Dr.WEB

Agent per Windows

Manuale dell'utente

Agent Dr.Web per Windows
Versione 13.0
Manuale dell'utente
23/01/2024

Doctor Web, Sede centrale in Russia

Indirizzo: 125124, Russia, Mosca, 3a via Yamskogo polya, 2, 12A

Sito web: https://www.drweb.com/

Telefono +7 (495) 789-45-87

Le informazioni sulle rappresentanze regionali e sedi sono ritrovabili sul sito ufficiale della società.

Doctor Web

Doctor Web — uno sviluppatore russo di strumenti di sicurezza delle informazioni.

Doctor Web offre efficaci soluzioni antivirus e antispam sia ad enti statali e grandi aziende che ad utenti privati.

Le soluzioni antivirus Dr.Web esistono a partire dal 1992 e dimostrano immancabilmente eccellenza nel rilevamento di programmi malevoli, soddisfano gli standard di sicurezza internazionali.

I certificati e premi, nonché la vasta geografia degli utenti testimoniano la fiducia eccezionale nei prodotti dell'azienda.

Siamo grati a tutti i nostri clienti per il loro sostegno delle soluzioni Dr.Web!

Sommario

1. Introduzione

Questo manuale contiene una descrizione dettagliata dell'installazione del prodotto Agent Dr.Web per Windows, nonché le raccomandazioni per l'utilizzo e la risoluzione dei problemi tipici associati alle minacce di virus. Principalmente, vengono considerate le modalità standard di funzionamento dei componenti del programma Dr.Web (con le impostazioni predefinite).

Gli Allegati contengono informazioni generali, nonché parametri aggiuntivi per la configurazione del programma Dr.Web, progettati per utenti esperti.

1.1. Segni e abbreviature utilizzati

Segni convenzionali

In questo manuale vengono utilizzati i seguenti simboli:

Simbolo	Commento
	Avviso di possibili situazioni di errore, nonché di punti importanti cui prestare particolare attenzione.
Rete antivirus	Un nuovo termine o un termine accentato nelle descrizioni.
<indirizzo_IP>	Campi in cui nomi di funzione vanno sostituiti con valori effettivi.
Salva	Nomi dei pulsanti di schermo, delle finestre, delle voci di menu e di altri elementi dell'interfaccia del programma.
CTRL	Nomi dei tasti della tastiera.
`C:\Windows\`	Nomi di file e directory, frammenti di codice.
Allegato A	Riferimenti incrociati ai capitoli del documento o collegamenti ipertestuali a risorse esterne.

Abbreviazioni

Nel testo del Manuale vengono utilizzate le seguenti abbreviazioni senza spiegazione:

- Dr.Web — Agent Dr.Web per Windows;
- FTP — (dall'inglese File Transfer Protocol) protocollo di trasferimento file;
- HTTP — (dall'inglese Hypertext Transfer Protocol) protocollo di trasferimento dell'ipertesto;
- IMAP — (dall'inglese Internet Message Access Protocol) protocollo a livello applicativo per l'accesso alla posta elettronica;

- IMAPS — (dall'inglese Internet Message Access Protocol Secure) protocollo sicuro a livello applicativo per l'accesso alla posta elettronica;
- MTU — (dall'inglese Maximum Transmission Unit) dimensione massima del pacchetto dati utile;
- NNTP — (dall'inglese Network News Transfer Protocol) protocollo di rete di trasmissione delle notizie;
- POP3 — (dall'inglese Post Office Protocol Version 3) protocollo dell'ufficio postale, versione 3;
- POP3S — (dall'inglese Post Office Protocol Version 3 Secure) protocollo sicuro dell'ufficio postale, versione 3;
- SIP — (dall'inglese Session Initiation Protocol) protocollo di avvio della sessione;
- SMTPS — (dall'inglese Simple Mail Transfer Protocol Secure) protocollo semplice sicuro di trasmissione dell'email;
- SO — sistema operativo;
- SSL — (dall'inglese Secure Sockets Layer) livello di socket sicuro;
- SW, software — programmi per computer.
- TCP — (dall'inglese Transmission Control Protocol) protocollo di controllo della trasmissione;
- TLS — (dall'inglese Transport Layer Security) protocollo di protezione del livello di trasporto;
- UAC — (dall'inglese User Account Control) controllo degli account utente;
- URL — (dall'inglese Uniform Resource Locator) identificatore uniforme di risorse;

2. Sul prodotto

Agent Dr.Web per Windows è studiato per proteggere la memoria di sistema, i dischi rigidi e i supporti rimovibili dei computer con i sistemi operativi della famiglia Windows da qualsiasi tipo di minacce: virus, rootkit, programmi trojan, spyware, adware, hacker e da altri oggetti malevoli provenienti da qualsiasi fonte esterna.

Agent Dr.Web per Windows è costituito da più moduli che si occupando di diverse funzionalità. Il motore antivirus e i database dei virus sono comuni a tutti i componenti e diverse piattaforme.

I componenti del prodotto vengono costantemente aggiornati e i database dei virus, i database delle categorie di risorse web e i database delle regole di filtraggio antispam dei messaggi email vengono regolarmente integrati con nuove firme delle minacce. Il continuo aggiornamento assicura il livello aggiornato della protezione dei dispositivi degli utenti, e inoltre delle applicazioni e dei dati utilizzati. Per una protezione aggiuntiva da programmi malevoli sconosciuti vengono utilizzati i metodi di analisi euristica implementati nel motore antivirus.

Agent Dr.Web per Windows è in grado di rilevare e rimuovere dal computer vari programmi indesiderati: adware, dialer, joke, riskware, hacktool. Per rilevare i simili programmi ed eseguire azioni sui file in cui sono contenuti, vengono utilizzati gli strumenti standard dei componenti antivirus Dr.Web.

Le informazioni sulla versione del prodotto, sulla lista dei componenti, sulla data dell'ultimo aggiornamento e il numero di identificazione di Agent Dr.Web sono ritrovabili sulla pagina **Supporto** sezione Sul programma.

2.1. Componenti di protezione e moduli di gestione

Agent Dr.Web per Windows include i seguenti componenti di protezione e moduli di gestione:

Componente/modulo	Descrizione
SpIDer Guard	Componente che risiede nella memoria operativa. Scansiona i file che vengono creati e i processi che vengono avviati, nonché rileva manifestazioni di attività di virus.
SpIDer Gate	Componente che viene utilizzato per la scansione antivirus del traffico HTTP. Con le impostazioni predefinite il monitoraggio internet SpIDer Gate controlla automaticamente il traffico HTTP in arrivo e blocca la trasmissione degli oggetti contenenti virus e altri programmi malevoli. Inoltre, di default è attivato il filtraggio URL dei siti sconsigliati e dei siti conosciuti come fonti di diffusione dei virus. Esegue il controllo sui protocolli HTTP, XMPP (Jabber) e TLS (SSL).

Componente/modulo	Descrizione
SpIDer Mail	Componente che intercetta le connessioni di qualsiasi client di posta in esecuzione sul computer ai server di posta sui protocolli POP3/SMTP/IMAP4/NNTP (IMAP4 sta per IMAPv4rev1), rileva e neutralizza le minacce prima ancora che il client di posta riceva le email dal server o invii un'email sul server di posta. SpIDer Mail può inoltre eseguire una scansione antispam delle email tramite Antispam Dr.Web.
Firewall Dr.Web	Firewall personale studiato per proteggere il computer da accessi non autorizzati dall'esterno e prevenire fughe di dati importanti attraverso la rete.
Office control	Componente che limita l'accesso a siti, file e cartelle, e inoltre consente di limitare il tempo di utilizzo di internet e del computer per ciascun account di Windows.
Analisi comportamentale	Componente che controlla l'accesso delle applicazioni agli oggetti critici del sistema e assicura l'integrità delle applicazioni in esecuzione.
Protezione dagli exploit	Componente che blocca oggetti malevoli che sfruttano le vulnerabilità nelle applicazioni.
Protezione dai ransomware	Componente che fornisce protezione dai virus cryptolocker.
Scanner	Scanner con interfaccia grafica che viene avviato su richiesta dell'utente ed esegue la scansione antivirus del computer.
Scanner console Dr.Web	La versione di Scanner con l'interfaccia a riga di comando.
Dr.Web per Microsoft Outlook	Plugin che controlla nelle caselle Microsoft Outlook la presenza di minacce e dello spam.
SpIDer Agent	Modulo attraverso cui si configura e si gestisce il funzionamento dei componenti del prodotto.

2.2. Metodi di rilevamento delle minacce

Tutti i prodotti antivirus sviluppati dall'azienda Doctor Web impiegano un intero set di metodi di rilevamento delle minacce, il che consente di controllare oggetti sospetti con la massima accuratezza.

Analisi basata sulle firme antivirali

Questo metodo di rilevamento viene impiegato in primo luogo. Si basa sulla ricerca delle firme delle minacce già conosciute nel contenuto dell'oggetto analizzato. La firma è una sequenza di byte continua finita, necessaria e sufficiente per identificare univocamente una minaccia. I contenuti dell'oggetto analizzato vengono confrontati con i checksum delle firme antivirali

anziché con le firme antivirali stesse, il che consente di ridurre notevolmente le dimensioni delle registrazioni nei database dei virus, mantenendo allo stesso tempo l'univocità della corrispondenza e, di conseguenza, la correttezza del rilevamento delle minacce e della cura degli oggetti infetti. I record nei database dei virus Dr.Web sono formati in modo tale che tramite un record sia possibile rilevare intere classi o famiglie di minacce.

Origins Tracing

Questa è una tecnologia unica Dr.Web che consente di rilevare le minacce nuove o modificate di cui il comportamento malevolo o i metodi di infezione sono già conosciuti e descritti nei database dei virus. Viene impiegata dopo l'analisi basata su firme e protegge gli utenti che utilizzano le soluzioni antivirus Dr.Web da minacce quale il trojan ransomware Trojan.Encoder.18 (anche conosciuto come "gpcode"). Inoltre, l'impiego della tecnologia Origins Tracing consente di ridurre notevolmente il numero di falsi positivi nell'analisi euristica. Ai nomi delle minacce rilevate tramite Origins Tracing viene aggiunto il postfisso `.Origin`.

Emulazione di esecuzione

Il metodo di emulazione di esecuzione del codice software viene utilizzato per rilevare virus polimorfi e cifrati quando la ricerca per checksum di firme antivirali è non applicabile o notevolmente ostacolata a causa di impossibilità di costruire le firme antivirali affidabili. Il metodo consiste nel simulare l'esecuzione del codice analizzato tramite un *emulatore* — un modello software del processore e dell'ambiente di esecuzione dei programmi. L'emulatore utilizza una zona di memoria protetta (*buffer di emulazione*). In tale caso le istruzioni non vengono trasmesse sulla CPU per essere effettivamente eseguite. Se il codice processato dall'emulatore è infetto, come risultato dell'emulazione verrà ripristinato il codice malevolo originale che può essere analizzato tramite l'analisi basata sulle firme antivirali.

Analisi euristica

L'analisi euristica si basa su un set di conoscenze *euristiche* (ipotesi la cui significatività statistica è stata empiricamente confermata) circa le caratteristiche del codice eseguibile malevolo o, al contrario, di quello sicuro. Ciascuna caratteristica del codice ha un determinato peso (cioè un numero che indica l'importanza e la validità di tale caratteristica). Il peso può essere sia positivo, se la caratteristica indica la presenza di un comportamento malevolo del codice, che negativo, se la caratteristica non è peculiare delle minacce informatiche. Sulla base del peso complessivo attribuito al contenuto dell'oggetto, l'analisi euristica calcola la probabilità di presenza in esso di un oggetto malevolo sconosciuto. Se questa probabilità eccede un determinato valore di soglia, l'analisi euristica conclude che l'oggetto analizzato è malevolo.

L'analisi euristica utilizza inoltre la tecnologia FLY-CODE — un algoritmo universale per lo spacchettamento di file. Questo meccanismo consente di costruire presupposti euristici sulla presenza di oggetti malevoli in oggetti compressi da programmi di impacchettamento (packer), e non solo da quelli conosciuti dagli sviluppatori del prodotto Dr.Web, ma anche da quelli nuovi, non ancora studiati. Nel controllo degli oggetti compressi viene inoltre utilizzata

la tecnologia di analisi dell'entropia strutturale che consente di rilevare minacce sulla base delle caratteristiche della posizione dei tratti di codice. Questa tecnologia, sulla base di un solo record del database dei virus, consente di rilevare una serie di varie minacce compresse dall'uguale packer polimorfo.

Siccome l'analisi euristica è un sistema di verifica delle ipotesi in condizioni di incertezza, essa può commettere errori sia del primo tipo (salta minacce sconosciute) e sia del secondo tipo (riconosce come malevolo un programma innocuo). Pertanto, agli oggetti contrassegnati dall'analisi euristica come "malevoli" viene attribuito lo stato "sospetti".

Analisi comportamentale

I metodi di analisi comportamentale consentono di analizzare la sequenza di azioni di tutti i processi nel sistema. Quando vengono rilevati segni di comportamento di programmi malevoli, le azioni di tale applicazione vengono bloccate.

Dr.Web Process Heuristic

La tecnologia di analisi comportamentale Dr.Web Process Heuristic protegge dai programmi malevoli più recenti e pericolosi che sono capaci di evitare il rilevamento tramite i meccanismi tradizionali di firme antivirali e analisi euristica.

Dr.Web Process Heuristic analizza il comportamento di ciascun programma in esecuzione e sulla base delle ultime conoscenze sul comportamento dei programmi malevoli, determina se un programma è pericoloso, dopo di che vengono adottate le misure necessarie per neutralizzare la minaccia. Ai nomi delle minacce rilevate tramite Dr.Web Process Heuristic viene aggiunto il prefisso `DPH`.

Questa tecnologia di protezione dati permette di minimizzare le perdite dalle azioni di un virus sconosciuto con il minimo consumo di risorse del sistema protetto.

Dr.Web Process Heuristic controlla tutti i tentativi di modifica del sistema:

- riconosce i processi dei programmi malevoli che modificano in modo indesiderabile i file dell'utente (per esempio, i tentativi di criptazione da parte dei trojan cryptolocker), compresi quelli situati in directory disponibili via rete;
- impedisce i tentativi dei programmi malevoli di integrarsi nei processi di altre applicazioni;
- protegge le porzioni critiche del sistema dalle modifiche da parte dei programmi malevoli;
- rileva e termina gli script e i processi malevoli, sospetti o inaffidabili;
- blocca la possibilità di modifica dei settori di avvio del disco da parte dei programmi malevoli per rendere impossibile l'avvio (per esempio, dei bootkit) sul computer;
- previene la disattivazione della modalità provvisoria di Windows, bloccando modifiche del registro;
- non permette ai programmi malevoli di modificare le regole di avvio di programmi;

- blocca il caricamento di driver nuovi o sconosciuti all'insaputa dell'utente;
- blocca l'esecuzione automatica di programmi malevoli, nonché di determinate applicazioni, come ad esempio anti-antivirus, non permettendo che si iscrivano al registro per il successivo avvio automatico;
- blocca i rami del registro responsabili dei driver di dispositivi virtuali, il che rende impossibile l'installazione di programmi trojan sotto le mentite spoglie di un nuovo dispositivo virtuale;
- non permette al software malevolo di compromettere il normale funzionamento dei servizi di sistema.

Dr.Web Process Dumper

L'analisi integrata delle minacce pacchettizzate Dr.Web Process Dumper aumenta significativamente il livello di rilevamento delle minacce apparentemente "nuove" — cioè che sono conosciute dal database dei virus Dr.Web, ma sono nascoste sotto packer nuovi, nonché elimina la necessità di aggiungere al database dei virus sempre nuovi record di minacce. La compattezza mantenuta dei database dei virus Dr.Web, a sua volta, non necessita di costante aumento dei requisiti di sistema e assicura le dimensioni tradizionalmente piccole degli aggiornamenti con la qualità di rilevamento e cura invariabilmente alta. Ai nomi delle minacce rilevate tramite Dr.Web Process Dumper viene aggiunto il prefisso `DPD`.

Dr.Web ShellGuard

La tecnologia Dr.Web ShellGuard protegge il computer dagli *exploit* — oggetti malevoli che cercano di sfruttare le vulnerabilità per ottenere il controllo sulle applicazioni attaccate o sul sistema operativo in generale. Ai nomi delle minacce rilevate tramite Dr.Web ShellGuard viene aggiunto il prefisso `DPH:Trojan.Exploit`.

Dr.Web ShellGuard protegge le applicazioni più comuni installate su computer con Windows:

- i browser (Internet Explorer, Mozilla Firefox, Google Chrome ecc.);
- le applicazioni MS Office;
- le applicazioni di sistema;
- le applicazioni che utilizzano le tecnologie java, flash e pdf;
- i lettori multimediali.

Protezione dagli injection

Injection — metodo utilizzato per incorporare codice malevolo nei processi in esecuzione sul dispositivo. Dr.Web monitora continuamente il comportamento di tutti i processi nel sistema e previene i tentativi di incorporazione se li considera malevoli. Ai nomi delle minacce rilevate tramite Protezione dagli injection viene aggiunto il prefisso `DPH:Trojan.Inject`.

Dr.Web controlla le seguenti caratteristiche dell'applicazione che ha avviato il processo:

- se l'applicazione è nuova;
- come è entrata nel sistema;

- dove è situata l'applicazione;
- come si chiama;
- se l'applicazione è inclusa nella lista delle affidabili;
- se ha una firma digitale valida da un'autorità di certificazione affidabile.

Dr.Web monitora lo stato del processo in esecuzione: controlla se thread remoti vengono creati nello spazio del processo, se codice estraneo viene incorporato nel processo attivo.

L'antivirus controlla le modifiche che vengono apportate dalle applicazioni, proibisce modifiche ai processi di sistema e privilegiati. Separatamente Dr.Web si occupa di prevenire che codice malevolo possa modificare la memoria dei browser più diffusi, per esempio quando si fanno acquisti su internet o si effettuano trasferimenti in banche online.

Protezione dai ransomware

Protezione dai ransomware — uno dei componenti di Protezione preventiva che fornisce la protezione dei file utente dai trojan cryptolocker. Questi programmi malevoli, entrando nel computer dell'utente, bloccano l'accesso ai dati tramite la cifratura, dopo di che estorcono denaro per la decriptazione. Ai nomi delle minacce rilevate tramite Protezione dai ransomware viene aggiunto il prefisso `DPH:Trojan.Encoder`.

Il componente analizza il comportamento del processo sospetto prestando attenzione in particolare alle ricerche di file, alla lettura e ai tentativi di modifica.

Vengono inoltre controllate le seguenti caratteristiche dell'applicazione:

- se l'applicazione è nuova;
- come è entrata nel sistema;
- dove è situata l'applicazione;
- come si chiama;
- se l'applicazione è affidabile;
- se ha una firma digitale valida da un'autorità di certificazione affidabile.

Viene inoltre verificata la natura della modifica al file. Quando vengono rilevati segni di comportamento del programma malevolo, le azioni dell'applicazione vengono bloccate, e vengono impediti i tentativi di modifica a file.

Metodo di apprendimento automatico

Viene utilizzato per cercare e neutralizzare oggetti malevoli che ancora non ci sono nei database dei virus. Il vantaggio di questo metodo consiste nel riconoscimento di un codice malevolo senza eseguirlo, solo in base alle sue caratteristiche.

Il rilevamento delle minacce è basato sulla classificazione degli oggetti malevoli secondo determinati segni. Tramite la tecnologia di apprendimento automatico basato sul metodo dei

vettori di supporto, frammenti di codice dei linguaggi di scripting vengono classificati e registrati nel database. In seguito gli oggetti di verifica vengono analizzati per conformità ai segni di codice malevolo. La tecnologia di apprendimento automatico automatizza l'aggiornamento della lista di questi segni e l'integrazione dei database dei virus.

Il metodo di apprendimento automatico risparmia in modo significativo le risorse del sistema operativo in quanto non richiede l'esecuzione di codice per rilevare le minacce, mentre l'addestramento automatico dinamico del classificatore può essere effettuato anche senza aggiornamento costante dei database dei virus, utilizzato nell'analisi basata sulle firme antivirali.

2.3. Requisiti di sistema

L'uso del programma Dr.Web è possibile su un computer che soddisfa i seguenti requisiti:

Parametro	Requisito
Processore	Con supporto del set di istruzioni i686
Sistema operativo	Per sistemi operativi a 32 bit: • Windows XP con pacchetto di aggiornamento SP2 o successivi; • Windows Vista con pacchetto di aggiornamento SP2 o successivi; • Windows 7 con pacchetto di aggiornamento SP1 o successivi; • Windows 8; • Windows 8.1; • Windows 10 22H2 o versioni precedenti; • Windows Server 2003 con pacchetto di aggiornamento SP1; • Windows Server 2008 con pacchetto di aggiornamento SP2 o successivi. Per sistemi operativi a 64 bit: • Windows Vista con pacchetto di aggiornamento SP2 o successivi; • Windows 7 con pacchetto di aggiornamento SP1 o successivi; • Windows 8; • Windows 8.1; • Windows 10 22H2 o versioni precedenti; • Windows 11 22H2 o versioni precedenti; • Windows Server 2008 con pacchetto di aggiornamento SP2 o successivi; • Windows Server 2008 R2 con pacchetto di aggiornamento SP1 o successivi; • Windows Server 2012; • Windows Server 2012 R2; • Windows Server 2016; • Windows Server 2019;

Parametro	Requisito
	• Windows Server 2022
Memoria operativa libera	512 MB o più
Risoluzione schermo	Risoluzione minima consigliata 1024×768
Supporto di ambienti virtuali e cloud	È supportato il funzionamento del programma nei seguenti ambienti: • VMware; • Hyper-V; • Xen; • KVM
Altro	Per l'aggiornamento dei database dei virus Dr.Web e dei componenti Dr.Web è richiesta la connessione al server di protezione centralizzata o a internet in Modalità mobile. Per il plugin Dr.Web per Microsoft Outlook è richiesto un client installato Microsoft Outlook di MS Office: • Outlook 2000; • Outlook 2002; • Outlook 2003; • Outlook 2007; • Outlook 2010 con pacchetto di aggiornamento SP2; • Outlook 2013; • Outlook 2016; • Outlook 2019; • Outlook 2021

In quanto l'azienda Microsoft ha terminato il supporto dell'algoritmo di hash SHA-1, prima di installare il programma Agent Dr.Web per Windows su Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2, è necessario assicurarsi che il sistema operativo supporti l'algoritmo di hash SHA-256. A tale scopo, installare tutti gli aggiornamenti consigliati da Windows Update. È possibile trovare informazioni dettagliate sui pacchetti di aggiornamento necessari sul sito ufficiale dell'azienda Doctor Web.

Agent Dr.Web per Windows versione 13.0 è compatibile solo con i plugin Dr.Web versione 12.0.

2.4. Verifica dell'antivirus

Verifica tramite il file EICAR

È possibile verificare l'operatività dei programmi antivirus che rilevano i virus sulla base delle firme antivirali, utilizzando il file di test EICAR (European Institute for Computer Anti-Virus Research).

Molti sviluppatori degli antivirus usano per questo scopo lo stesso programma standard `test.com`. Questo programma è stato specificamente sviluppato affinché l'utente, senza esporre a pericolo il proprio computer, possa vedere come l'antivirus installato segnalerà il rilevamento di un virus. Il programma test.com non è malevolo di per sé, ma viene processato come un virus dalla maggior parte dei programmi antivirus. Dr.Web denomina questo "virus" nel seguente modo: `EICAR Test File (Not a Virus!)`. Gli altri programmi antivirus lo denominano in un modo simile.

Il programma `test.com` è un file COM di 68 byte e come risultato della sua esecuzione nella console viene visualizzato il messaggio di testo: `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`

Il file `test.com` è costituito solo da caratteri testuali che formano la seguente stringa:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Se si creerà un file contenente la stringa sopracitata e si salverà il file sotto il nome `test.com`, come risultato si otterrà un programma che è il "virus" descritto sopra.

Quando funziona in modalità ottimale, SpIDer Guard non interrompe l'avvio del file di test EICAR e non determina questa operazione come pericolosa poiché questo file non rappresenta alcuna minaccia al computer. Tuttavia, quando tale file viene copiato o creato sul computer, SpIDer Guard elabora automaticamente il file come un programma malevolo e di default lo mette in Quarantena.

3. Installazione, modifica e rimozione del programma

Prima di iniziare a installare Agent Dr.Web per Windows, leggere i requisiti di sistema. Si consiglia inoltre di eseguire le seguenti azioni:

- installare tutti gli aggiornamenti critici rilasciati dall'azienda Microsoft per la versione del sistema operativo in uso (maggiori informazioni sull'aggiornamento di SO Windows e SO Windows Server); se il sistema operativo non è più supportato dal produttore, si consiglia di passare a una versione più moderna del sistema operativo;
- controllare il file system tramite gli strumenti di sistema ed eliminare i problemi rilevati;
- rimuovere dal computer altri programmi antivirus per prevenire possibili incompatibilità dei loro componenti con i componenti Dr.Web;
- se verrà installato Firewall Dr.Web, è necessario rimuovere dal computer i firewall;
- a partire da Windows Server 2016, disattivare manualmente Windows Defender utilizzando i criteri di gruppo;
- chiudere le applicazioni attive.

> ⚠ L'installazione di Dr.Web deve essere eseguita da un utente con i permessi dell'amministratore di tale computer.

L'installazione, la modifica e la rimozione di Dr.Web possono essere effettuate in due modi:

1. Da remoto — dal server di protezione centralizzata via rete. Viene effettuata dall'amministratore della rete antivirus, l'intervento dell'utente non è richiesto.
2. Localmente — direttamente sulla macchina dell'utente. In questo caso per l'installazione di Dr.Web può essere utilizzato l'installer completo o il pacchetto di installazione individuale.

È possibile installare Dr.Web in una delle seguenti modalità:

- in modalità riga di comando;
- in modalità installazione guidata.

3.1. Installazione tramite l'installer completo

L'installer completo `drweb-13.0.0-xxxxxxx-esuite-agent-full-windows.exe` installa allo stesso tempo Agent Dr.Web e il pacchetto antivirus. I parametri di connessione al server e i parametri di autenticazione della postazione sul server non sono inclusi nell'installer.

Installazione in modalità installazione guidata

Seguire le istruzioni del programma di installazione. A ciascun passaggio prima dell'inizio della copiatura dei file sul computer sono possibili le seguenti operazioni:

- per ritornare al passaggio precedente del programma di installazione, premere il pulsante **Indietro**;
- per andare al passaggio successivo del programma, premere il pulsante **Avanti**;
- per interrompere l'installazione, premere il pulsante **Esci**.

Per installare Dr.Web

1. Avviare il pacchetto di installazione fornito dall'amministratore. Si apre la finestra dell'Installazione guidata di Dr.Web.

> Se sulla postazione sono già installati programmi antivirus, l'Installazione guidata cercherà di rimuoverli. Se il tentativo non è riuscito, è necessario rimuovere in autonomo il software antivirus utilizzato sulla postazione.

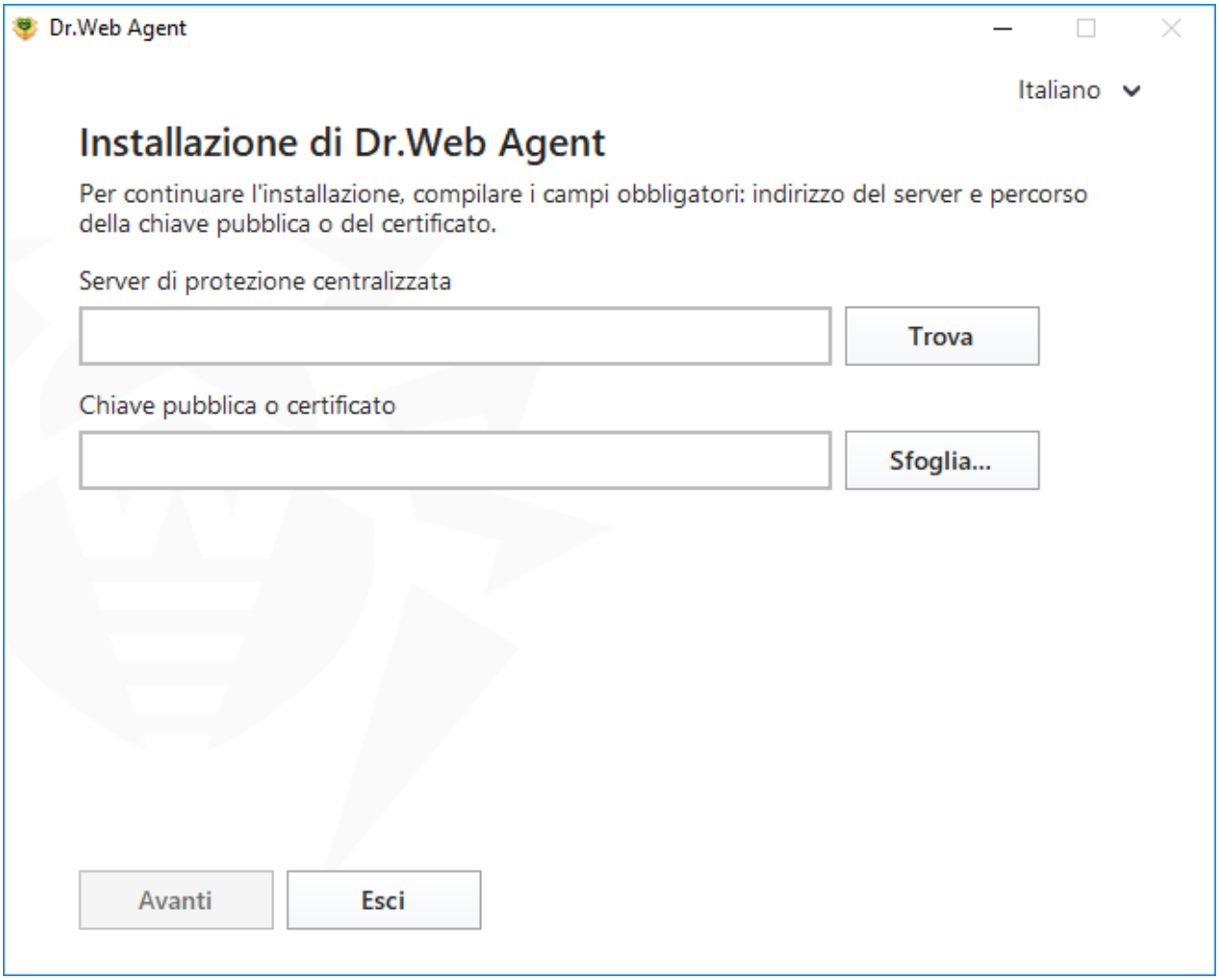

Immagine 1. Installazione guidata

2. Nel campo **Server di protezione centralizzata** inserire l'indirizzo di rete del server da cui verrà installato Dr.Web, e nel campo **Chiave pubblica o certificato** indicare il percorso completo della chiave di cifratura pubblica (`drwcsd.pub`) o del certificato con l'estensione `.pem` situato sul computer.

   Per cercare server attivi e indicare i parametri di ricerca, premere il pulsante **Trova**.

   Premere il pulsante **Avanti**.

3. L'Installazione guidata informerà che il software è pronto per l'installazione.

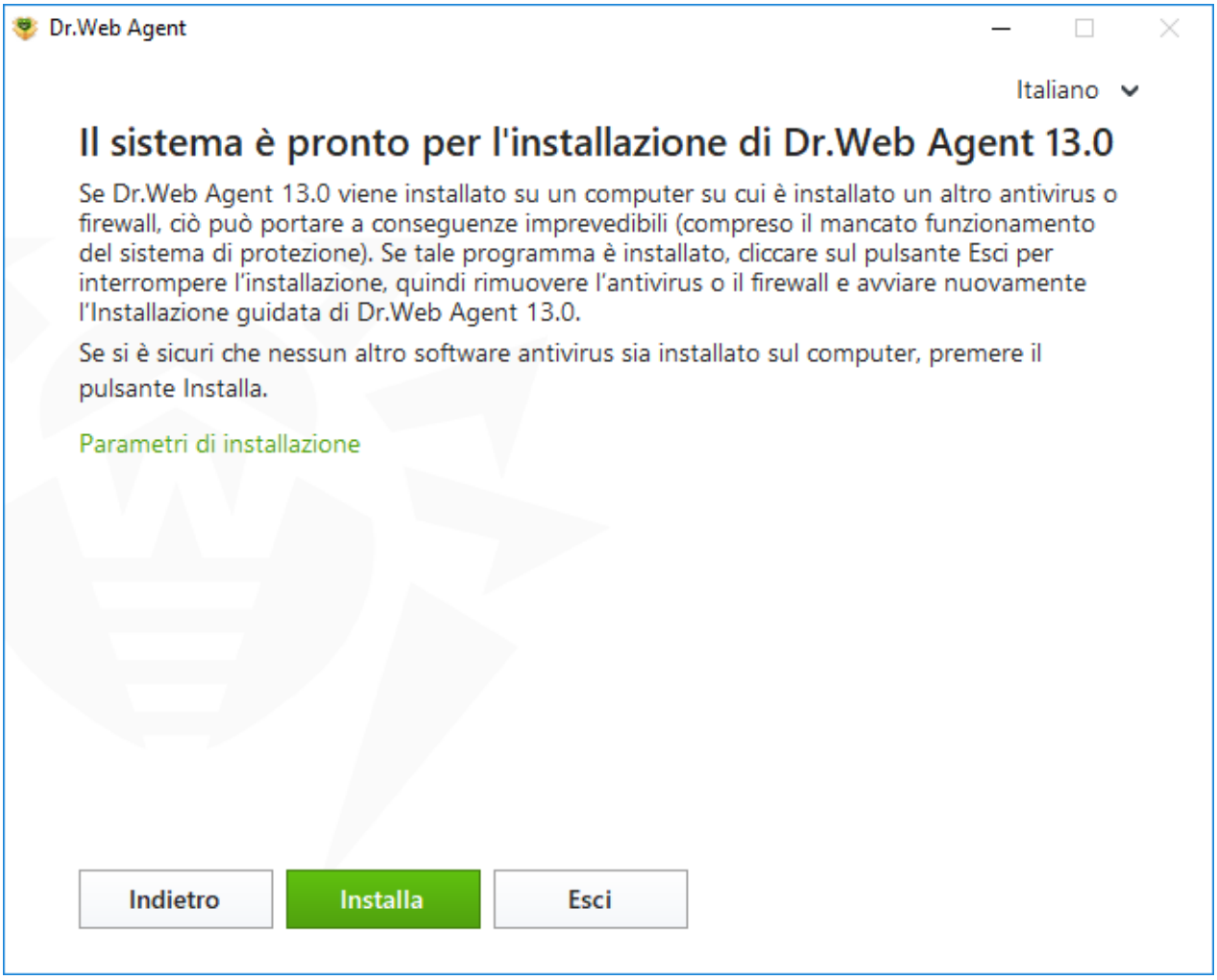

Immagine 2. Il software è pronto per l'installazione

   È possibile avviare il processo di installazione con i parametri predefiniti premendo **Installa**.

   Per selezionare i componenti da installare, indicare il percorso di installazione e alcuni parametri di installazione aggiuntivi, cliccare sul link **Parametri di installazione**. Questa opzione è destinata agli utenti esperti.

4. Se al passaggio precedente si è premuto il pulsante **Installa**, passare al passaggio 8. Altrimenti, si apre la finestra **Parametri di installazione**.

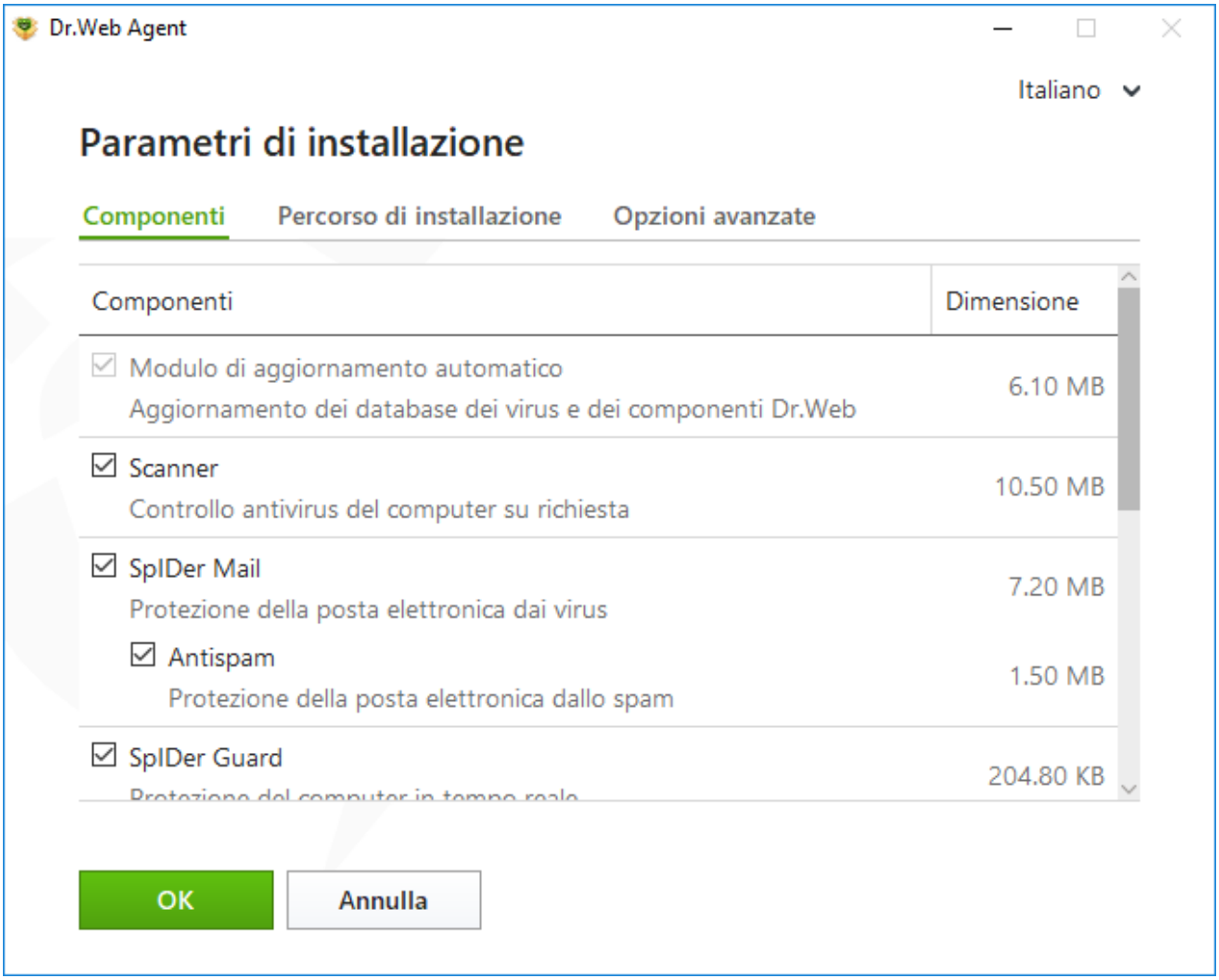

Immagine 3. Parametri di installazione

Nella scheda **Componenti** è possibile selezionare i componenti Dr.Web da installare.

Spuntare i flag di fronte ai componenti che si vogliono installare sul computer. Di default sono selezionati tutti i componenti ad eccezione di Firewall Dr.Web.

5. Nella scheda **Percorso di installazione** è possibile indicare la cartella in cui verrà installato **Agent Dr.Web per Windows**. Di default è la cartella DrWeb situata nella cartella `Program Files` sul disco di sistema. Per modificare il percorso di installazione, premere il pulsante **Sfoglia** e indicare il percorso desiderato.
6. Nella scheda **Opzioni avanzate** è possibile indicare le impostazioni aggiuntive.

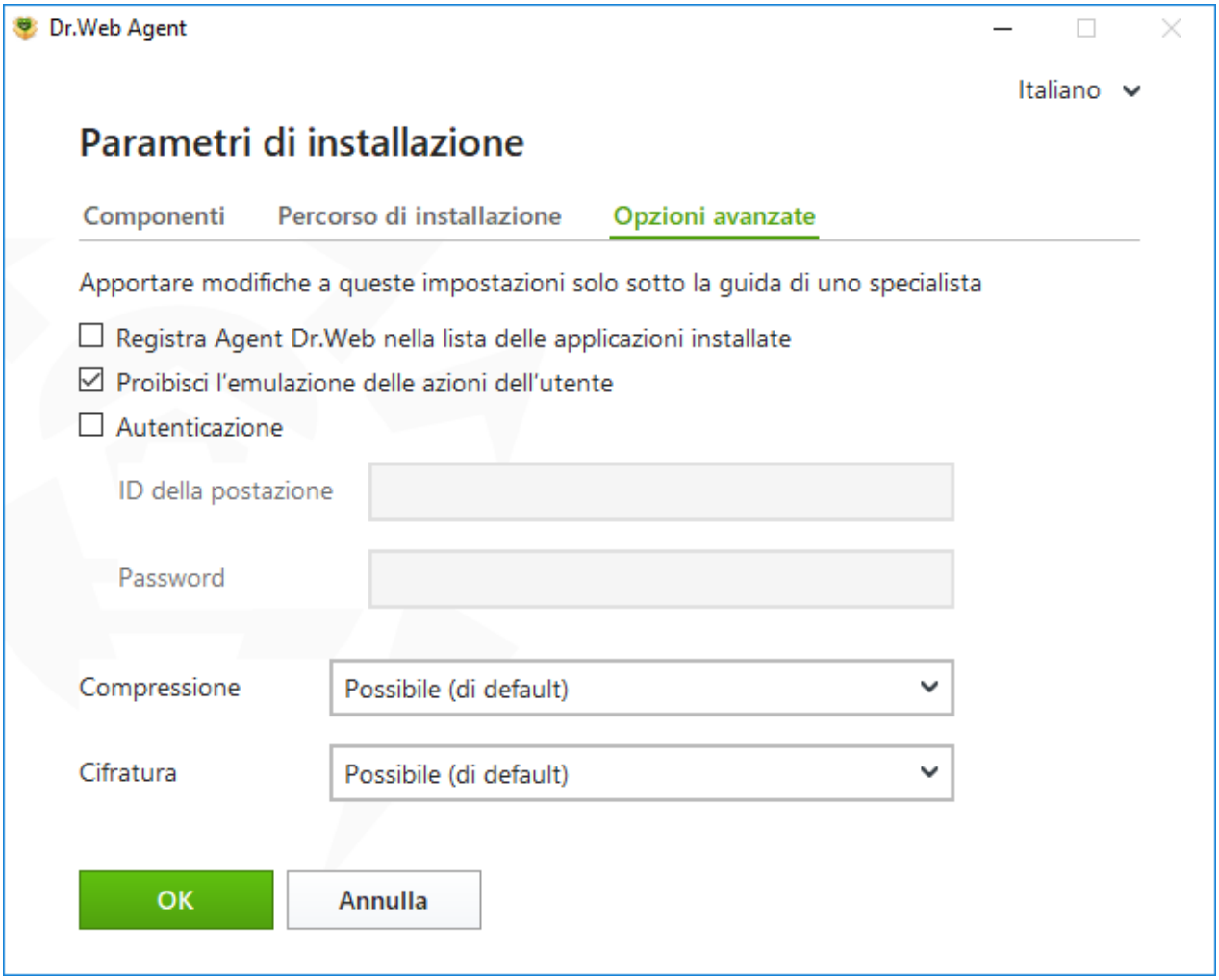

Immagine 4. Opzioni avanzate dei parametri di installazione

Sono disponibili le seguenti opzioni:

- **Registra l'Agent Dr.Web nella lista dei programmi installati**. Questa opzione consente, tra le altre cose, di rimuovere e modificare i componenti del programma Dr.Web tramite il Pannello di controllo di Windows.
- **Proibisci l'emulazione delle azioni dell'utente** Consente di prevenire modifiche alle impostazioni Dr.Web, eseguite da software di terze parti. Tra le altre cose, sarà proibita l'esecuzione di script che emulano il funzionamento della tastiera e del mouse nelle finestre Dr.Web (per esempio script per la modifica delle impostazioni Dr.Web e altre operazioni finalizzate a modificare il funzionamento di Dr.Web).
- Per l'autenticazione manuale sul server di protezione centralizzata spuntare il flag **Autenticazione**. Quindi è necessario impostare i parametri di autenticazione della postazione:
  - **ID della postazione** — identificatore della postazione sul server;
  - **Password** — password di accesso al server.

