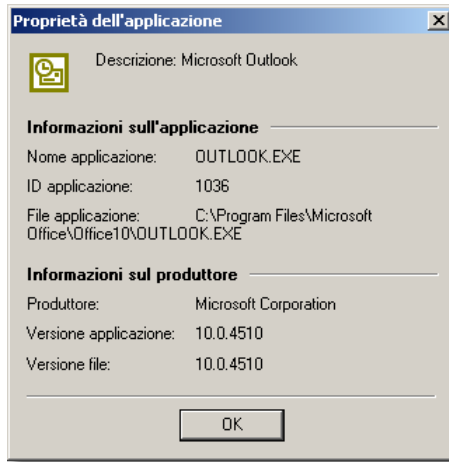


Fig. 37. La finestra di dialogo **Proprietà dell'applicazione**

La finestra di dialogo **Proprietà dell'applicazione** contiene una sezione di informazioni relative all'applicazione, con i seguenti elementi:

- **Nome dell'applicazione** – il nome del file eseguibile
- **ID applicazione** – l'identificativo dell'applicazione
- **File applicazione** – il percorso completo del file eseguibile


Sotto alla sezione **Informazioni sull'applicazione** si trova un'altra sezione chiamata **Informazioni sul produttore**, che contiene i seguenti elementi:

- **Produttore** – il nome del produttore
- **Versione applicazione** – la versione del programma
- **Versione file** – la versione del file eseguibile



## 7.1.2. Connessioni stabilite



*Per consultare l'elenco delle connessioni di rete correntemente stabilite,*

selezionare **Connessioni stabilite** nel sottomenu **Mostra** del menu **Visualizza** (cfr. fig. 38). Inoltre è possibile premere il pulsante  nella barra degli strumenti.

Si apre la finestra di dialogo **Connessioni stabilite**.

Ogni riga dell'elenco contiene i dati relativi a una singola connessione stabilita. Le connessioni stabilite sono indicate con l'icona  se stabilite dal proprio computer, o dall'icona  se ricevute dall'esterno.

L'elenco contiene inoltre i seguenti dati relativi alle connessioni:

- **Indirizzo remoto** – l'indirizzo e la porta di una macchina remota con cui è stabilita una connessione.
- **Indirizzo locale** – l'indirizzo e la porta del proprio computer.
- **Applicazione** – l'applicazione che ha stabilito questa connessione.

L'elenco può essere organizzato in base a ciascuna delle categorie sopra descritte.

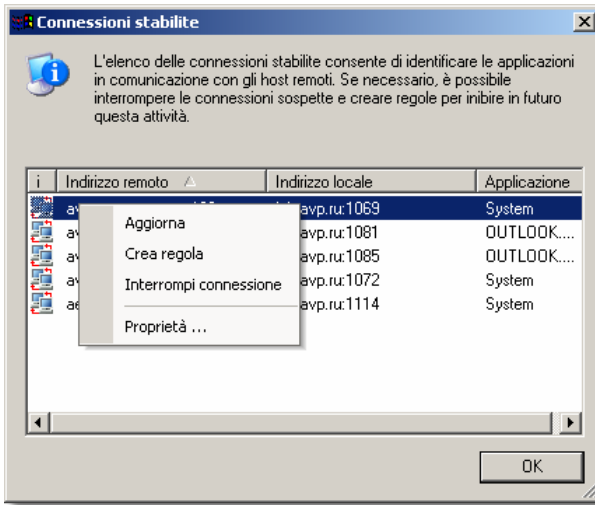


Fig. 38. La finestra di dialogo **Connessioni stabilite**

L'elenco delle connessioni stabilite attive è aggiornato automaticamente due volte al secondo.

Se necessario, è possibile interrompere le connessioni non desiderate e/o creare apposite regole per inibire in futuro questa attività. Per fare questo, usare gli appositi comandi del menu contestuale della finestra di dialogo:

- **Aggiorna** – aggiorna l'elenco delle applicazioni attive su richiesta dell'utente.
- **Crea regola** - consente di creare una regola per una connessione selezionata. Il programma avvia la Composizione guidata delle regole per applicazioni, quindi inserisce automaticamente i dati relativi alla connessione selezionata negli appositi campi.
- **Interrompi connessione** – interrompe la connessione selezionata dall'elenco.



**Attenzione!** Se si interrompe forzatamente una connessione, l'applicazione relativa potrà funzionare in maniera non corretta.

- **Proprietà** - visualizza maggiori dati sulla connessione selezionata nell'elenco(cfr. fig. 39).



Fig. 39. La finestra di dialogo **Proprietà della connessione**

La sezione **Connessione** della finestra di dialogo **Proprietà della connessione** contiene i seguenti elementi:


- **Direzione** – il tipo di connessione: in uscita o in entrata
- **Indirizzo remoto** - il nome simbolico o l'indirizzo IP della macchina remota
- **Porta remota** – il numero della porta remota
- **Porta locale** – il numero della porta locale

Sotto la sezione **Connessione** vi sono le sezioni **Informazioni sull'applicazione** e **Informazioni sul produttore** (cfr. paragrafo 7.1.1 a pag. 75).

### 7.1.3. Porte aperte



*Per consultare l'elenco delle porte correntemente attive,*

selezionare **Porte aperte** nel sottomenu **Mostra** del menu **Visualizza** (cfr. fig. 40). Inoltre è possibile premere il pulsante  nella barra degli strumenti.

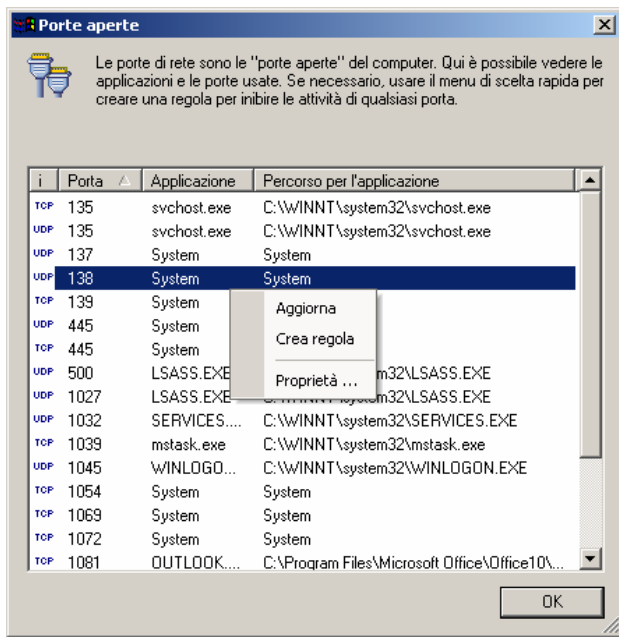
Si apre la finestra di dialogo **Porte aperte**.