In questo caso la postazione otterrà l'accesso senza una conferma manuale da parte dell'amministratore sul server.

Nelle liste a cascata **Compressione** e **Crittografia** impostare le modalità corrispondenti per il traffico tra il server e Dr.Web.

Per salvare le modifiche apportate, premere **OK**, dopo di che premere il pulsante **Installa**.

7. Inizierà l'installazione di Dr.Web. Non è richiesto alcun intervento da parte dell'utente.
8. Dopo il completamento dell'installazione il programma avviserà della necessità di riavviare il computer. Premere il pulsante **Riavvia adesso**.

Installazione in modalità riga di comando

Per avviare l'installazione di Dr.Web in modalità riga di comando, andare alla cartella in cui si trova il pacchetto, dopo di che inserire il nome del file eseguibile di installazione (`drweb-13.0.0-xxxxxxx-esuite-agent-full-windows.exe`) con i parametri richiesti.

La lista completa dei parametri della riga di comando per i pacchetti di installazione è riportata in Allegato A.

3.2. Installazione tramite il pacchetto di installazione individuale

Quando si installa il programma utilizzando il pacchetto di installazione individuale, il prodotto viene installato via rete.

Il pacchetto di installazione individuale include l'installer di Agent Dr.Web e un set di parametri per la connessione al Server Dr.Web e l'autenticazione della postazione sul server Dr.Web.

Installazione in modalità installazione guidata

Seguire le istruzioni del programma di installazione. A ciascun passaggio prima dell'inizio della copiatura dei file sul computer sono possibili le seguenti operazioni:

- per ritornare al passaggio precedente del programma di installazione, premere il pulsante **Indietro**;
- per andare al passaggio successivo del programma, premere il pulsante **Avanti**;
- per interrompere l'installazione, premere il pulsante **Esci**.

Per installare Dr.Web

1. Avviare il pacchetto di installazione `drweb_ess_windows_<nome postazione>.exe` fornito dall'amministratore. Si apre l'Installazione guidata di Dr.Web.

Se sulla postazione sono già installati programmi antivirus, l'Installazione guidata cercherà di rimuoverli. Se il tentativo non è riuscito, è necessario rimuovere in autonomo il software antivirus utilizzato sulla postazione.

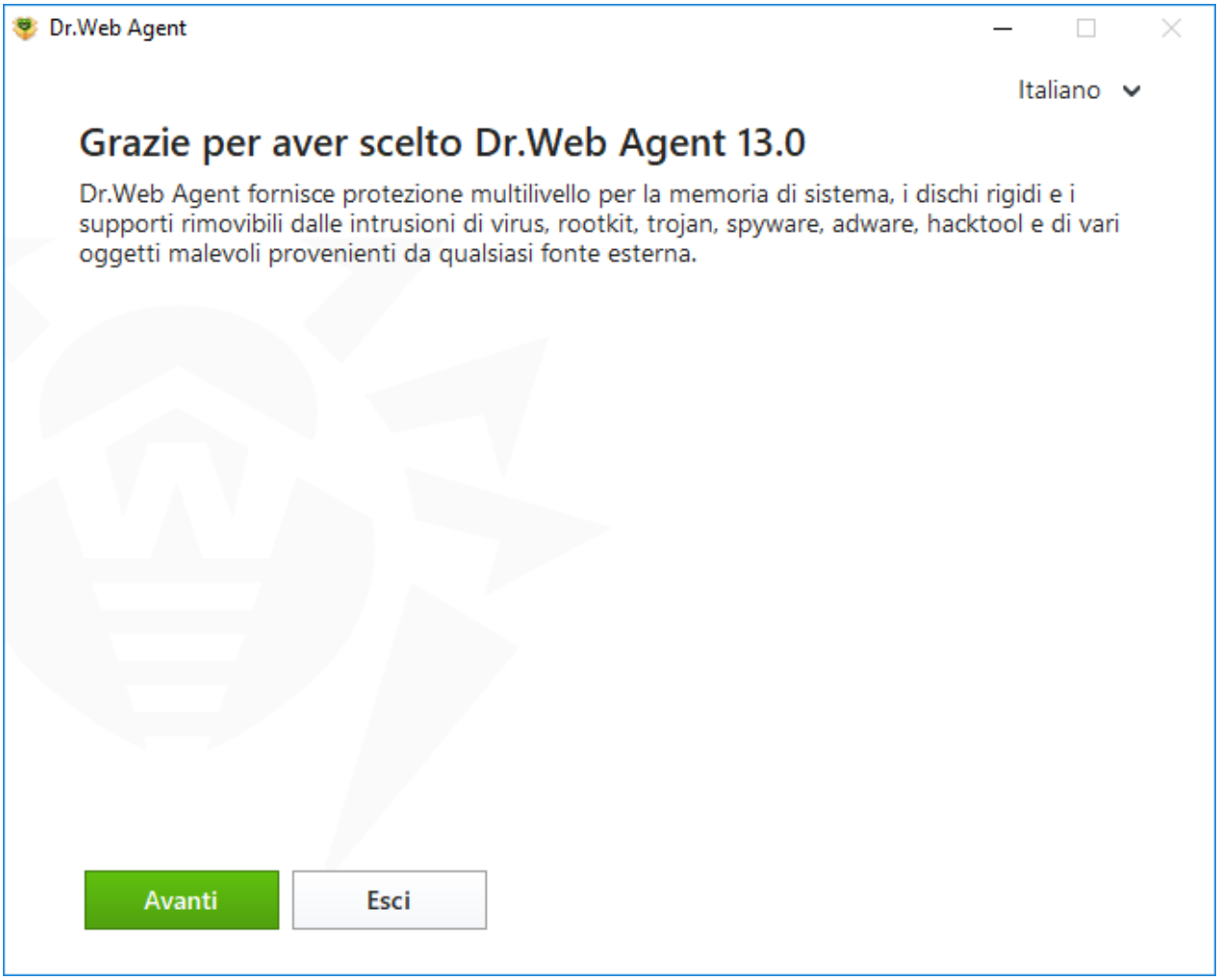

Immagine 5. Installazione guidata

2. Premere **Avanti**.
3. Al passaggio successivo della procedura guidata indicare il percorso della chiave di cifratura pubblica (`drwcsd.pub`) o del certificato con l'estensione `.pem` situato sul computer.

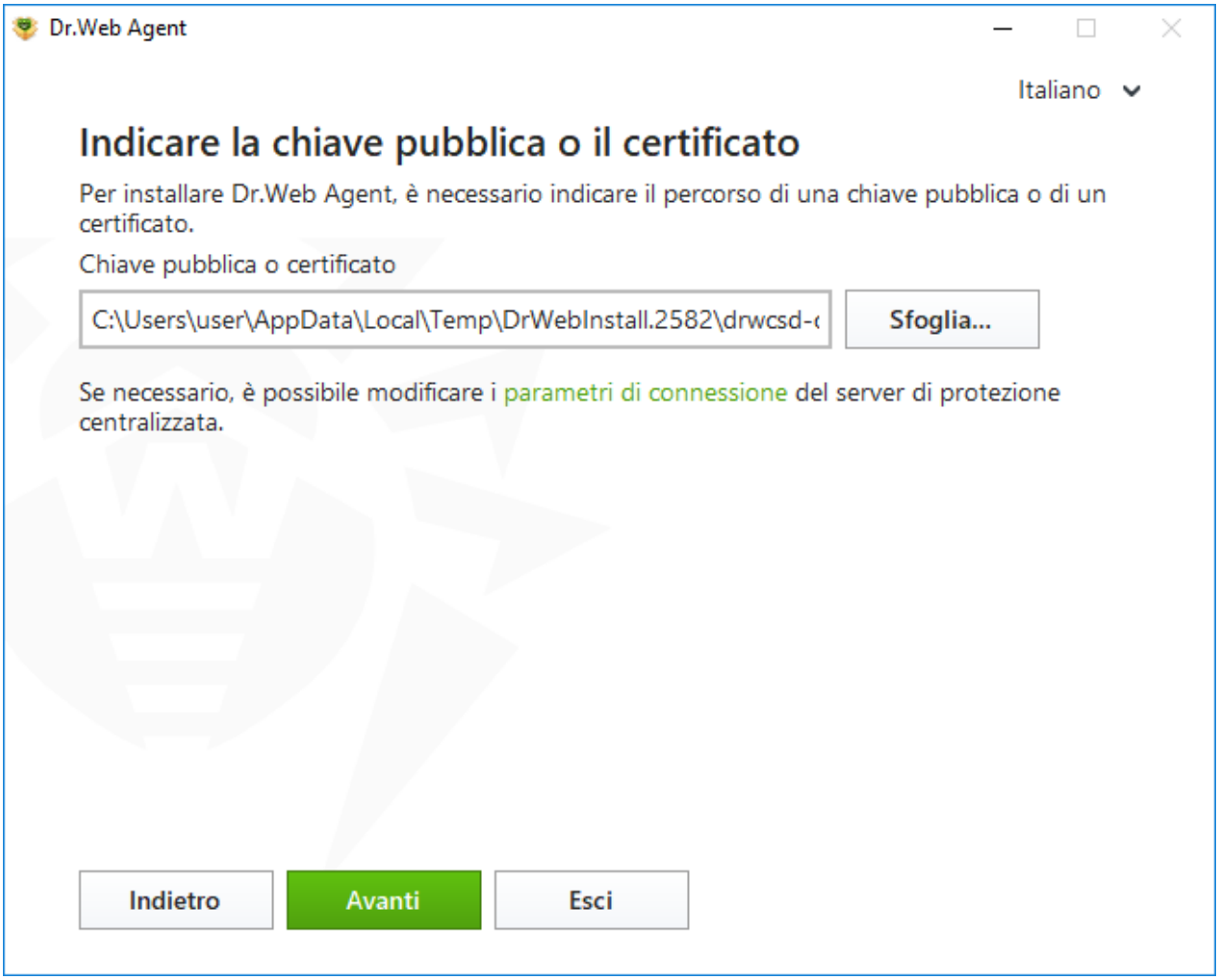

Immagine 6. Indicazione della chiave pubblica o del certificato

4. Se necessario, è possibile modificare i parametri di connessione al server di protezione centralizzata. A questo scopo, fare clic sul link corrispondente. Si apre la finestra **Parametri di connessione**. Nel caso di installazione tramite il pacchetto di installazione individuale, tutti i parametri di connessione sono già indicati.

   Si raccomanda vivamente di non cambiare nulla senza il consenso dell'amministratore della rete antivirus.

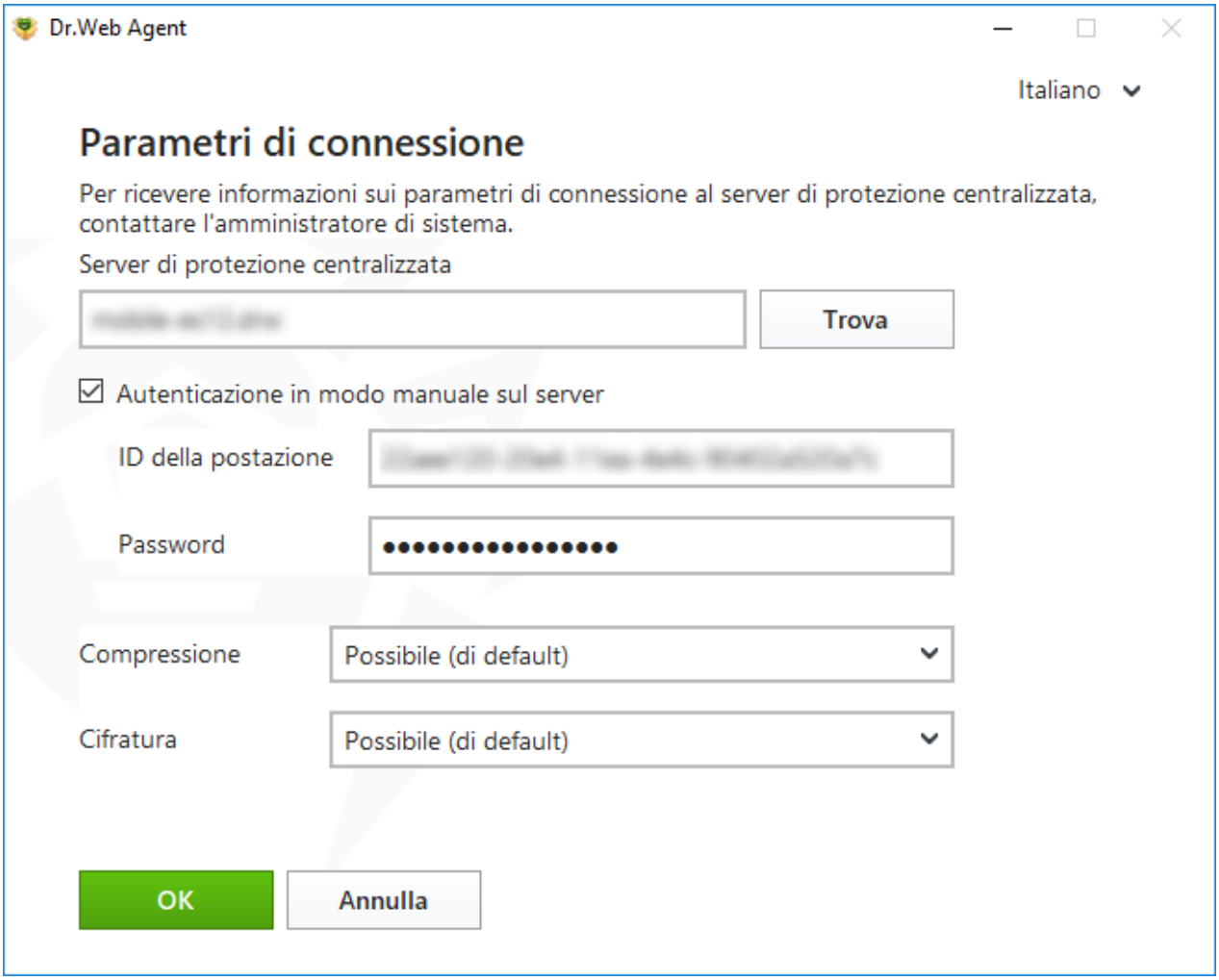

Immagine 7. Impostazione dei parametri della connessione al server di protezione centralizzata

Per informazioni sui parametri della connessione al server di protezione centralizzata contattare l'amministratore.

Nel campo **Server di protezione centralizzata** è possibile impostare l'indirizzo di rete del server da cui verrà installato Dr.Web. Di default, nel campo sono indicati i dati del server su cui è stato creato il file di installazione. Per cercare server attivi e indicare i parametri di ricerca, premere il pulsante **Trova**.

Per l'opzione di autenticazione manuale sul server attivare il flag corrispondente. Quindi è necessario impostare i parametri di autenticazione della postazione:

- **ID della postazione** — identificatore della postazione sul server;
- **Password** — password di accesso al server.

In questo caso la postazione otterrà l'accesso senza una conferma manuale da parte dell'amministratore sul server.

Se Dr.Web viene installato tramite un file di installazione creato nel Pannello di controllo Dr.Web, i campi **ID della postazione** e **Password** per l'opzione di autenticazione manuale vengono compilati automaticamente.

Nelle liste a cascata **Compressione** e **Crittografia** impostare le rispettive modalità per il traffico tra il server e Dr.Web.

Per salvare le modifiche apportate, premere **OK**, dopo di che premere **Avanti**.

Se la connessione non è stata stabilita, controllare i parametri di rete in base al link e/o ripetere il tentativo di connessione premendo il pulsante corrispondente.

5. Se la connessione al server di protezione centralizzata è riuscita, si apre una finestra con un messaggio che dice che il software è pronto per l'installazione. È possibile avviare il processo di installazione con i parametri predefiniti premendo il pulsante **Installa**.

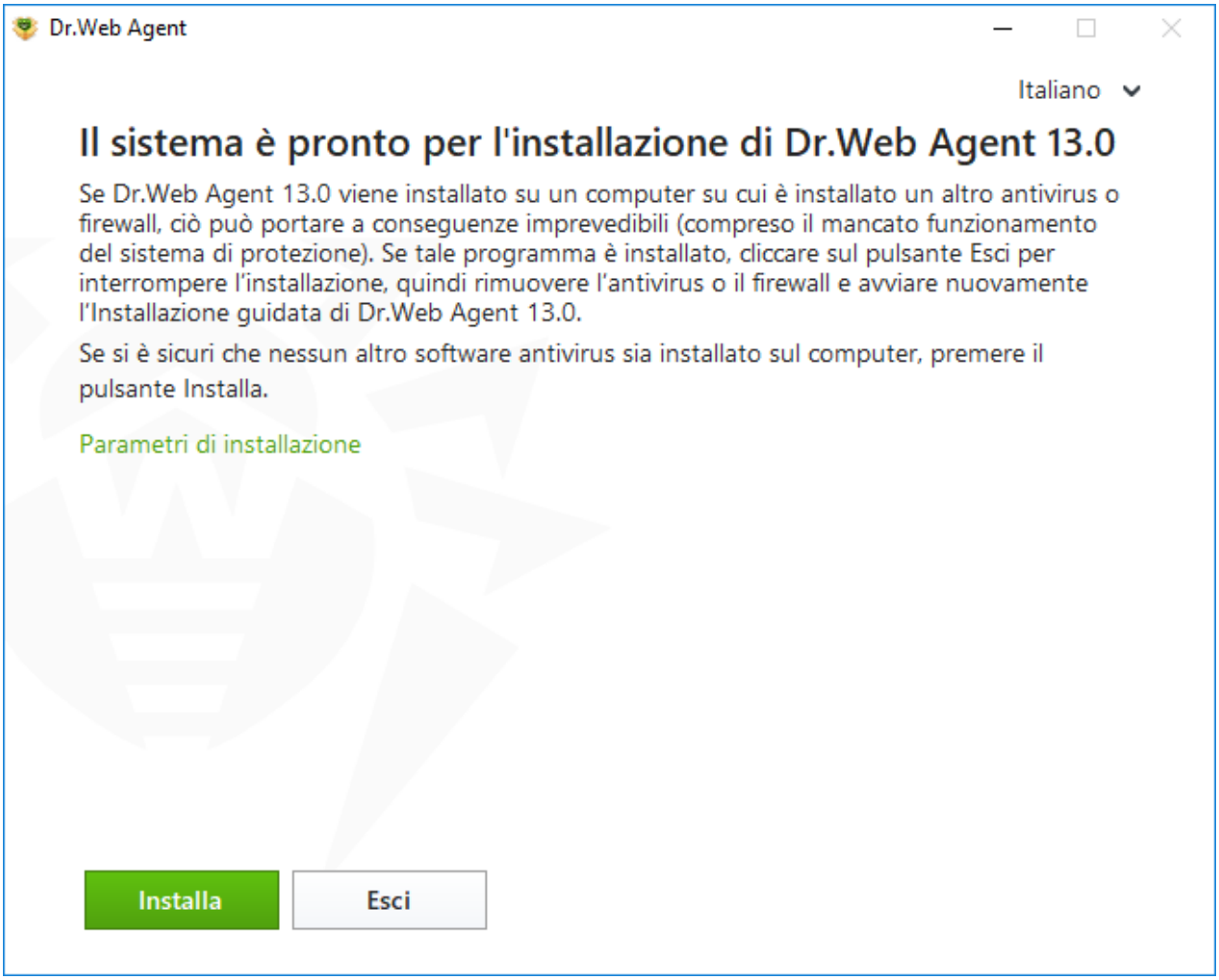

Immagine 8. Il software è pronto per l'installazione

Per selezionare i componenti da installare, indicare il percorso di installazione e alcuni parametri di installazione aggiuntivi, cliccare sul link **Parametri di installazione**. Questa opzione è destinata agli utenti esperti.

6. Se al passaggio precedente è stato premuto il pulsante **Installa**, andare al passaggio 9. Altrimenti, si apre la finestra **Parametri di installazione**.

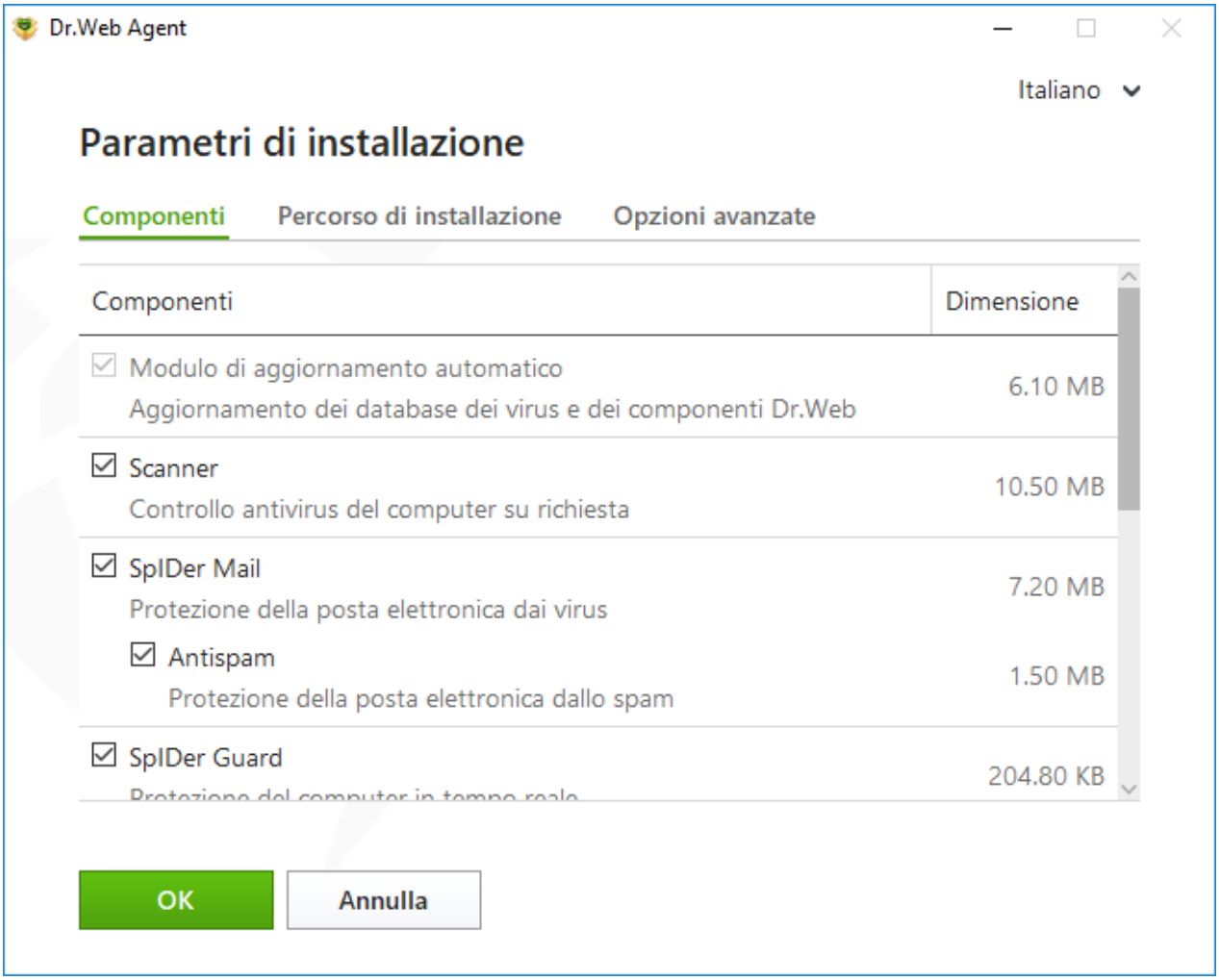

Immagine 9. Parametri di installazione

Nella scheda **Componenti** è possibile selezionare i componenti Dr.Web da installare.

Spuntare i flag di fronte ai componenti che si vogliono installare sul computer. Di default sono selezionati tutti i componenti ad eccezione di Firewall Dr.Web.

7. Nella scheda **Percorso di installazione** è possibile indicare la cartella in cui verrà installato **Agent Dr.Web per Windows**. Di default è la cartella DrWeb situata nella cartella `Program Files` sul disco di sistema. Per modificare il percorso di installazione, premere il pulsante **Sfoglia** e indicare il percorso desiderato.
8. Nella scheda **Opzioni avanzate** è possibile indicare impostazioni aggiuntive per l'installazione del programma Dr.Web.

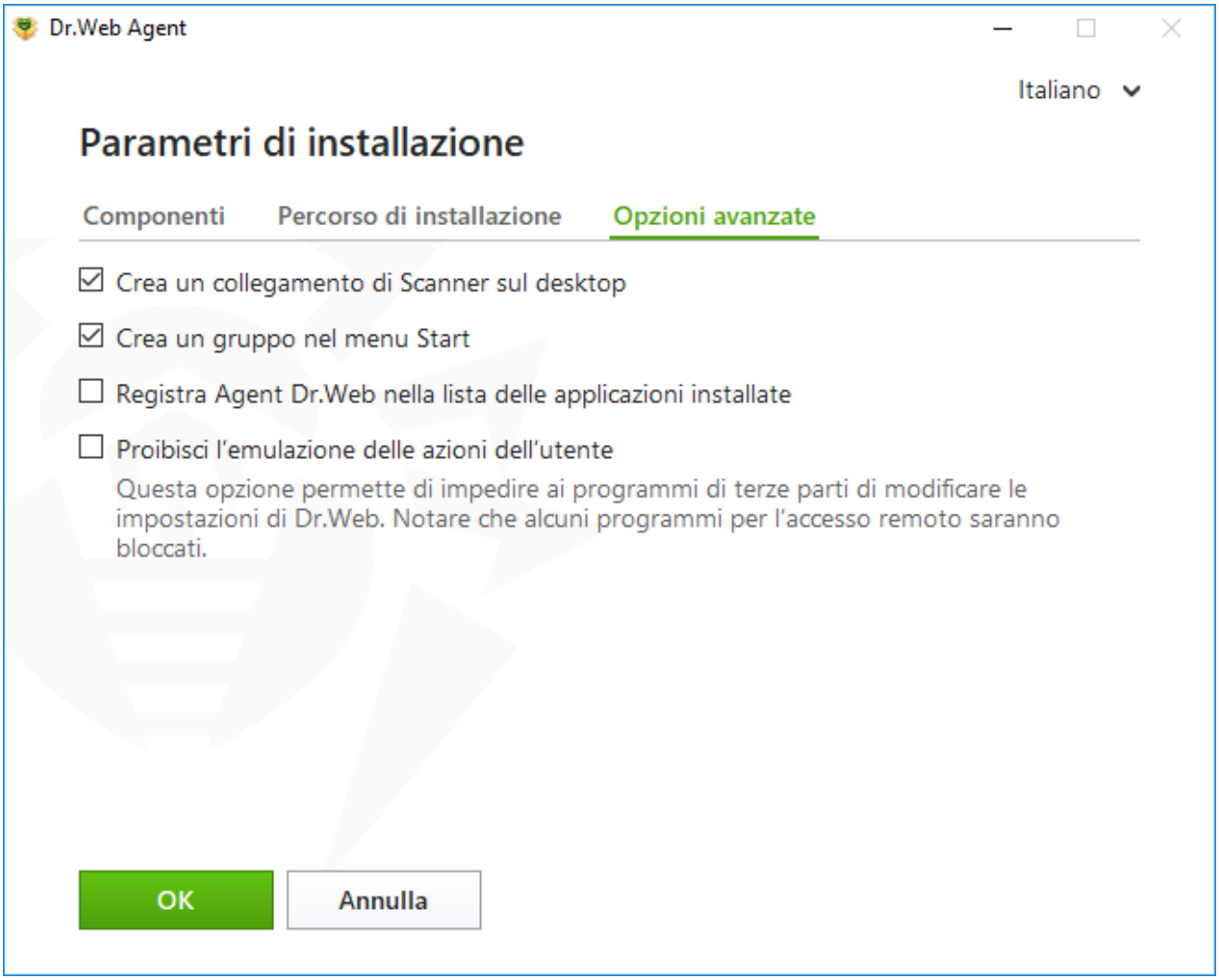

Immagine 10. Opzioni avanzate dei parametri di installazione

Se necessario, attivare il flag **Registra l'Agent Dr.Web nella lista dei programmi installati**. Questa opzione consente di rimuovere e modificare i componenti del programma Dr.Web tramite il Pannello di controllo di Windows.

L'opzione **Proibisci l'emulazione delle azioni dell'utente** consente di prevenire modifiche alle impostazioni Dr.Web, eseguite da software di terze parti. Tra le altre cose, sarà proibita l'esecuzione di script che emulano il funzionamento della tastiera e del mouse nelle finestre Dr.Web (per esempio script per la modifica delle impostazioni Dr.Web e altre operazioni finalizzate a modificare il funzionamento di Dr.Web).

Per salvare le modifiche apportate, premere **OK**, quindi premere **Installa**

9. Inizierà l'installazione di Dr.Web. Non è richiesto alcun intervento da parte dell'utente.
10. Dopo il completamento dell'installazione la procedura guidata avviserà della necessità di riavviare il computer. Premere il pulsante **Riavvia adesso**.

Installazione in modalità riga di comando

Per avviare l'installazione di Dr.Web in modalità riga di comando, andare alla cartella in cui si trova il pacchetto, dopo di che inserire il nome del file eseguibile di installazione (`drweb_ess_windows_<nome postazione>.exe`) con i parametri richiesti.

La lista completa dei parametri della riga di comando per i pacchetti di installazione è riportata in Allegato A.

Errore del servizio BFE durante l'installazione del programma Dr.Web

Per il funzionamento di alcuni componenti di Dr.Web è necessario che sia in esecuzione il servizio modulo di filtraggio di base (BFE). Se questo servizio è mancante o danneggiato, l'installazione di Dr.Web sarà impossibile. Un servizio BFE danneggiato o mancante può indicare la presenza di minacce per la sicurezza del computer.

Se il tentativo di installazione di Dr.Web è terminato con l'errore del servizio BFE, eseguire le seguenti azioni:

1. Eseguire una scansione del sistema della postazione tramite l'utility di cura CureNet! dall'azienda Doctor Web. È possibile richiedere una versione di prova dell'utility (diagnostica senza funzione di cura) sull'indirizzo: https://download.drweb.com/curenet/.

   Per informazioni sulle condizioni di uso e sul costo della versione completa dell'utility, consultare l'indirizzo https://estore.drweb.com/utilities/.
2. Ripristinare il servizio BFE. Per i sistemi operativi Windows 7 e versioni successive è possibile utilizzare l'utility per la risoluzione dei problemi nel funzionamento del firewall dall'azienda Microsoft. Sui sistemi operativi Windows Server avviare o riavviare manualmente il servizio BFE. Se non è possibile avviare il servizio BFE, o il servizio è assente nella lista, contattare il servizio di supporto tecnico dell'azienda Microsoft.
3. Avviare l'Installazione guidata di Dr.Web ed eseguire l'installazione secondo la procedura standard sopra riportata.

Se il problema persiste, contattare il servizio di supporto tecnico dell'azienda Doctor Web.

3.3. Modifica dei componenti del programma

> La modifica dei componenti del programma è possibile se è stata autorizzata dall'amministratore della rete antivirus.

La modifica dei componenti del programma viene effettuata tramite Rimozione/modifica dei componenti guidata. È possibile aprire Rimozione/modifica dei componenti guidata in due modi:

- se è disponibile il file di installazione, avviarlo;

- dal Pannello di controllo di Windows:
  1. Andare alla sezione del Pannello di controllo di Windows dedicata all'installazione e alla rimozione dei programmi.
  2. Nella lista dei programmi installati selezionare la riga **Dr.Web Agent**.
  3. Premere il pulsante **Modifica**.

Per rimuovere o aggiungere componenti

1. Nella finestra di Rimozione/modifica dei componenti guidata premere **Modifica componenti**:

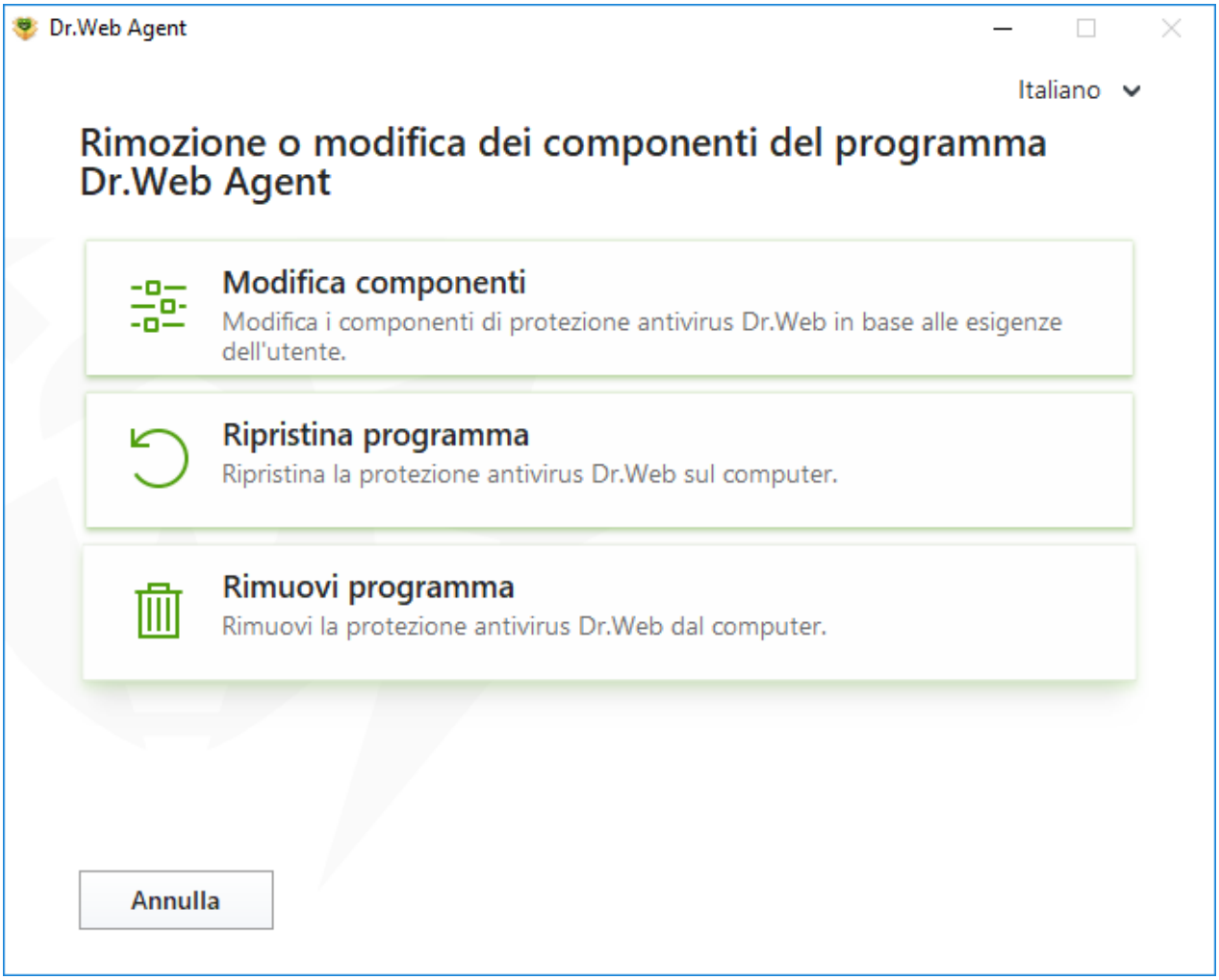

Immagine 11. Procedura guidata di rimozione/modifica dei componenti

2. Nella finestra che si è aperta spuntare i flag di fronte ai componenti che si vogliono aggiungere, o togliere i flag di fronte ai componenti da rimuovere.
3. Premere **Applica**.

Nella finestra di Rimozione/modifica dei componenti guidata sono inoltre disponibili le seguenti opzioni:

- **Ripristina programma**, se è necessario ripristinare la protezione antivirus sul computer. Questa funzione viene utilizzata quando alcuni componenti del programma Dr.Web sono stati danneggiati.
- **Rimuovi programma**, per rimuovere tutti i componenti installati.

3.4. Rimozione e reinstallazione del programma

Per la rimozione locale di Dr.Web questa opzione deve essere consentita dall'amministratore sul server di protezione centralizzata.

Dopo la rimozione di Dr.Web il computer non sarà protetto da virus e altri programmi malevoli.

Rimozione di Dr.Web tramite il Pannello di controllo di Windows

Questo metodo di rimozione è disponibile solo se tramite l'Installazione guidata è stato spuntato il flag **Registra l'Agent Dr.Web nella lista dei programmi installati**.

Se Dr.Web è stato installato in background, la rimozione di Dr.Web tramite i mezzi standard sarà disponibile solo se nell'installazione è stata utilizzata l'opzione `-regagent`.

Se è disponibile il file di installazione, si possono saltare i passaggi 1–3. Avviare il file di installazione e andare al passaggio 4.

Per rimuovere Agent Dr.Web per Windows avviare il componente di rimozione di programmi del sistema operativo Windows.

1. Nella lista che si è aperta selezionare la riga con il nome del programma.
2. Premere il pulsante **Rimuovi**.
3. Nella finestra **Parametri da conservare** spuntare i flag di fronte agli elementi da mantenere dopo la rimozione del programma. Gli oggetti e le impostazioni salvati possono essere utilizzati dal programma in caso di un'altra installazione. Di default sono selezionate tutte le opzioni — **Quarantena**, **Impostazioni Dr.Web Agent** e **Copie di file protette**. Premere il pulsante **Avanti**.
4. Nella finestra successiva per confermare la rimozione di Dr.Web, premere il pulsante **Rimuovi**.
5. Le modifiche diventeranno effettive dopo il riavvio del computer. È possibile differire il processo di riavvio, premendo il pulsante **Riavvia più tardi**. Premere il pulsante **Riavvia adesso** per completare immediatamente la procedura di rimozione dei componenti o modifica della lista dei componenti Dr.Web.

Rimozione in modalità riga di comando

Per rimuovere Dr.Web in modalità riga di comando, inserire il nome del file eseguibile (`win-es-agent-setup.exe`) con i parametri richiesti.

> ⚠ Il file `win-es-agent-setup.exe` è situato nella cartella `C:\ProgramData\Doctor Web\Setup\`.

Per esempio se viene eseguito il seguente comando, Dr.Web verrà rimosso in background e il computer verrà riavviato:

```
win-es-agent-setup.exe /instMode remove /silent yes
```

Reinstallazione di Dr.Web

1. Ottenere dall'amministratore della rete antivirus il pacchetto di installazione attuale.
2. Rimuovere il prodotto come descritto sopra.
3. Riavviare il computer.
4. Di nuovo installare il programma utilizzando il pacchetto di installazione ottenuto. Durante la fase di installazione indicare il percorso del file della chiave.
5. Riavviare il computer.

4. Menu del programma

Dopo l'installazione del programma Dr.Web, all'area di notifica di Windows viene aggiunta l'icona che rispecchia lo stato del programma. Per aprire il menu Dr.Web, fare clic sull'icona . Se il programma non è in esecuzione, nel menu **Start** espandere il gruppo **Dr.Web** e selezionare la voce **Centro sicurezza**.

L'icona Dr.Web non viene visualizzata nell'area di notifica se l'amministratore della rete antivirus ha impostato tale opzione sul server di protezione centralizzata.

Nel menu Dr.Web è possibile vedere lo stato della protezione, e inoltre ottenere l'accesso agli strumenti di gestione e alle impostazioni principali del programma.

Non è possibile modificare le impostazioni e disattivare qualche componente se l'amministratore del server di protezione centralizzata a cui si connette Dr.Web non ha autorizzato tali azioni.

Per accedere ai parametri dei componenti, è necessario immettere la password, se nelle impostazioni è stata attivata l'opzione **Proteggi da password le impostazioni di Dr.Web**.

Se si è dimenticata la password delle impostazioni del prodotto, rivolgersi all'amministratore della rete antivirus.

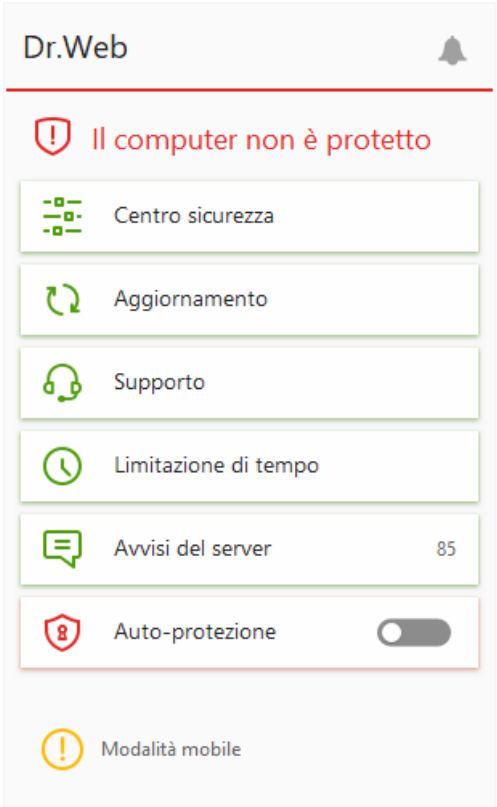

Immagine 12. Menu del programma

Voci del menu del programma

Stato di protezione del computer. Se tutti i componenti del programma sono attivi, viene visualizzato lo stato **Il computer è protetto**. Se uno o più componenti di protezione sono disattivati, lo stato cambia in **Il computer non è protetto**.

Centro sicurezza. Apre una finestra con l'accesso alle impostazioni principali, ai parametri dei componenti di protezione, compreso il componente Office control, e alle eccezioni.

Aggiornamento (compare solo quando Dr.Web è in modalità mobile). Informazioni sullo stato di aggiornamento dei database dei virus e sull'tempo dell'ultimo aggiornamento. Avvia l'aggiornamento dei componenti del programma e dei database dei virus.

Supporto. Apre la finestra del supporto.

Limitazione di tempo (compare se è attivata l'opzione del componente Office control, che limita il tempo di utilizzo del computer e di internet). Brevi informazioni sulle limitazioni del tempo di utilizzo del computer e di internet, nonché sulla durata della pausa nel caso di limitazione di intervalli di tempo.

Avvisi del server (compare quando ci sono avvisi e se l'opzione corrispondente è attivata sul server). Apre la finestra di visualizzazione degli avvisi del server.

Auto-protezione (compare se Auto-protezione viene disattivata). Utilizzando un interruttore, è possibile attivare nuovamente l'Auto-protezione.

Stato della connessione al server. Lo stato viene visualizzato solo se la postazione non è attualmente connessa al server. Nel caso di connessione riuscita, lo stato nel menu non viene visualizzato.

Vengono visualizzati, in totale, cinque stati:

Segno	Stato
	• La postazione è in attesa di conferma sul server • Modalità mobile • Connessione al server di protezione centralizzata
	• Nessuna connessione con il server • Errore di connessione

Pulsante **Avvisi attuali**  . Apre la finestra Avvisi attuali.

Possibili stati del programma

L'icona Dr.Web rispecchia lo stato attuale del programma:

Icona Dr.Web	Descrizione
	Tutti i componenti necessari per la protezione del computer sono in esecuzione e funzionano correttamente, è stabilita una connessione al server di protezione centralizzata.
	Auto-protezione o almeno uno dei componenti sono disattivati o i database dei virus sono obsoleti, il che indebolisce la protezione dell'antivirus e del computer; o il programma è in attesa di connessione al server, ma la connessione non è ancora stata stabilita. Probabilmente, il server ha rifiutato la connessione della postazione o ha negato l'accesso alle sue risorse. Attivare Auto-protezione o il componente disattivato, attendere che la connessione al server venga stabilita o rivolgersi all'amministratore della rete antivirus se non è possibile stabilire la connessione.
	Il programma è in attesa di avvio dei componenti dopo la partenza del sistema operativo, attendere l'avvio dei componenti del programma; o un errore si è verificato nel corso dell'avvio di uno dei componenti chiave di Dr.Web, il computer è a rischio di infezione. Se l'icona non cambia, rivolgersi all'amministratore della rete antivirus.
	Al momento Scanner Dr.Web esegue una scansione.

5. Centro sicurezza

La finestra **Centro sicurezza** fornisce accesso a tutti i componenti, gli strumenti, le statistiche e le impostazioni del programma.

Per andare alla finestra Centro sicurezza

1. Aprire il menu Dr.Web .
2. Selezionare la voce **Centro sicurezza**.

Per andare alla finestra Centro sicurezza dal menu Start

1. Nel menu **Start** espandere il gruppo **Dr.Web**.
2. Premere **Centro sicurezza**.

Immagine 13. Finestra Centro sicurezza

Gruppi di impostazioni

La finestra principale fornisce accesso ai seguenti gruppi di impostazioni:

- La scheda principale di **Centro sicurezza** — accesso a tutti i componenti di protezione e gli strumenti:
  - File e rete;
  - Protezione preventiva;

- Dispositivi;
- Office control;
- Gestione quarantena;
- Eccezioni;

- Scheda Statistiche — statistiche sui principali eventi di funzionamento del programma;
- Pulsante nella parte superiore della finestra — accesso alle impostazioni del programma;
- Pulsante nella parte superiore della finestra — accesso alla finestra **Supporto** in cui è possibile assemblare un report per il servizio di supporto tecnico e visualizzare informazioni sulla versione del prodotto e sulla data dell'ultimo aggiornamento dei componenti e dei database dei virus;
- Pulsante nella parte superiore della finestra — accesso alla finestra **Avvisi attuali** in cui è possibile visualizzare gli avvisi importanti di eventi di funzionamento del programma.

Modalità amministratore

Per l'accesso a tutti i gruppi di impostazioni, è necessario cambiare Dr.Web a modalità amministratore facendo clic sul lucchetto nella parte inferiore della finestra. Quando Dr.Web funziona in modalità amministratore, il lucchetto è "aperto".

In qualsiasi modalità c'è pieno accesso allo strumento **Gestione quarantena**. Inoltre, senza cambiare Dr.Web a modalità amministratore, è possibile attivare qualsiasi componente di protezione e avviare Scanner. La disattivazione di componenti di protezione, il passaggio ai parametri dei componenti e alle impostazioni del programma sono possibili solo in modalità amministratore.

> Non è possibile modificare le impostazioni e disattivare qualche componente se l'amministratore del server di protezione centralizzata a cui si connette Dr.Web non ha autorizzato tali azioni.

Stati di protezione

Nella parte superiore della finestra viene visualizzato lo stato di sicurezza del sistema.

- **Il computer è protetto** — tutti i componenti sono attivati e funzionanti, l'Auto-protezione è attivata, la licenza è valida. Viene visualizzato in verde.
- **Il computer non è protetto** — viene visualizzato se uno dei componenti di protezione è disattivato. Viene visualizzato in rosso. Anche la piastrella del componente disattivato è evidenziata in rosso.

6. Avvisi attuali

Questa finestra contiene avvisi importanti sugli eventi di funzionamento del programma. Gli avvisi in questa sezione duplicano alcuni degli avvisi sullo schermo.

Per andare agli avvisi attuali dal Menu del programma

1. Aprire il menu Dr.Web .
2. Premere il pulsante . Sopra l'icona viene visualizzato il numero di avvisi salvati.
3. Si aprirà la finestra con gli avvisi sugli eventi.

Per andare agli avvisi attuali dal Centro sicurezza

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella parte superiore della finestra del programma premere .
3. Si aprirà la finestra con gli avvisi sugli eventi.

Immagine 14. Finestra degli avvisi attuali

Periodo di conservazione degli avvisi

Il periodo di conservazione degli avvisi è di due settimane. Quando problemi vengono risolti, vengono cancellati anche i relativi avvisi.

Tipi di avvisi

Avvisi critici	
Minacce	• È stata rilevata una minaccia. • È necessario riavviare il computer per neutralizzare le minacce. • I database dei virus sono obsoleti.
Connessione al server	• La connessione al server è vietata. • Errore di connessione al server.
Divieto di accesso a oggetti e dispositivi	• Il dispositivo è bloccato in conformità alle impostazioni.
Avvisi importanti	
Aggiornamento	• È necessario riavviare il computer per rendere effettivi gli aggiornamenti.
Avvisi di informazione insignificanti	
Nuova versione	• È disponibile una nuova versione del prodotto.
Nuovo messaggio	• L'amministratore ha inviato un nuovo messaggio.

Impostazioni di visualizzazione

Le impostazioni di visualizzazione degli avvisi attuali duplicano le impostazioni degli avvisi a comparsa. Se si desidera modificare le impostazioni di visualizzazione in modo che determinati avvisi non vengano visualizzati negli avvisi attuali, nella finestra **Impostazioni degli avvisi** è necessario togliere il flag nella colonna **Schermo** di fronte alla voce richiesta (vedi sezione Impostazioni degli avvisi).

7. Impostazioni del programma

Per passare alla modifica delle impostazioni del programma

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
3. Nella parte superiore della finestra del programma premere .
4. Si aprirà la finestra con le impostazioni del programma.

> La modifica delle impostazioni è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui si connette Dr.Web.
>
> Se nelle impostazioni generali è stato selezionato il flag **Proteggi da password le impostazioni di Dr.Web**, viene richiesta la password per l'accesso alle impostazioni principali Dr.Web.

In questa sezione:

- Generali — protezione con password delle impostazioni, selezione della lingua del programma, selezione del colore del tema dell'interfaccia.
- Avvisi — configurazione della visualizzazione degli avvisi sullo schermo.
- Auto-protezione — configurazione dei parametri di sicurezza aggiuntivi.
- Parametri di scansione dei file — configurazione dei parametri di funzionamento di Scanner.
- Server — configurazione dei parametri di connessione al server di protezione centralizzata.
- Avvisi del server — configurazione dei parametri di visualizzazione di Avvisi del server.

7.1. Impostazioni generali

Alle impostazioni generali appartengono le seguenti impostazioni:

- protezione con password delle impostazioni del programma;
- selezione del colore del tema dell'interfaccia;
- selezione della lingua del programma;
- impostazioni di log di funzionamento;
- impostazioni di quarantena;
- impostazioni di rimozione automatica dei record delle statistiche.

Per aprire le impostazioni generali

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.

2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
3. Nella parte superiore della finestra del programma premere .
4. Si apre la finestra con le impostazioni principali del programma. Nella parte sinistra della finestra selezionare **Generali**.

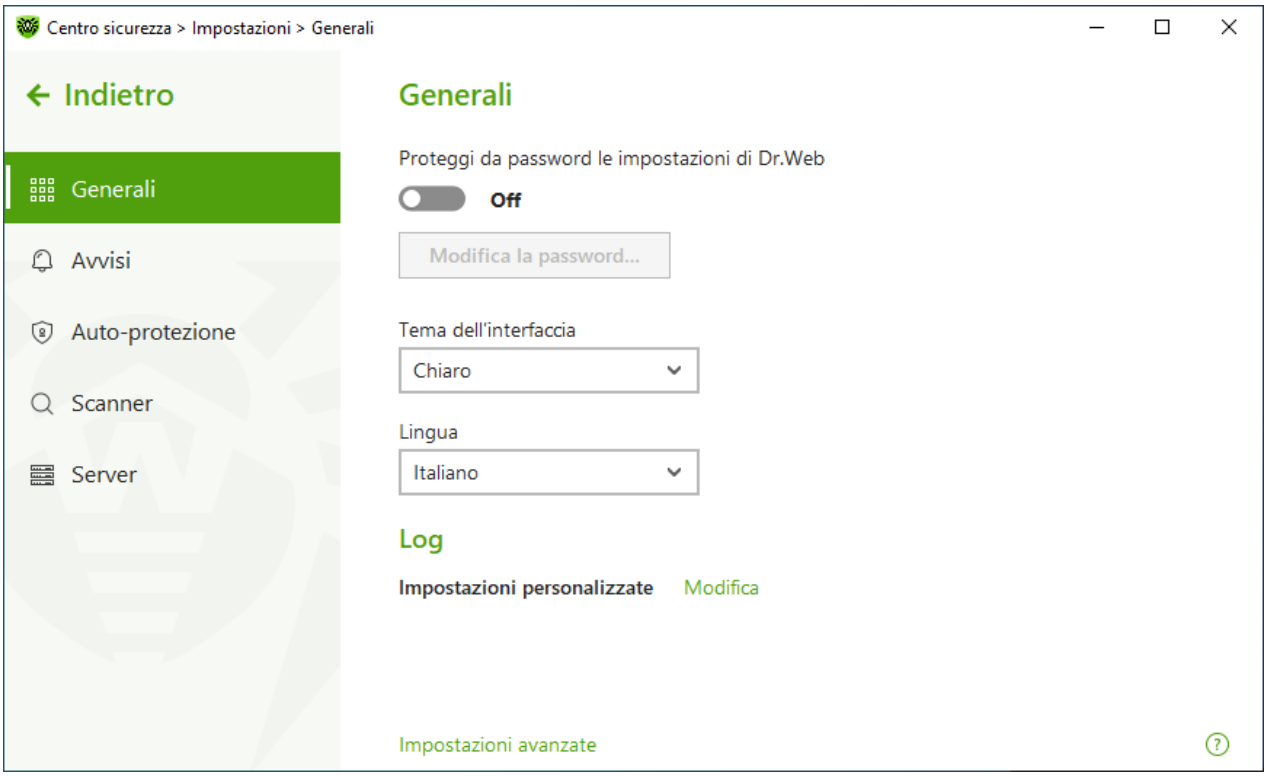

Immagine 15. Impostazioni generali

7.1.1. Protezione con password delle impostazioni del programma

È possibile limitare l'accesso alle impostazioni Dr.Web sul computer tramite una password. La password verrà richiesta ogni volta che si accede alle impostazioni Dr.Web.

Per impostare la password

1. Nella finestra di modifica delle impostazioni generali attivare l'opzione **Proteggi da password le impostazioni di Dr.Web** utilizzando l'interruttore corrispondente .

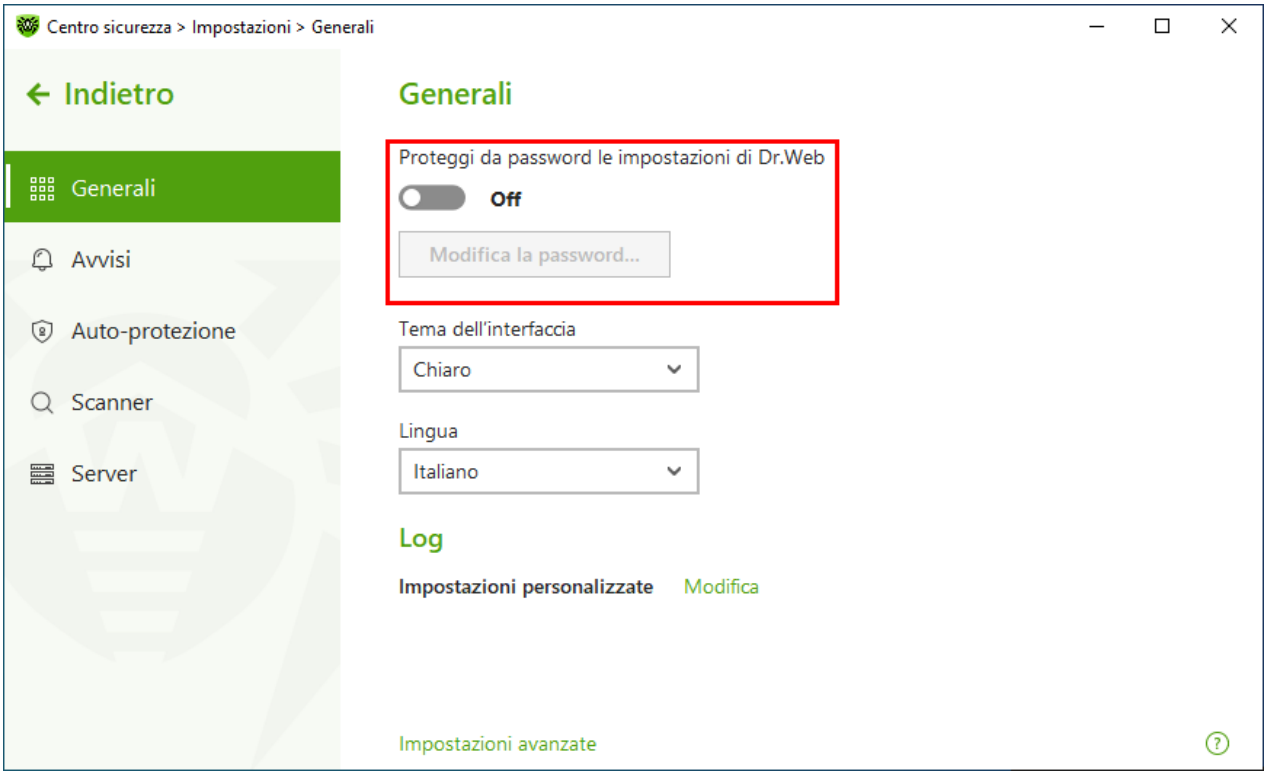

Immagine 16. Protezione con password delle impostazioni

2. Nella finestra che si è aperta impostare una password e confermarla.
3. Premere il pulsante **OK**.

> Se si è dimenticata la password delle impostazioni del prodotto, rivolgersi all'amministratore della rete antivirus

7.1.2. Selezione del colore del tema dell'interfaccia

Se necessario, è possibile cambiare il colore del tema dell'interfaccia del programma. Per fare ciò, nella lista a cascata **Tema dell'interfaccia** selezionare una delle opzioni:

- **Chiaro** per utilizzare il tema chiaro del programma.
- **Scuro** per utilizzare il tema scuro del programma.
- **Di sistema** per utilizzare il colore dell'interfaccia corrispondente al tema selezionato nel sistema operativo. Questa opzione è selezionata di default.

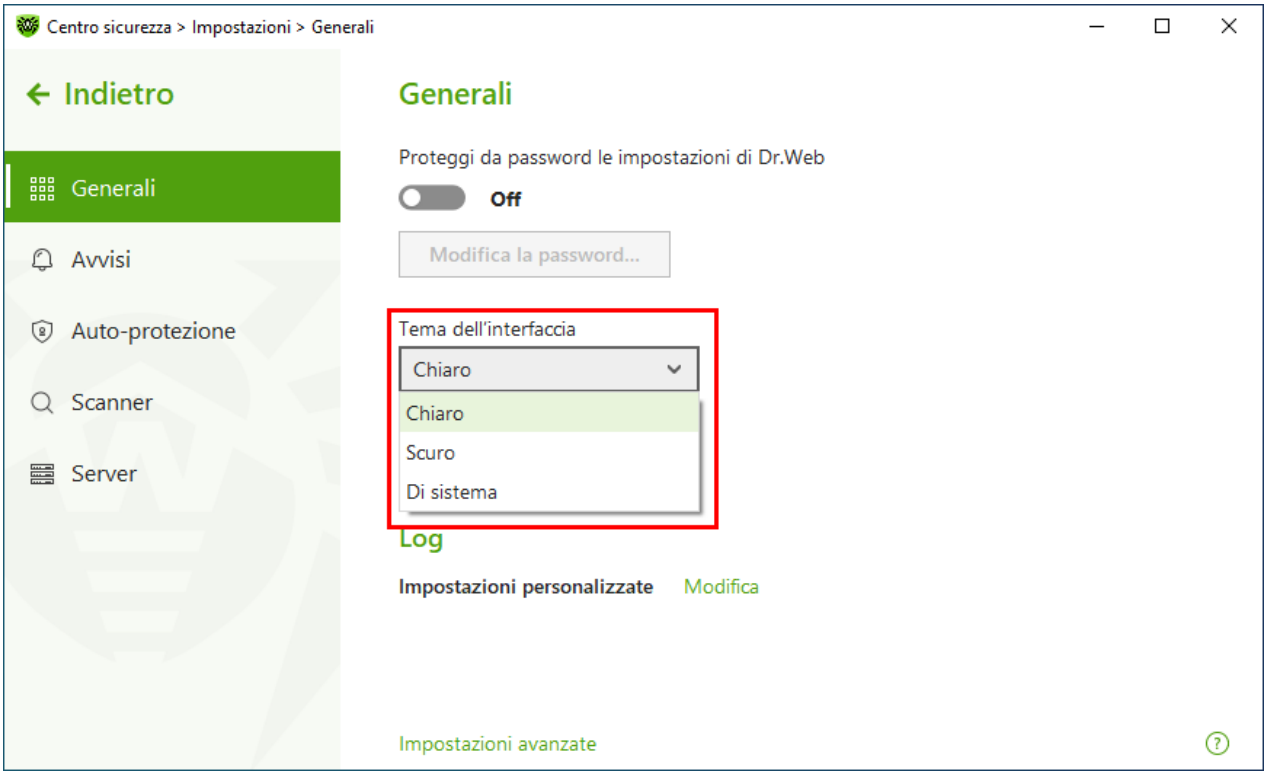

Immagine 17. Selezione del colore del tema dell'interfaccia

Il tema scuro è disponibile solo su computer con il sistema operativo Windows 10 (a partire dalla versione 1909), Windows 11 e Windows Server 2019 (a partire dalla versione 1809) e versioni successive. Le impostazioni di selezione del colore del tema dell'interfaccia sono nascoste per le versioni precedenti del sistema operativo.

Per la corretta visualizzazione del tema scuro dell'interfaccia è necessario che sia installato l'aggiornamento KB5011503 o successivo.

7.1.3. Selezione della lingua del programma

Se necessario, è possibile cambiare la lingua dell'interfaccia del programma. La lista delle lingue viene automaticamente completata e contiene tutte le localizzazioni dell'interfaccia grafica Dr.Web attualmente disponibili. Per fare questo, nella lista a cascata **Lingua** selezionare la lingua desiderata.

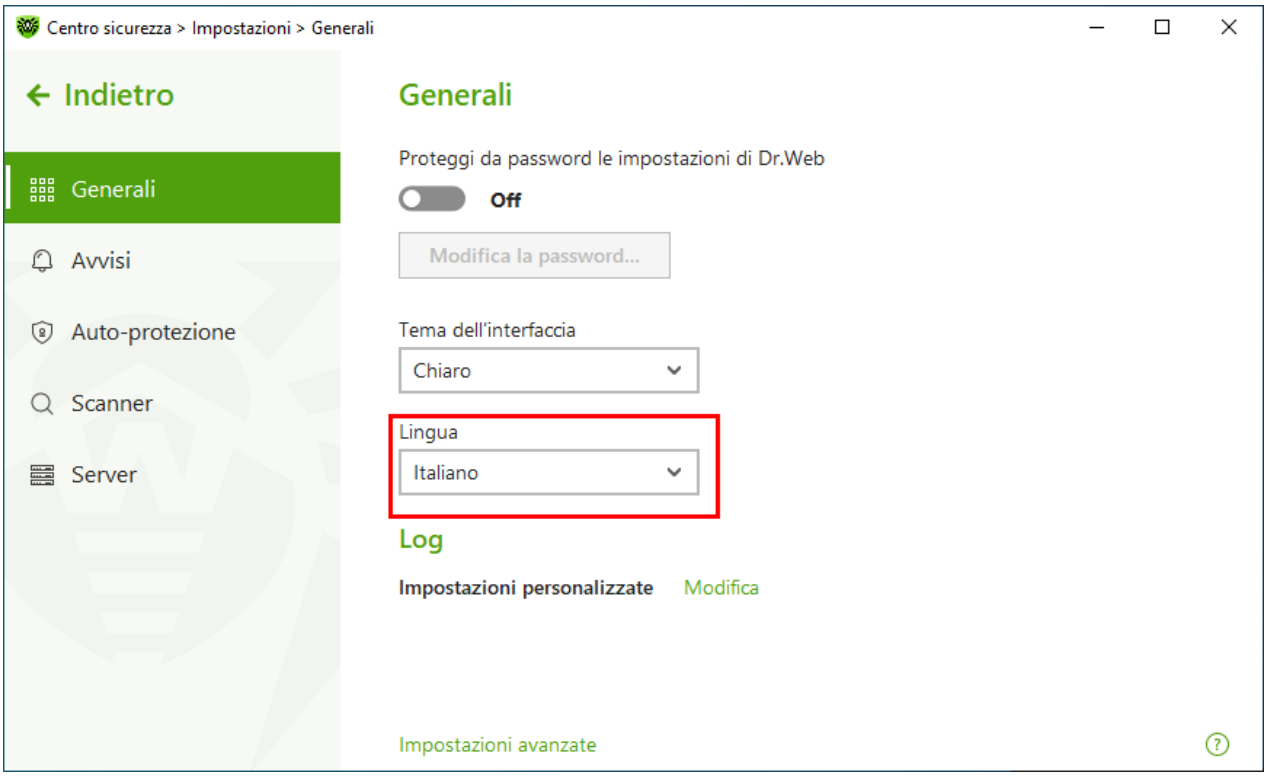

Immagine 18. Selezione della lingua del programma

7.1.4. Log di funzionamento Dr.Web

È possibile attivare il log dettagliato sul funzionamento di uno o più componenti o servizi Dr.Web.

Per modificare le impostazioni di log

1. Nella sezione delle impostazioni **Log** premere il pulsante **Modifica**.

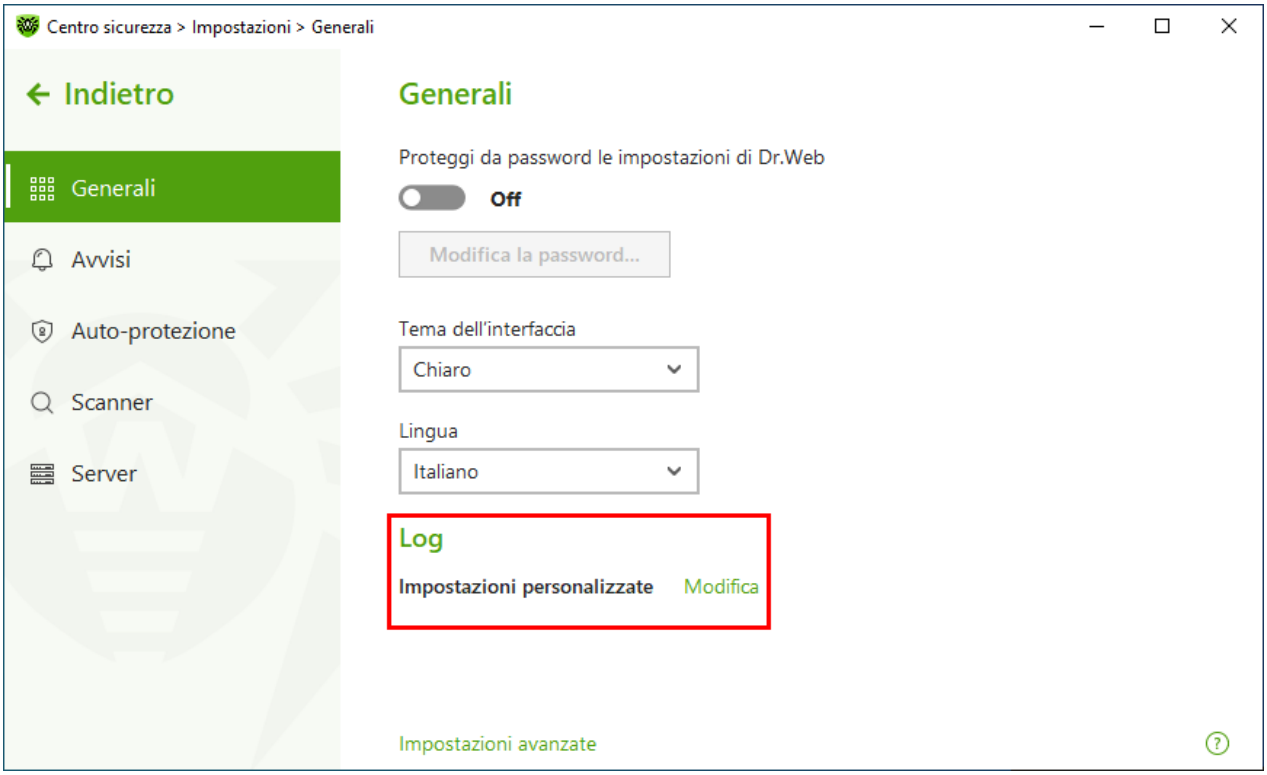

Immagine 19. Impostazioni generali. Log

Si apre la finestra delle impostazioni di log dettagliato:

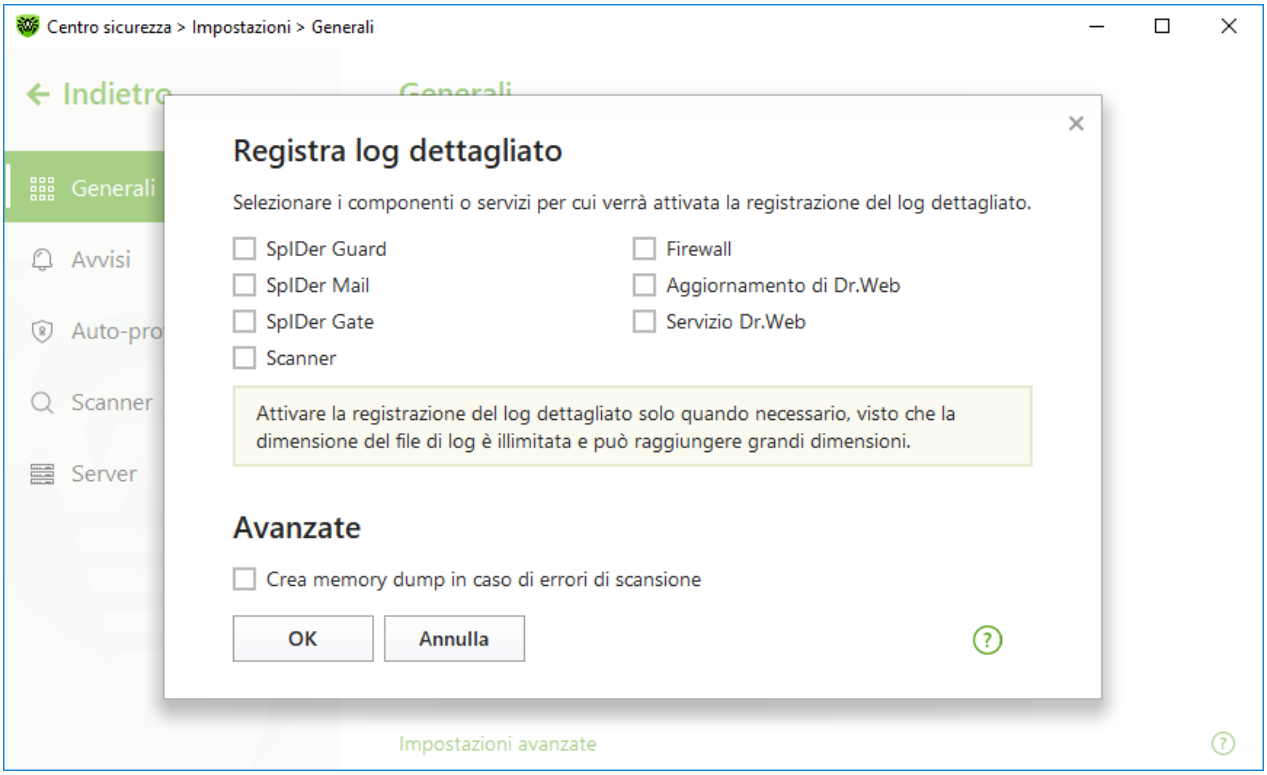

Immagine 20. Impostazioni di log di funzionamento

2. Selezionare i componenti, moduli o servizi per i quali verrà attivato il log dettagliato. Di default per tutti i componenti Dr.Web il log è in modalità standard in cui vengono registrate le seguenti informazioni:

Componente	Informazione
SpIDer Agent	Esecuzione degli aggiornamenti, avvio e arresto di SpIDer Agent, eventi di virus, connessione al server di protezione centralizzata, stato di funzionamento dei componenti Dr.Web, gestione delle impostazioni (importazione, esportazione), avvisi di errori, avvisi di riavvio del sistema. Si consiglia di utilizzare questa modalità per ottenere informazioni dettagliate sulle fonti di errori nel funzionamento del programma.
SpIDer Guard	Aggiornamenti, avvio e arresto di SpIDer Guard, eventi di virus, dati sui file controllati, sui nomi dei packer e sui contenuti degli oggetti composti (archivi compressi, file di email o container di file). Si consiglia di utilizzare questa modalità per determinare gli oggetti che il monitor del file system SpIDer Guard controlla più spesso. Se necessario, aggiungere tali oggetti alla lista delle eccezioni, il che può ridurre il carico di lavoro del computer.
SpIDer Mail	Aggiornamenti, avvio e arresto dell'antivirus di posta SpIDer Mail, eventi di virus, parametri di intercettazione delle connessioni, nonché dati sui file controllati, sui nomi dei packer e sui contenuti degli archivi compressi. Si consiglia di utilizzare questa modalità per controllare le impostazioni di intercettazione delle connessioni con i server di posta.
SpIDer Gate	Aggiornamento, avvio e arresto del monitoraggio internet SpIDer Gate, eventi di virus, parametri di intercettazione delle connessioni, nonché dati sui file controllati, i nomi di packer e i contenuti di archivi compressi. Si consiglia di utilizzare questa modalità per ottenere informazioni più dettagliate sugli oggetti controllati e sul funzionamento del monitoraggio internet.
Scanner	Aggiornamento delle versioni dei moduli di scansione e delle informazioni sui database dei virus, avvio e arresto di Scanner, minacce rilevate, nonché dati sui nomi di packer e sui contenuti di archivi compressi controllati.
Firewall	Informazioni sulle richieste che arrivano nel servizio e sulle decisioni su di esse, informazioni sulle connessioni sconosciute con il motivo della richiesta, nonché informazioni sugli errori. Quando viene attivata la modalità di log dettagliato, vengono raccolti i dati sui pacchetti di rete (i log pcap).
Aggiornamento di Dr.Web	Lista dei file Dr.Web aggiornati e il loro status di download, informazioni sul funzionamento degli script ausiliari, data e ora di un aggiornamento, informazioni sul riavvio dei componenti Dr.Web dopo un aggiornamento.
Servizio Dr.Web	Informazioni sui componenti Dr.Web, modifica delle impostazioni dei componenti, attivazione e disattivazione dei componenti, eventi della protezione preventiva, connessione al server di protezione centralizzata.

Creazione dei memory dump

L'impostazione **Crea memory dump in caso di errori di scansione** consente di salvare informazioni utili sul funzionamento di alcuni componenti Dr.Web, il che successivamente darà la possibilità agli specialisti Doctor Web di eseguire un'analisi più completa del problema e suggerire una soluzione. È consigliabile attivare questa impostazione su richiesta del personale di supporto tecnico dell'azienda Doctor Web, o quando si verificano errori di scansione dei file o di neutralizzazione delle minacce. Un memory dump viene salvato come un file con l'estensione `.dmp` nella cartella `%PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\`.

Log dettagliato

Se sono attivati log dettagliati, viene registrata la quantità massima di informazioni sul funzionamento dei componenti Dr.Web. Ciò porterà alla disattivazione dei limiti di dimensione dei file di log e ridurrà le prestazioni di Dr.Web e del sistema operativo. Questa modalità dovrebbe essere utilizzata solo se si verificano problemi nel funzionamento dei componenti o su richiesta dell'amministratore della rete antivirus.

1. Per attivare la modalità di log dettagliato per uno dei componenti di Dr.Web, spuntare il flag corrispondente.
2. Salvare le modifiche premendo il pulsante **OK**.

Non è possibile modificare le impostazioni di log se l'amministratore del server di protezione centralizzata a cui si connette Dr.Web non ha autorizzato l'uso di tali operazioni.

Di default i file di log hanno una dimensione limitata pari a 10 MB (per il componente SpIDer Guard — 100 MB). Se eccede la dimensione massima, il file di log viene troncato fino alla:

- dimensione impostata se le informazioni registrate durante la sessione non eccedono la dimensione consentita;
- dimensione della sessione corrente se le informazioni registrate durante la sessione eccedono la dimensione consentita.

7.1.5. Impostazioni di quarantena

Per non sovraccaricare il disco, è possibile configurare le impostazioni di conservazione degli oggetti in quarantena come il tempo di conservazione degli oggetti e la creazione della cartella di quarantena sul supporto rimovibile.

Per modificare le impostazioni di conservazione delle minacce rilevate

1. Nella finestra di modifica delle impostazioni generali cliccare sul link **Impostazioni avanzate**.

2. Nella sezione delle impostazioni **Quarantena** attivare o disattivare l'opzione richiesta utilizzando l'interruttore .

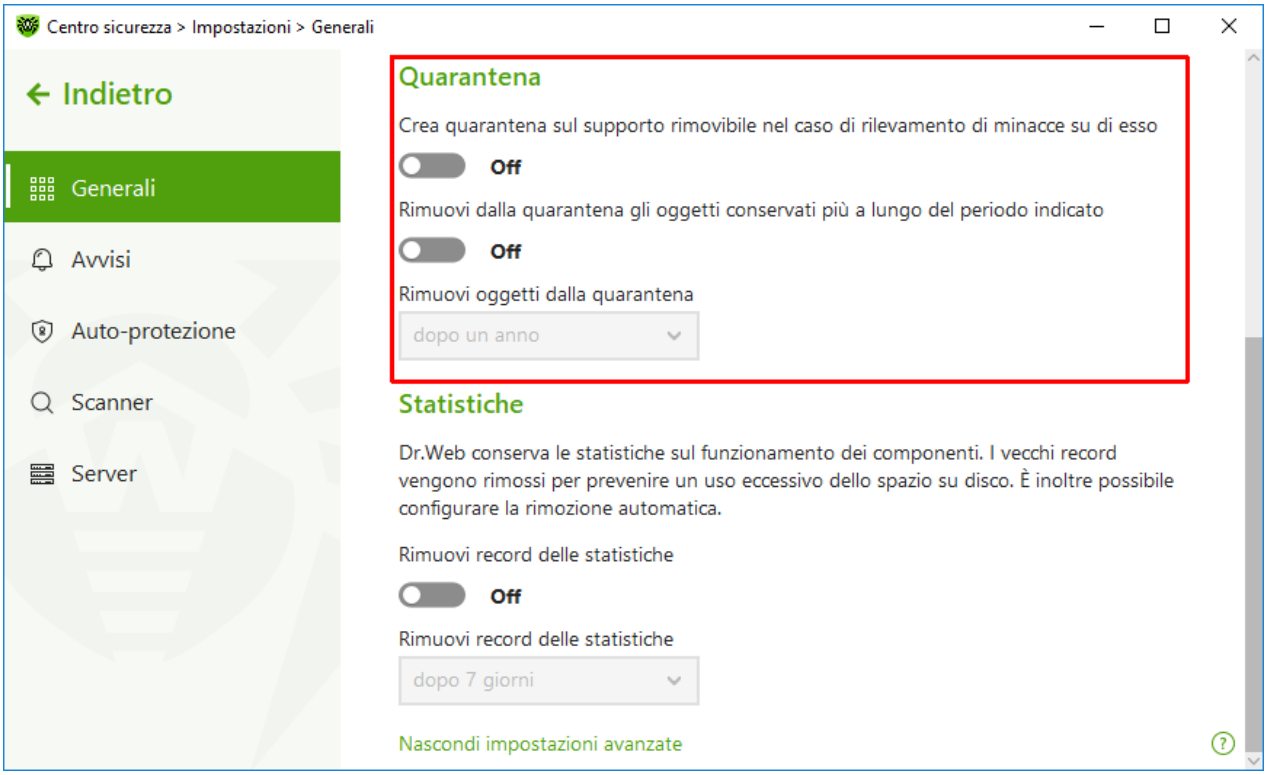

Immagine 21. Impostazioni di quarantena

3. Attivando la rimozione automatica di oggetti dalla quarantena, selezionare il tempo dal menu a cascata. Gli oggetti conservati più a lungo del periodo di tempo indicato verranno rimossi.

Creazione di una quarantena su un supporto rimovibile

L'opzione **Crea quarantena sul supporto rimovibile nel caso di rilevamento di minacce su di esso** al rilevamento di una minaccia su un supporto rimovibile consente di creare una cartella di quarantena sullo stesso supporto e di mettere in questa cartella le minacce senza cifratura preliminare. Su un supporto rimovibile una cartella di quarantena viene creata solo se il supporto è scrivibile. L'utilizzo di cartelle separate e la rinuncia alla cifratura sui supporti rimovibili consentono di prevenire possibili perdite di dati.

Se l'opzione è disattivata, le minacce rilevate sui supporti rimovibili vengono messe in quarantena sul disco locale.

Rimozione automatica di oggetti dalla quarantena

Per evitare un uso eccessivo dello spazio su disco, attivare la rimozione automatica di oggetti dalla quarantena.

7.1.6. Rimozione automatica dei record delle statistiche

Di default, Dr.Web conserva il numero ottimale di record delle statistiche per evitare un uso eccessivo dello spazio su disco. In aggiunta a questo, è possibile attivare la rimozione automatica dei record conservati più a lungo del tempo indicato.

Per attivare o disattivare la rimozione automatica dei record delle statistiche

1. Nella finestra di modifica delle impostazioni generali cliccare sul link **Impostazioni avanzate**.
2. Nella sezione delle impostazioni **Statistiche** attivare o disattivare la rimozione automatica dei record delle statistiche utilizzando l'interruttore .

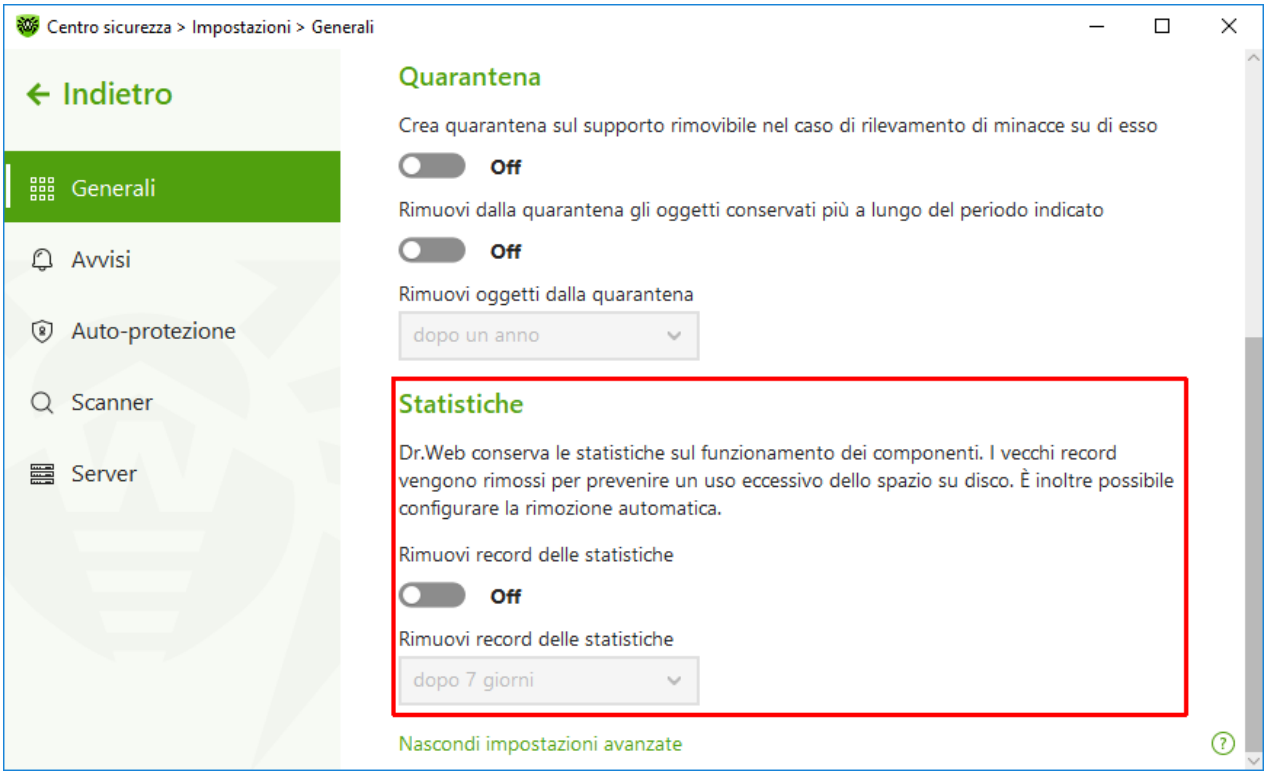

Immagine 22. Impostazioni delle statistiche

3. Attivando la rimozione automatica dei record delle statistiche, selezionare il tempo dal menu a cascata. I record conservati più a lungo del periodo di tempo indicato verranno rimossi.