Ogni riga dell'elenco contiene i dati relativi a una singola porta aperta. Le porte aperte sono indicate dall'icona **TCP** o **UDP**, in base al tipo di porta aperta.

L'elenco contiene inoltre i seguenti dati relativi alle porte:

- **Porta locale** – il numero della porta
- **Applicazione** – l'applicazione interessata
- **Percorso per l'applicazione** – il percorso completo del file eseguibile

L'elenco può essere organizzato in base a ciascuna delle categorie sopra descritte.

Fig. 40. La finestra di dialogo **Porte aperte**

L'elenco delle porte aperte viene aggiornato automaticamente due volte al secondo.

Se necessario, è possibile creare una regola che inibisca la connessione alla porta selezionata. Per fare questo, usare gli appositi comandi del menu contestuale della finestra di dialogo:

- **Aggiorna** – aggiorna l'elenco delle porte aperte su richiesta dell'utente.
- **Crea regola** – consente di creare una regola per una porta selezionata. Il programma avvia la Composizione guidata delle regole per applicazioni, quindi inserisce automaticamente i dati relativi alla porta selezionata negli appositi campi.
- **Proprietà** – visualizza maggiori dati sulla porta selezionata nell'elenco (cfr. fig. 41).

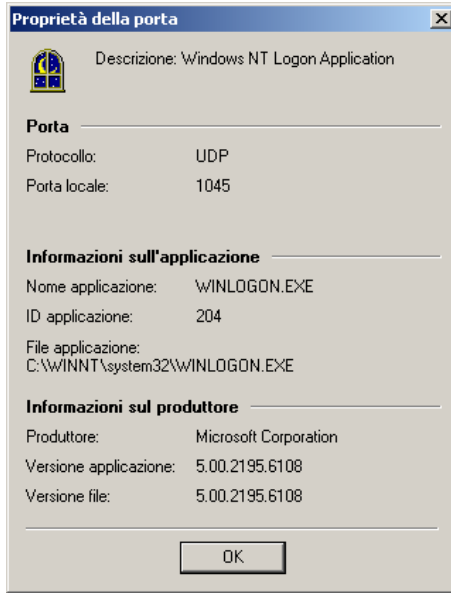


Fig. 41. La finestra di dialogo **Proprietà della porta**

La sezione **Porta** della finestra di dialogo **Proprietà della porta** contiene i seguenti elementi:

- **Protocollo** – il nome del protocollo usato
- **Porta locale** – il numero della porta locale

Sotto la sezione **Porta** vi sono le sezioni **Informazioni sull'applicazione** e **Informazioni sul produttore** (cfr. paragrafo 7.1.1 a pag. 75).

## 7.2. Uso dei registri

Gli eventi di rete che si verificano nel computer vengono monitorati e salvati nei *registri*. Tipi di eventi diversi vengono salvati in registri diversi:

- Il registro **Sicurezza** contiene i dati relativi agli attacchi più recenti subiti dal computer (cfr. paragrafo 6.5 a pag. 71).

- Il registro dell'**Attività delle applicazioni** contiene i dati relativi agli eventi da registrare come definiti dalla Composizione guidata delle regole delle applicazioni (cfr. paragrafo 6.3.2.3 a pag. 61).
- Il registro del **Filtraggio pacchetti** contiene i dati relativi agli eventi da registrare come definiti dalla Composizione guidata delle regole di filtraggio pacchetti (cfr. paragrafo 6.4.2.2 a pag. 69).

Tutti i registri possono essere consultati e configurati in un'unica finestra (la *finestra* **Registri**).

È possibile usare questa finestra per limitare le dimensioni dei registri, impostare i registri in modo da cancellarli ogni volta che il programma viene riavviato, o memorizzare i risultati di più di una sessione (cfr. paragrafo 7.2.4 a pag. 91).

Se necessario, è possibile cancellare i registri manualmente.

Inoltre è possibile salvare questi registri sul disco fisso.

## 7.2.1. Visualizzazione della finestra dei registri



Per visualizzare la finestra **Registri**,

selezionare il tipo di registro desiderato dal sottomenu **Registri** del menu **Visualizza**.

Si apre la finestra **Registri** (cfr. fig. 42).

## 7.2.2. Il layout della finestra Registri

La finestra Registri contiene i seguenti tre elementi:

- Menu
- Tabella dei rapporti
- Schede che consentono di passare da un tipo di registro all'altro.

### 7.2.2.1. Menu

Nella parte superiore della finestra Registri si trova una *barra dei menu*.

Tabella 4

Elemento di menu	Funzione
File → Salva su file	Salva il registro corrente su di un file
File → Chiudi	Chiude la finestra del registro
Guida in linea → Sommario ...	Aprire gli argomenti della Guida
Guida in linea → Kaspersky Anti-Hacker sul the Web	Aprire il sito web di Kaspersky Lab
Guida in linea → Informazioni su Kaspersky Anti-Hacker	Visualizza un riquadro con i dati relativi al programma e informazioni sui tasti usati

### 7.2.2.2. Tabella dei rapporti

La tabella dei rapporti visualizza le informazioni salvate nel tipo di registro selezionato. È possibile consultare questo registro per mezzo della barra di scorrimento sulla destra.

La tabella dei rapporti ha un menu contestuale che contiene di default i due seguenti comandi e può essere esteso in base al tipo di registro selezionato:

- **Cancella il registro** – cancella il registro selezionato.
- **Scorrimento automatico registro** - visualizza sempre l'ultimo evento registrato in fondo alla tabella dei rapporti.
- **Non registrare questo evento** – disabilita ulteriori registrazioni dell'evento selezionato. Questo comando è disponibile in tutti i registri ad eccezione di quello degli attacchi hacker.