7.2. Impostazioni degli avvisi

È possibile configurare i parametri di ricezione degli avvisi sugli eventi di funzionamento Dr.Web critici e importanti.

In questa sezione:

- Configurazione dei parametri di avvisi

Se necessario, configurare i parametri di ricezione degli avvisi sugli eventi di funzionamento Dr.Web critici e importanti.

Per aprire le impostazioni di avvisi

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
3. Nella parte superiore della finestra del programma premere .
4. Si apre la finestra con le impostazioni principali del programma. Nella parte sinistra della finestra selezionare **Avvisi**.

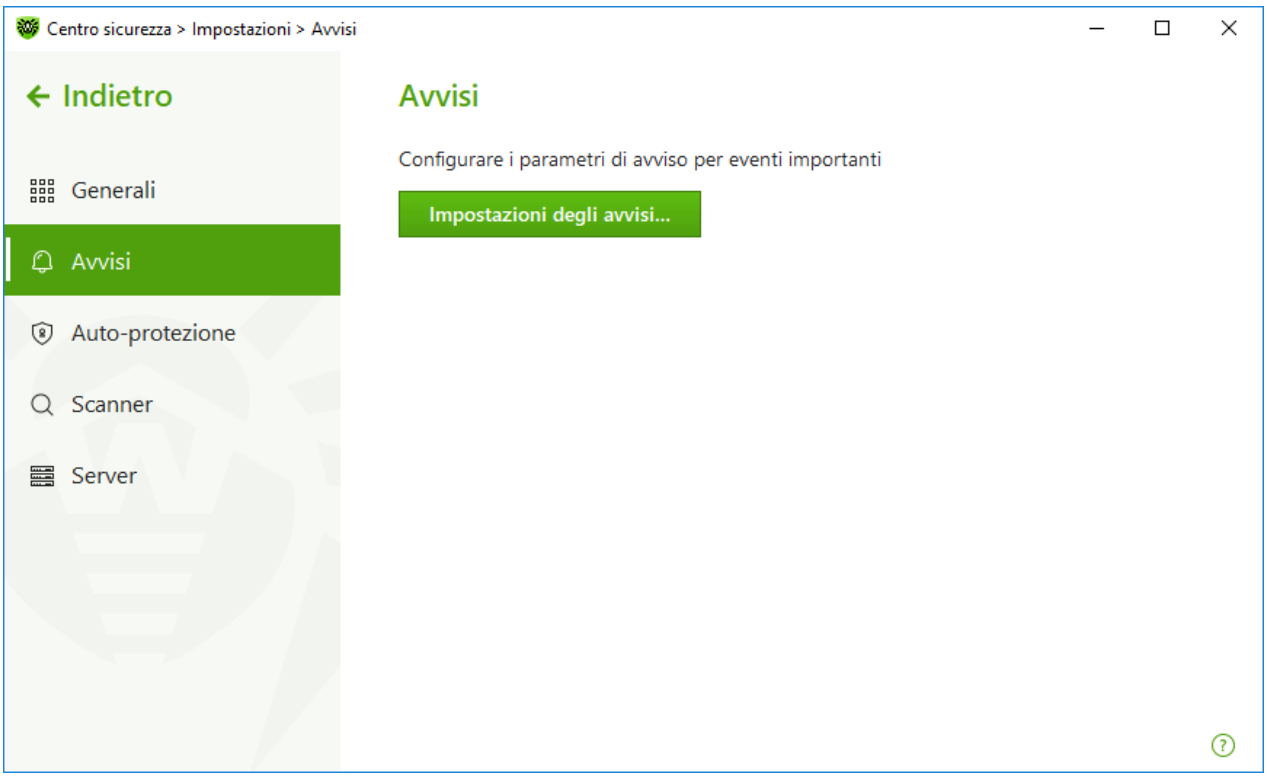

Immagine 23. Impostazioni di avviso

Per configurare i parametri degli avvisi

1. Premere il pulsante **Impostazioni degli avvisi**.
2. Selezionare gli avvisi che si desidera ricevere. Per visualizzare gli avvisi, spuntare i flag di fronte ai tipi di avvisi richiesti.

   Se non si desidera ricevere avvisi su un evento, deselezionare i flag.

Tipo di avviso	Descrizione
È stata rilevata una minaccia	Avvisi sulle minacce rilevate dai componenti SpIDer Guard e SpIDer Gate.

Tipo di avviso	Descrizione
	Di default gli avvisi sono attivati.
Avvisi critici	Avvisi critici sui seguenti eventi: • Sono state rilevate connessioni che aspettano una risposta del Firewall. • Il login e la password sono già utilizzati per la connessione al server di protezione centralizzata. Di default gli avvisi sono attivati.
Avvisi importanti	Avvisi importanti sui seguenti eventi: • Il tempo di utilizzo del computer è scaduto. • I database dei virus sono obsoleti (quando si lavora in Modalità mobile). • Dispositivo bloccato. • È stato impedito un tentativo di modifica della data e dell'ora di sistema. • L'accesso all'oggetto protetto è bloccato dal componente Analisi comportamentale. • L'accesso all'oggetto protetto è bloccato da Protezione dagli exploit. • L'accesso all'oggetto protetto è bloccato da Protezione dai ransom • L'avvio del processo è bloccato dall'amministratore. • L'installazione del pacchetto MSI è bloccata dall'amministratore. • L'avvio dello script è bloccato dall'amministratore. • Al processo è proibito il caricamento dell'oggetto. • Al processo è proibita la creazione del file eseguibile. • Al processo è proibita la modifica del file eseguibile. Di default gli avvisi sono disattivati.
Avvisi secondari	Avvisi secondari sui seguenti eventi: • URL bloccata dal modulo Office control. • URL bloccata da SpIDer Gate. • Il tempo di utilizzo di internet è scaduto. • L'accesso all'oggetto protetto è bloccato dal componente Office control. • L'amministratore della rete antivirus ha avviato il processo di scansione del computer. • Il processo di scansione del computer è stato avviato secondo il calendario. • La scansione del computer è completata. • Aggiornamento riuscito. • Errore di aggiornamento. Di default gli avvisi sono disattivati.

3. Se necessario, impostare i parametri aggiuntivi di visualizzazione degli avvisi sullo schermo:

Flag	Descrizione
Non visualizzare avvisi in modalità a schermo intero	Visualizzazione degli avvisi durante l'utilizzo di applicazioni in modalità a schermo intero (visualizzazione di film, immagini ecc.). Deselezionare questo flag per ricevere avvisi sempre.
Visualizza gli avvisi del Firewall su uno schermo separato in modalità a schermo intero	Visualizzazione degli avvisi da Firewall su un desktop separato durante il funzionamento di applicazioni in modalità a schermo intero (giochi, video). Deselezionare questo flag affinché gli avvisi vengano visualizzati sullo stesso desktop su cui è in esecuzione un'applicazione in modalità a schermo intero.

Gli avvisi circa alcuni eventi non rientrano nei gruppi sopraelencati e vengono sempre visualizzati all'utente:

- installazione degli aggiornamenti critici per cui è necessario riavviare il computer;
- riavvio del computer per completare la neutralizzazione delle minacce;
- riavvio automatico;
- una richiesta per consentire a un processo di modificare un oggetto;
- un messaggio inviato dall'amministratore del server di protezione centralizzata;
- connessione al server riuscita;
- è stata collegata una nuova tastiera.

7.3. Auto-protezione

È possibile configurare i parametri di protezione di Dr.Web stesso da influenze non autorizzate, per esempio da parte dei programmi la cui attività malevola è mirata ai programmi antivirus, nonché da danneggiamenti accidentali.

In questa sezione:

- Attivazione e disattivazione dell'auto-protezione
- Divieto di modifica della data e dell'ora di sistema

Per andare alle impostazioni di Auto-protezione

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
3. Nella parte superiore della finestra del programma premere .
4. Si apre la finestra con le impostazioni principali del programma. Nella parte sinistra della finestra selezionare **Auto-protezione**.

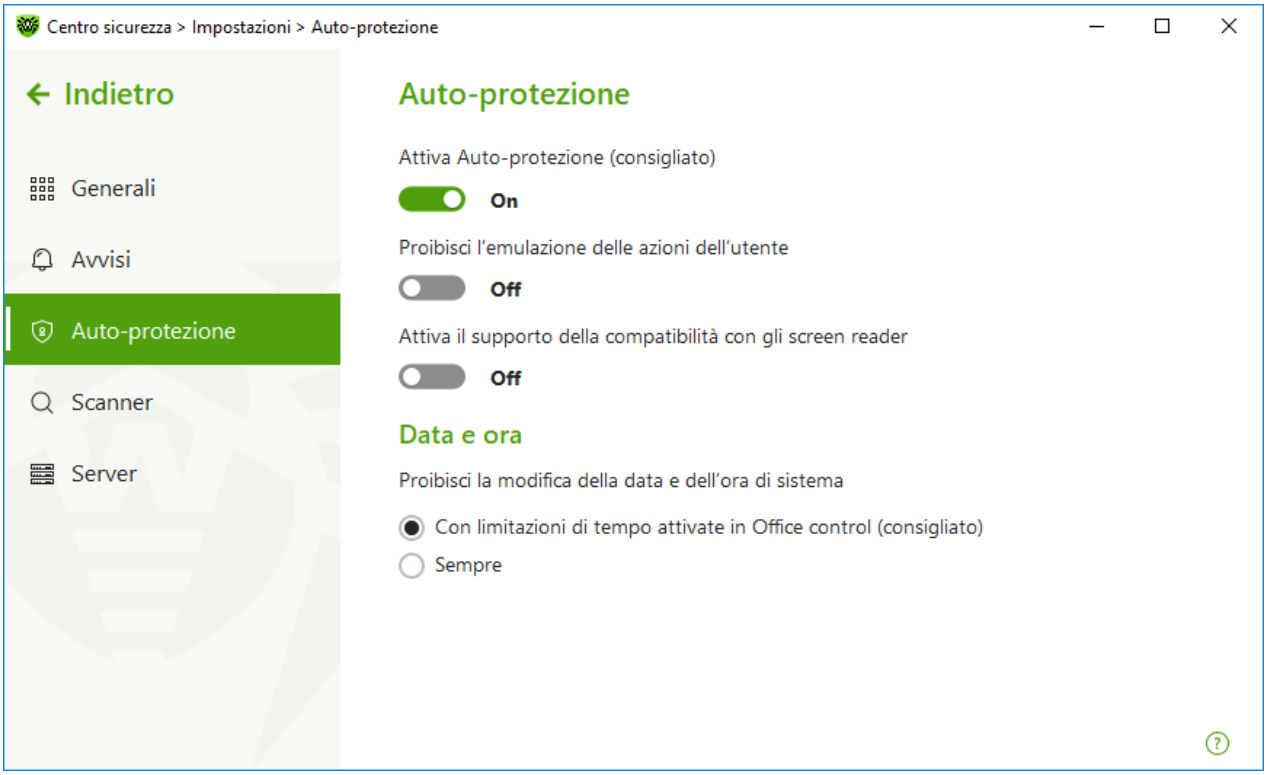

Immagine 24. Parametri di protezione Dr.Web

Impostazioni di Auto-protezione

L'impostazione **Attiva Auto-protezione (consigliato)** consente di proteggere i file e i processi di Dr.Web da accessi non autorizzati. Auto-protezione è attivata di default. Non è consigliabile disattivare Auto-protezione.

In caso di problemi con l'uso dei programmi di deframmentazione, si consiglia di disattivare temporaneamente il modulo Auto-protezione.

Per tornare a un punto di ripristino del sistema, è necessario disattivare il modulo Auto-protezione.

L'impostazione **Proibisci l'emulazione delle azioni dell'utente** consente di prevenire modifiche alle impostazioni Dr.Web, eseguite da software di terze parti. Tra le altre cose, sarà proibita l'esecuzione di script che emulano il funzionamento della tastiera e del mouse nelle finestre Dr.Web (per esempio script per la modifica delle impostazioni Dr.Web e altre operazioni finalizzate a modificare il funzionamento di Dr.Web).

L'impostazione **Attiva il supporto della compatibilità con gli screen reader** consente di utilizzare screen reader come ad esempio JAWS e NVDA per vocalizzare gli elementi dell'interfaccia Dr.Web. Questa funzione rende l'interfaccia del programma accessibile per persone con disabilità.

Data e ora

Alcuni programmi malevoli modificano deliberatamente la data e l'ora di sistema. In questo caso, i database dei virus del programma antivirus non vengono aggiornati secondo il calendario impostato, la licenza può essere identificata come scaduta, e i componenti di protezione verranno disabilitati.

L'impostazione **Proibisci la modifica della data e dell'ora di sistema** consente di bloccare la modifica manuale e automatica della data e dell'ora di sistema, nonché del fuso orario. Questa limitazione viene impostata per tutti gli utenti del sistema. Questa impostazione consentirà un funzionamento più accurato della funzione di limitazione di tempo nel modulo Office control. Se nel modulo Office control sono impostate limitazioni al tempo di utilizzo del computer o di internet, questa impostazione si attiva automaticamente. È possibile configurare la ricezione degli avvisi per il caso in cui viene fatto un tentativo di modifica dell'ora di sistema.

7.4. Parametri di scansione dei file

È possibile configurare le impostazioni di funzionamento dello scanner, e inoltre, modificare le azioni predefinite utilizzate al rilevamento di oggetti malevoli. Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi e non dovrebbero essere modificate senza necessità.

Per andare ai parametri di scansione dei file

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
3. Nella parte superiore della finestra del programma premere .
4. Si apre la finestra con le impostazioni principali del programma. Nella parte sinistra della finestra selezionare **Scanner**.

> La modifica delle impostazioni del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

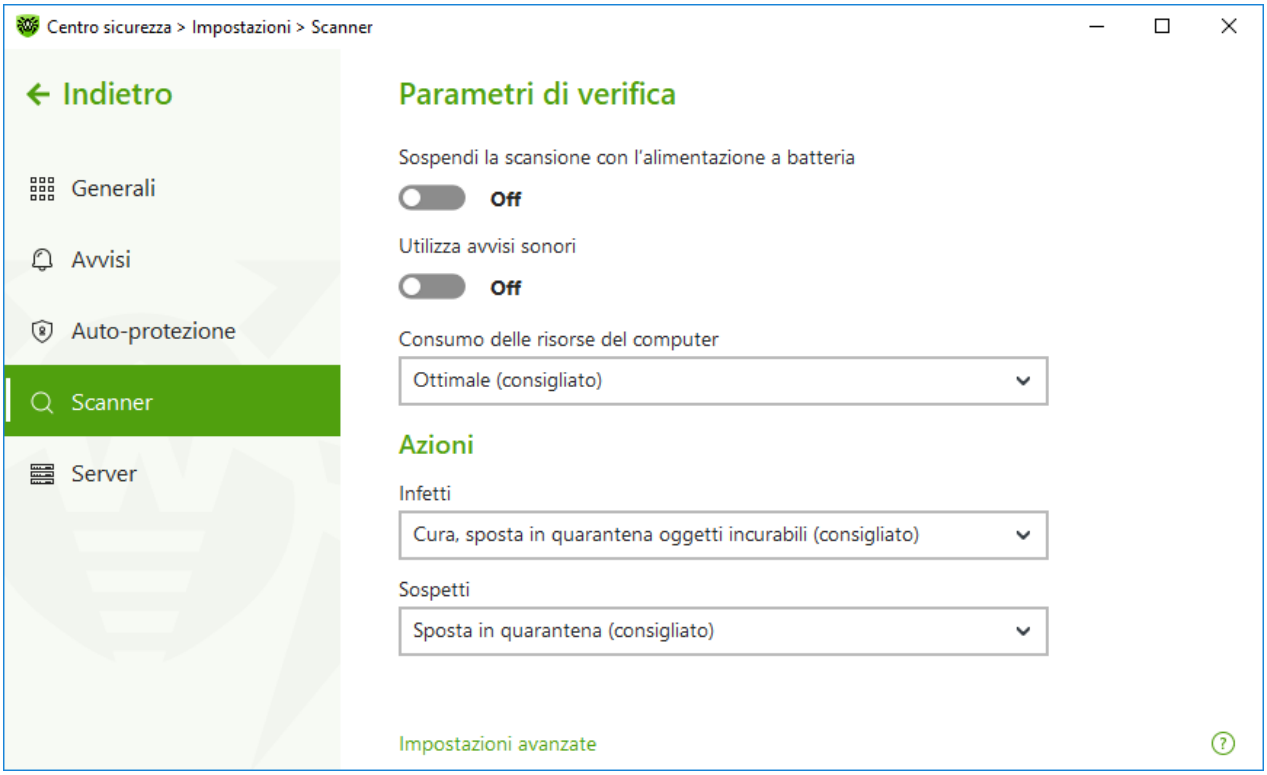

Immagine 25. Configurazione di Scanner

Parametri di verifica

In questo gruppo sono disponibili i parametri generali di funzionamento di Scanner Dr.Web:

- **Sospendi la scansione con l'alimentazione a batteria**. Attivare questa opzione affinché la scansione venga sospesa se il computer passa all'alimentazione a batteria. Di default l'opzione è disattivata.
- **Utilizza avvisi sonori**. Attivare questa opzione affinché Scanner Dr.Web accompagni con un segnale sonoro il rilevamento e la neutralizzazione di ciascuna minaccia. Di default l'opzione è disattivata.
- **Consumo delle risorse del computer**. Questa opzione imposta le restrizioni sul consumo delle risorse del computer da parte di Scanner Dr.Web. Di default, è impostato il valore ottimale.

Azioni

In questo gruppo di impostazioni viene configurata la reazione di Scanner al rilevamento di file infetti o sospetti e programmi malevoli.

La reazione viene configurata separatamente per ciascuna categoria di oggetti:

- **Infetti** — oggetti infettati da un virus conosciuto e (presumibilmente) curabile;

- **Sospetti** — oggetti presumibilmente infettati da un virus o contenenti un oggetto malevolo;
- vari oggetti potenzialmente pericolosi.

Di default Scanner cerca di curare i file infettati da un virus conosciuto e potenzialmente curabile e mette in Quarantena gli altri oggetti più pericolosi. È possibile modificare la reazione di Scanner al rilevamento di ciascun tipo di oggetti separatamente. Le reazioni possibili dipendono dal tipo di minaccia. Le azioni predefinite sono ottimali e sono contrassegnate come consigliate.

Esistono le seguenti azioni applicabili agli oggetti rilevati:

Azione	Descrizione
Cura, sposta in quarantena oggetti incurabili	Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà spostato in quarantena. Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).
Cura, rimuovi oggetti incurabili	Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà rimosso. Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).
Rimuovi	Per rimuovere l'oggetto. Nessun'azione verrà eseguita in caso dei settori di avvio.
Sposta in quarantena	Per spostare l'oggetto nella cartella speciale Quarantena. Nessun'azione verrà eseguita in caso dei settori di avvio.
Ignora	Per saltare l'oggetto senza eseguire alcun'azione e per non visualizzare avvisi. Questa azione è possibile solo per i programmi malevoli: adware, dialer, joke, riskware e hacktool.

Se il programma rileva un virus o un codice sospetto all'interno degli oggetti composti (archivi compressi, file di email o container di file), le azioni applicabili alle minacce all'interno di tali oggetti vengono eseguite con l'intero oggetto e non soltanto con la sua parte infetta.

Funzionalità avanzate

Per andare alle impostazioni avanzate, nella finestra **Parametri di verifica** (vedi immagine Impostazioni di scanner) fare clic sul link **Impostazioni avanzate**.

Può essere disattivata la scansione di pacchetti di installazione, archivi compressi e file di email. Di default, la scansione di tali oggetti è attivata.

Si può inoltre configurare il comportamento di Scanner dopo la fine della scansione:

- **Non applicare azione**. Scanner visualizzerà una tabella con la lista delle minacce rilevate.
- **Neutralizza le minacce rilevate**. Scanner applicherà automaticamente le azioni alle minacce rilevate.
- **Neutralizza le minacce rilevate e spegni il computer**. Scanner applicherà automaticamente le azioni alle minacce rilevate e quindi spegnerà il computer.

7.5. Server

È possibile visualizzare e modificare i parametri di interazione di Dr.Web con il server di protezione centralizzata, nonché configurare le impostazioni di Modalità mobile di Dr.Web. L'amministratore della rete antivirus può vietare di modificare i parametri di interazione con il server, in tale caso i pulsanti e i flag saranno non disponibili per la gestione.

In questa sezione:

- Parametri di connessione
- Impostazioni di connessione al server di protezione centralizzata
- Certificati
- Parametri di connessione della postazione
- Impostazioni avanzate
- Modalità mobile

Per andare ai parametri di interazione della postazione con il server

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
3. Nella parte superiore della finestra del programma premere .
4. Si apre la finestra con le impostazioni principali del programma. Nella parte sinistra della finestra selezionare **Server**.

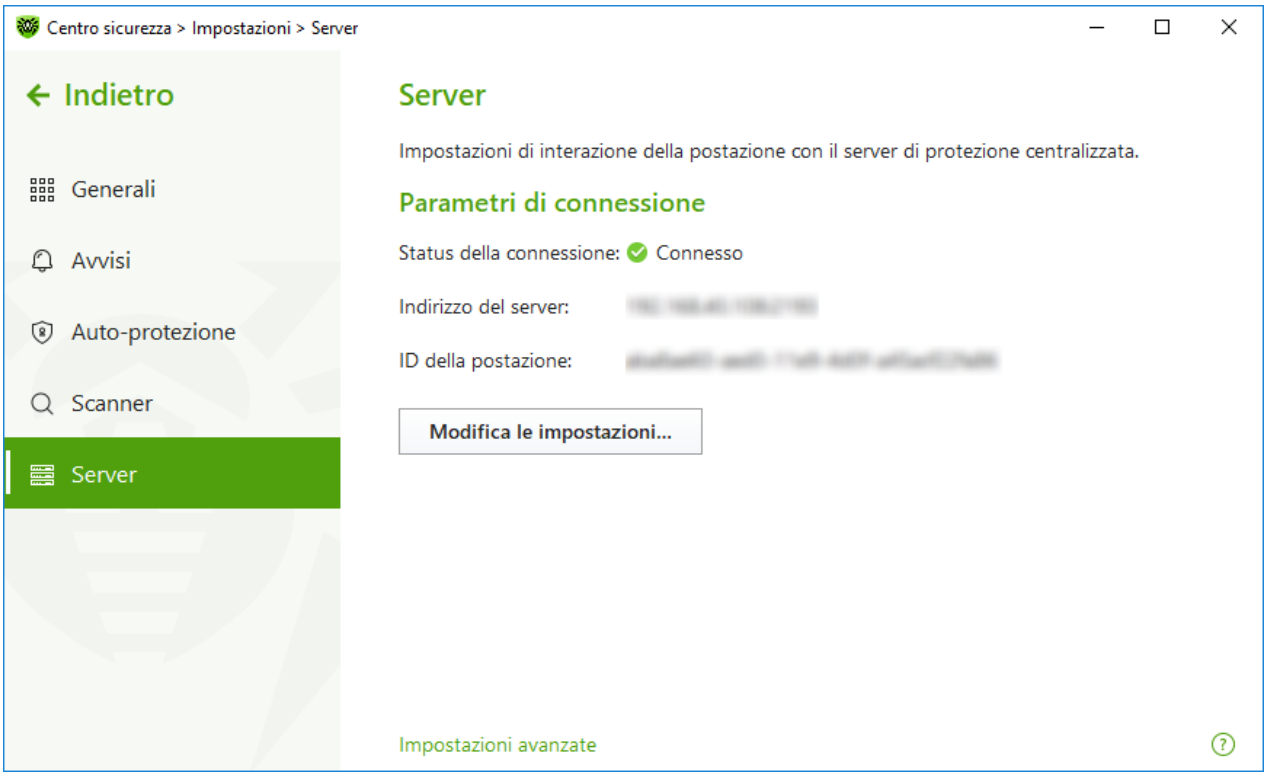

Immagine 26. Impostazioni di connessione della postazione

Parametri di connessione

Nel gruppo **Parametri di connessione** vengono visualizzati:

- **Status della connessione** — stato della connessione della postazione al server di protezione centralizzata;
- **Indirizzo del server** — indirizzo del server di protezione centralizzata a cui è connessa la postazione;
- **ID della postazione** — identificatore della postazione per la connessione al server.

È possibile visualizzare e gestire le impostazioni della connessione al server, se l'amministratore della rete ha concesso tali permessi.

> ⚠ Le impostazioni della connessione al server di protezione centralizzata possono essere modificate solo in coordinamento con l'amministratore della rete antivirus, altrimenti il computer verrà disconnesso dalla rete antivirus.

Impostazioni di connessione

Per modificare le impostazioni della connessione al server corrente o per aggiungere un altro server, premere **Modifica le impostazioni**. Si apre la finestra **Impostazioni di connessione** del server:

Immagine 27. Impostazioni della connessione al server

La tabella elenca tutti i server a cui la postazione può essere connessa. È possibile rimuovere i server dalla tabella e aggiungerne di nuovi.

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — configurazione della connessione a un altro server. Nella finestra che si è aperta è necessario indicare l'indirizzo del server di protezione centralizzata, fornito dall'amministratore.
- Pulsante 🗑 — rimozione di una riga.

Certificati

Un prerequisito per la connessione della postazione al server di protezione centralizzata è la disponibilità di un certificato valido. Il certificato può essere univoco per ciascun server specifico o adatto per più server. È possibile aggiungere più certificati per la connessione a più server. Un certificato valido viene fornito dall'amministratore della rete antivirus.

Di default è indicato il certificato che è stato utilizzato durante l'installazione del programma, se sul server non veniva effettuata una sostituzione delle chiavi di cifratura programmata. Se una sostituzione delle chiavi è stata effettuata, verrà indicato l'ultimo dei certificati generati. Per visualizzare la lista dei certificati disponibili o aggiungere un altro certificato, andare al link **Lista dei certificati**.

Per aggiungere un nuovo certificato, premere il pulsante ⊕ e nella finestra che si è aperta selezionare il file richiesto.

Per rimuovere un certificato non utilizzato, premere il pulsante .

Parametri di connessione della postazione

Per modificare i parametri di connessione della postazione

1. Nella finestra **Parametri di connessione della postazione** indicare l'identificatore della postazione e la password per la connessione al server. Questi dati vengono forniti dall'amministratore del server.
2. Premere **OK** per salvare le modifiche.

Per resettare i parametri di connessione e connettersi come un nuovo arrivo al server di protezione centralizzata

1. Nella finestra **Parametri di connessione della postazione** premere **Resetta i parametri e connettiti come un nuovo arrivo**.
2. Nella finestra che si è aperta confermare di voler resettare i parametri di connessione della postazione e connettersi come un nuovo arrivo. Notare che questa azione è irreversibile.
3. Dopo la conferma della registrazione della postazione sul server di protezione centralizzata Dr.Web otterrà i nuovi identificatore e password. Essi verranno utilizzati per la connessione al server.

Parametri di connessione di agent virtuale

Con determinate impostazioni sul lato server, la postazione può essere connessa a Server di scansione. In questo caso, la postazione è considerata *agent virtuale* e trasmette al server richieste di scansione di file e URL. I database dei virus e i filtri incorporati non sono conservati sulla postazione.

Se è utilizzato Server di scansione, sulla postazione è visualizzato un gruppo di impostazioni **Parametri di connessione di agent virtuale** con i seguenti dati:

- stato della connessione della postazione a Server di scansione;
- ID di Server di scansione.

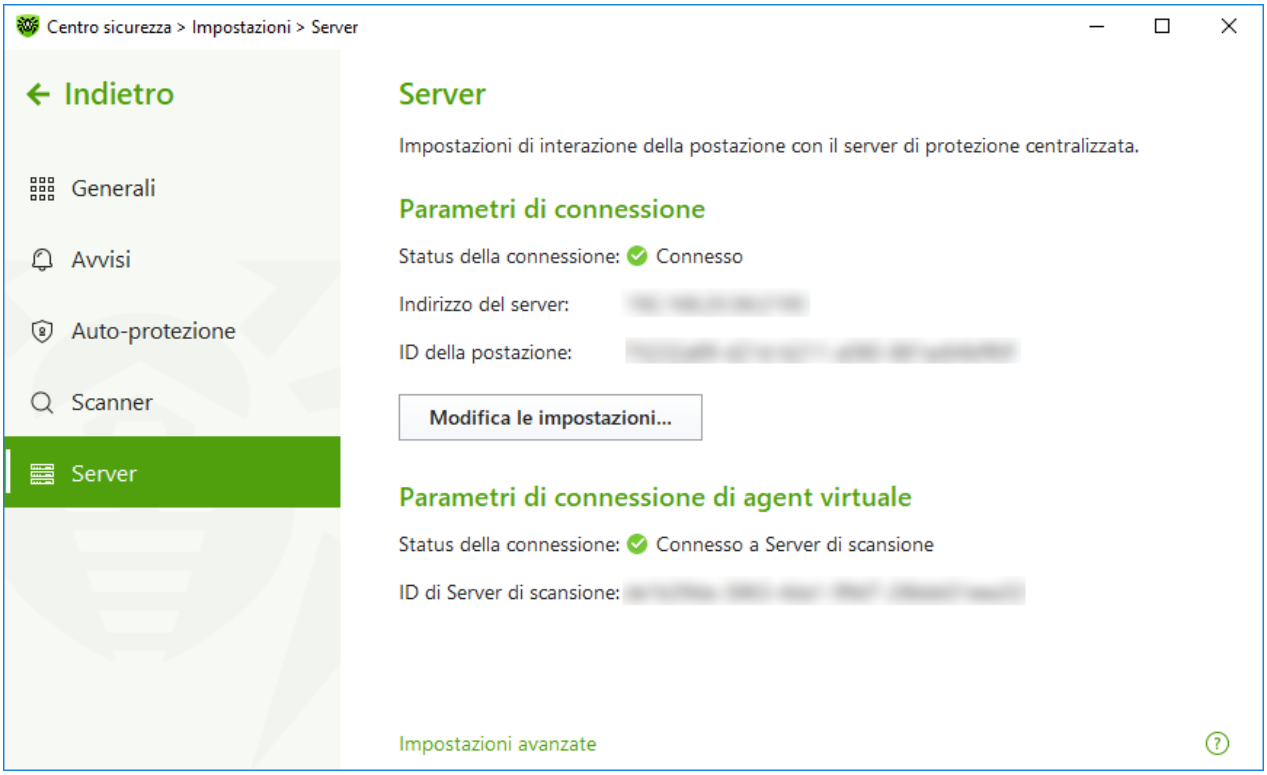

Immagine 28. Connessione a Server di scansione

Se la connessione a Server di scansione è assente, la postazione non è protetta. È necessario contattare l'amministratore della rete antivirus.

Impostazioni avanzate

Per andare alle impostazioni avanzate, nella finestra **Server** (vedi immagine Impostazioni di connessione postazione) fare clic sul link **Impostazioni avanzate**. Nel gruppo **Impostazioni avanzate** è possibile selezionare le seguenti opzioni:

- **Sincronizza l'ora del sistema con l'ora del server** — per sincronizzare l'ora di sistema sul computer con quella del server di protezione centralizzata. In questa modalità Dr.Web imposta periodicamente l'ora di sistema sul computer in conformità all'ora del server.
- **Usa la Modalità mobile se la connessione al server è assente** — per ottenere tempestivamente gli aggiornamenti dei database dei virus.

Modalità mobile

Se il computer non avrà la connessione al server di protezione centralizzata per un lungo tempo, per ottenere tempestivamente gli aggiornamenti dai server dell'azienda Doctor Web, si consiglia di impostare la modalità mobile di funzionamento di Dr.Web. A questo scopo spuntare il flag **Usa la Modalità mobile se la connessione al server è assente**.

Il flag **Usa la Modalità mobile se la connessione al server è assente** sarà disponibile a condizione che sul server di protezione centralizzata nei permessi della postazione sia consentita la **Modifica della configurazione di Agent Dr.Web**.

In Modalità mobile Dr.Web tenta di connettersi al server di protezione centralizzata, fa tre tentativi e se non sono riusciti, aggiorna i database dei virus dai server dell'azienda Doctor Web. I tentativi di rilevamento del server di protezione centralizzata si susseguono continuamente a intervalli di circa un minuto.

Per configurare le impostazioni di Modalità di funzionamento mobile

1. Premere il pulsante **Configura**. Si apre la finestra **Modalità mobile**.
2. Dalla lista a cascata **Ricevi gli aggiornamenti** si può selezionare la periodicità con cui verrà controllata la disponibilità degli aggiornamenti sui server dell'azienda Doctor Web.

   Se nella lista **Ricevi gli aggiornamenti** viene selezionata l'opzione **Manualmente**, gli aggiornamenti automatici non verranno eseguiti. Sarà possibile avviare l'aggiornamento nel menu Dr.Web.

3. Se si usa un server proxy, impostare il flag corrispondente. In questo caso saranno attivi i campi:

Impostazione	Descrizione
Indirizzo	Indicare l'indirizzo del server proxy.
Porta	Indicare la porta del server proxy.
Login	Indicare il nome dell'account per la connessione al server proxy.
Password	Indicare la password dell'account utilizzato per la connessione al server proxy.
Tipo di autenticazione	Selezionare il tipo di autenticazione richiesto per la connessione al server proxy.

4. Dopo aver finito di modificare, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per uscire dalla finestra senza salvare le modifiche.

In modalità mobile solo i database dei virus vengono aggiornati.

Se il flag **Usa la Modalità mobile se la connessione al server è assente** viene deselezionato prima che riprenda la comunicazione con il server di protezione centralizzata, i database dei virus non verranno più aggiornati, ma la ricerca del server continuerà.

Tutte le modifiche che vengono impostate per la postazione sul server di protezione centralizzata entreranno in vigore non appena riprenderà la comunicazione di Dr.Web con il server.

7.6. Avvisi del server

Per la comodità di gestione degli avvisi sul server di protezione centralizzata l'amministratore della rete ha la possibilità di attivare l'invio degli avvisi sulla postazione. In questo caso nella finestra **Generali** comparirà la voce **Avvisi del server**.

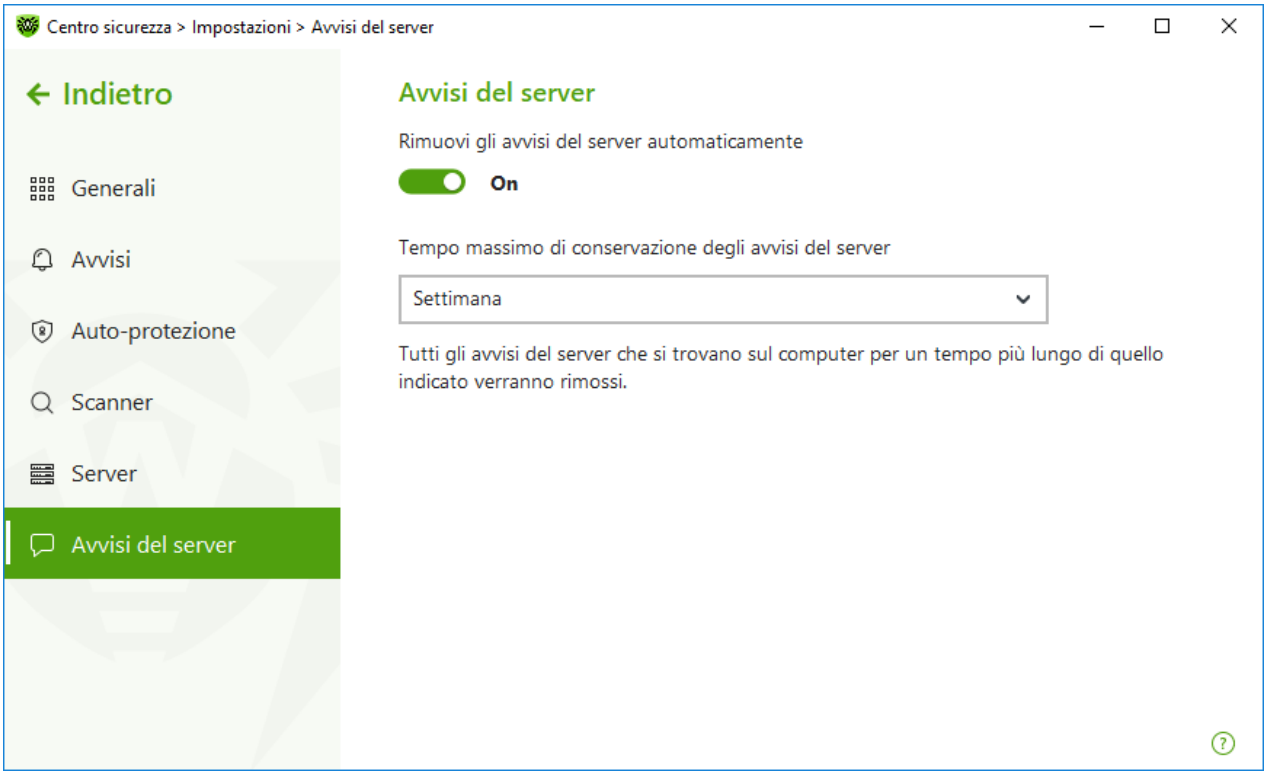

Immagine 29. Impostazioni di rimozione automatica degli avvisi del server

Per attivare o disattivare la rimozione automatica degli avvisi del server

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
3. Nella parte superiore della finestra del programma premere .
4. Si apre la finestra con le impostazioni principali del programma. Nella parte sinistra della finestra selezionare **Avvisi del server**.
5. Attivare o disattivare l'opzione **Rimuovi gli avvisi del server automaticamente** utilizzando l'interruttore .
6. Quando viene attivata la rimozione degli avvisi automatica, nella voce **Tempo massimo di conservazione degli avvisi del server** nella lista a cascata selezionare il periodo di tempo richiesto. Gli avvisi verranno rimossi dopo questo periodo.

8. File e rete

Questo gruppo di impostazioni fornisce accesso ai parametri dei principali componenti di protezione e allo Scanner.

Per andare al gruppo di impostazioni File e rete

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.

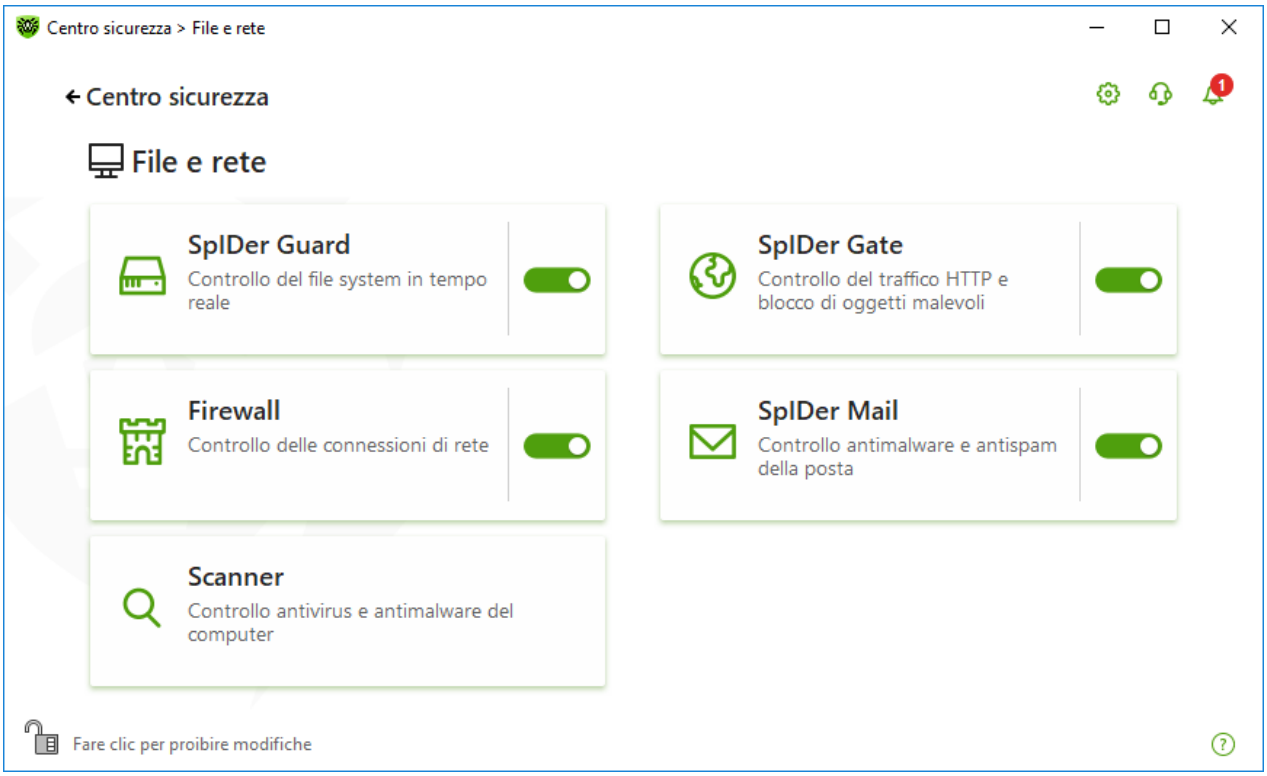

Immagine 30. Finestra File e rete

Attivazione e disattivazione dei componenti di protezione

Attivare o disattivare il componente richiesto utilizzando l'interruttore .

Per andare ai parametri dei componenti

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella del componente richiesto.

In questa sezione:

- Monitor del file system SplDer Guard — componente che controlla in tempo reale i file durante l'apertura, l'avvio o la modifica, nonché i processi che vengono avviati.

- Monitor di internet SpIDer Gate — componente che controlla il traffico HTTP.
- Antivirus della posta SpIDer Mail — componente che controlla la presenza di oggetti malevoli e dello spam nelle email.
- Firewall — componente che controlla le connessioni e la trasmissione di dati attraverso la rete, e inoltre blocca le connessioni sospette a livello di pacchetto e di applicazione.
- Scanner — componente che esegue la scansione degli oggetti su richiesta o secondo un calendario.
- Dr.Web per Microsoft Outlook — plugin Dr.Web per Microsoft Outlook.

Per *disattivare* qualche componente, Dr.Web deve essere in modalità amministratore. Per questo scopo, cliccare sul lucchetto nella parte inferiore della finestra del programma.

8.1. Protezione del file system in tempo reale

Il monitor del file system SpIDer Guard protegge il computer in tempo reale e ne impedisce l'infezione. SpIDer Guard si avvia al caricamento del sistema operativo e controlla i file durante l'apertura, l'avvio o la modifica, nonché monitora le azioni dei processi in esecuzione.

Per attivare o disattivare il monitor del file system

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Attivare o disattivare il monitor del file system SpIDer Guard utilizzando l'interruttore .