- **Crea regola** – consente di creare una regola per un evento selezionato. La regola recentemente creata viene collocata all'inizio dell'elenco di regole, con il più alto livello di priorità.

### 7.2.2.3. Schede

Le seguenti schede alla base della finestra **Registri** consentono di passare da un tipo di registro all'altro:

- Sicurezza
- Attività delle applicazioni
- Filtraggio pacchetti

## 7.2.3. Selezione del registro

### 7.2.3.1. Registro di Sicurezza

Il registro di **Sicurezza** consente di consultare l'elenco di tutti gli attacchi rilevati ai danni del computer (cfr. paragrafo 6.5 a pag. 71).



*Per visualizzare il registro di **Sicurezza**,*

*selezionare **Sicurezza** dal sottomenu **Registri** del menu **Visualizza**.*

Viene visualizzata la finestra **Registri** nella modalità scheda **Sicurezza** (cfr. fig. 42). Il registro contiene i seguenti dati:

- **Data e ora** – la data e l'ora in cui il computer è stato attaccato.
- **Descrizione dell'evento** – la descrizione dell'attacco, inclusi il tipo di attacco e l'indirizzo dell'autore dell'attacco, se rilevato.

L'elenco degli eventi può essere organizzato solo per data e ora.

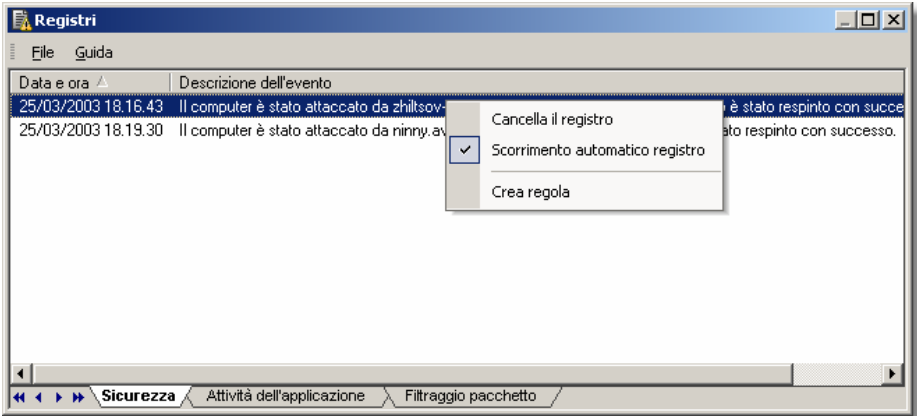


Fig. 42. La pagina dei registri di **sicurezza**

### 7.2.3.2. Attività delle applicazioni

Il registro **Attività dell'applicazione** consente di consultare i dati delle applicazioni con l'opzione di registro abilitata dalla composizione guidata delle regole per applicazioni (cfr. paragrafo 6.3.2.3 a pag. 61).



*Per visualizzare il registro delle **attività delle applicazioni**,*

selezionare il registro **Attività delle applicazioni** dal sottomenu **Registri** del menu **Visualizza**.

Viene visualizzata la finestra **Registri** nella modalità scheda **Attività delle applicazioni** (cfr. fig. 43). Il registro contiene i seguenti dati:

- **Data e ora** – la data e l'ora in cui l'evento si è verificato.
- **Applicazione** – il nome dell'applicazione relativa e il percorso completo del file eseguibile.
- **Descrizione attività** – i dati dell'attività.
- **Indirizzo locale** – l'indirizzo locale.
- **Indirizzo remoto** – l'indirizzo remoto.

L'elenco degli eventi può essere organizzato solo per data e ora.

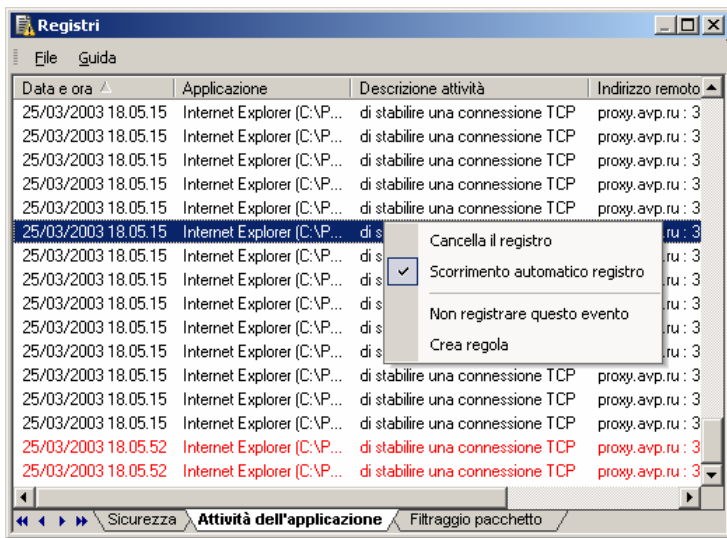


Fig. 43. La pagina del **registro delle attività delle applicazioni**

### 7.2.3.3. Filtraggio pacchetti

Il registro del **Filtraggio pacchetti** consente di visualizzare i dati relativi agli eventi di filtraggio pacchetti per i quali è stata abilitata l'opzione di registro per mezzo della composizione guidata delle regole di filtraggio pacchetti (cfr. paragrafo 6.4.2.2 a pag. 69).



*Per visualizzare il **registro di filtraggio pacchetti**,*

selezionare **Filtraggio pacchetti** nel sottomenu **Registri** del menu **Visualizza**.

Viene visualizzata la finestra **Registri** nella modalità scheda **Filtraggio pacchetti** (cfr. fig. 44). Il registro contiene i seguenti dati:

- **Data e ora** – la data e l'ora in cui l'evento si è verificato.
- **Direzione** – il tipo di pacchetto: in uscita o in entrata.

- **Protocollo** – il nome del protocollo.
- **Indirizzo locale** – l'indirizzo locale.
- **Indirizzo remoto** – l'indirizzo remoto.
- **Regola applicata** – il nome della regola adottata.

Le voci relative ai pacchetti consentiti sono di colore nero, mentre quelle relative ai pacchetti bloccati sono di colore rosso.

L'elenco degli eventi può essere organizzato solo per data e ora.

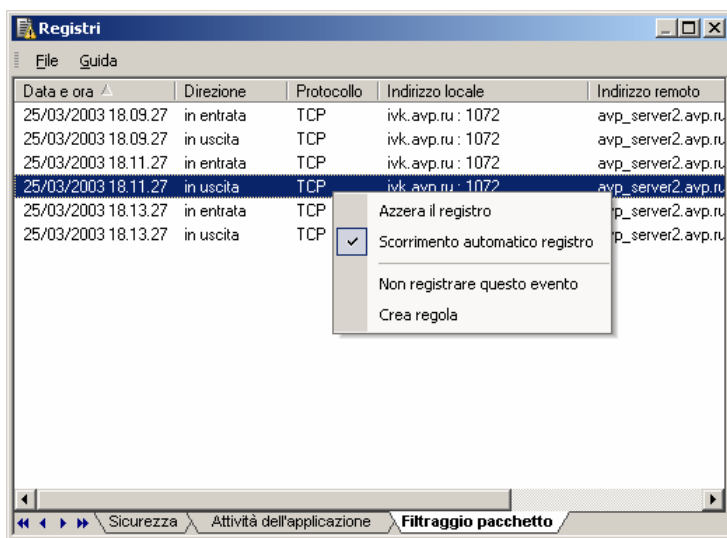


Fig. 44. La pagina del **registro di filtraggio pacchetti**

## 7.2.4. Definizione delle impostazioni dei registri



*Per definire le impostazioni dei registri,*

selezionare **Impostazioni** nel menu **Assistenza** e aprire la scheda **Registri** (cfr. fig. 45).

È possibile definire i valori per le seguenti opzioni:

- Cancellare i registri all'avvio del programma** – se selezionata, questa opzione cancella tutti i registri del programma all'apertura dello stesso.
- Dimensioni massime del registro (Kb)** – se selezionata, questa opzione consente di limitare le dimensioni del file di registro. Specificare le dimensioni massime del file di registro nel campo riservato al testo. Quando il file di registro raggiunge la dimensione massima, il programma inizia a rimuovere le voci più obsolete man mano che ne vengono aggiunte di nuove.



La casella di controllo di cui sopra consente di definire le dimensioni di un UNICO file di registro. Durante il calcolo dello spazio su disco necessario per le normali prestazioni del programma, il risultato deve essere moltiplicato per tre.

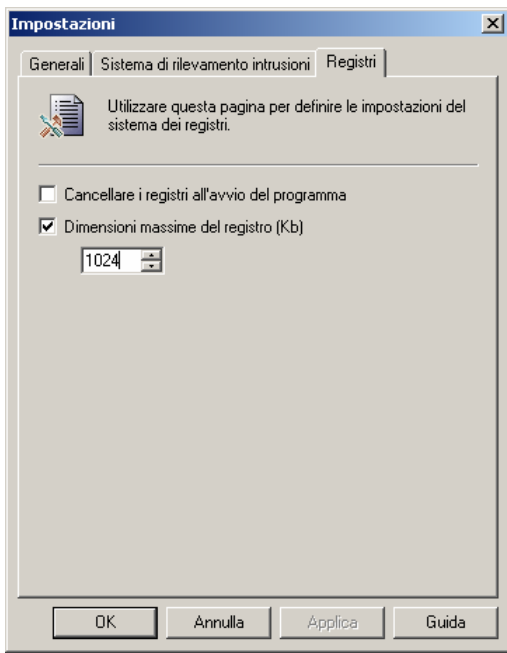


Fig. 45. La finestra di dialogo **Impostazioni** nella modalità scheda **Registri**

## 7.2.5. Salvataggio del registro su file



*Per salvare su file il registro selezionato nella finestra **Registri**,*

selezionare **Salva su file** dal menu **File**. Specificare il nome del file nella finestra di dialogo visualizzata. Il registro sarà salvato come testo semplice.

---

# APPENDICE A. INDICE

Avvertimenti sugli eventi, 40  
CD di installazione, 7  
Contratto di licenza, 7, 8  
Finestra di autoistruzione, 21, 38, 41  
Livelli di sicurezza, 6, 17, 21, 22, 37, 40  
Regole applicazione, 21, 45  
Regole di filtraggio pacchetti, 21, 60  
Scala di sicurezza, 32, 40  
Servizio di assistenza tecnica, 9, 94  
Sistema di rilevamento intrusioni, 7, 22, 24, 68

---

# APPENDICE B. DOMANDE FREQUENTI



Durante una sessione di lavoro, il computer visualizza un errore ed è possibile verificare se è stato provocato da Kaspersky Anti-Hacker.



Selezionare temporaneamente il livello di sicurezza **Consenti tutto** oppure scaricare Kaspersky Anti-Hacker dalla memoria del computer. Verificare se la situazione cambia. Se lo stesso errore si verifica di nuovo, non dipende da Kaspersky Anti-Hacker. Se il computer non visualizza alcun errore, rivolgersi al Servizio di assistenza tecnica di Kaspersky Lab.

---

## APPENDICE C. KASPERSKY LAB

Kaspersky Lab è un gruppo privato di società internazionali dedito allo sviluppo di software antivirus, con sede a Mosca (Russia) e uffici di rappresentanza altolocali nel Regno Unito, negli Stati Uniti, in Cina, Francia e Polonia. Fondata nel 1997, Kaspersky Lab è incentrata sullo sviluppo, il marketing e la distribuzione di software e tecnologie informatiche di sicurezza all'avanguardia.