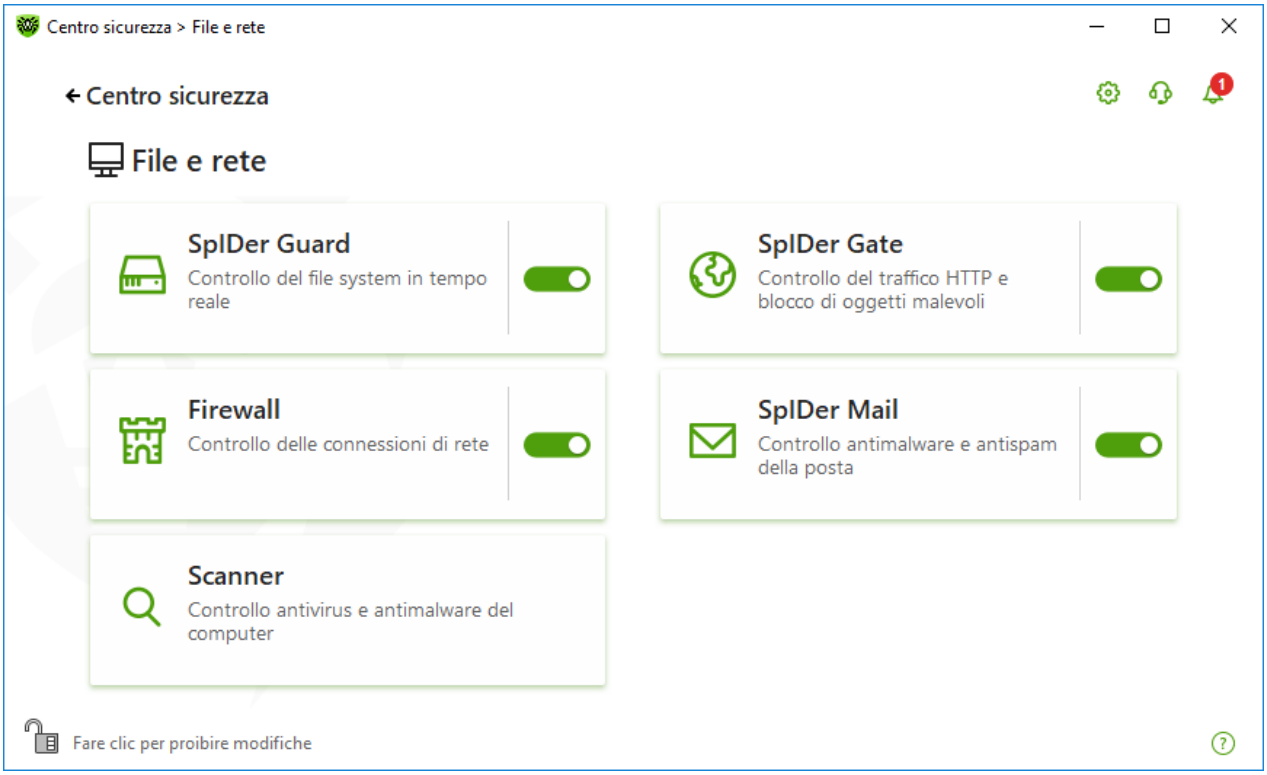

Immagine 31. Attivazione/disattivazione di SpIDer Guard

In questa sezione:

- Caratteristiche del funzionamento di SpIDer Guard
- Controllo di supporti rimovibili
- Azioni che vengono applicate alle minacce rilevate
- Selezione della modalità di controllo tramite il monitor SpIDer Guard
- Impostazioni avanzate

Vedi inoltre:

- Esclusione di file e cartelle dal controllo
- Esclusione di applicazioni dal controllo

Caratteristiche del funzionamento di SpIDer Guard

Con le impostazioni predefinite SpIDer Guard controlla al volo sul disco rigido solo i file che vengono creati o modificati, sui supporti rimovibili — tutti i file che vengono aperti. Inoltre, SpIDer Guard monitora costantemente le azioni dei processi in esecuzione, caratteristiche dei virus, e se le rileva, blocca tali processi.

> Il componente SpIDer Guard non controlla i file all'interno degli archivi, degli archivi della posta elettronica e dei container di file. Se un file in archivio o in allegato di posta è infetto, la minaccia verrà rilevata al momento dell'estrazione del file, prima che possa comparire la possibilità di infezione del computer.

Di default SpIDer Guard si avvia automaticamente a ogni caricamento del sistema operativo e il monitor del file system avviato SpIDer Guard non può essere scaricato dalla memoria durante la sessione corrente di funzionamento del sistema operativo.

> È possibile l'incompatibilità del programma Dr.Web con MS Exchange Server. In caso di problemi, aggiungere i database e il registro delle transazioni di MS Exchange Server alla lista delle eccezioni di SpIDer Guard.

Parametri del monitor del file system SpIDer Guard

Quando SpIDer Guard rileva oggetti infetti, applica a essi le azioni in base ai parametri configurati. Le impostazioni predefinite del programma sono ottimali per la maggior parte dei casi, non dovrebbero essere modificate senza necessità.

Per andare ai parametri del componente SpIDer Guard

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella **SpIDer Guard**. Si aprirà la finestra dei parametri del componente.

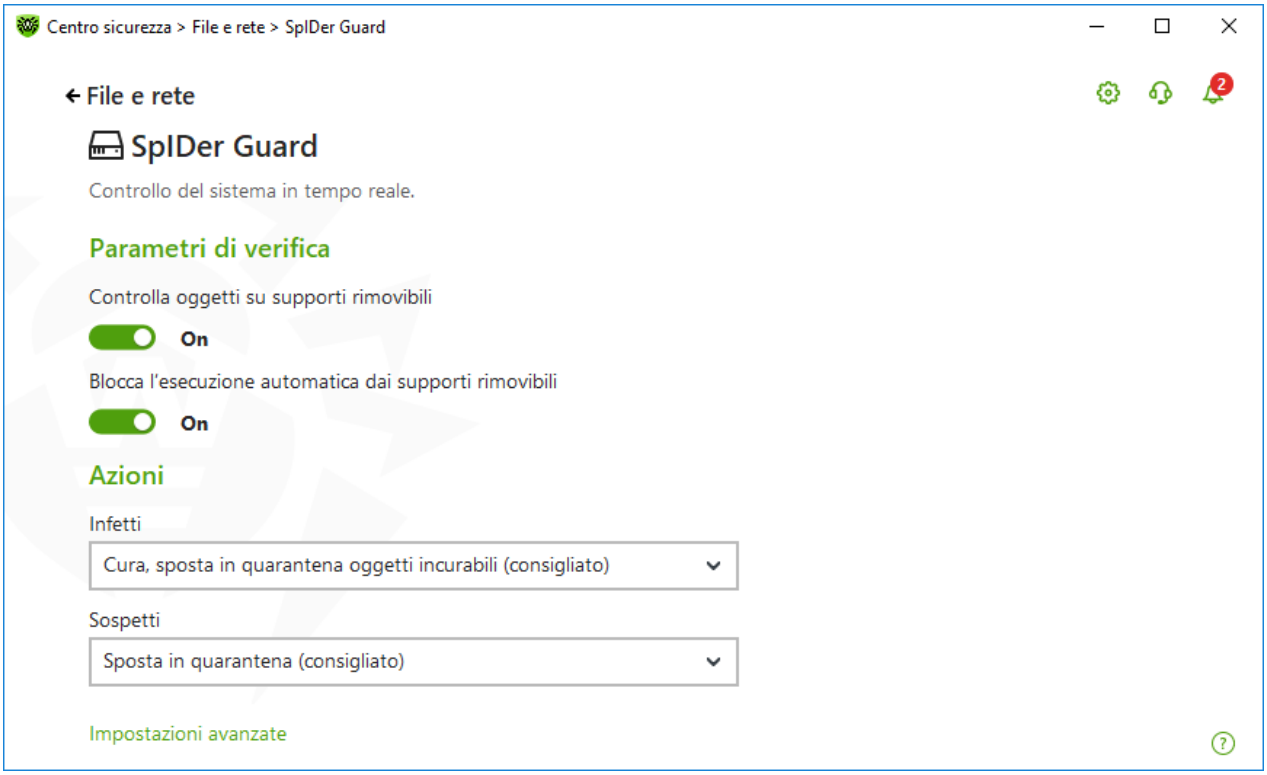

Immagine 32. Parametri del monitor del file system

Controllo di supporti rimovibili

SpIDer Guard controlla di default i file su supporti di memorizzazione rimovibili (dischi CD/DVD, memoria flash ecc.) alla creazione, la lettura, la modifica e l'avvio di questi file, e inoltre, blocca l'esecuzione automatica del loro contenuto attivo. Questo metodo aiuta a prevenire l'infezione del computer attraverso supporti rimovibili in quanto SpIDer Guard monitora l'accesso al file system in tempo reale e blocca l'esecuzione di codice malevolo.

Alcuni supporti rimovibili (in particolare hard disk portatili con interfaccia USB) possono essere presentati nel sistema come dischi rigidi. In questo caso, nell'area di notifica di Windows non viene visualizzata l'icona "Rimozione sicura dell'hardware ed espulsione supporti". Alla lettura di un file da tale disco, SpIDer Guard non lo controlla a meno che non sia selezionata la modalità paranoicale, pertanto, è consigliato eseguire la scansione antivirus tramite Scanner Dr.Web di tali dischi al loro collegamento al computer.

È possibile attivare o disattivare le opzioni **Controlla oggetti su supporti rimovibili** e **Blocca l'esecuzione automatica dai supporti rimovibili** utilizzando l'interruttore nel gruppo di impostazioni **Parametri di verifica**.

In caso di problemi con l'installazione dei programmi che utilizzano il file `autorun.inf`, disattivare temporaneamente l'opzione **Blocca l'esecuzione automatica dai supporti rimovibili**.

Azioni che vengono applicate alle minacce rilevate

In questo gruppo di impostazioni è possibile configurare le azioni che Dr.Web deve applicare alle minacce nel caso di rilevamento di esse tramite il monitor del file system SpIDer Guard.

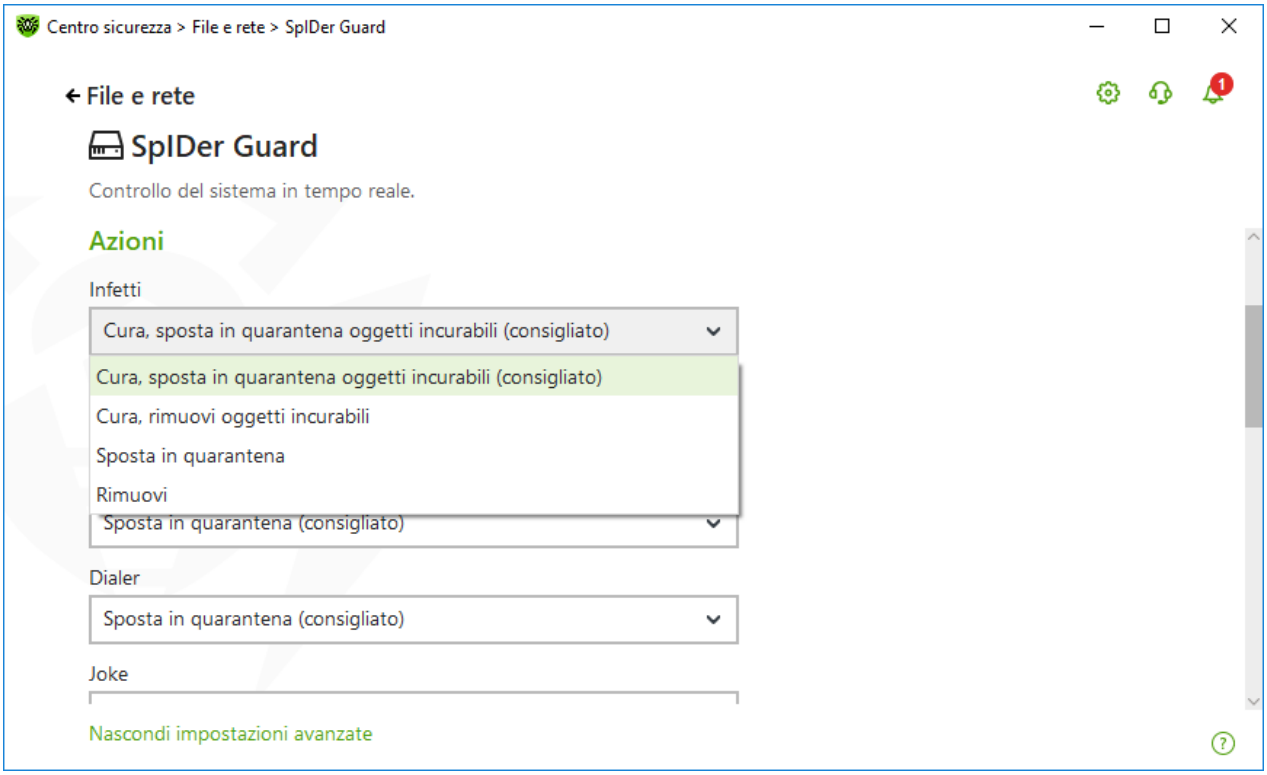

Immagine 33. Configurazione delle azioni da applicare alle minacce

Le azioni vengono impostate separatamente per ciascun tipo di oggetti malevoli e sospetti. La lista delle azioni disponibili dipende dal tipo di oggetti. Di default le azioni consigliate sono impostate per ciascun tipo di oggetti. Le copie di backup degli oggetti elaborati vengono salvate in Quarantena.

Possibili azioni

Le seguenti azioni possono essere applicate alle minacce:

Azione	Descrizione
Cura, sposta in quarantena oggetti incurabili	Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà spostato in quarantena. Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).
Cura, rimuovi oggetti incurabili	Per ripristinare l'oggetto allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà rimosso. Questa azione è disponibile solo per gli oggetti infettati da un virus conosciuto curabile, esclusi i trojan e i file infetti all'interno degli oggetti composti (archivi compressi, file di email o container di file).

Azione	Descrizione
Rimuovi	Per rimuovere l'oggetto. Nessun'azione verrà eseguita in caso dei settori di avvio.
Sposta in quarantena	Per spostare l'oggetto nella cartella speciale Quarantena. Nessun'azione verrà eseguita in caso dei settori di avvio.
Ignora	Per saltare l'oggetto senza eseguire alcun'azione e per non visualizzare avvisi. Questa azione è possibile solo per i programmi malevoli: adware, dialer, joke, riskware e hacktool.
Informa	Per visualizzare un avviso e saltare l'oggetto senza eseguire alcun'azione. Questa azione è possibile solo per gli oggetti sospetti e i programmi malevoli.

Modalità di controllo tramite il componente SpIDer Guard

Per accedere a questa e alla seguente sezione, fare clic sul link **Impostazioni avanzate**.

In questo gruppo di impostazioni è possibile selezionare la modalità di controllo dei file tramite il monitor SpIDer Guard.

Modalità	Descrizione
Ottimale, si usa di default	In questa modalità il controllo viene eseguito solo nei seguenti casi: • per oggetti sui dischi rigidi — all'avvio o creazione dei file, nonché al tentativo di scrittura nei file esistenti o nei settori di avvio; • per oggetti sui supporti rimovibili — a qualsiasi accesso ai file o ai settori di avvio (lettura, scrittura, avvio). È consigliata per l'uso dopo una scansione di tutti i dischi rigidi tramite Scanner Dr.Web. In tale caso, verrà esclusa la possibilità di infiltrazione sul computer di nuovi virus o altri programmi malevoli attraverso i supporti rimovibili, ma non verranno ricontrollati gli oggetti puliti già controllati.
Paranoicale	In questa modalità in caso di qualsiasi accesso (creazione, lettura, scrittura, avvio) vengono controllati tutti i file e i settori di avvio sui dischi rigidi e di rete, nonché sui supporti rimovibili. Questa modalità fornisce il massimo livello di protezione, ma aumenta notevolmente il carico di lavoro del computer.

Funzionalità avanzate

In questo gruppo di impostazioni è possibile configurare i parametri di scansione al volo che verranno utilizzati indipendentemente dalla modalità selezionata del monitor del file system SpIDer Guard. È possibile attivare:

- l'uso dell'analisi euristica;
- la verifica dei programmi e moduli che vengono caricati;
- la verifica dei file di installazione;
- la verifica dei file su unità di rete (non consigliato);
- la verifica della presenza di rootkit sul computer (consigliato);
- la verifica degli script eseguiti da Windows Script Host e Power Shell (per Windows 10, Windows 11).

Analisi euristica

Di default SpIDer Guard esegue la scansione utilizzano l'analisi euristica. Se l'opzione è disattivata, la scansione si basa soltanto sulle firme dei virus conosciuti.

Controllo in background della presenza di infezioni

Antirootkit incluso in Dr.Web permette di monitorare in background la presenza nel sistema operativo di minacce composte, e se necessario, esegue la cura di un'infezione attiva.

Quando questa impostazione è attiva, Antirootkit Dr.Web risiede costantemente nella memoria. A differenza della scansione dei file al volo, eseguita dal componente SpIDer Guard, la ricerca dei rootkit viene effettuata nel BIOS di sistema del computer e nelle aree critiche di Windows, quali gli oggetti in esecuzione automatica, i processi e moduli in esecuzione, la memoria operativa, i MBR/VBR dei dischi ecc.

Uno dei principali criteri di Antirootkit Dr.Web è che funziona, risparmiando le risorse del sistema operativo (tempo di CPU, RAM libera ecc.), nonché tenendo conto delle prestazioni dell'hardware.

Quando scopre minacce, Antirootkit Dr.Web avvisa l'utente della minaccia e neutralizza gli effetti pericolosi.

Durante la verifica in background della presenza di rootkit vengono esclusi dalla verifica i file e le cartelle indicate nella scheda corrispondente.

La verifica in background della presenza di rootkit è attivata di default.

8.2. Controllo del traffico web

Il componente SpIDer Gate controlla il traffico HTTP e blocca la trasmissione degli oggetti che contengono programmi malevoli. Attraverso il protocollo HTTP funzionano i browser, i gestori di download e altre applicazioni che utilizzano internet.

> ⚠ Il traffico cifrato non viene controllato per evitare malfunzionamenti durante l'uso di risorse di rete. Questo è dovuto al fatto che per stabilire le connessioni sicure in una rete aziendale, invece dei certificati dei software installati, viene utilizzato il certificato Dr.Web, il che può portare a errori di programmi che utilizzano un protocollo sicuro per la connessione e monitorano l'integrità del traffico.

Con le impostazioni predefinite SpIDer Gate effettua inoltre il filtraggio dei siti sconsigliati e dei siti conosciuti come fonti di diffusione dei virus.

SpIDer Gate risiede nella memoria operativa del computer e si riavvia automaticamente al caricamento di Windows.

Per attivare e disattivare il controllo del traffico web e il filtraggio dei siti sconsigliati

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Attivare o disattivare il monitor di internet SpIDer Gate utilizzando l'interruttore.

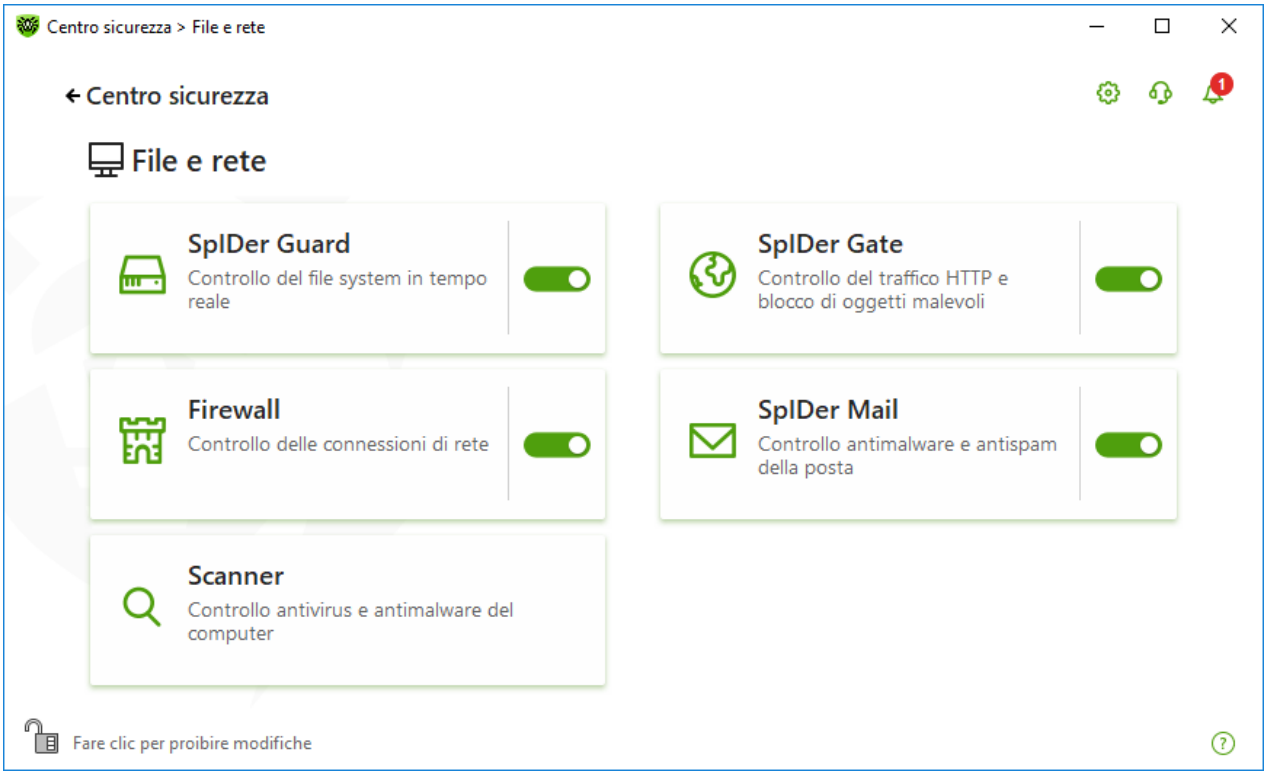

Immagine 34. Attivazione/disattivazione di SpIDer Gate

In questa sezione:

- Controllo del traffico e delle URL nei client di messaggistica istantanea
- Parametri di blocco dei siti
- Blocco dei programmi
- Blocco degli oggetti non controllati o danneggiati
- Controllo di archivi e pacchetti di installazione
- Uso delle risorse di sistema durante il controllo
- Direzione del traffico controllato

Vedi inoltre:

- Esclusione di siti dal controllo
- Esclusione di applicazioni dal controllo

Parametri di controllo del traffico web

Le impostazioni predefinite di SpIDer Gate sono ottimali nella maggior parte dei casi, non dovrebbero essere modificate senza necessità.

La modifica dei parametri del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per andare ai parametri del componente SpIDer Gate

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto" ). Altrimenti, cliccare sul lucchetto  .
2. Fare clic sulla piastrella **SpIDer Gate**. Si aprirà la finestra dei parametri del componente.

Immagine 35. Parametri di controllo del traffico HTTP

Controllo del traffico e delle URL nei client di messaggistica istantanea

Nel gruppo di impostazioni **Parametri di verifica** è possibile attivare la scansione dei link e file trasmessi attraverso i client dei sistemi di messaggistica istantanea (client IM), per esempio Agent Mail.ru, ICQ, nonché client che utilizzano il protocollo Jabber. Viene controllato solo il traffico in arrivo. Di default l'opzione è attivata.

Alle minacce trovate vengono applicate le seguenti azioni:

Oggetto	Azione
Controllo dei link	
Siti conosciuti come fonti di diffusione dei virus	Vengono bloccati automaticamente.
Siti sconsigliati e URL aggiunte su richiesta di titolari dell'diritto d'autore	Vengono bloccati in base ai parametri nel gruppo di impostazioni **Parametri di blocco**.
Controllo dei file	
Virus	Vengono bloccati automaticamente.
Programmi malevoli: • sospetti; • riskware; • dialer; • hacktool; • adware; • joke.	Vengono bloccati in base ai parametri nel gruppo di impostazioni **Blocca programmi**.

Nel controllo dei link in messaggi trasmessi si tiene conto anche dei siti e delle applicazioni esclusi dal controllo.

Parametri di blocco dei siti

Nel gruppo di impostazioni **Parametri di blocco** è possibile impostare il blocco automatico dell'accesso alle URL aggiunte su richiesta del titolare del diritto, nonché ai siti sconsigliati, conosciuti come inaffidabili. Per fare questo, attivare l'opzione corrispondente.

Per consentire l'accesso ai siti richiesti, indicare le eccezioni nel gruppo di impostazioni del programma **Eccezioni**.

SpIDer Gate blocca di default l'accesso ai siti conosciuti come fonti di virus o di altri tipi di programmi malevoli. Il controllo tiene conto di una lista di siti esclusi dal controllo.

Blocco dei programmi

Per accedere a questa e alle seguenti sezioni, fare clic sul link **Impostazioni avanzate**.

Il componente SpIDer Gate può bloccare i seguenti programmi malevoli:

- sospetti;

- riskware;
- dialer;
- hacktool;
- adware;
- joke.

Per attivare il blocco dei programmi malevoli, cliccare sul link **Impostazioni avanzate** e utilizzare gli interruttori corrispondenti nel gruppo di impostazioni **Blocca programmi**. È attivato di default il blocco dei programmi sospetti e degli adware, nonché dei dialer.

Blocco degli oggetti

SpIDer Gate può bloccare oggetti non controllati o danneggiati. Di default queste opzioni sono disattivate. Per accedere alle impostazioni di blocco degli oggetti, cliccare sul link **Impostazioni avanzate**.

Funzionalità avanzate

Le impostazioni **Controlla archivi** e **Controlla pacchetti di installazione**. Di default queste opzioni sono disattivate.

L'impostazione **Livello di consumo delle risorse di sistema**. In alcuni casi, Dr.Web non è in grado di determinare la dimensione finale di un file, per esempio durante il download del file. In questo caso, il file viene inviato per la verifica in parti. Questo richiede l'uso delle risorse del computer. È possibile configurare il livello di utilizzo delle risorse di sistema e così determinare la frequenza con cui i file di dimensioni sconosciute verranno inviati per la verifica. Con il massimo utilizzo delle risorse del computer, i file verranno inviati più spesso e la verifica dei file verrà eseguita più velocemente, ma il carico sul processore sarà aumentato.

L'impostazione **Modalità di controllo del traffico**. Di default viene controllato solo il traffico in arrivo. Se necessario, selezionare il tipo di traffico HTTP controllato.

Il controllo del traffico tiene conto dei parametri impostati del componente SpIDer Gate, della white list di siti e delle applicazioni escluse dal controllo.

8.3. Controllo della posta elettronica

Il controllo della posta elettronica viene eseguito dal componente SpIDer Mail. L'antivirus della posta SpIDer Mail viene installato di default, risiede permanentemente in memoria e viene avviato automaticamente all'avvio del sistema operativo. SpIDer Mail può inoltre controllare la posta per la presenza di spam tramite Antispam Dr.Web.

Il traffico cifrato non viene controllato per evitare malfunzionamenti durante l'uso di risorse di rete. Questo è dovuto al fatto che per stabilire le connessioni sicure in una rete aziendale, invece dei certificati dei software installati, viene utilizzato il certificato Dr.Web, il che può portare a errori di programmi che utilizzano un protocollo sicuro per la connessione e monitorano l'integrità del traffico.

Per controllare il traffico email cifrato, utilizzare il plugin Dr.Web per Microsoft Outlook o i prodotti server Dr.Web Mail Security Suite.

Per attivare o disattivare il controllo della posta elettronica

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Attivare o disattivare l'antivirus della posta SpIDer Mail utilizzando l'interruttore.

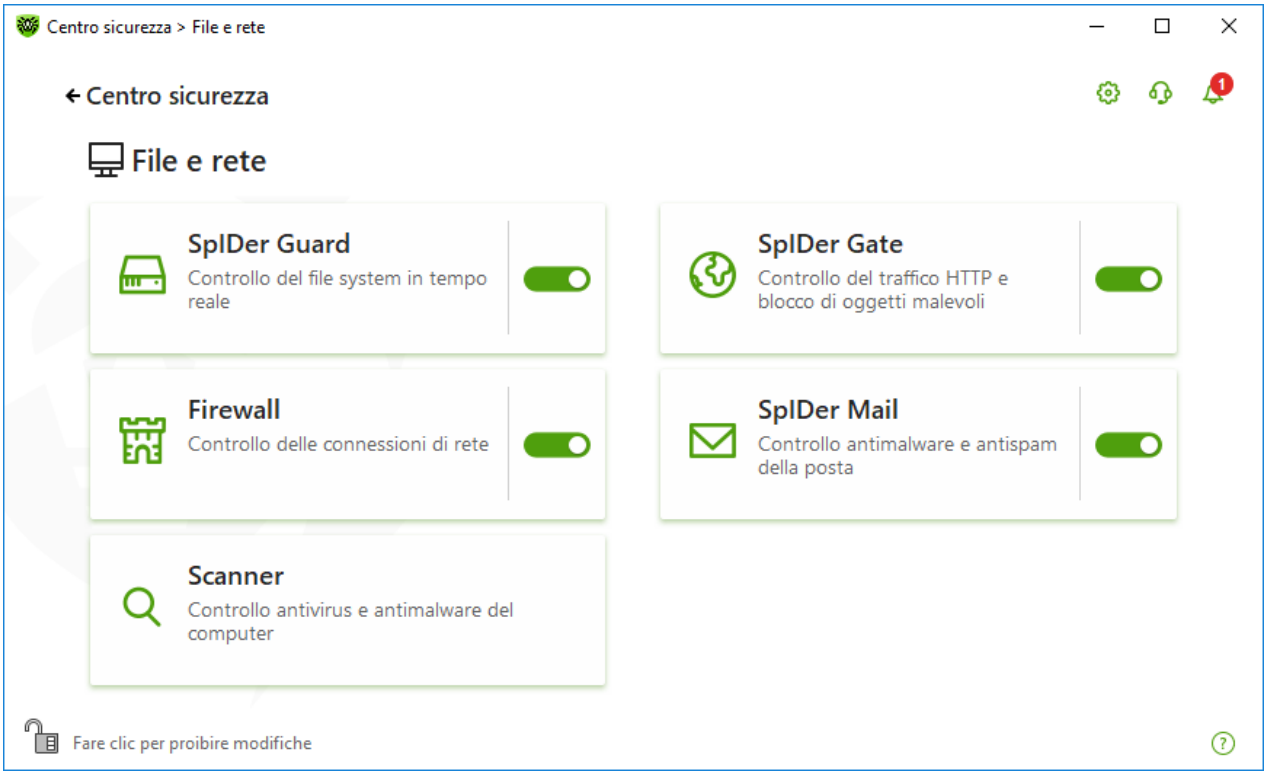

Immagine 36. Attivazione/disattivazione di SpIDer Mail

In questa sezione:

- Caratteristiche di elaborazione delle email
- Controllo di email tramite altri strumenti

Vedi inoltre:

- Parametri di controllo di email
- Parametri di Antispam

Caratteristiche di elaborazione delle email

SpIDer Mail riceve invece del client di posta tutte le email in ingresso e le controlla. Se non ci sono minacce, un'email viene trasferita al client di posta come se venisse direttamente dal server. In modo simile vengono controllate le email in uscita prima dell'invio sul server.

La reazione dell'antivirus della posta SpIDer Mail al rilevamento delle email in ingresso infette e sospette, nonché delle email che non hanno superato il controllo (per esempio le email con una struttura eccessivamente complessa) di default è la seguente:

Tipo di email	Azione
Email infette	Da tali email viene rimosso il contenuto malevolo (questa azione si chiama *cura* dell'email), quindi le email vengono consegnate in modo normale.
Email con oggetti sospetti	Vengono spostate in Quarantena come file separati, al programma di posta viene inviata una relativa notifica (questa azione si chiama *spostamento* dell'email). Le email spostate vengono rimosse dal server POP3 o IMAP4.
Email non infette ed email che non hanno superato il controllo	Vengono trasmesse senza modifiche (*vengono lasciate passare*).

Le *email in uscita* infette o sospette non vengono trasmesse sul server, l'utente viene notificato del rifiuto di invio del messaggio (di regola, in tale caso il programma di posta salva l'email).

Controllo di email tramite altri strumenti

Scanner può rilevare virus in alcuni formati di caselle di posta, però l'antivirus della posta SpIDer Mail ha una serie di vantaggi rispetto ad esso:

- non tutti i formati di caselle di posta dei programmi popolari sono supportati da Scanner Dr.Web; se viene utilizzo SpIDer Mail, le email infette non arrivano nemmeno nelle caselle di posta;
- Scanner controlla le caselle di posta solo su richiesta dell'utente, e non al momento della ricezione della posta. Tale verifica è impegnativa e può richiedere molto tempo.

8.3.1. Parametri di controllo di email

Di default SpIDer Mail cerca di curare le email infettate da un virus conosciuto e potenzialmente curabile. Le email incurabili e sospette, nonché gli adware e i dialer vengono messi in Quarantena. Le altre email vengono trasmesse dal monitor di posta senza modifica (*vengono saltate*). I parametri di controllo email predefiniti sono ottimali nella maggior parte dei casi e non dovrebbero essere modificati senza necessità.

In questa sezione:

- Azioni che vengono applicate alle minacce rilevate
- Configurazione dei parametri di controllo di email
- Scansione degli archivi compressi

Parametri di controllo di email

Le impostazioni predefinite di SpIDer Mail sono ottimali per un utente principiante e assicurano il massimo livello di protezione con il minimo intervento dell'utente. Tuttavia, in questo caso vengono bloccate alcune funzioni dei programmi di posta (per esempio l'invio di un'email su molteplici indirizzi può essere percepito come mailing di massa, non viene riconosciuto uno spam ricevuto), nonché viene persa la possibilità di ottenere informazioni utili dalle email automaticamente distrutte (dalla parte di testo non infetta).

La modifica dei parametri del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per iniziare a modificare i parametri di controllo di email

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
4. Fare clic sulla piastrella **SpIDer Mail**. Si aprirà la finestra dei parametri del componente.

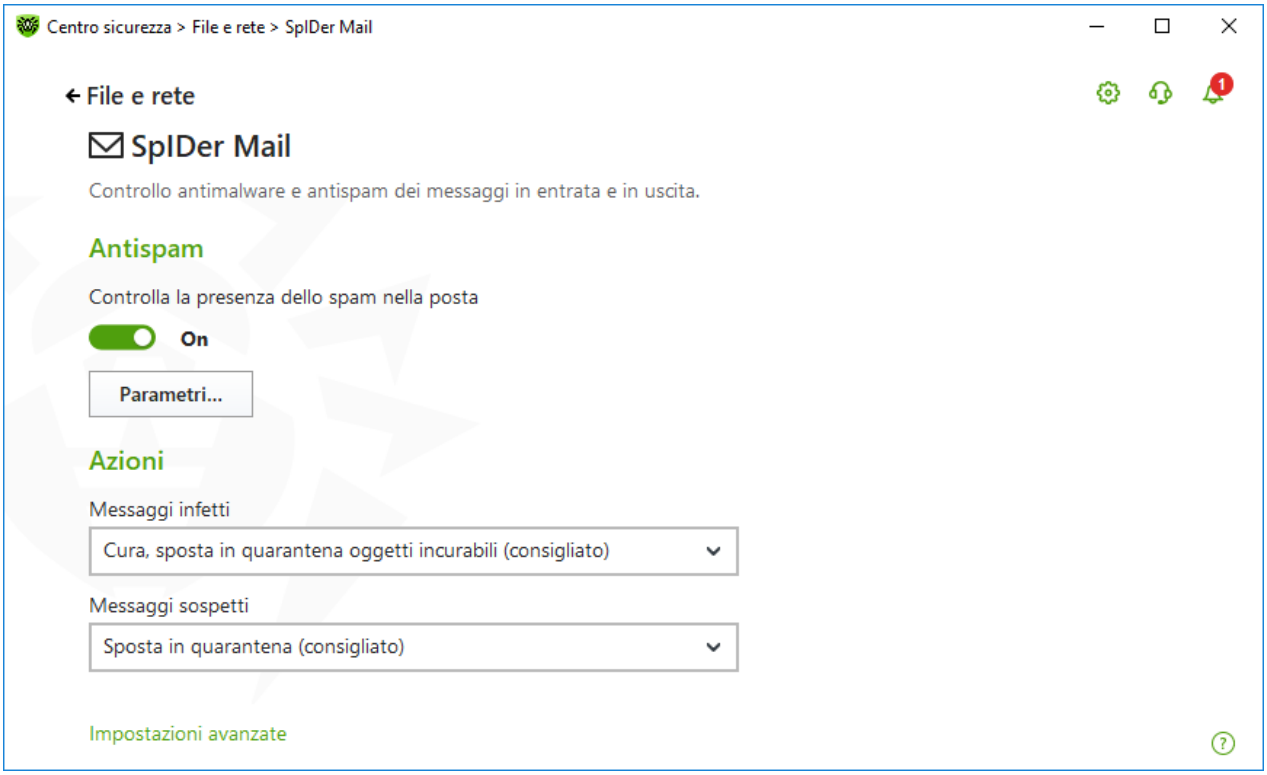

Immagine 37. Parametri di controllo di email

Azioni che vengono applicate alle minacce rilevate

In questo gruppo di impostazioni è possibile configurare le azioni che Dr.Web deve applicare alle email se rileva in esse una minaccia.

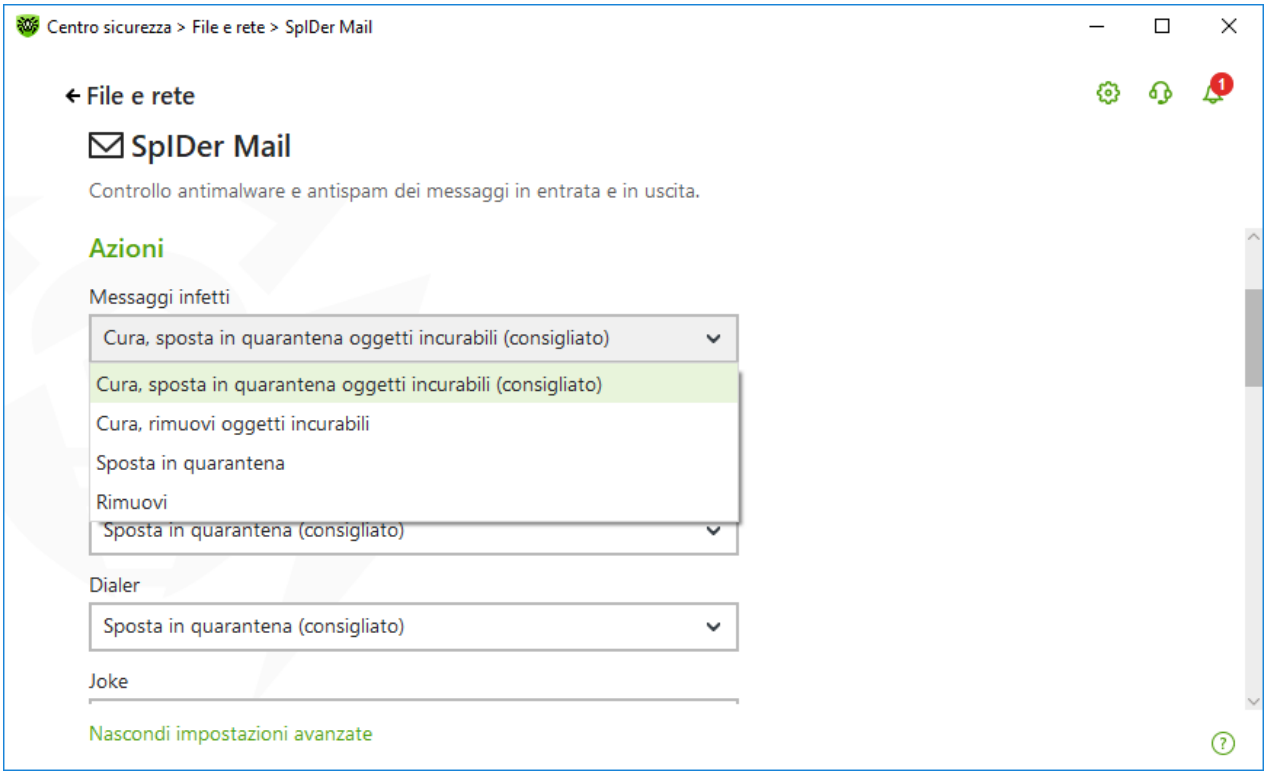

Immagine 38. Configurazione delle azioni da applicare alle email

Possibili azioni

Le seguenti azioni possono essere applicate alle minacce:

Azione	Descrizione
Cura, sposta in quarantena oggetti incurabili	Per ripristinare l'email allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà spostato in quarantena. Questa azione è possibile solo per le email infettate da un virus conosciuto curabile, esclusi i trojan i quali vengono rimossi al rilevamento. La cura di file in archivi non è possibile a prescindere dal tipo di virus. Porta al rifiuto di trasmissione dell'email.
Cura, rimuovi oggetti incurabili	Per ripristinare l'email allo stato precedente all'infezione. Se il virus è incurabile o se il tentativo di trattamento non è riuscito, l'oggetto verrà eliminato. Porta al rifiuto di trasmissione dell'email.
Rimuovi	Per eliminare l'email. In questo caso l'email non viene inoltrata al destinatario, invece al programma di posta viene trasmessa una notifica di operazione eseguita. Porta al rifiuto di trasmissione dell'email.

Azione	Descrizione
Sposta in quarantena	Per spostare l'email nella cartella speciale Quarantena. In questo caso l'email non viene inoltrata al destinatario, invece al programma di posta viene trasmessa una notifica di operazione eseguita. Porta al rifiuto di trasmissione dell'email.
Ignora	Per trasmettere l'email senza applicare ad essa alcune azioni.

È possibile aumentare l'affidabilità della protezione antivirus rispetto al livello impostato di default. Per questo scopo, fare clic sul link **Impostazioni avanzate** e selezionare dalla lista **Non controllati** la voce **Sposta in quarantena**. In questo caso è consigliabile controllare successivamente tramite Scanner Dr.Web i file con i messaggi spostati.

La protezione da email sospette può essere disattiva solo se il computer è protetto addizionalmente tramite il monitor di file SpIDer Guard permanentemente residente nella memoria.

Configurazione dei parametri di controllo di email

Per accedere ai parametri di controllo di email, fare clic sul link **Impostazioni avanzate**.

Azioni eseguite sulle email

In questo gruppo di impostazioni vengono indicate le azioni addizionali sulle email elaborate dal monitor di posta SpIDer Mail.

Impostazione	Descrizione
Aggiungi l'intestazione 'X-AntiVirus' ai messaggi	È un'impostazione predefinita. Se viene utilizzata questa impostazione, alle intestazioni di tutte le email elaborate dal monitor di posta SpIDer Mail vengono aggiunte informazioni circa la verifica dell'email e la versione di Dr.Web. Il formato dell'intestazione che viene aggiunta non è modificabile.
Rimuovi email modificate sul server	Se viene utilizzata questa impostazione, le email in ingresso rimosse o spostate in quarantena dal monitor di posta SpIDer Mail vengono rimosse sul server di posta indipendentemente dalle impostazioni del programma di posta.

Ottimizzazione della scansione

È possibile impostare una condizione al verificarsi della quale le email con una struttura complessa di cui la scansione consuma troppe risorse vengono riconosciute come non controllate. A tale scopo attivare l'opzione **Timeout della scansione di un'email** e impostare il tempo massimo entro cui viene controllata un'email. Dopo il tempo indicato il monitor di posta SpIDer Mail interrompe la scansione dell'email. Il valore di default è di 250 secondi.