Kaspersky Lab è uno dei leader mondiali nel settore della sicurezza dei dati e delle tecnologie antivirus. L'azienda è stata la prima a sviluppare molte delle funzionalità che costituiscono oggi parte essenziale della moderna protezione antivirus: un database esterno con moduli specializzati incorporati, una funzione di ricerca all'interno dei file archivio e compressi, una protezione antivirus integrata per Linux, ecc. Oltre al software antivirus, Kaspersky Lab è attiva nello sviluppo di software per la sicurezza generale dei dati. La linea attuale di prodotti comprende Kaspersky® Inspector e Kaspersky® WEB Inspector, le cui funzionalità esclusive garantiscono agli utenti un controllo completo su qualsiasi alterazione non autorizzata del file system e del contenuto di un Web server.

Tra le funzionalità in fase di implementazione, vi sono Kaspersky® Anti-Hacker per la protezione della postazione di lavoro dagli attacchi dei pirati informatici, e Kaspersky® Anti-Spam per la prevenzione a livello di impresa dei messaggi indesiderati e dell'uso scorretto della posta elettronica da parte dei dipendenti. Il prodotto principale di Kaspersky Lab, Kaspersky® Anti-Virus (precedentemente noto come AVP), è in costante sviluppo dal 1989 e ha ottenuto recensioni positive da numerose riviste specializzate e centri di ricerca antivirus quale miglior prodotto antivirus sul mercato.

Kaspersky® Anti-Virus copre tutti i più affidabili metodi di protezione antivirus: scanner antivirus, intercettori istantanei di virus residenti, utility di verifica dell'integrità e behavior blocker. Kaspersky® Anti-Virus supporta tutti i sistemi operativi e le applicazioni più diffusi, offre protezione antivirus per gateway di posta (MS Exchange Server, Lotus Notes/Domino, Sendmail, Qmail, Postfix e Exim), firewall e server Web. Tutti i prodotti Kaspersky Lab si basano sul database Kaspersky di oltre 60.000 virus noti e tutti gli altri tipi di codici maligni. I prodotti sono inoltre basati su un'esclusiva tecnologia euristica efficace perfino contro le minacce future: l'analizzatore di codici euristici incorporato, in grado di rilevare fino al 92% di virus ignoti, e l'unico behavior blocker al mondo per MS Office 2000, che offre una protezione totale garantita contro qualsiasi macrovirus.

## C.1. Altri prodotti Kaspersky Lab

### Kaspersky Anti-Virus Personal Pro

Pacchetto progettato per offrire una protezione antivirus completa ai computer domestici con sistema operativo Windows 98/ME/2000/NT/XP oltre alle applicazioni di MS Office 2000. Kaspersky Anti-Virus Personal Pro include un'applicazione di facile utilizzo per il prelievo quotidiano automatico degli aggiornamenti del database antivirus e dei moduli del programma. L'esclusivo sistema di analisi euristica di seconda generazione rileva con efficacia i virus ignoti. Kaspersky Anti-Virus Personal presenta un'interfaccia migliorata sotto molti aspetti, agevolando più che mai l'uso del programma.

Kaspersky Anti-Virus® Personal Pro presenta le seguenti funzioni:

- **Scansione manuale** di dischi locali;
- **Protezione in tempo reale automatica antivirus** di tutti i file;
- **Filtro posta** che esamina e ripara tutti i messaggi in entrata e in uscita (POP3) e rileva con efficacia i virus nei database della posta;
- **Behavior blocker** che garantisce la massima protezione delle applicazioni di MS Office dai virus;
- **Scansione archivi** – Kaspersky Anti-Virus riconosce oltre 700 formati di archivi e file compressi e ne garantisce la scansione antivirus automatica dei contenuti e la rimozione dei codici maligni dagli archivi **ZIP**, **CAB**, **RAR** e **ARJ**.

### Kaspersky® Security for PDA

Kaspersky® offre un'affidabile protezione antivirus dei dati memorizzati su PDA con Palm OS o Windows CE, e di qualsiasi informazione trasferita da un PC o scheda di estensione, file ROM e database. Il software contiene una combinazione di strumenti antivirus mirati:

- uno **scanner antivirus**, usato per la scansione manuale di tutti i dati memorizzati (sia sul PDA stesso che su qualsiasi scheda di estensione) e
- un **monitor antivirus** che intercetta i virus durante il trasferimento di dati con l'utility HotSync™ o prelevati da dispositivi portatili.

Esso offre l'accesso criptato al dispositivo e codifica tutti i dati memorizzati nel dispositivo e nelle schede di memoria.

### **Kaspersky Anti-Virus® Business Optimal**

Il pacchetto è stato sviluppato per garantire una protezione completa dei dati per reti aziendali di piccole e medie dimensioni.

Kaspersky Anti-Virus® Business Optimal include la protezione antivirus completa<sup>1</sup> per:

- *workstation* con Windows 95/98/ME, Windows NT/2000/XP Workstation e Linux;
- *file server e application server* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell NetWare, FreeBSD, BSDi e OpenBSD, e Linux;
- *Sistemi di posta*: Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; MS ISA Server.

Il kit di distribuzione di Kaspersky Anti-Virus® Business Optimal comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

La vasta gamma di programmi antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

### **Kaspersky® Corporate Suite**

Questo pacchetto è stato sviluppato al fine di offrire una protezione totale dei dati di reti aziendali di qualsiasi dimensione e complessità. I componenti del pacchetto garantiscono la protezione di tutti i nodi di una rete aziendale, anche in ambienti informatici misti. Kaspersky® Corporate Suite supporta la maggior parte dei sistemi operativi e delle applicazioni in uso nelle aziende. Tutti i componenti del pacchetto sono gestiti da una console mediante un'unica interfaccia utente. Kaspersky® Corporate Suite è un affidabile sistema di protezione di alto livello totalmente compatibile con le esigenze specifiche di ogni configurazione di rete.

Kaspersky® Corporate Suite include la protezione antivirus completa per:

---

<sup>1</sup> In base al tipo di kit di distribuzione.

- *Workstation* con Windows 98/ME, Windows NT/2000/XP e Linux;
- *file server e application server* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell NetWare, FreeBSD, OpenBSD, e Linux;
- *Sistemi di posta*, inclusi Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; MS ISA Server.
- *Computer portatili* (PDA).

Il kit di distribuzione di Kaspersky® Corporate Suite comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

## **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, tutti i moderni metodi di filtraggio della posta elettronica (inclusi gli elenchi RBL e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam funziona come filtro controllando tutta la posta in entrata alla ricerca di oggetti identificati come spam. Il software è compatibile con qualsiasi sistema di posta già in uso presso il cliente, e può essere installato sia su server mail esistenti sia su server dedicati.

L'elevato grado di efficacia di Kaspersky® Anti-Spam è consentito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico.

## **Kaspersky® Anti-Spam Personal**

Kaspersky® Anti-Spam Personal è studiato per garantire la protezione di Microsoft Outlook e Microsoft Outlook Express dai messaggi di posta elettronica indesiderati (spam).

Il pacchetto Kaspersky® Anti-Spam Personal è un potente strumento che garantisce l'intercettazione dello spam nel flusso di messaggi in arrivo mediante i protocolli POP3 e IMAP4 (solo per Microsoft Outlook).

Il processo di filtraggio comporta l'analisi di tutti gli attributi della lettera (indirizzi e intestazioni del mittente e del destinatario), il filtraggio dei contenuti (analisi dei contenuti della lettera, compresi oggetto e allegati), nonché una serie di esclusivi algoritmi linguistici ed euristici.

L'elevato grado di efficacia del programma è garantito anche grazie all'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico.

## C.2. Recapiti

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab che sarà lieta di offrire consigli su qualsiasi problematica relativa ai suoi prodotti, sia per telefono che per e-mail.

Supporto tecnico	Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina <a href="http://www.kaspersky.com/supportinter.html">http://www.kaspersky.com/supportinter.html</a>
Informazioni di carattere generale	WWW: <a href="http://www.kaspersky.com">http://www.kaspersky.com</a> <a href="http://www.viruslist.com">http://www.viruslist.com</a> E-mail: <a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>

---

# APPENDICE D. CONTRATTO DI LICENZA

Contratto di licenza standard con l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO CON VALORE LEGALE ("CONTRATTO"), RELATIVO ALLA LICENZA DEL SOFTWARE SPECIFICATO ("SOFTWARE") PRODOTTO DA KASPERSKY LAB ("KASPERSKY LAB").

ACQUISTANDO IL SOFTWARE TRAMITE INTERNET FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE (SIA ESSO UNA PERSONA FISICA O UNA PERSONA GIURIDICA) ACCETTA DI ESSERE VINCOLATO DALLE CONDIZIONI DEL PRESENTE CONTRATTO E DI DIVENTARNE PARTE. QUALORA L'UTENTE NON ACCETTI TUTTE LE CLAUSOLE DEL PRESENTE CONTRATTO, DOVRÀ SELEZIONARE IL PULSANTE CHE INDICA CHE NON SI ACCETTANO LE CONDIZIONI DEL PRESENTE CONTRATTO E ASTENERSI DALL'INSTALLARE IL SOFTWARE.

ACQUISTANDO IL SOFTWARE SU UN SUPPORTO FISICO E ROMPENDO IL SIGILLO DEL CD, L'UTENTE (SIA ESSO UNA PERSONA FISICA O UNA PERSONA GIURIDICA) ACCETTA DI ESSERE VINCOLATO DAL PRESENTE CONTRATTO. QUALORA L'UTENTE NON ACCETTI TUTTE LE CLAUSOLE DEL PRESENTE CONTRATTO, NON DOVRÀ ROMPERE IL SIGILLO DEL CD NÉ SCARICARE, INSTALLARE O USARE IL PRESENTE SOFTWARE. L'UTENTE HA IL DIRITTO DI RESTITUIRE IL PRESENTE SOFTWARE E OTTENERE UN RIMBORSO COMPLETO. IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SCADE 30 GIORNI DOPO L'ACQUISTO PRESSO UN DISTRIBUTORE O UN RIVENDITORE KASPERSKY LAB AUTORIZZATO. IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SPETTA SOLO ALL'ACQUIRENTE ORIGINARIO.

Qualsiasi riferimento al "Software" nel presente documento sarà da intendersi comprensivo di chiave di attivazione ("File di identificazione chiave") fornita da Kaspersky Lab come parte integrante del Software.

1. Concessione di licenza. Previo pagamento dei canoni di licenza applicabili, e in base ai termini e alle condizioni del presente Contratto, Kaspersky Lab conferisce all'utente il diritto non esclusivo e non trasferibile di usare una copia

della versione specificata del Software e della documentazione che lo accompagna (la "Documentazione") per il periodo di validità del presente Contratto, esclusivamente per scopi interni. L'utente può installare una copia del Software su un computer, workstation, agenda elettronica o altro dispositivo elettronico per il quale il Software è stato progettato (ciascuno denominato "Dispositivo del cliente"). Se la licenza del Software si riferisce a una suite o pacchetto con più di un prodotto Software specificato, questa licenza è valida per tutti i prodotti specificati di tale Software, con le limitazioni o clausole d'uso specificate nel listino prezzi applicabile o sulla confezione del prodotto, applicabili individualmente a ciascuno dei prodotti di tale Software.

1.1 Uso. Il Software è concesso in licenza come prodotto singolo; esso non può essere utilizzato su più di un Dispositivo del cliente o da più di un utente simultaneamente, fatta eccezione per i casi specificati in questa Sezione.

1.1.1 Il Software è "in uso" su un Dispositivo del cliente quando è caricato nella memoria temporanea (per esempio random access memory o RAM) oppure installato nella memoria permanente (per esempio disco fisso, CD-ROM o altro dispositivo di memorizzazione) di quel Dispositivo del cliente. Questa licenza autorizza l'utente a realizzare solo le copie di backup di questo Software necessarie per l'utilizzo ai termini di legge ed esclusivamente a fini di backup, a condizione che tutte le copie di cui sopra contengano tutte le necessarie informazioni sui diritti di proprietà del Software. Sarà cura dell'utente registrare il numero e l'ubicazione di tutte le copie del Software e della Documentazione e adottare ogni ragionevole precauzione volta a proteggere il Software dalla copia o dall'uso non autorizzati.

1.1.2 Qualora l'utente metta in vendita il Dispositivo del cliente su cui è installato il Software, egli dovrà accertarsi che tutte le copie del Software siano state precedentemente cancellate.