Scansione degli archivi compressi

Attivare l'opzione **Controlla archivi** affinché SpIDer Mail controlli il contenuto degli archivi trasmessi via email. Se necessario, attivare le seguenti opzioni e configurare i parametri di controllo degli archivi:

- **Dimensione massima di un file da estrarre da archivio**. Se un archivio decompresso eccederà la dimensione indicata, SpIDer Mail non lo decomprimerà e non lo controllerà. Di default è impostato il valore di 30720 KB;
- **Livello di nidificazione massimo in un archivio**. Se il livello di nidificazione eccede il valore impostato, SpIDer Mail controllerà l'archivio solo fino al livello indicato. Di default è impostato il valore 64.

Un parametro non ha limitazioni, se è impostato il valore 0.

Funzionalità avanzate

Questo gruppo di impostazioni permette di configurare i parametri addizionali di scansione della posta elettronica:

- uso dell'analisi euristica — in questa modalità vengono utilizzati meccanismi speciali che permettono di individuare nella posta elettronica oggetti sospetti che con grande probabilità sono infettati da virus ancora sconosciuti. Per disattivare l'analisi euristica, utilizzare l'interruttore **Usa l'analisi euristica (consigliato)**;
- controllo di pacchetti di installazione. Di default questa impostazione è disattivata.

Configurazione degli avvisi

Dopo aver eseguito un'azione impostata, di default SpIDer Mail può visualizzare un relativo avviso nell'area di notifica di Windows. È possibile configurare la visualizzazione degli avvisi sullo schermo.

8.3.2. Parametri di Antispam

Le impostazioni predefinite di SpIDer Mail, incluso Antispam, sono ottimali nella maggior parte dei casi, non dovrebbero essere modificate senza necessità.

Per attivare e disattivare il controllo antispam della posta

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
4. Fare clic sulla piastrella **SpIDer Mail**. Si aprirà la finestra dei parametri del componente.

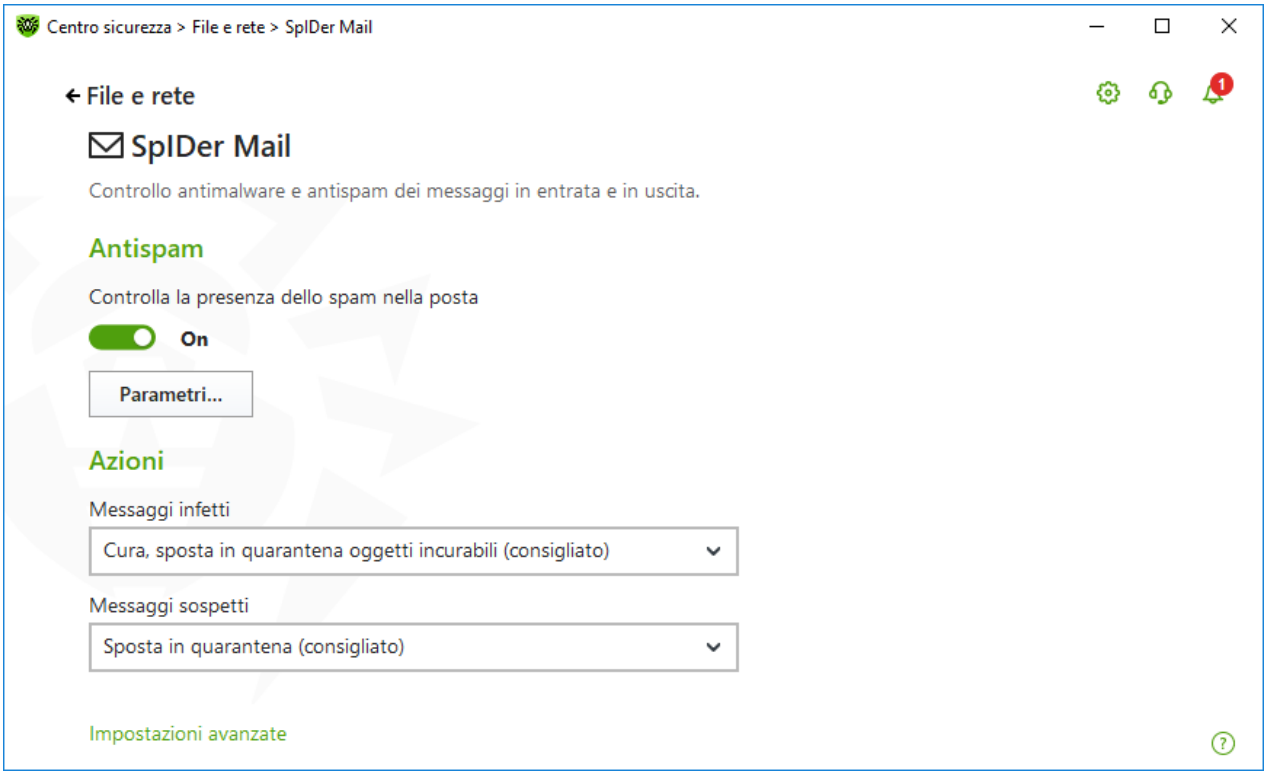

Immagine 39. Parametri di controllo della posta

5. Nella sezione delle impostazioni **Antispam** attivare o disattivare il controllo antispam della posta utilizzando l'interruttore corrispondente.

Configurazione dei parametri di funzionamento di Antispam

1. Nel gruppo di impostazioni **Antispam** premere il pulsante **Parametri**.

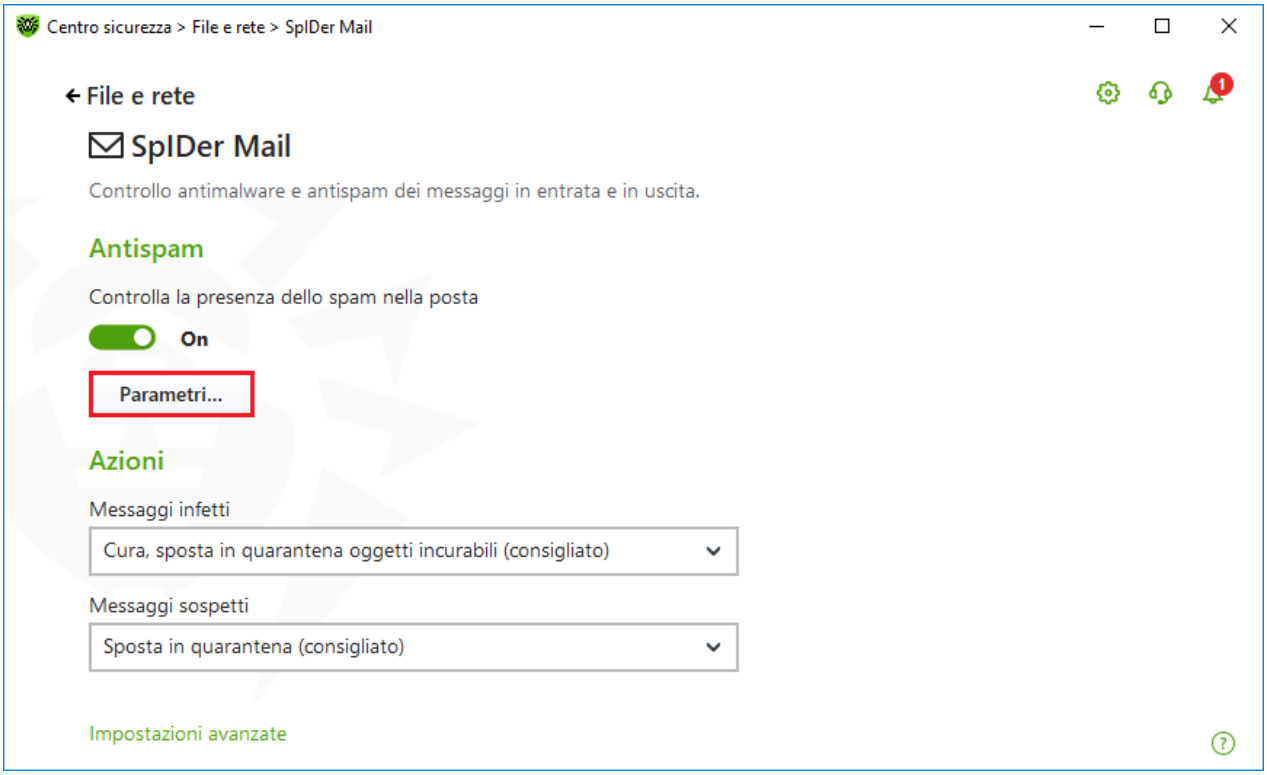

Immagine 40. Modifica dei parametri di Antispam

2. Nella finestra che si è aperta **Parametri di Antispam** attivare o disattivare le opzioni richieste.

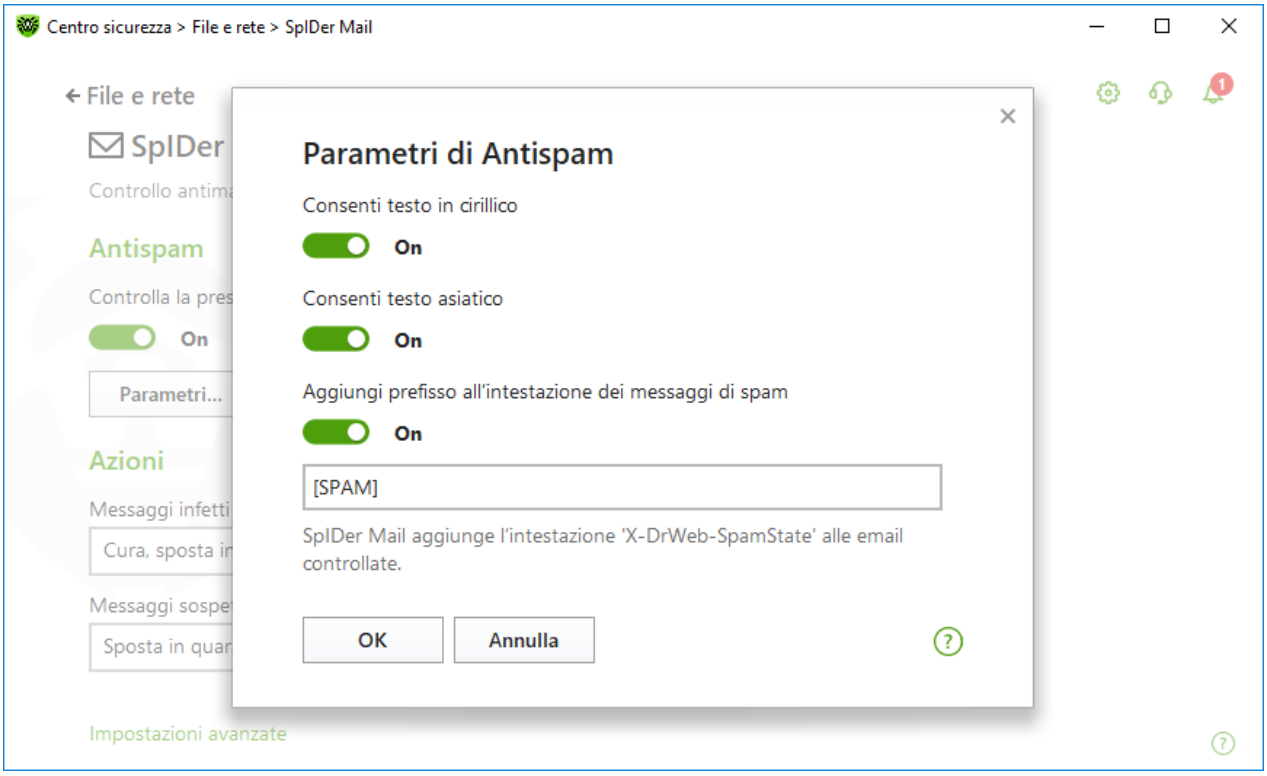

Immagine 41. Parametri di Antispam

Impostazioni di controllo disponibili (attivate di default)

Impostazione	Descrizione
Consenti testo in cirillico	Questa impostazione comanda al componente SpIDer Mail di non classificare come spam senza analisi preliminare le email scritte nella codifica cirillica stabilita. Se questo flag è deselezionato, con grande probabilità il filtro contrassegnerà tali email come spam.
Consenti testo asiatico	Questa impostazione comanda al componente SpIDer Mail di non classificare come spam senza analisi preliminare le email scritte nelle codifiche delle lingue asiatiche più comuni. Se questo flag è deselezionato, con grande probabilità il filtro contrassegnerà tali email come spam.
Aggiungi prefisso all'intestazione dei messaggi di spam	All'inizio dell'oggetto dei messaggi di spam di default viene aggiunta la sottostringa "[SPAM]". È possibile modificare questo valore. Questa impostazione prescrive al componente SpIDer Mail di aggiungere il prefisso specificato agli oggetti delle email riconosciute come spam. L'aggiunta del prefisso aiuterà l'utente a creare le regole per il filtraggio delle email contrassegnate come spam in quei client di posta (per esempio, MS Outlook Express) in cui non è possibile configurare filtri per intestazione dell'email.

3. Cliccare su **OK** per salvare le impostazioni.

Informazioni aggiuntive

Tecnologie del filtro antispam

Le tecnologie del filtro antispam Dr.Web sono costituite da regole che condizionatamente possono essere divise in alcuni gruppi:

- **L'Analisi euristica** — tecnologia di analisi empirica di tutte le parti dell'email: campo dell'intestazione, corpo, contenuto dell'allegato.
- **Il filtraggio della controazione** — tecnologia che consiste nel riconoscimento degli espedienti utilizzati dagli spammer per raggirare filtri antispam.
- **L'analisi basata sulle firme HTML** — tecnologia con cui i messaggi che includono il codice HTML vengono confrontati con i campioni della libreria delle firme HTML dell'antispam. Tale confronto, in combinazione con i dati sulle dimensioni delle immagini di solito utilizzate dai mittenti dello spam protegge gli utenti dai messaggi di spam contenenti link di pagine web.
- **L'analisi semantica** — tecnologia con cui le parole ed espressioni di un messaggio vengono confrontate in base a un dizionario speciale con le parole e locuzioni tipiche dello spam. Vengono sottoposte all'analisi sia le parole, le espressioni e i caratteri visibili che quelli visivamente nascosti tramite espedienti tecnici speciali.

- **La tecnologia anti-scamming** — tecnologia di filtraggio dei messaggi scamming e pharming a cui appartengono le cosiddette "truffe alla nigeriana", i messaggi sulle vincite alla lotteria, al casinò, le false email di banche.
- **Il filtraggio dello spam tecnico** — tecnologia di determinazione dei cosiddetti messaggi bounce che nascono come reazione ai virus o come manifestazione dell'attività di virus. Un modulo speciale dell'antispam identifica tali messaggi come indesiderati.

Elaborazione delle email da parte del filtro antispam

Il componente SpIDer Mail aggiunge a tutte le email controllate le seguenti intestazioni:

- `X-DrWeb-SpamState: <valore>` dove <*valore*> indica se l'email è spam (`Yes`) secondo l'opinione del monitor di posta SpIDer Mail o se non lo è (`No`);
- `X-DrWeb-SpamVersion: <versione>` dove <*versione*> — la versione della libreria di Antispam Dr.Web;
- `X-DrWeb-SpamReason: <punteggio di spam>` dove <*punteggio di spam*> — l'elenco dei punteggi attribuiti all'email secondo le varie categorie di appartenenza allo spam.

Utilizzare queste intestazioni e il prefisso nell'oggetto dell'email (se è selezionata l'opzione corrispondente) per configurare il filtraggio dello spam da parte del programma di posta in uso.

Se per la ricezione delle email si usano i protocolli IMAP/NNTP, configurare il programma di posta in uso in modo che le email vengano caricate dal server di posta per intero, senza visualizzazione in anteprima delle intestazioni. Questo è necessario per il corretto funzionamento del filtro antispam.

Il filtro antispam processa messaggi di posta redatti in conformità con lo standard MIME RFC 822.

Per aumentare la qualità di funzionamento del filtro antispam, è possibile segnalare all'azienda Doctor Web errori di riconoscimento dello spam.

Correzione di errori di riconoscimento

Se si rileva un errore nel funzionamento del filtro antispam:

1. Creare una nuova email e allegare ad essa il messaggio riconosciuto nel modo sbagliato. I messaggi inviati nel testo di email non verranno analizzati.
2. Inviare l'email con l'allegato su uno dei seguenti indirizzi:
   - un'email erroneamente classificata come spam — sull'indirizzo nonspam@drweb.com;
   - un messaggio di spam non riconosciuto dal sistema di filtraggio — sull'indirizzo spam@drweb.com.

8.4. Firewall

Firewall Dr.Web è progettato per proteggere il computer da accessi non autorizzati dall'esterno e prevenire le fughe di dati importanti sulla rete. Questo componente consente di controllare la connessione e il trasferimento dei dati sulla rete e bloccare le connessioni sospette a livello di pacchetto e applicazione.

Firewall fornisce i seguenti vantaggi:

- scansione e filtraggio di tutto il traffico in arrivo e in uscita;
- controllo delle connessioni a livello di applicazione;
- filtraggio dei pacchetti a livello di rete;
- un passaggio rapido da un set di regole a un altro;
- registrazione degli eventi.

Per attivare o disattivare Firewall

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Attivare o disattivare Firewall utilizzando l'interruttore .

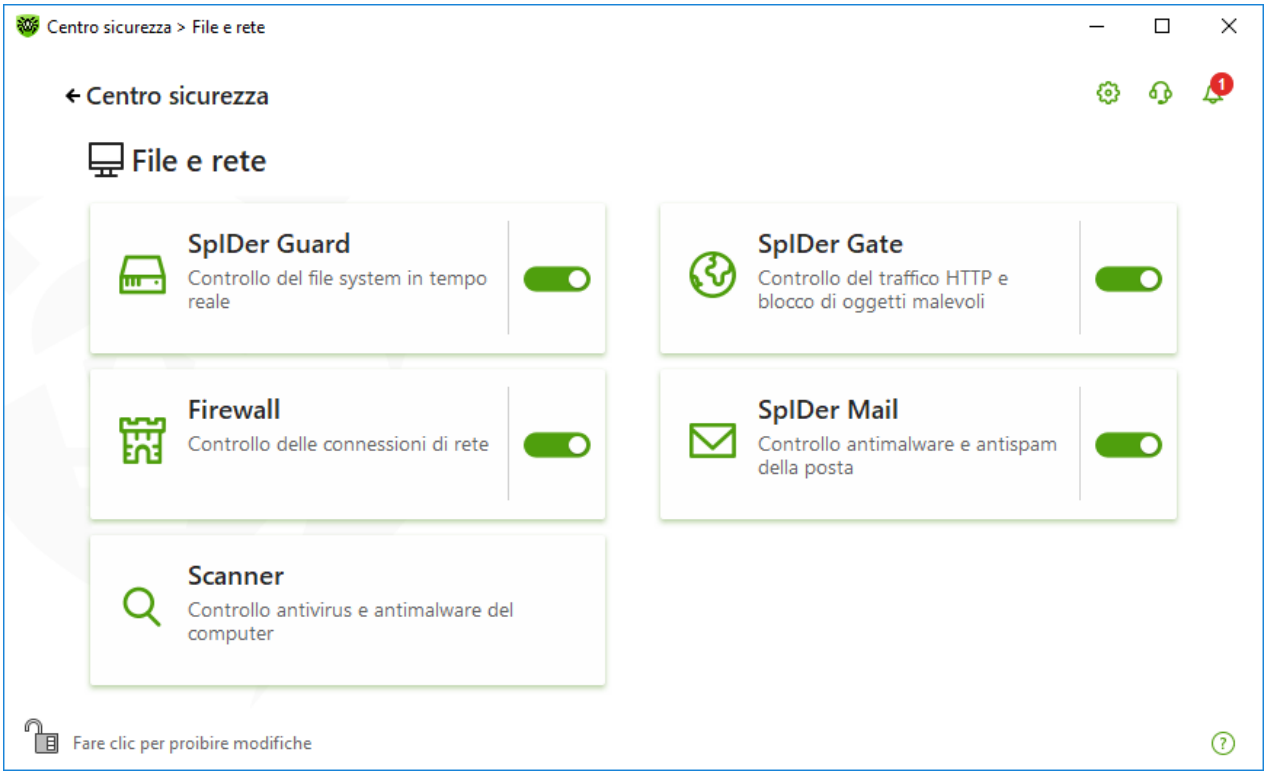

Immagine 42. Attivazione/disattivazione di Firewall

In questa sezione:

- Configurazione di Firewall

- Parametri per applicazioni
- Regole per applicazioni
- Configurazione dei parametri delle regole per applicazioni
- Parametri per reti
- Filtro dei pacchetti
- Set di regole di filtraggio pacchetti
- Creazione di una regola di filtraggio

8.4.1. Parametri di funzionamento di Firewall

In questa sezione è possibile configurare i seguenti parametri di funzionamento di Firewall:

- selezionare la modalità di funzionamento del programma;
- configurare la lista delle applicazioni autorizzate;
- configurare i parametri per le reti conosciute.

> ⚠ Per accedere ai parametri di Firewall, viene richiesta la password se nelle Impostazioni è stata attivata l'opzione **Proteggi da password le impostazioni di Dr.Web**.

Di default Firewall non crea regole per le applicazioni conosciute. A prescindere dalla modalità di funzionamento si effettua la registrazione degli eventi.

Le impostazioni predefinite del programma sono ottimali per la maggior parte degli usi e non dovrebbero essere modificate senza necessità.

Per andare alla selezione della modalità di funzionamento e ai parametri del componente Firewall

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto" ). Altrimenti, cliccare sul lucchetto  .
2. Fare clic sulla piastrella **Firewall**. Si aprirà la finestra dei parametri del componente.

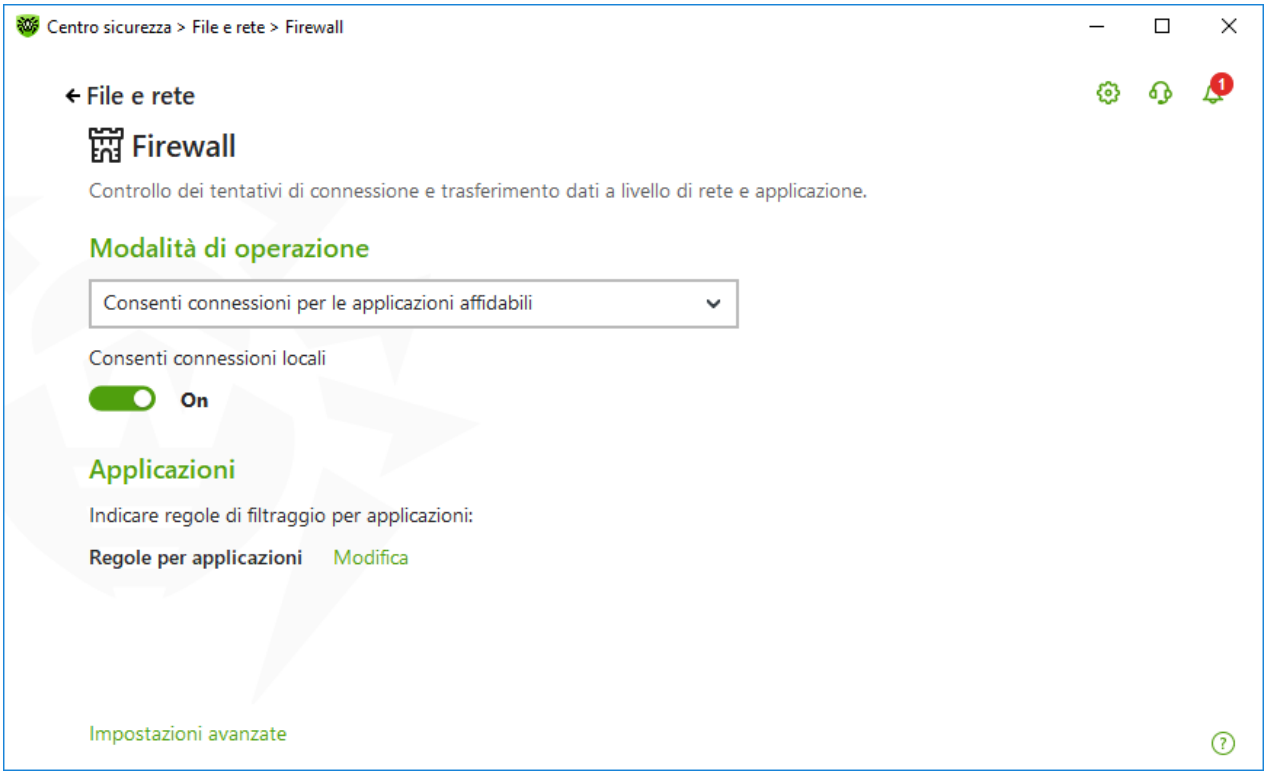

Immagine 43. Parametri di Firewall

L'impostazione **Consenti connessioni locali** permette a tutte le applicazioni di stabilire liberamente le connessioni locali (dall'interfaccia o all'interfaccia 127.0.0.1 (localhost)) sul computer. Questa opzione viene utilizzata dopo la verifica della conformità delle connessioni alle regole impostate. Disattivare questa opzione affinché le regole di filtraggio vengano utilizzate a prescindere da quello se una connessione avviene attraverso la rete o all'interno del computer.

Selezione della modalità di funzionamento

Selezionare una delle seguenti modalità di funzionamento:

Modalità di operazione	Descrizione
Consenti connessioni per le applicazioni affidabili	Questa modalità si usa di default. In questa modalità a tutte le applicazioni affidabili è consentito l'accesso alle risorse di rete, compreso internet. Alle applicazioni affidabili appartengono: le applicazioni di sistema o quelle aventi il certificato Microsoft, nonché applicazioni con una firma digitale valida. Le regole per tali applicazioni non vengono visualizzate nella lista delle regole. Nel caso di altre applicazioni Firewall fornisce la possibilità di proibire o consentire una volta manualmente una connessione sconosciuta, nonché creare una regola per essa. Quando rileva un tentativo di accesso alle risorse di rete da parte del sistema operativo o di un'applicazione utente, Firewall controlla

Modalità di operazione	Descrizione
	se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole, viene visualizzato un avviso corrispondente in cui viene chiesto di selezionare una soluzione provvisoria o creare una regola in base a cui in seguito verranno elaborate tali connessioni.
Consenti connessioni sconosciute	In questa modalità l'accesso alle risorse di rete, compreso internet, viene concesso a tutte le applicazioni sconosciute per le quali non sono impostate regole di filtraggio. Al rilevamento di un tentativo di connessione Firewall non visualizza alcun messaggio.
Modalità interattiva	In questa modalità all'utente viene concesso il completo controllo della reazione di Firewall al rilevamento di una connessione sconosciuta. Quando rileva un tentativo di accesso alle risorse di rete da parte del sistema operativo o di un'applicazione utente, Firewall controlla se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole, viene visualizzato un avviso corrispondente in cui viene chiesto di selezionare una soluzione provvisoria o creare una regola in base a cui in seguito verranno elaborate tali connessioni.
Blocca connessioni sconosciute	In questa modalità vengono bloccate automaticamente tutte le connessioni sconosciute alle risorse di rete, compreso internet. Quando scopre un tentativo di accesso alle risorse di rete da parte del sistema operativo o di un'applicazione dell'utente, Firewall controlla se le regole di filtraggio sono impostate per questi programmi. Se non ci sono regole di filtraggio, Firewall blocca automaticamente l'accesso alla rete e non visualizza alcun avviso. Se sono impostate le regole di filtraggio per questa connessione, vengono eseguite le azioni indicate nelle regole.

Parametri per applicazioni

Tramite il filtraggio a livello di applicazione è possibile controllare l'accesso di specifici programmi e processi alle risorse di rete, nonché consentire o proibire a queste applicazioni di avviare altri processi. È possibile impostare regole sia per le applicazioni dell'utente che per quelle di sistema.

In questa sezione è possibile gestire i set di regole di filtraggio, creando nuove regole, modificando quelle esistenti o eliminando regole non richieste. Un'applicazione viene identificata in modo univoco dal percorso completo del file eseguibile. Per indicare il kernel del sistema operativo Microsoft Windows (il processo system per cui non c'è il file eseguibile corrispondente) si usa il nome `SYSTEM`.

Per ciascun programma non può esserci più di un set di regole di filtraggio.

Se viene creata una regola di blocco per un processo o impostata la modalità Blocca connessioni sconosciute e quindi viene disattivata la regola di blocco o modificata la modalità di funzionamento, il blocco rimarrà attivo fino al successivo tentativo di connessione dopo il riavvio del processo.

Regole per applicazioni

Per andare alla finestra Regole per le applicazioni

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**.
3. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
4. Fare clic sulla piastrella **Firewall**. Si aprirà la finestra dei parametri del componente.
5. Nella sezione delle impostazioni **Regole per le applicazioni** premere **Modifica**. Si aprirà una finestra con una lista di applicazioni per cui sono impostate le regole.

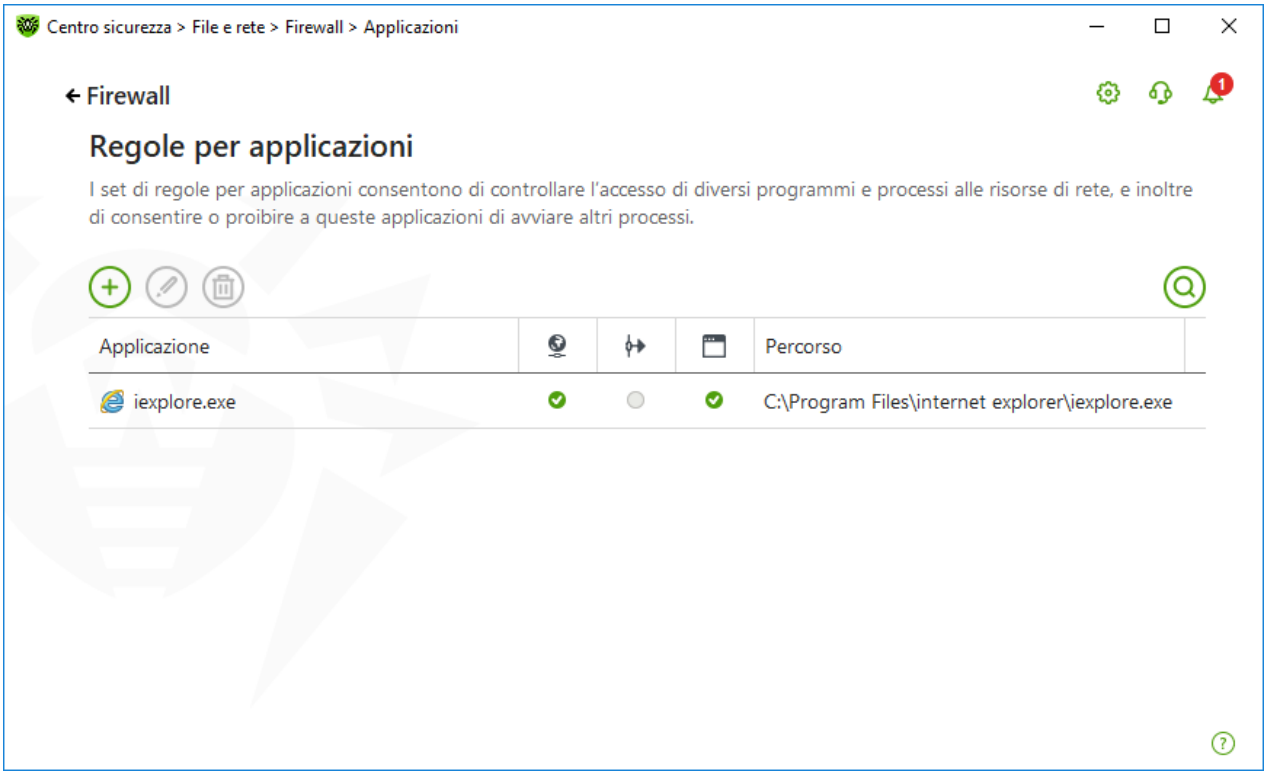

Immagine 44. Regole per applicazioni

6. Per andare alla creazione di un nuovo set di regole o alla modifica di un set di regole esistente, premere il pulsante o selezionare un'applicazione dalla lista e premere il pulsante. Per cercare la regola richiesta, premere il pulsante.

Per le applicazioni che sono già rimosse dal computer le regole non vengono rimosse automaticamente. È possibile rimuovere tali regole, selezionando la voce **Rimuovi le regole non utilizzate** nel menu contestuale della lista.

Modifica di un set di regole esistente o creazione di un nuovo set di regole

È possibile configurare l'accesso di un'applicazione alle risorse di rete e inoltre proibire o consentire l'avvio di altre applicazioni nella finestra **Nuovo set di regole per l'applicazione** (o **Modifica il set di regole per <*nome dell'applicazione*>**).

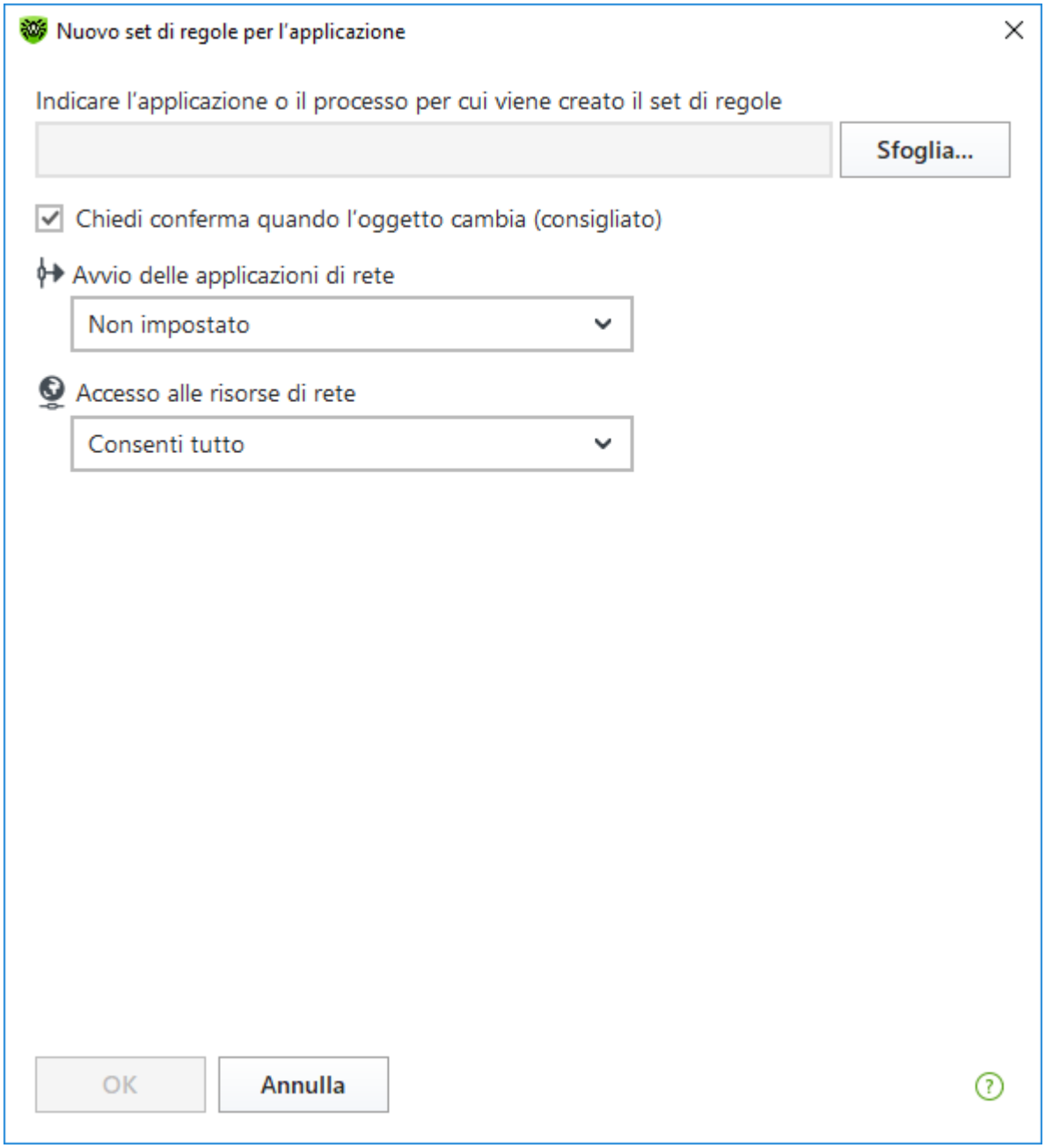

Immagine 45. Creazione di un nuovo set di regole

Avvio di altre applicazioni

Per consentire o proibire a un'applicazione di avviare altre applicazioni, dalla lista a cascata **Avvio delle applicazioni di rete** selezionare:

- **Consenti** per consentire all'applicazione di avviare processi;
- **Blocca** per proibire all'applicazione di avviare processi;
- **Non impostato**. In questo caso a questa applicazione vengono applicate le impostazioni della modalità di funzionamento di Firewall selezionata.

Accesso alle risorse di rete

1. Selezionare la modalità di accesso alle risorse di rete:
   - **Consenti tutto** — tutte le connessioni dell'applicazione saranno consentite;
   - **Blocca tutto** — tutte le connessioni dell'applicazione sono proibite;
   - **Non impostato** — in questo caso a questa applicazione vengono applicate le impostazioni della modalità di funzionamento di Firewall selezionata;
   - **Personalizzato** — in questa modalità è possibile creare un set di regole che consentono o proibiscono alcune connessioni dell'applicazione.
2. Se è selezionata la modalità di accesso alle risorse di rete **Personalizzato**, più in basso viene visualizzata una tabella con le informazioni sul set di regole per questa applicazione.

Parametro	Descrizione
Attivato	Stato della regola.
Azione	Indica l'azione eseguita da Firewall quando un programma tenta di connettersi a internet: • **Blocca pacchetti** — blocca il tentativo di connessione; • **Consenti pacchetti** — consenti la connessione.
Nome regola	Il nome della regola.
Tipo di connessione	La direzione della connessione: • **In arrivo** — la regola si applica se una connessione viene avviata dalla rete a un programma sul computer; • **In uscita** — la regola si applica se una connessione viene avviata da un programma sul computer; • **Qualsiasi** — la regola si applica a prescindere dalla direzione della connessione.
Descrizione	Una descrizione della regola da parte dell'utente.

3. Se necessario, modificare un set di regole predefinito o creare un nuovo set di regole per l'applicazione.
4. Se si è scelta la creazione di una nuova regola o la modifica di una regola esistente, configurarne i parametri nella finestra che si è aperta.
5. Dopo aver finito di modificare un set di regole, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per rifiutare le modifiche. Le modifiche apportate a un set di regole vengono salvate se si passa a un altra modalità.

Spuntare il flag **Chiedi conferma quando l'oggetto cambia (consigliato)** se si vuole che l'accesso di un'applicazione alle risorse di rete venga richiesto di nuovo quando le applicazioni vengono modificate o aggiornate.

Creazione delle regole per applicazioni dalla finestra di avviso di Firewall

Quando Firewall funziona in modalità interattiva Consenti connessioni per le applicazioni affidabili, è possibile creare un set di regole direttamente dalla finestra di avviso di tentativo di connessione non autorizzata.

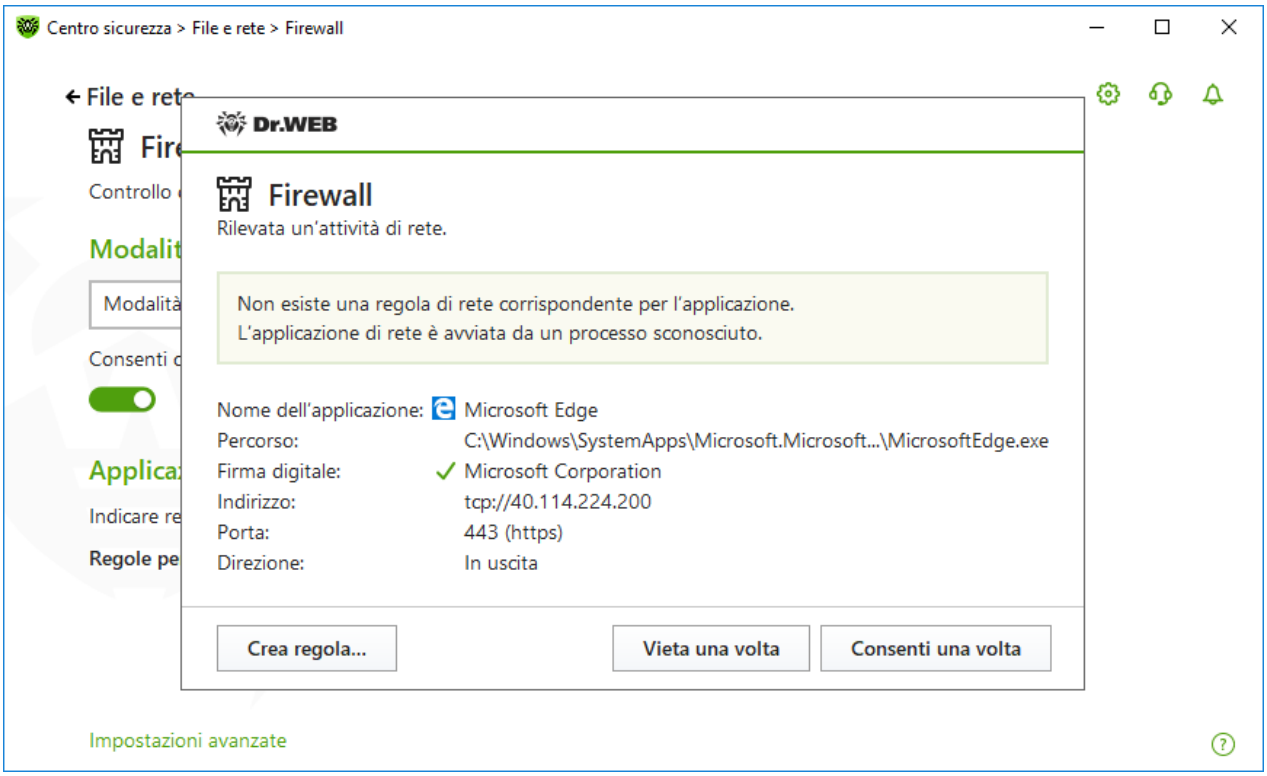

Immagine 46. Esempio di avviso su un tentativo di accesso alla rete

Se viene utilizzato un account con permessi limitati (Ospite), Firewall Dr.Web non visualizza all'utente gli avvisi di tentativi di accesso alla rete. Gli avvisi verranno visualizzati sotto l'account amministratore, se tale sessione è attiva contemporaneamente alla sessione ospite.

Per impostare regole per applicazioni

1. Quando viene rilevato un tentativo di un'applicazione di connessione alla rete, leggere le seguenti informazioni:

Campo	Descrizione
Nome dell'applicazione	Il nome del programma. Assicurarsi che il percorso indicato nel campo **Percorso** corrisponda alla posizione corretta del programma.
Percorso	Il percorso completo del file eseguibile dell'applicazione e il suo nome.