1.1.3 È fatto divieto all'utente di decompilare, decodificare, disassemblare o altrimenti ridurre qualsiasi parte di questo Software in forma leggibile o consentire a terzi di farlo. Le informazioni di interfaccia necessarie per ottenere l'interoperabilità del Software con programmi informatici creati autonomamente saranno fornite da Kaspersky Lab su richiesta, previo pagamento dei costi e delle spese ragionevolmente sostenuti per ottenere e fornire tali informazioni. Nel caso in cui Kaspersky Lab informi l'utente di non avere intenzione di mettere a disposizione tali informazioni per qualsiasi ragione, inclusi (senza limitazione) i costi, l'utente sarà autorizzato ad adottare le misure necessarie per ottenere l'interoperabilità, a condizione di poter soltanto decodificare o decompilare nella misura concessa per legge.

1.1.4 È fatto divieto all'utente di effettuare o consentire a terzi di effettuare copie (oltre a quelle espressamente consentite ai sensi del presente contratto),

correggere errori o altrimenti modificare, adattare o tradurre il Software, oppure derivare altre applicazioni dal Software stesso.

1.1.5 È fatto divieto all'utente di concedere in locazione, in leasing o in prestito a terzi il Software o trasferire o cedere in sublicenza a terzi i diritti a lui conferiti dalla licenza.

1.2 Uso in modalità server. Il Software può essere usato su un Dispositivo del cliente o su o come server ("Server") in un ambiente multiutente o dirette ("Modalità server") solo se tale uso è consentito in base al listino prezzi applicabile o alla confezione del Software. È necessaria una licenza a parte per ogni Dispositivo del cliente o "postazione" che possa collegarsi al Server in qualsiasi momento, a prescindere dal fatto che tali Dispositivi del cliente o postazioni autorizzati mediante licenza siano collegati simultaneamente o accedano o facciano effettivamente uso del Software. L'uso di software o di hardware che riducano il numero dei Dispositivi del cliente o postazioni che accedono direttamente a o fanno uso del Software (per esempio software o hardware "multiplexing" o "pooling") non riduce il numero delle licenze necessarie (vale a dire, il numero delle licenze necessarie corrisponde al numero di input distinti al "front end" del software o hardware multiplexing o pooling). Se il numero di Dispositivi del cliente o postazioni in grado di collegarsi al Software supera il numero di licenze ottenute, l'utente è tenuto a installare un meccanismo adeguato in grado di verificare che l'uso fatto del Software non superi le limitazioni d'uso specificate per la licenza ottenuta. Questa licenza autorizza l'utente a effettuare o scaricare le copie della Documentazione per ogni Dispositivo del cliente o postazione autorizzati mediante licenza, necessarie per l'uso consentito dalla legge, a condizione che ciascuna di tali copie contenga tutte le informazioni sui diritti di proprietà della Documentazione stessa.

1.3 Licenze per volume di acquisto. Se il Software è stato ceduto in base alle condizioni di licenza per volume di acquisto specificate nella fattura o nella confezione del Software, l'utente può effettuare, usare o installare un numero di copie supplementari del Software su altrettanti Dispositivi del cliente, come specificato nelle condizioni di licenza per volume di acquisto. L'utente deve disporre di meccanismi adeguati a garantire che il numero di Dispositivi del cliente su cui il Software è stato installato non superi il numero di licenze ottenute. Questa licenza autorizza l'utente a effettuare o scaricare una copia della Documentazione per ogni copia supplementare autorizzata dalla licenza per volume di acquisto, a condizione che ciascuna copia contenga tutte le informazioni sui diritti di proprietà del Documento.

2. Durata. Il presente Contratto è valido per la durata di [un (1)] anno, salvo risoluzione anticipata e in tal caso fino alla data di tale risoluzione, come esposto nel presente documento. Il presente Contratto si intenderà automaticamente risolto in caso di mancata osservanza da parte dell'utente di qualsivoglia condizione, limitazione o altro requisito qui specificato. Al momento della

risoluzione o della scadenza del presente Contratto, l'utente dovrà distruggere immediatamente tutte le copie del Software e della Documentazione in suo possesso. L'utente può recedere in qualsiasi momento dal presente Contratto distruggendo tutte le copie del Software e della Documentazione in suo possesso.

### 3. Assistenza.

(i) Kaspersky Lab metterà a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito, per la durata di un anno, previo:

(a) pagamento del canone corrente per i servizi di assistenza;

(b) compilazione del Modulo di richiesta dei Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale si richiede all'utente di fornire il proprio File di identificazione chiave fornito all'utente da Kaspersky Lab con il presente Contratto. È assoluta discrezione di Kaspersky Lab stabilire se l'utente abbia soddisfatto questa condizione per l'ottenimento dei Servizi di assistenza.

(ii) I Servizi di assistenza saranno sospesi alla scadenza, se non rinnovati annualmente mediante pagamento del canone annuale corrente per i servizi e in seguito alla compilazione del Modulo di richiesta dei Servizi di assistenza.

(iii) Con la compilazione del Modulo di richiesta dei Servizi di assistenza, l'utente accetta le condizioni esposte nell'Informativa sulla tutela della privacy applicata da Kaspersky Lab e allegata al presente Contratto, e acconsente esplicitamente al trasferimento dei propri dati all'esterno dei propri confini nazionali, come specificato nell'Informativa sulla tutela della privacy.

(iv) Per "Servizi di assistenza" si intendono

(a) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;

(b) Assistenza tecnica estesa a mezzo posta elettronica o tramite linea telefonica diretta messa a disposizione dal Fornitore e/o Rivenditore;

4. Diritti di proprietà. Il presente Software è protetto dalle leggi sul diritto d'autore. Tutti i diritti, titoli e interessi in e sul Software, compresi tutti i diritti d'autore, brevetti, marchi e altri diritti sull'approprietà intellettuale sono proprietà e possesso di Kaspersky Lab e dei suoi fornitori. Il possesso, l'installazione o l'uso del Software non trasferisce all'utente alcun titolo alla proprietà intellettuale del Software, né alcun diritto sul Software, fatta eccezione per i casi espressamente indicati in questo Contratto.