Campo	Descrizione
Firma digitale	La firma digitale dell'applicazione.
Indirizzo	Il protocollo e l'indirizzo dell'host a cui l'applicazione tenta di connettersi.
Porta	La porta su cui l'applicazione tenta di connettersi.
Direzione	La direzione della connessione.

2. Decidere sull'operazione adatta in questo caso e selezionare l'azione corrispondente nella parte inferiore della finestra:
   - per vietare una volta la connessione dell'applicazione sulla porta specificata, selezionare l'azione **Vieta una volta**;
   - per consentire una volta all'applicazione di connettersi sulla porta specificata, selezionare l'azione **Consenti una volta**;
   - per andare al modulo di creazione della regola di filtraggio, selezionare l'azione **Crea la regola**. Si apre una finestra in cui è possibile selezionare una regola predefinita o creare manualmente una regola per applicazioni.
3. Premere il pulsante **OK**. Firewall eseguirà l'operazione impostata e la finestra di avviso si chiuderà.

In alcuni casi, il sistema operativo Windows non consente di identificare in modo univoco un servizio che funziona come un processo di sistema. Quando Firewall scopre un tentativo di connessione da parte di un processo di sistema, notare la porta indicata nelle informazioni sulla connessione. Se si utilizza un'applicazione che può connettersi sulla porta indicata, consentire questa connessione.

Se il programma che tenta di stabilire la connessione è già conosciuto da Firewall (cioè per esso sono impostate regole di filtraggio), ma viene avviato da un'altra applicazione sconosciuta (processo padre), Firewall visualizza un avviso corrispondente.

Per impostare regole per processi padre

1. Quando Firewall scopre un tentativo di connessione alla rete da parte di un'applicazione avviata da un programma sconosciuto da Firewall, leggere le informazioni sul file eseguibile del programma padre.
2. Quando si deciderà sull'operazione adatta in questo caso, eseguire una delle seguenti azioni:
   - per bloccare una volta solo la connessione dell'applicazione alla rete, premere il pulsante **Blocca**;
   - per consentire una volta solo all'applicazione di connettersi alla rete, premere il pulsante **Consenti**;
   - per creare una regola, premere **Crea la regola** e nella finestra che si è aperta configurare le impostazioni necessarie per il processo padre.

3. Premere il pulsante **OK**. Firewall eseguirà l'operazione impostata e la finestra di avviso si chiuderà.

Inoltre, è possibile una situazione in cui un'applicazione sconosciuta viene avviata da un'altra applicazione sconosciuta. In tale caso l'avviso includerà le informazioni corrispondenti, e alla selezione di **Crea la regola** si aprirà una finestra in cui è possibile configurare le regole sia per le applicazioni che per i processi padre.

Configurazione dei parametri della regola

Le regole di filtraggio regolano la comunicazione di rete di un programma con specifici host sulla rete.

Per creare o modificare una regola

1. Nella voce **Accesso alle risorse di rete** selezionare la modalità **Personalizzato**.
2. Nella finestra **Modifica il set di regole per** premere il pulsante ⊕ per aggiungere una nuova regola, o selezionare una regola dalla lista e premere il pulsante ✎ per modificare la regola.
3. Impostare i seguenti parametri della regola:

Parametro	Descrizione
Generale	
Nome regola	Il nome della regola che viene creata/modificata.
Descrizione	Una breve descrizione della regola.
Azione	Indica l'azione eseguita da Firewall quando un programma tenta di connettersi a internet: • **Blocca pacchetti** — blocca il tentativo di connessione; • **Consenti pacchetti** — consenti la connessione.
Stato	Stato della regola: • **Attivato** — la regola viene applicata; • **Disattivato** — la regola non viene temporaneamente applicata.
Tipo di connessione	La direzione della connessione: • **In arrivo** — la regola si applica se una connessione viene avviata dalla rete a un programma sul computer; • **In uscita** — la regola si applica se una connessione viene avviata da un programma sul computer; • **Qualsiasi** — la regola si applica a prescindere dalla direzione della connessione.

Parametro	Descrizione
Registrazione del log	Modalità di registrazione del log: • **Attivato** — registra eventi; • **Disattivato** — non salvare informazioni sulla regola.
Impostazioni della regola	
Protocollo	I protocolli del livello di rete e di trasporto attraverso cui avviene la connessione. Sono supportati i seguenti protocolli del livello di rete: • IPv4; • IPv6; • IP all — un protocollo IP di qualsiasi versione. Sono supportati i seguenti protocolli del livello di trasporto: • TCP; • UDP; • TCP & UDP — protocollo TCP o UDP; • RAW.
Indirizzo locale/Indirizzo remoto	L'indirizzo IP dell'host remoto che partecipa alla connessione. È possibile indicare sia un indirizzo specifico (**Pari a**) che un intervallo di indirizzi (**Nell'intervallo**), nonché una maschera di una sottorete specifica (**Maschera**) o maschere di tutte le sottoreti in cui il computer ha un indirizzo di rete (**MY_NETWORK**). Per impostare la regola per tutti gli host, selezionare la variante **Qualsiasi**.
Porta locale/Porta remota	La porta su cui avviene la connessione. È possibile indicare sia una porta specifica (**Pari a**) che un intervallo di porte (**Nell'intervallo**). Per impostare la regola per tutte le porte, selezionare la variante **Qualsiasi**.

4. Premere il pulsante **OK**.

Parametri per reti

Il filtraggio a livello di pacchetto consente di controllare l'accesso alla rete a prescindere dai programmi che avviano la connessione. Le regole vengono applicate a tutti i pacchetti di rete di un determinato tipo che vengono trasmessi tramite una delle interfacce di rete del computer.

Questo tipo di filtraggio fornisce metodi di controllo generali a differenza del filtraggio a livello di applicazione.

Filtro dei pacchetti

Nella finestra **Rete** è possibile impostare un set di regole di filtraggio dei pacchetti trasmessi attraverso una specifica interfaccia.

Per andare alla finestra Rete

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta selezionare la sezione **File e rete**.
3. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto.
4. Fare clic sulla piastrella **Firewall**. Si aprirà la finestra dei parametri del componente.
5. Espandere il gruppo **Impostazioni avanzate**.
6. Nella sezione delle impostazioni **Parametri di utilizzo per le reti conosciute** premere **Modifica**. Si aprirà una finestra con una lista di interfacce di rete per cui sono impostate le regole.

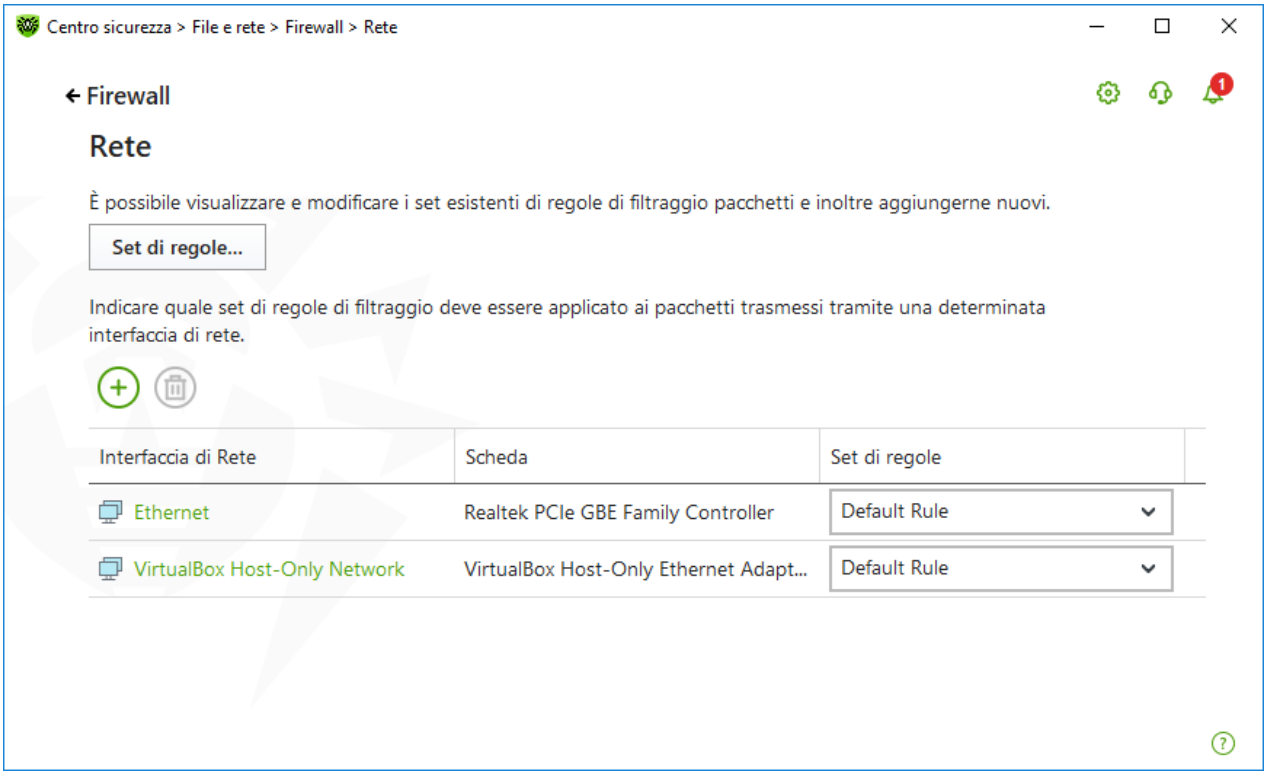

Immagine 47. Set di regole per interfacce di rete

7. Trovare nella lista l'interfaccia desiderata e abbinarla al set di regole corrispondente. Se nella lista non è disponibile un set di regole adatto, crearlo.

Firewall viene fornito con i seguenti set di regole predefiniti:

- **Default Rule** — le regole che descrivono le configurazioni di rete più comuni ed attacchi diffusi (si usa di default per tutte le nuove interfacce);
- **Allow All** — tutti i pacchetti vengono consentiti;
- **Block All** — tutti i pacchetti vengono bloccati.

Per un utilizzo comodo e un passaggio veloce tra le modalità di filtraggio, si possono impostare ulteriori set di regole.

Per vedere tutte le interfacce disponibili o aggiungere alla tabella una nuova interfaccia, premere il pulsante ⊕. Nella finestra che si è aperta è possibile indicare quali interfacce devono essere sempre visualizzate nella tabella. Le interfacce attive verranno visualizzate automaticamente nella tabella.

Le interfacce di rete non attive possono essere cancellate dalla tabella visualizzata, premendo il pulsante 🗑.

Per visualizzare i parametri di un'interfaccia di rete, fare clic sul suo nome.

Impostazioni del filtro pacchetti

Per gestire i set di regole esistenti e per aggiungerne nuovi, andare alla finestra **Impostazioni del filtro pacchetti** premendo il pulsante **Set di regole**.

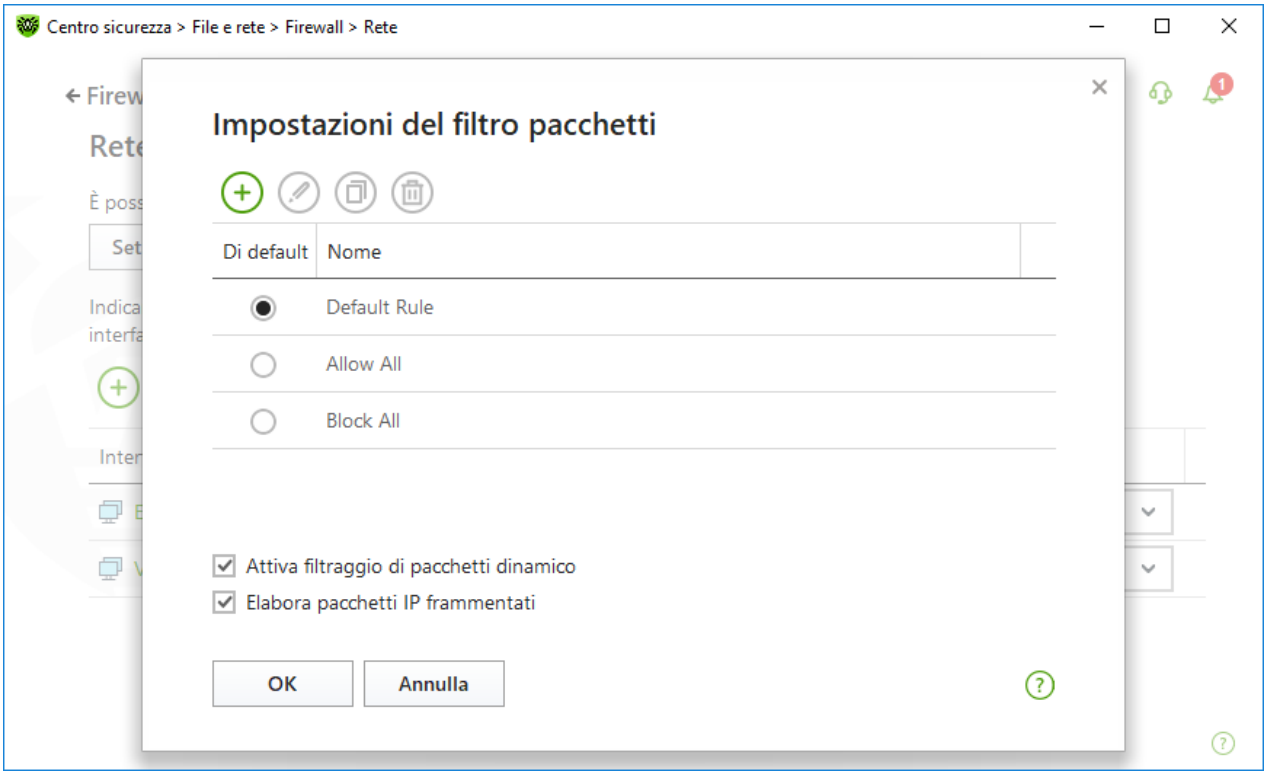

Immagine 48. Finestra Impostazioni del filtro pacchetti

Su questa pagina è possibile:

- gestire i set di regole di filtraggio creando nuove regole, modificando quelle esistenti o eliminando regole non richieste;
- impostare i parametri di filtraggio addizionali.

Gestione del set di regole

Per gestire un set di regole, eseguire una delle seguenti azioni:

- per creare un set di regole per un'interfaccia di rete, premere ⊕;
- per modificare un set di regole esistente, selezionarlo dalla lista e premere ✎;
- per aggiungere una copia di un set di regole esistente, premere ⧉. La copia viene aggiunta sotto il set di regole selezionato;
- per rimuovere un set di regole selezionato, premere 🗑.

Impostazioni avanzate

Per configurare le impostazioni avanzate del filtraggio pacchetti, nella finestra **Impostazioni del filtro pacchetti** selezionare i seguenti flag:

Flag	Descrizione
Attiva filtraggio di pacchetti dinamico	Spuntare questo flag per tenere conto dello stato della connessione TCP nel filtraggio e per far passare solo i pacchetti di cui il contenuto corrisponde allo stato attuale. In tale caso vengono bloccati tutti i pacchetti che vengono trasmessi nei limiti della connessione ma non soddisfano le specifiche del protocollo. Questo meccanismo consente di proteggere meglio il computer dagli attacchi DoS (Denial of Service, Negazione del servizio), dalla scansione delle risorse, dall'introduzione di dati e da altre operazioni malevole. Inoltre, è consigliabile selezionare questo flag se vengono utilizzati i protocolli con algoritmi complessi di trasmissione di dati (FTP, SIP ecc.). Deselezionare questo flag per filtrare pacchetti senza tenere conto delle connessioni TCP.
Elabora pacchetti IP frammentati	Spuntare questo flag per elaborare correttamente la trasmissione di grandi quantità di dati. La dimensione massima del pacchetto (MTU — Maximum Transmission Unit) può variare in diverse reti, perciò nella trasmissione alcuni pacchetti IP possono essere suddivisi in più frammenti. In caso di utilizzo di questa opzione, a tutti i pacchetti frammentati viene applicata la stessa azione prevista dalle regole di filtraggio per il pacchetto principale (il primo). Deselezionare questo flag per elaborare tutti i pacchetti separatamente.

Premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per uscire dalla finestra senza salvare le modifiche.

Set di regole di filtraggio pacchetti

Nella finestra **Modifica set di regole** viene visualizzata una lista delle regole di filtraggio pacchetti, incluse in uno specifico set. Si può gestire la lista aggiungendo nuove regole o modificando quelle esistenti, nonché si può cambiare l'ordine di esecuzione delle regole. Le regole vengono applicate consecutivamente secondo l'ordine nella lista.

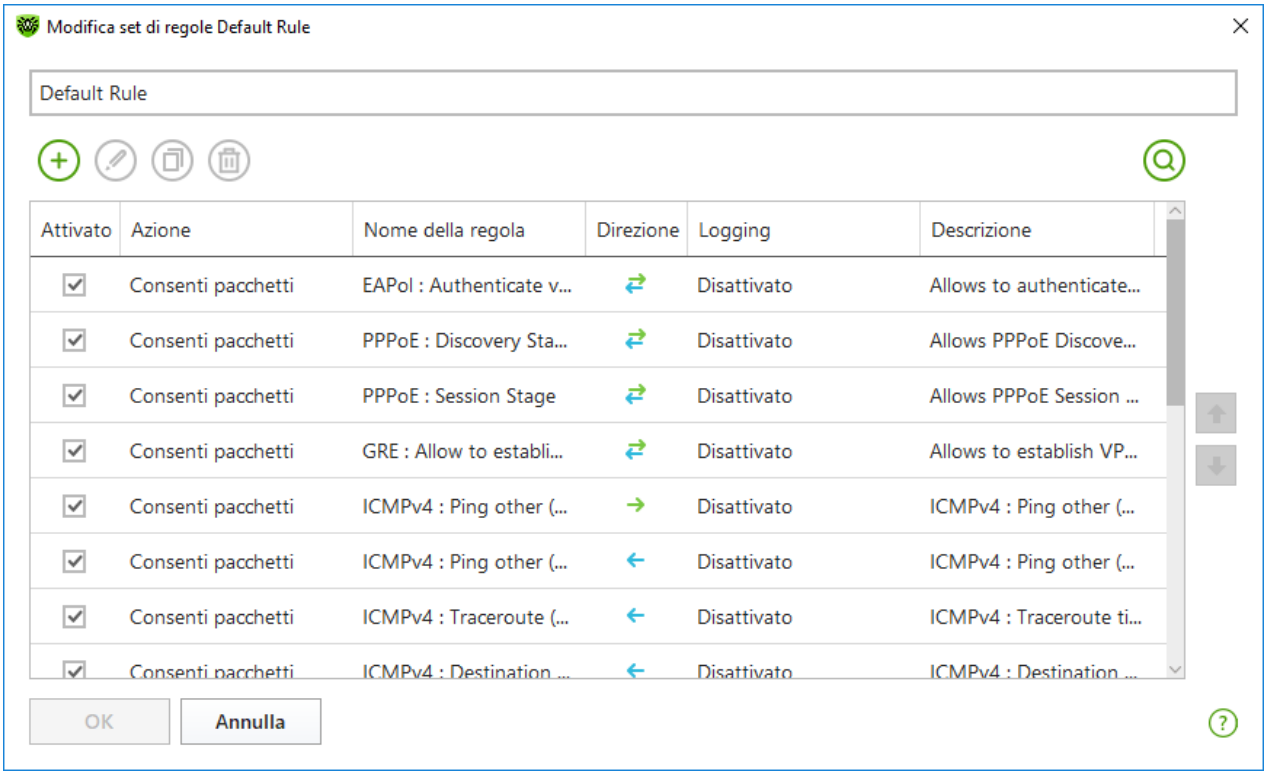

Immagine 49. Set di regole di filtraggio pacchetti

Per ogni regola nella lista vengono fornite le seguenti brevi informazioni:

Parametro	Descrizione
Attivato	Stato della regola.
Azione	Indica l'azione eseguita da Firewall quando elabora un pacchetto: • **Blocca pacchetti** — blocca il pacchetto; • **Consenti pacchetti** — trasmetti il pacchetto.
Nome regola	Il nome della regola.
Direzione	La direzione della connessione: • ← — la regola si applica se il pacchetto viene ricevuto dalla rete;

Parametro	Descrizione
	• → — la regola si applica se il pacchetto viene inviato dal computer; • ⇄ – la regola si applica a prescindere dalla direzione della connessione.
Registrazione del log	Modalità di registrazione di eventi. Indica quali informazioni devono essere registrate nel log: • **Solo le intestazioni** — registra nel log soltanto le intestazioni dei pacchetti; • **Pacchetto intero** — registra nel log il pacchetto per intero; • **Disattivato** — non salvare informazioni sul pacchetto.
Descrizione	Una breve descrizione della regola.

Per modificare o creare un set di regole

1. Se necessario, impostare un nome o modificare il nome del set di regole.
2. Creare regole di filtraggio, utilizzando le seguenti opzioni:
   - per aggiungere una nuova regola, premere ⊕. La regola viene aggiunta in cima alla lista;
   - per modificare una regola selezionata, premere ✎;
   - per aggiungere una copia di una regola selezionata, premere il pulsante ⧉. La copia viene aggiunta davanti alla regola selezionata;
   - per rimuovere una regola selezionata, premere 🗑;
   - per trovare la regola richiesta nella lista, premere 🔍.
3. Se si è scelta la creazione di una nuova regola o la modifica di una regola esistente, configurarne i parametri.
4. Utilizzare le frecce a destra della lista per definire l'ordine di esecuzione delle regole. Le regole vengono eseguite consecutivamente secondo l'ordine nella lista.
5. Dopo aver finito di modificare la lista, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per rifiutare le modifiche.

⚠ I pacchetti per cui non ci sono regole nel set vengono bloccati automaticamente. Le eccezioni sono i pacchetti che vengono autorizzati dalle regole nel Filtro delle applicazioni.

Configurazione dei parametri della regola di filtraggio

Per aggiungere o modificare una regola di filtraggio

1. Nella finestra di configurazione del set di regole per il filtro dei pacchetti premere il pulsante ⊕ o il pulsante ✎. Si apre la finestra di creazione o modifica della regola di filtraggio pacchetti.

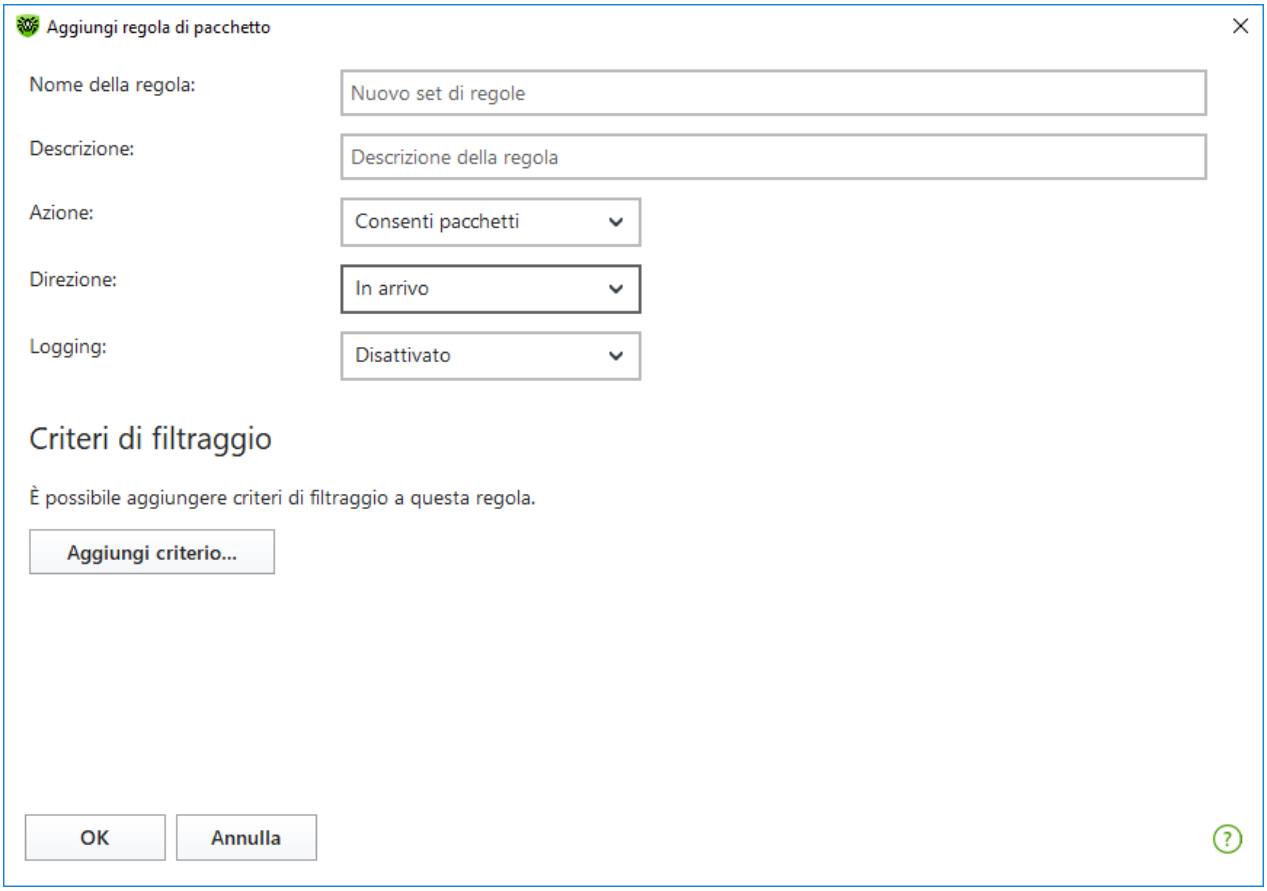

Immagine 50. Aggiunta di una regola di filtraggio

2. Impostare i seguenti parametri della regola:

Parametro	Descrizione
Nome regola	Il nome della regola che viene creata/modificata.
Descrizione	Una breve descrizione della regola.
Azione	Indica l'azione eseguita da Firewall quando elabora un pacchetto: • **Blocca pacchetti** — blocca il pacchetto; • **Consenti pacchetti** — trasmetti il pacchetto.
Direzione	La direzione della connessione: • **In arrivo** — la regola si applica se il pacchetto viene ricevuto dalla rete; • **In uscita** — la regola si applica se il pacchetto viene inviato dal computer; • **Qualsiasi** — la regola si applica a prescindere dalla direzione della connessione.
Registrazione del log	Modalità di registrazione di eventi. Indica quali informazioni devono essere registrate nel log: • **Pacchetto intero** — registra nel log il pacchetto per intero; • **Solo le intestazioni** — registra nel log soltanto le intestazioni dei pacchetti; • **Disattivato** — non salvare informazioni sul pacchetto.

3. Se necessario, aggiungere un criterio di filtraggio, per esempio, un protocollo di trasporto o di rete, premendo il pulsante **Aggiungi criterio**. Si aprirà la finestra **Aggiungi criterio di filtraggio**:

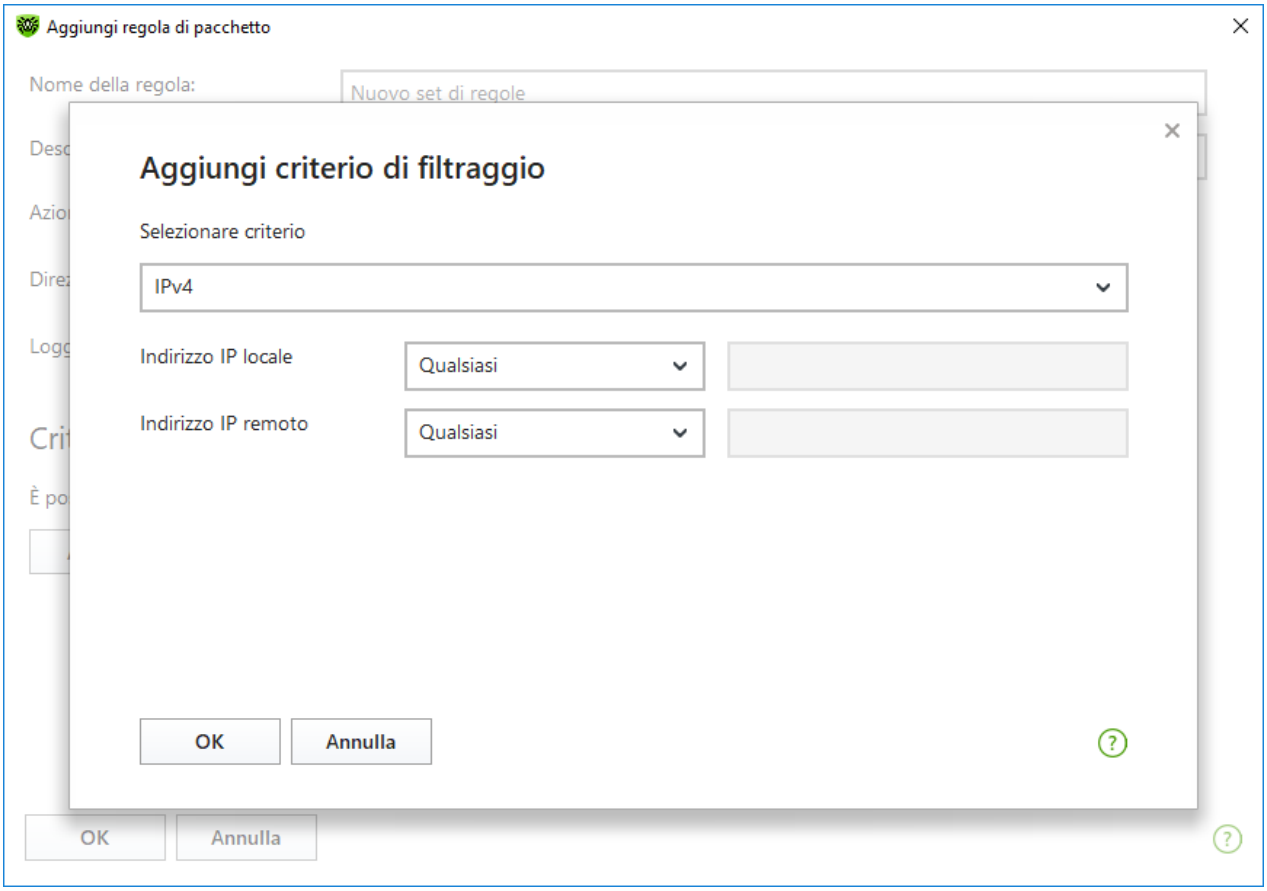

Immagine 51. Aggiunta di un criterio di filtraggio

Selezionare il criterio desiderato nella lista a cascata. Nella stessa finestra è possibile configurare i parametri per il criterio selezionato. È possibile aggiungere qualsiasi numero desiderato di criteri. In tale caso, affinché l'azione dalla regola venga applicata a un pacchetto, il pacchetto deve soddisfare tutti i criteri della regola.

Per alcune intestazioni sono disponibili criteri di filtraggio addizionali. Tutti i criteri aggiunti vengono visualizzati nella finestra di modifica della regola di pacchetto e sono modificabili.

4. Dopo aver finito di modificare, premere il pulsante **OK** per salvare le modifiche apportate o il pulsante **Annulla** per uscire dalla finestra senza salvare le modifiche.

Se non è stato aggiunto alcun criterio di filtraggio, questa regola consentirà o bloccherà tutti i pacchetti (a seconda dell'impostazione nel campo **Azione**).

Se in questa regola all'interno dell'intestazione IPv4 per i parametri **Indirizzo IP locale** e **Indirizzo IP remoto** viene impostato il valore **Qualsiasi**, la regola funzionerà per qualsiasi pacchetto che contenga l'intestazione IPv4 e che sia stato inviato dall'indirizzo fisico del computer locale.

8.5. Scansione del computer

La scansione antivirus del computer viene eseguita dal componente Scanner. Scanner controlla i settori di avvio, la memoria, nonché singoli file e oggetti inclusi in strutture complesse (archivi compressi, container di file, email con allegati). La scansione viene eseguita con l'utilizzo di tutti i metodi di rilevamento delle minacce.

Al rilevamento di un oggetto malevolo Scanner solo avvisa della minaccia. Il report sui risultati della scansione viene riportato in una tabella in cui è possibile selezionare l'azione richiesta per elaborare l'oggetto malevolo o sospetto rilevato. È possibile applicare le azioni predefinite a tutte le minacce rilevate o selezionare un metodo di elaborazione richiesto per singoli oggetti.

Le azioni predefinite sono ottimali nella maggior parte dei casi, ma se necessario, è possibile modificarle nella finestra di configurazione dei parametri di funzionamento del componente Scanner. Mentre l'azione per un singolo oggetto può essere selezionata dopo la fine di una scansione, le impostazioni generali per la neutralizzazione di tipi di minacce specifici devono essere configurate prima dell'inizio della scansione.

Vedi inoltre:

- Parametri di scansione dei file
- Avvio della scansione e le modalità di scansione
- Neutralizzazione delle minacce rilevate

8.5.1. Avvio della scansione e le modalità di scansione

Per avviare la scansione dei file

Se si usano i sistemi operativi Windows Vista, Windows Server 2003 e versioni successive, è consigliabile avviare Scanner con i permessi di amministratore. Altrimenti, non verranno controllati i file e le cartelle a cui non ha accesso un utente senza permessi di amministratore (comprese le cartelle di sistema).

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **File e rete**, quindi sulla piastrella **Scanner**.

Inoltre, è possibile avviare una scansione di file, espandendo nel menu **Start** il gruppo **Dr.Web** e selezionando la voce **Scanner Dr.Web**.

3. Selezionare la modalità di scansione richiesta:
   - la voce **Rapida** per verificare le sole aree critiche di Windows;
   - la voce **Completa** per verificare tutti i file su dischi logici e supporti rimovibili;

- la voce **Personalizzata** per verificare i soli oggetti specificati dall'utente. Si apre la finestra di selezione dei file da verificare tramite Scanner.

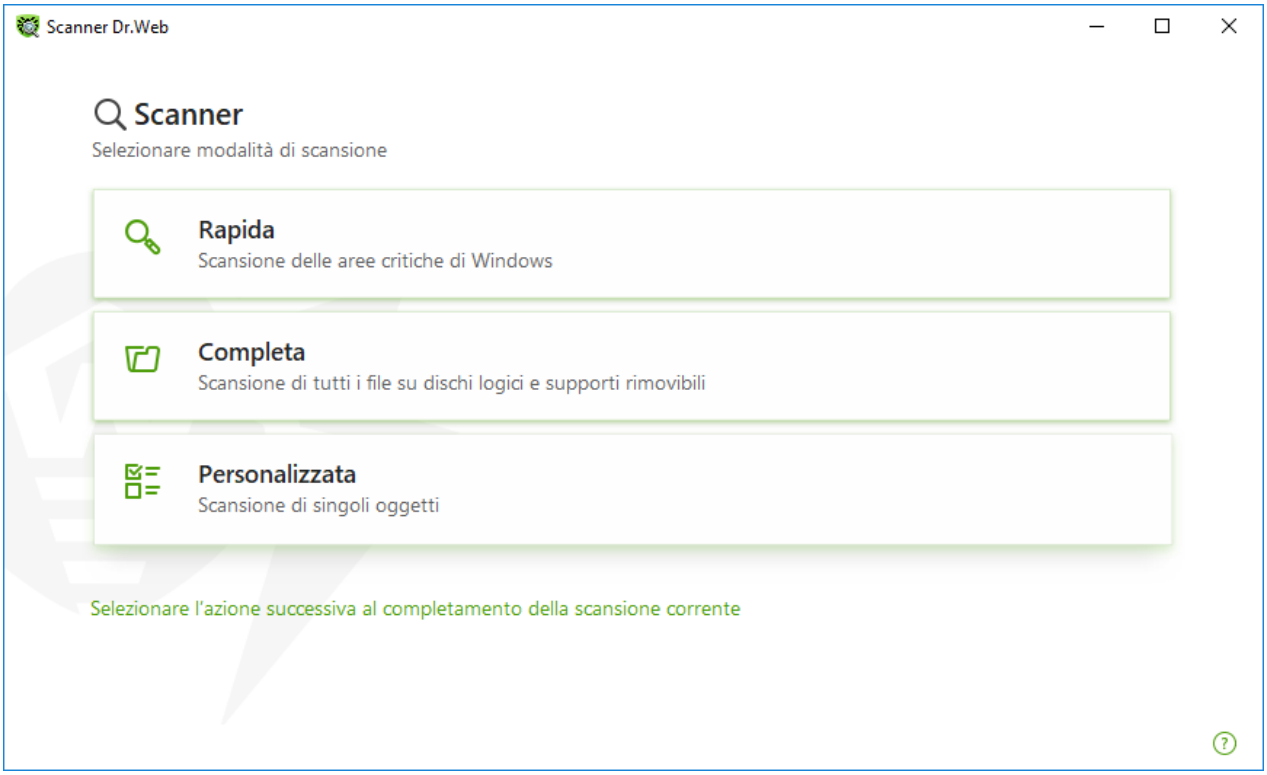

Immagine 52. Selezione della modalità di scansione

È inoltre possibile selezionare un'azione dopo il processo di scansione corrente facendo clic sul link corrispondente nella parte inferiore della finestra. Questa azione non dipende da quella selezionata nelle impostazioni di Scanner e non influisce sulle impostazioni generali.

4. Inizierà il processo di scansione. Per sospendere la scansione, premere il pulsante **Pausa**, per arrestare completamente la scansione, premere il pulsante **Stop**.

> Il pulsante **Pausa** non è disponibile durante la scansione della memoria operativa e dei processi.

Dopo la fine di una scansione Scanner informa delle minacce rilevate e propone di neutralizzarle.

Per verificare un file o una cartella specifica

1. Invocare il menu contestuale cliccando con il tasto destro del mouse sul nome di un file o una cartella (sul Desktop o nell'Esplora risorse del sistema operativo Windows).
2. Selezionare la voce **Scansiona tramite Dr.Web**. La verifica verrà eseguita in base alle impostazioni predefinite.

Descrizione delle modalità di scansione

Modalità di controllo	Descrizione
Rapida	In questa modalità vengono controllati i seguenti oggetti: • settori di avvio di tutti i dischi; • memoria operativa; • cartella principale del disco di avvio; • cartella di sistema di Windows; • cartella "Documenti"; • file temporanei; • punti di ripristino del sistema; • ricerca dei rootkit (se il processo di scansione è stato avviato dall'account amministratore). ⚠ Gli archivi compressi e i file di email non vengono controllati in questa modalità.
Completa	In questa modalità viene eseguita una scansione completa della memoria operativa e di tutti i dischi rigidi (compresi i settori di avvio), nonché viene controllata la presenza di rootkit.
Personalizzata	In questa modalità è possibile controllare qualsiasi file e cartella, nonché oggetti come memoria operativa, settori di avvio ecc. Per aggiungere oggetti alla lista della scansione, premere il pulsante ⊕.

8.5.2. Neutralizzazione delle minacce rilevate

Dopo la fine di una scansione Scanner informa delle minacce rilevate e propone di neutralizzarle.

⚠ Se nelle impostazioni di Scanner Dr.Web è stata selezionata la voce **Neutralizza le minacce rilevate** o **Neutralizza le minacce rilevate e spegni il computer** per l'impostazione **Al termine della scansione**, la neutralizzazione delle minacce verrà eseguita in maniera automatica.

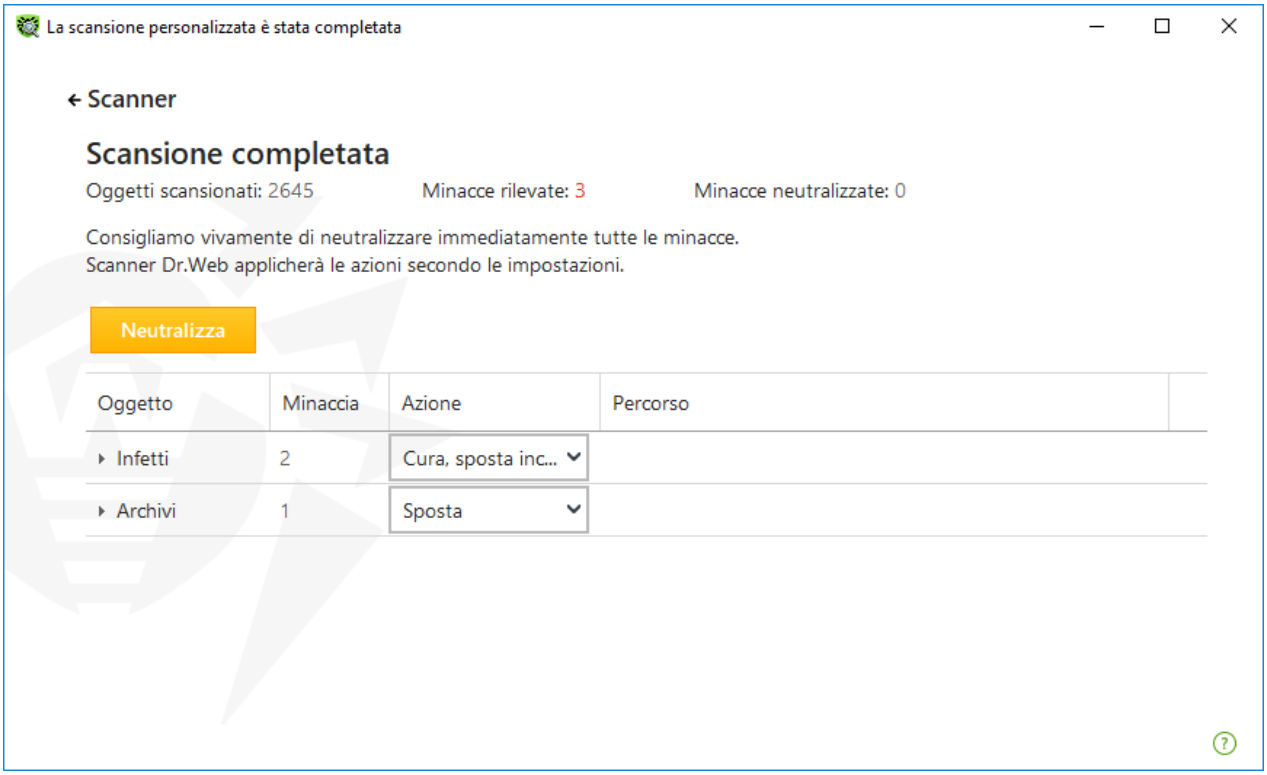

Immagine 53. Selezione dell'azione dopo la fine della scansione

La tabella con i risultati della scansione contiene le seguenti informazioni:

Colonna	Descrizione
Oggetto	In questa colonna è indicato il nome dell'oggetto infetto o sospetto (nome di file — se è infetto un file, **Boot sector** se è infetto un settore di avvio, **Master Boot Record** se è infetto l'MBR di un disco rigido).
Minaccia	In questa colonna è indicato il nome del virus o di una variante del virus secondo la classificazione interna dell'azienda Doctor Web. Nel caso di oggetti sospetti viene indicato che l'oggetto "è probabilmente infetto" e viene specificato il tipo di possibile virus secondo la classificazione dell'analisi euristica.
Azione	In questa colonna è indicata l'azione per la minaccia trovata secondo le impostazioni di Scanner. Tramite la lista a cascata è possibile impostare un'azione per la minaccia selezionata.
Percorso	In questa colonna è indicato il percorso completo del file corrispondente.