5. **Confidenzialità.** L'utente concorda che il Software e la Documentazione, inclusi il design e la struttura specifica dei singoli programmi e il File di identificazione chiave costituiscono informazioni confidenziali di proprietà di Kaspersky Lab. È fatto divieto all'utente di rivelare, fornire o altrimenti mettere a disposizione di terzi tali informazioni confidenziali in qualsiasi forma senza il previo consenso scritto di Kaspersky Lab. L'utente è tenuto ad adottare ragionevoli misure di sicurezza volte a proteggere tali informazioni confidenziali ma, senza limitarsi a quanto sopra, dovrà fare tutto quanto in suo potere per garantire la sicurezza del File di identificazione chiave.

## 6. Garanzia limitata

(i) Kaspersky Lab garantisce che per [90] giorni dal primo prelievo o installazione, il Software fornirà prestazioni sostanzialmente conformi alle funzionalità descritte nella Documentazione, se operato correttamente e secondo le modalità specificate nella Documentazione.

(ii) L'utente si assume interamente la responsabilità relativa alla scelta di questo Software per la soddisfazione delle proprie esigenze. Kaspersky Lab non garantisce che il Software e/o la relativa Documentazione saranno idonei a soddisfare tali esigenze, né che l'uso sarà privo di interruzioni e di errori;

(iii) L'unico rimedio per l'utente e l'unica responsabilità a carico di Kaspersky Lab in caso di violazione della garanzia come da paragrafo (i) consiste, a discrezione di Kaspersky Lab, nella riparazione, sostituzione o rimborso del Software qualora tale violazione venga riferita a Kaspersky Lab o a chi in sua vece durante il periodo di validità della garanzia. L'utente è tenuto a fornire tutte le informazioni ragionevolmente necessarie ad assistere il Fornitore nella soluzione del problema;

(iv) La garanzia come da (i) decade qualora l'utente (a) apporti o consenta di apportare qualsivoglia modifica a questo Software senza il consenso di Kaspersky Lab, (b) usi il Software per fini non conformi all'uso previsto o (c) usi il Software secondo modalità diverse da quanto consentito dal presente Contratto;

(v) Le garanzie e le condizioni specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilità di fornire o al ritardo nella fornitura del Software o della Documentazione che, se non fosse per questo paragrafo (v), potrebbero verificarsi tra Kaspersky Lab e voi o sarebbero altrimenti impliciti o incorporati nel presente Contratto o in qualsiasi altro contratto collaterale, per disposizione statutaria, legislazione vigente o altro, che con ciò sarebbero esclusi (inclusi, senza limitazione, le condizioni implicite, le garanzie o altri termini relativi all'adeguatezza della qualità, all'idoneità allo scopo o all'uso di competenza e cura ragionevoli).

## 7. Limitazione della responsabilità

(i) Nessun elemento del presente Contratto escluderà o limiterà la responsabilità di Kaspersky Lab per (i) frode o illecito, (ii) decesso o danni alla persona provocati dalla sua violazione dei doveri di diligenza previsti dalla legislazione vigente o da qualsivoglia violazione per negligenza di clausole di questo Contratto, (iii) qualsiasi violazione degli obblighi previsti dal Sale of Goods Act 1979, s. 12, o dal Supply of Goods and Services Act 1982, s. 2, o (iv) qualsiasi responsabilità non escludibile per legge.

(ii) Ai sensi del paragrafo (i), il Fornitore non avrà alcuna responsabilità (né a fini del contratto, frode, restituzione o in nessun'altra maniera) per nessuna delle seguenti perdite o danni (siano tali perdite o danni previsti, prevedibili, noti o altrimenti):

(a) Perdita di redditi;

(b) Perdita di profitti effettivi o previsti (incluse le perdite di profitti su contratti);

(c) Perdita di uso di denaro;

(d) Perdita di risparmi previsti;

(e) Perdita di affari;

(f) Perdita di opportunità;

(g) Perdita di goodwill;

(h) Perdita di reputazione;

(i) Perdita, danneggiamento o corruzione di dati; o

(j) Qualsiasi perdita indiretta o consequenziale o danno di qualsivoglia natura (inclusi, a scanso equivoci, ove tali perdite o danni siano del tipo specificato nel paragrafo (ii), (a) fino a (ii), (i).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

8. La struttura e l'interpretazione del presente Contratto dovranno essere regolate in conformità con le legislazioni di Inghilterra e Galles. Le parti si sottopongono

alla giurisdizione delle corti di Inghilterra e Galles, salvo il diritto di Kaspersky Lab in qualità di parte ricorrente, di avviare il ricorso in qualsiasi corte della giurisdizione competente.

9. (i) Il presente Contratto costituisce l'accordo complessivo intercorso tra le parti in merito al soggetto dello stesso e sostituisce qualsivoglia accordo, azione e promessa precedentemente intercorsi tra l'utente e Kaspersky Lab, sia orali che scritti, che possano essere scaturiti o implicitamente risultati da qualsivoglia documento scritto o dichiarazione durante gli accordi tra noi o i nostri rappresentanti, precedentemente al presente Contratto, e qualsiasi precedente contratto intercorso tra le parti relativamente all'oggetto di cui sopra cesserà di avere effetto a partire dalla Data di decorrenza. Fatta eccezione per quanto disposto nei paragrafi (ii) - (iii), non si riconosce all'utente alcun rimedio per affermazioni non veritiere su cui l'utente stesso abbia fatto affidamento alla stipula del presente Contratto ("Dichiarazione erronea") e Kaspersky Lab declina qualsiasi responsabilità oltre a quella derivante dalle condizioni esplicite del presente Contratto.

(ii) Nessun elemento del presente Contratto escluderà o limiterà la responsabilità di Kaspersky Lab per qualsivoglia Dichiarazione erronea resa nella consapevolezza della sua inesattezza.

(iii) La responsabilità di Kaspersky Lab per Dichiarazioni erronee in merito a questioni fondamentali, incluse le questioni fondamentali ai fini della capacità del produttore di adempiere agli obblighi previsti dal presente Contratto, sarà soggetta alle limitazioni di responsabilità esposte nel paragrafo 7 (iii).