Neutralizzazione di tutte le minacce nella tabella

Per ciascuna minaccia è indicata un'azione secondo le impostazioni di Scanner. Per neutralizzare tutte le minacce utilizzando le azioni indicate nella tabella, premere il pulsante **Neutralizza**.

Per modificare l'azione per una minaccia, indicata nella tabella

1. Selezionare un oggetto o un gruppo di oggetti.
2. Nela colonna **Azione** nella lista a cascata selezionare l'azione desiderata.
3. Premere il pulsante **Neutralizza**. Scanner inizierà a neutralizzare tutte le minacce elencate nella tabella.

Neutralizzazione delle minacce selezionate

È inoltre possibile neutralizzare le minacce selezionate separatamente. Per fare questo:

1. Selezionare un oggetto, più oggetti (tenendo premuto il tasto CTRL) o un gruppo di oggetti.
2. Aprire il menu contestuale facendo clic con il tasto destro del mouse e selezionare l'azione desiderata. Scanner inizierà a neutralizzare solo la minaccia selezionata (le minacce selezionate).

Limitazioni alla neutralizzazione delle minacce

Esistono le seguenti limitazioni:

- non è possibile curare oggetti sospetti;
- non è possibile spostare o rimuovere gli oggetti che non sono file (per esempio settori di avvio);
- non è possibile applicare qualsiasi azione a singoli file situati all'interno di archivi compressi, pacchetti di installazione o inclusi come parte di email — in tali casi l'azione viene applicata solo all'intero oggetto.

Report sul funzionamento di Scanner

Di default un report dettagliato sul funzionamento del componente viene salvato nel file di log `dwscanner.log` situato nella cartella `%USERPROFILE%\Doctor Web`.

8.5.3. Funzionalità avanzate

Questa sezione contiene informazioni sulle funzionalità aggiuntive dello Scanner:

- Avvio dello Scanner con i parametri della riga di comando
- Scanner console

Avvio dello Scanner con i parametri della riga di comando

È possibile avviare Scanner in modalità a riga di comando. Tale modo permette di configurare come parametri di avvio le impostazioni addizionali della sessione di scansione corrente e una lista di oggetti da scansionare.

La sintassi del comando di avvio è la seguente:

`[<percorso_del_programma>]dwscanner [<opzioni>] [<oggetti>]`

Opzioni — parametri della riga di comando che configurano le impostazioni del programma. Se non sono presenti, la scansione viene eseguita con le impostazioni salvate in precedenza (o con le impostazioni predefinite, se non sono state modificate). Le opzioni iniziano con il carattere "/" e, come gli altri parametri della riga di comando, vengono separate da spazi.

La lista degli oggetti di scansione può essere vuota o contenere diversi elementi separati da spazi. Se il percorso degli oggetti di scansione non è indicato, la ricerca viene eseguita nella cartella di installazione di Dr.Web.

Le seguenti varianti di indicazione degli oggetti di scansione vengono più comunemente utilizzate:

- `/FAST` — esegui una scansione rapida del sistema.
- `/FULL` — esegui una scansione completa di tutti i dischi rigidi e supporti rimovibili (compresi i settori di avvio).
- `/LITE` — esegui una scansione iniziale del sistema con cui vengono controllati la memoria operativa e i settori di avvio di tutti i dischi, inoltre esegui una verifica della presenza di rootkit.

Scanner console

La lista dei componenti Dr.Web include anche Scanner console che consente di eseguire le scansioni in modalità a riga di comando, e inoltre fornisce ampie possibilità di configurazione.

Scanner console mette oggetti sospetti in Quarantena.

Per avviare Scanner console, utilizzare il seguente comando:

`[<percorso_del_programma>]dwscancl [<opzioni>] [<oggetti>]`

Un'opzione inizia con il carattere "/", più opzioni vengono separate da spazi. La lista degli oggetti di scansione può essere vuota o contenere diversi elementi separati da spazi.

La lista delle opzioni di Scanner console è contenuta in Allegato A.

Codici di output:

0 — la scansione è stata completata con successo, nessun oggetto infetto è stato trovato

1 — la scansione è stata completata con successo, sono stati trovati degli oggetti infetti

10 — sono impostate delle opzioni non valide

12 — Scanning Engine non è in esecuzione

255 — la scansione è stata interrotta dall'utente

8.6. Dr.Web per Microsoft Outlook

Funzioni principali del componente

Il plugin Dr.Web per Microsoft Outlook svolge le seguenti funzioni:

- scansione antivirus dei file allegati delle email in arrivo;
- controllo antispam della posta;
- rilevamento e neutralizzazione di programmi malevoli;
- analisi euristica per un'ulteriore protezione dai virus sconosciuti.

Configurazione del plugin Dr.Web per Microsoft Outlook

La configurazione dei parametri e la visualizzazione delle statistiche di funzionamento del programma si effettuano attraverso l'applicazione di posta Microsoft Outlook sezione **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare il plugin Dr.Web per Microsoft Outlook e premere il pulsante **Impostazioni dell'estensione**).

La scheda **Antivirus Dr.Web** nelle impostazioni dell'applicazione Microsoft Outlook è disponibile solo se l'utente ha i permessi per la modifica di queste impostazioni.

Nella scheda **Antivirus Dr.Web** viene visualizzato lo stato attuale della protezione (attivata/disattivata). Inoltre, dalla scheda si può accedere alle seguenti funzioni del programma:

- Log — consente di configurare la registrazione degli eventi del programma;
- Controllo allegati — consente di configurare la scansione della posta elettronica e definire le azioni del programma eseguite sugli oggetti malevoli rilevati;
- Filtro antispam — consente di definire le azioni del programma eseguite sui messaggi di spam, nonché creare una white list e una black list di indirizzi email;
- Statistiche — visualizza i dati sugli oggetti controllati e processati dal programma.

8.6.1. Scansione antivirus

Dr.Web per Microsoft Outlook impiega diversi metodi di rilevamento virus. Agli oggetti malevoli trovati vengono applicate le azioni definite dall'utente: il programma può curare oggetti infetti, eliminarli o spostarli in Quarantena per isolarli e conservarli in sicurezza.

Il programma Dr.Web per Microsoft Outlook rileva i seguenti oggetti malevoli:

- oggetti infetti;
- file-bomba o archivi-bomba;
- adware;
- hacktool;
- dialer;
- joke;
- riskware;
- spyware;
- trojan;
- worm e virus.

Azioni

Dr.Web per Microsoft Outlook consente di configurare la reazione del programma ai file infetti o sospetti e programmi malevoli rilevati durante il controllo degli allegati di posta elettronica.

Per configurare la scansione degli allegati e definire le azioni che il programma applicherà agli oggetti malevoli rilevati, nell'applicazione di posta Microsoft Outlook selezionare **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare il plugin Dr.Web per Microsoft Outlook e premere il pulsante **Impostazioni dell'estensione**) e premere il pulsante **Scansione allegati**.

La finestra **Scansione allegati** è disponibile solo se l'utente possiede i permessi dell'amministratore del sistema.

Nel sistema operativo Windows Vista e versioni successive, quando si fa clic sul pulsante **Scansione allegati**:

- Se l'UAC è attivato: all'amministratore viene visualizzata una richiesta per confermare le azioni del programma, a un utente senza i permessi di amministratore viene visualizzata una richiesta per inserire le credenziali dell'amministratore del sistema;
- Se l'UAC è disattivato: l'amministratore può modificare le impostazioni del programma, un utente non può avere l'accesso alla modifica delle impostazioni.

Nella finestra **Scansione allegati** è possibile configurare le azioni che il programma applicherà a diverse categorie di oggetti controllati, nonché le azioni per il caso di un errore di scansione. Inoltre, si può attivare o disattivare la scansione degli archivi.

Per impostare le azioni da applicare a oggetti malevoli rilevati, si utilizzano le seguenti impostazioni:

- la lista a cascata **Infetti** imposta la reazione al rilevamento degli oggetti infettati dai virus conosciuti e (presumibilmente) curabili;
- la lista a cascata **Non curati** imposta la reazione al rilevamento degli oggetti infettati da un virus conosciuto incurabile, nonché per i casi quando il tentativo di cura non è riuscito;
- la lista a cascata **Sospetti** imposta la reazione al rilevamento degli oggetti presumibilmente infettati da un virus (rilevati tramite l'analisi euristica);
- la sezione **Programmi malevoli** imposta la reazione al rilevamento dei seguenti software indesiderati:
  - adware;
  - dialer;
  - joke;
  - hacktool;
  - riskware;
- la lista a cascata **Se la scansione va in errore** consente di configurare le azioni del programma per il caso se la scansione dell'allegato non è possibile, per esempio se l'allegato è un file corrotto o un file protetto da password;
- il flag **Controlla archivi** consente di attivare o disattivare la scansione dei file allegati che sono archivi compressi. Impostare questo flag per attivare la scansione — togliere la spunta per disattivarla.

Le reazioni disponibili dipendono dal tipo di evento di virus.

Sono previste le seguenti azioni applicabili agli oggetti rilevati:

- **Cura** (l'azione è disponibile solo per oggetti infetti) — significa che il programma tenterà di curare l'oggetto infetto;
- **Elimina** — significa che l'oggetto verrà eliminato;
- **Sposta in quarantena** — significa che l'oggetto verrà isolato nella cartella di Quarantena;
- **Ignora** — significa che l'oggetto verrà saltato senza modifiche.

8.6.2. Controllo antispam

Dr.Web per Microsoft Outlook esegue la scansione antispam di tutti i messaggi di posta utilizzando Antispam Dr.Web e filtra i messaggi in base alle impostazioni definite dall'utente.

Per configurare la scansione dei messaggi per spam, nell'applicazione di posta Microsoft Outlook selezionare **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft

Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare il plugin Dr.Web per Microsoft Outlook e premere il pulsante **Impostazioni dell'estensione**) e premere il pulsante **Filtro antispam.** Si apre la finestra di configurazione del Filtro antispam.

La finestra **Filtro antispam** è disponibile solo se l'utente possiede i permessi di amministratore del sistema.

Nei sistemi operativi Windows Vista e versioni successive, quando si fa clic sul pulsante **Filtro antispam**:

- se l'UAC è attivato: all'amministratore viene visualizzata una richiesta per confermare le azioni del programma, a un utente senza i permessi di amministratore viene visualizzata una richiesta per inserire le credenziali dell'amministratore del sistema;
- se l'UAC è disattivato: l'amministratore può modificare le impostazioni del programma, un utente non può avere l'accesso alla modifica delle impostazioni.

Configurazione del filtro antispam

Per configurare i parametri del filtro antispam

1. Spuntare il flag **Esegui la scansione antispam della posta** per attivare il filtro antispam.
2. Se si vuole aggiungere uno specifico testo all'intestazione di un messaggio riconosciuto come spam, spuntare il flag **Aggiungi prefisso all'oggetto dell'email**. Il testo da aggiungere può essere immesso nel campo di testo a destra del flag. Di default viene aggiunto il prefisso ***SPAM***.
3. I messaggi controllati possono essere contrassegnati come letti nelle proprietà dell'email. A tale scopo è necessario impostare il flag **Segna il messaggio come già letto**. Di default, il flag **Segna il messaggio come già letto** è impostato.
4. Inoltre è possibile configurare le white list e black list per eseguire il filtraggio delle email.

Se alcune email sono state riconosciute in modo sbagliato, è possibile inviarle su indirizzi email speciali per l'analisi e il miglioramento della qualità di funzionamento del filtro:

- le email erroneamente riconosciute come spam possono essere inviate sull'indirizzo nonspam@drweb.com;
- le email di spam non riconosciute e saltate possono essere inviate sull'indirizzo spam@drweb.com.

Tutti i messaggi devono essere inviati solo come un allegato (e non all'interno del corpo del messaggio).

White list e black list

La white list e la black list di indirizzi email vengono utilizzate per filtrare i messaggi.

Per visualizzare e modificare la white list o la black list, nelle impostazioni filtro antispam premere rispettivamente il pulsante **White list** o **Black list**.

Per aggiungere un indirizzo alla white list o alla black list

1. Premere il pulsante **Aggiungi**.
2. Immettere l'indirizzo email nel campo appropriato.
3. Premere il pulsante **OK** nella finestra **Modifica la lista**.

Per modificare un indirizzo nella lista

1. Selezionare l'indirizzo nella lista, premere il pulsante **Modifica**.
2. Modificare le informazioni desiderate.
3. Premere il pulsante **OK** nella finestra **Modifica la lista**.

Per cancellare un indirizzo dalla lista

1. Selezionare l'indirizzo nella lista.
2. Premere il pulsante **Rimuovi**.

Nella finestra **White list e black list** premere il pulsante **OK** per salvare le modifiche apportate.

White list

Se l'indirizzo di un mittente è aggiunto alla white list, la relativa email non viene analizzata tramite Antispam. Metodi di immissione:

- per aggiungere alla lista un determinato mittente, immettere il suo indirizzo email completo (per esempio `mail@example.net`). Tutte le email ricevute da questo indirizzo verranno consegnate senza controllo antispam;
- ciascun elemento della lista può contenere soltanto un indirizzo email o una maschera di indirizzi email;
- per aggiungere alla lista dei mittenti un determinato tipo di indirizzi, immettere una maschera che definisce questi indirizzi. La maschera imposta un template per la determinazione dell'oggetto. Può includere caratteri normali ammissibili negli indirizzi email, nonché il carattere specifico "`*`" che sostituisce qualsiasi sequenza di caratteri (anche una vuota).

  Per esempio sono ammissibili le seguenti varianti:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

Il carattere "*" può essere messo soltanto all'inizio o alla fine di un indirizzo.

Il carattere "@" è obbligatorio.

- per assicurarsi di ricevere le email dagli indirizzi email in uno specifico dominio, utilizzare il carattere "`*`" invece del nome utente. Per esempio per ricevere tutte le email dai mittenti nel dominio example.net, immettere `*@example.net`;
- per assicurarsi di ricevere le email dagli indirizzi email con uno specifico nome utente da qualsiasi dominio, utilizzare il carattere "*" invece del nome a dominio. Per esempio per ricevere tutte le email dai mittenti con il nome della casella di posta "mariorossi", immettere `mariorossi@*`.

Black list

Se l'indirizzo di un mittente è aggiunto alla black list, lo status di spam viene attribuito alla relativa email senza ulteriore analisi. Metodi di immissione:

- per aggiungere alla lista un determinato mittente, immettere il suo indirizzo email completo (per esempio `spam@spam.it`). Tutte le email ricevute da questo indirizzo verranno riconosciute automaticamente come lo spam;
- ciascun elemento della lista può contenere soltanto un indirizzo email o una maschera di indirizzi email;
- per aggiungere alla lista dei mittenti un determinato tipo di indirizzi, immettere una maschera che definisce questi indirizzi. La maschera imposta un template per la determinazione dell'oggetto. Può includere caratteri normali ammissibili negli indirizzi email, nonché il carattere specifico "`*`" che sostituisce qualsiasi sequenza di caratteri (anche una vuota).

  Per esempio sono ammissibili le seguenti varianti:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

Il carattere "*" può essere messo soltanto all'inizio o alla fine di un indirizzo.

Il carattere "@" è obbligatorio.

- per assicurarsi di contrassegnare come spam le email dagli indirizzi email in uno specifico dominio, utilizzare il carattere "`*`" invece del nome utente. Per esempio per contrassegnare come spam tutte le email dai mittenti nel dominio spam.it, immettere `*@spam.it`;
- per assicurarsi di contrassegnare come spam le email dagli indirizzi email con uno specifico nome utente da qualsiasi dominio, utilizzare il carattere "`*`" invece del nome a dominio. Per

esempio per contrassegnare come spam tutte le email dai mittenti con il nome della casella di posta "ivanov", immettere `ivanov@*`.

8.6.3. Registrazione degli eventi

Dr.Web per Microsoft Outlook registra errori ed eventi nei seguenti log:

- log di registrazione degli eventi del sistema operativo (Event Log);
- log di testo di debug.

Log del sistema operativo

Nel log di registrazione degli eventi del sistema operativo (Event Log) vengono registrate le seguenti informazioni:

- messaggi sull'avvio e arresto del programma;
- impostazioni dei moduli del software: dello scanner, del motore, dei database dei virus (le informazioni vengono registrate ad avvio del programma e ad aggiornamento dei moduli);
- messaggi sul rilevamento dei virus.

Per visualizzare il log di registrazione degli eventi del sistema operativo

1. Aprire il **Pannello di controllo** del sistema operativo.
2. Selezionare la sezione **Amministrazione** → **Visualizza eventi**.
3. Nella parte sinistra della finestra **Visualizza eventi** selezionare la voce **Applicazione**. Si apre una lista degli eventi registrati nel log dalle applicazioni utente. La fonte dei messaggi Dr.Web per Microsoft Outlook è l'applicazione Dr.Web per Microsoft Outlook.

Log di testo di debug

Nel log di testo di debug vengono registrate le seguenti informazioni:

- messaggi sul rilevamento dei virus;
- messaggi sugli errori di scrittura o lettura dei file, errori di analisi degli archivi o dei file protetti da password;
- impostazioni dei moduli del software: dello scanner, del motore, dei database dei virus;
- messaggi sui crash del motore del software.

Per configurare la registrazione degli eventi

1. Nella scheda **Antivirus Dr.Web** premere il pulsante **Log**. Si apre la finestra di configurazione del log.
2. Per registrare le informazioni massimamente dettagliate sugli eventi, spuntare il flag **Registra log dettagliato**. Di default gli eventi vengono registrati in modalità normale.

La registrazione di un log di testo dettagliato del programma porta a un calo delle prestazioni del sistema, pertanto, si consiglia che la registrazione degli eventi massima venga attivata solo nel caso di errori di funzionamento dell'applicazione Dr.Web per Microsoft Outlook.

3. Premere il pulsante **OK** per salvare le modifiche.

La finestra **Log** è disponibile solo se l'utente possiede i permessi dell'amministratore del sistema.

Nel sistema operativo Windows Vista e versioni successive, quando si fa clic sul pulsante **Log**:

- se l'UAC è attivato: all'amministratore viene visualizzata una richiesta per confermare le azioni del programma, a un utente senza i permessi di amministratore viene visualizzata una richiesta per inserire le credenziali dell'amministratore del sistema;
- se l'UAC è disattivato: l'amministratore può modificare le impostazioni del programma, un utente non può avere l'accesso alla modifica delle impostazioni.

Per visualizzare il log degli eventi del programma

1. Nella scheda **Antivirus Dr.Web** premere il pulsante **Log**. Si apre la finestra di configurazione del log.
2. Premere il pulsante **Mostra nella cartella**. Si apre la cartella in cui è memorizzato il log.

8.6.4. Statistiche di scansione

Nell'applicazione di posta Microsoft Outlook sezione **Servizi** → **Impostazioni** → scheda **Antivirus Dr.Web** (in caso di Microsoft Outlook 2010 sezione **File** → **Impostazioni** → **Estensioni** selezionare **Dr.Web per Microsoft Outlook** e premere il pulsante **Impostazioni dell'estensione**) sono contenute le informazioni statistiche circa il numero totale di oggetti controllati e processati dal programma.

Gli oggetti sono suddivisi nelle seguenti categorie:

- **Controllati** — il numero totale di oggetti e messaggi controllati;
- **Infetti** — il numero totale di oggetti infetti negli allegati email;
- **Sospetti** — il numero di messaggi presumibilmente infettati da un virus (rilevati tramite l'analisi euristica);
- **Curati** — il numero di oggetti curati con successo dal programma;
- **Non controllati** — il numero di oggetti di cui la scansione non è possibile o durante la cui scansione si sono verificati errori;
- **Puliti** — il numero di oggetti e messaggi che non contengono oggetti malevoli.

Quindi viene indicato il numero di oggetti a cui sono state applicate le azioni:

- **Spostati** — il numero di oggetti spostati in Quarantena;
- **Rimossi** — il numero di oggetti eliminati dal sistema;
- **Ignorati** — il numero di oggetti saltati senza modifiche;
- **Messaggi di spam** — il numero di messaggi riconosciuti come spam.

Di default le statistiche vengono salvate nel file `drwebforoutlook.log` situato nella cartella `%USERPROFILE%\Doctor Web`.

Le informazioni statistiche vengono accumulate durante una sessione. Dopo il riavvio del computer o dopo il riavvio di Agent Dr.Web per Windows le statistiche vengono azzerate.

9. Protezione preventiva

In questo gruppo di impostazioni è possibile configurare la reazione di Dr.Web alle azioni di applicazioni di terzi che possono portare all'infezione del computer, e selezionare il livello di protezione dagli exploit.

Per andare al gruppo di impostazioni Protezione preventiva

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Protezione preventiva**.

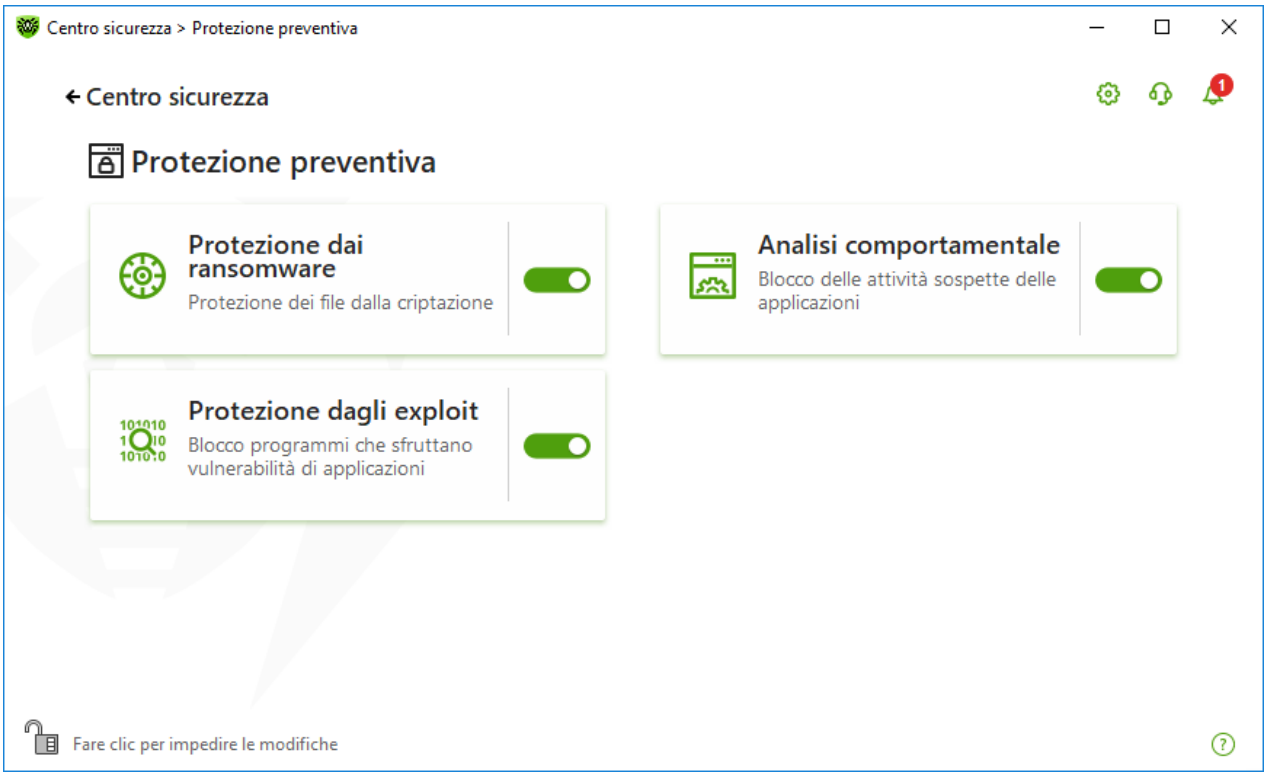

Immagine 54. Finestra Protezione preventiva

Attivazione e disattivazione dei componenti di protezione

Attivare o disattivare il componente richiesto utilizzando l'interruttore .

Per andare ai parametri dei componenti

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella del componente richiesto.

L'attivazione e disattivazione di Protezione preventiva e la modifica dei parametri dei componenti sono possibili se sono state autorizzate dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

In questa sezione:

- Protezione dai ransomware — parametri di divieto della criptazione di file utente.
- Analisi comportamentale — parametri di divieto dell'accesso delle applicazioni agli oggetti di sistema.
- Protezione dagli exploit — parametri di divieto dell'uso di vulnerabilità delle applicazioni.

Per *disattivare* uno dei componenti, Dr.Web deve essere in modalità amministratore. A questo scopo, cliccare sul lucchetto nella parte inferiore della finestra del programma.

9.1. Protezione dai ransomware

Il componente Protezione dai ransomware consente di rintracciare i processi che cercano di criptare i file utente secondo un algoritmo conosciuto che indica che tali processi sono una minaccia per la sicurezza del computer. A tali processi appartengono i *trojan cryptolocker*. Arrivando sul computer dell'utente, tali programmi malevoli bloccano l'accesso ai dati, dopodiché estorcono denaro per la decriptazione. Sono tra i programmi malevoli più diffusi e ogni anno infliggono gravi perdite sia alle aziende che agli utenti comuni. La principale via di infezione sono messaggi email inviati in massa contenenti un file malevolo o un link a un virus.

Secondo le statistiche dell'azienda Doctor Web, la decriptazione dei file danneggiati dal trojan è possibile solo nel 10% dei casi, pertanto, il metodo di contrasto più efficace è prevenire l'infezione. Recentemente, il numero di utenti colpiti da questo tipo di virus diminuisce. Ciononostante, il numero di richieste di decriptazione dati inviate al servizio di supporto tecnico Doctor Web raggiunge 1000 al mese.

Per attivare o disattivare il componente Protezione dai ransomware

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Protezione preventiva**.
3. Attivare o disattivare il componente Protezione dai ransomware utilizzando l'interruttore .

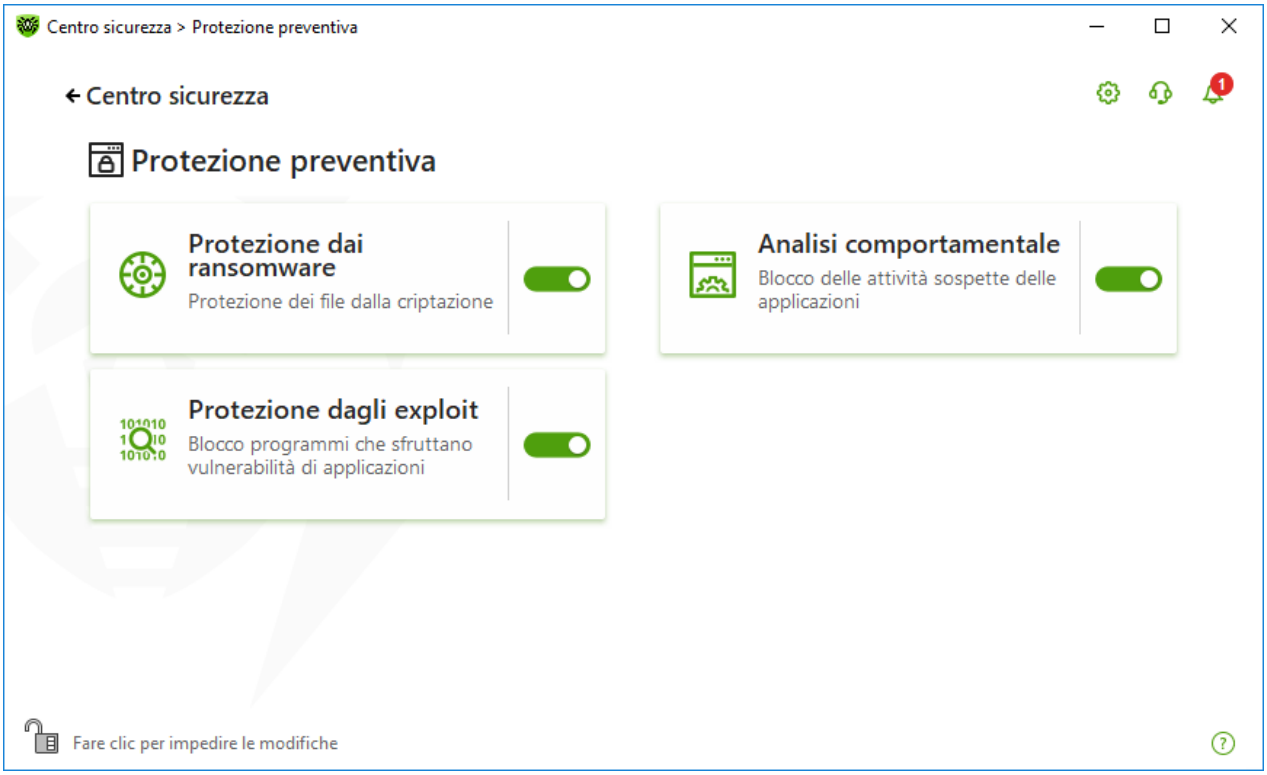

Immagine 55. Attivazione/disattivazione del componente Protezione dai ransomware

La modifica dei parametri del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui si connette Dr.Web.

In questa sezione:

- Configurazione della reazione ai tentativi di criptazione file da parte delle applicazioni
- Regole separate per applicazioni

Reazione Dr.Web ai tentativi di criptazione file da parte delle applicazioni

Per configurare i parametri del componente Protezione dai ransomware

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella **Protezione dai ransomware**. Si aprirà la finestra dei parametri del componente.
3. Dal menu a cascata selezionare un'azione la quale verrà utilizzata per tutte le applicazioni.

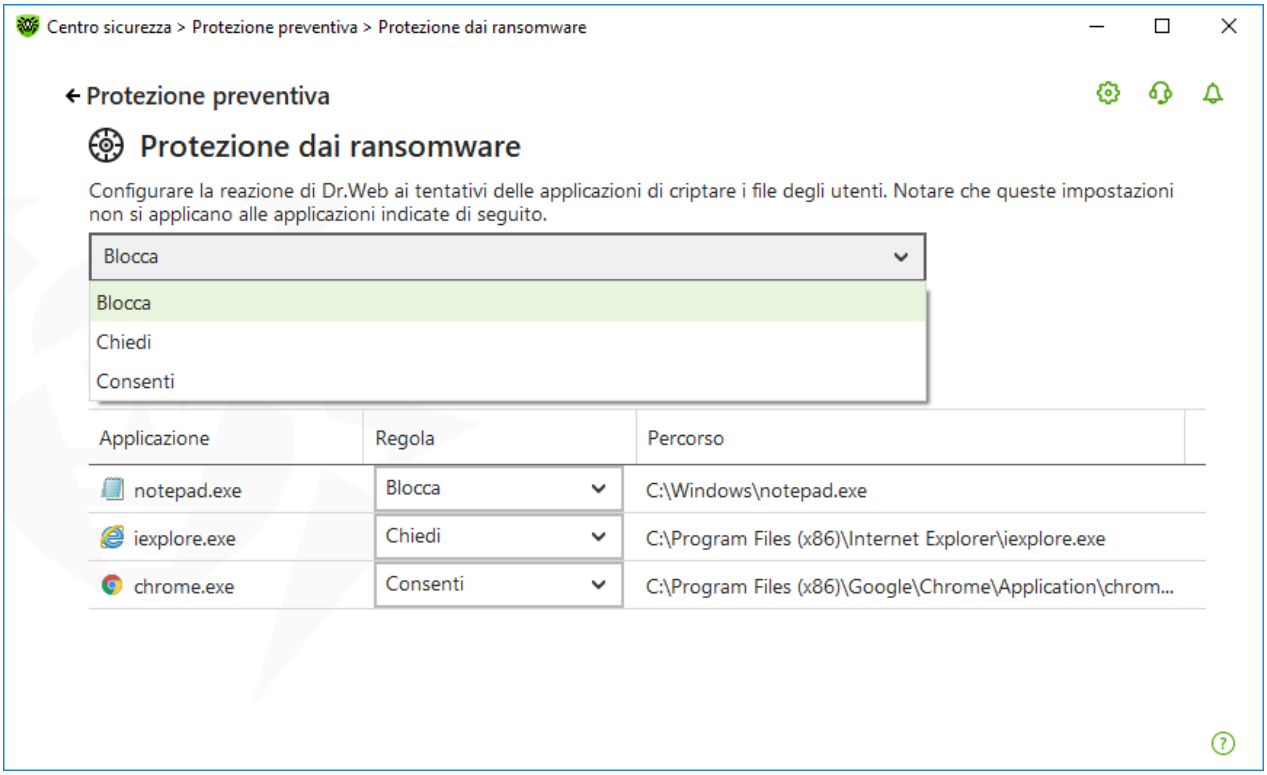

Immagine 56. Selezione della reazione Dr.Web

- **Consenti** — a tutte le applicazioni sarà consentito modificare i file utente.
- **Blocca** — la criptazione di file utente sarà proibita a tutte le applicazioni. Questa modalità è impostata di default. Quando un'applicazione tenta di criptare i file utente, verrà visualizzato un avviso:

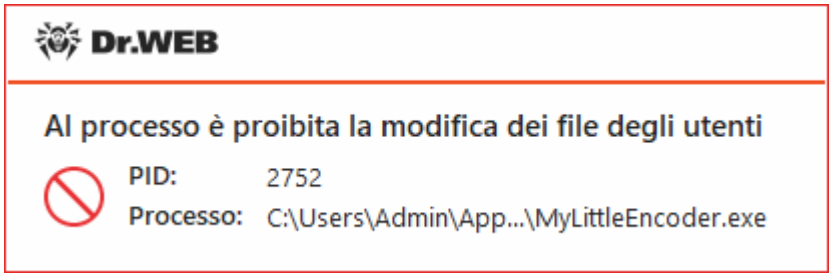

Immagine 57. Esempio di avviso sul divieto di modifica dei file utente

- **Chiedi** — quando un'applicazione tenta di criptare un file utente, verrà visualizzato un avviso in cui è possibile proibire all'applicazione questa attività o ignorarla:

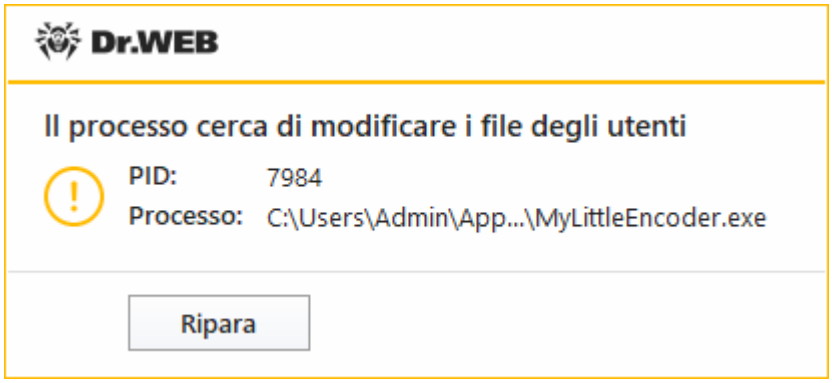

Immagine 58. Esempio di avviso sul tentativo di modifica dei file utente

- Se si preme il pulsante **Ripara**, il processo verrà bloccato e messo in quarantena. Anche se l'applicazione viene ripristinata dalla quarantena, non sarà in grado di funzionare fino al riavvio del computer.
- Se si chiude la finestra dell'avviso, l'applicazione non verrà neutralizzata.

Ricezione degli avvisi

È possibile configurare la visualizzazione sullo schermo degli avvisi sulle attività del componente Protezione dai ransomware.

Vedi inoltre:

- Avvisi

Regole separate per applicazioni

È possibile configurare la reazione del componente Protezione dai ransomware alle attività di singole applicazioni. Per fare ciò, è necessario aggiungere un'applicazione alla lista e selezionare la reazione del componente richiesta. Per la gestione degli oggetti nella lista sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — aggiunta di un'applicazione alla lista delle applicazioni con regole separate.
- Pulsante 🗑 — rimozione di un'applicazione dalla lista delle applicazioni con regole separate.

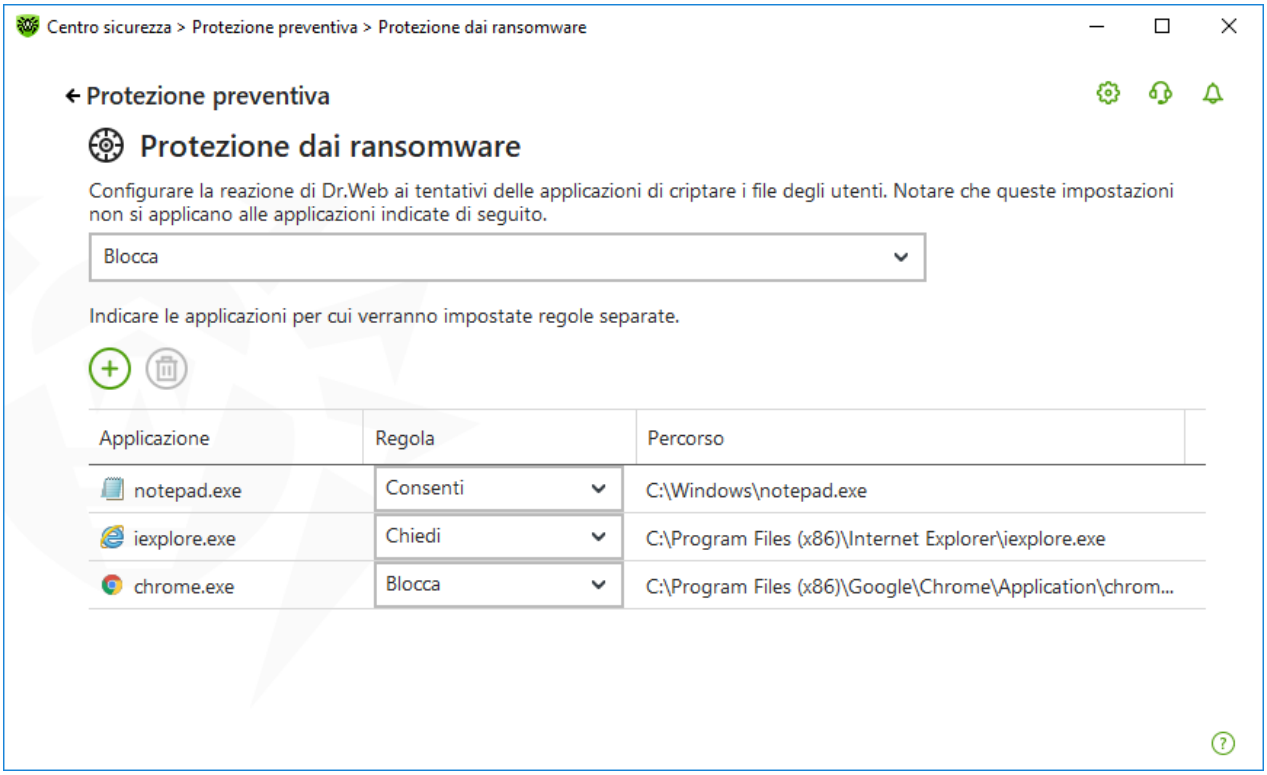

Immagine 59. Applicazioni per cui non è applicabile la regola generale

Per aggiungere un'applicazione alla lista

1. Premere il pulsante ⊕.
2. Nella finestra che si è aperta premere il pulsante **Sfoglia** e indicare il percorso del file eseguibile dell'applicazione.

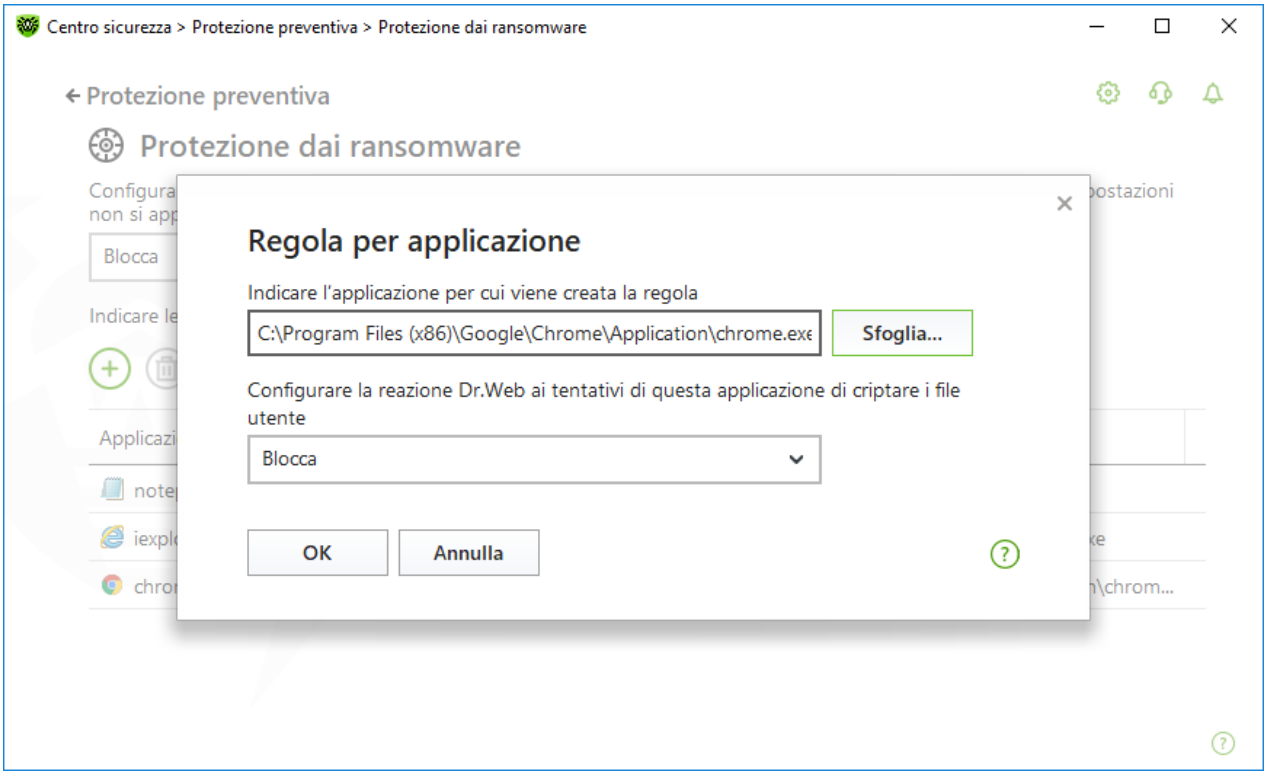

Immagine 60. Selezione della regola per un'applicazione

3. Selezionare la reazione richiesta dalla lista a cascata.
4. Premere **OK**.

È anche possibile modificare una regola già impostata.

Per modificare la reazione Dr.Web per le applicazioni con regole impostate

1. Sulla schermata principale dei parametri del componente Protezione dai ransomware selezionare l'applicazione richiesta.
2. Nella riga corrispondente nella colonna **Regola** selezionare dalla lista a cascata la reazione richiesta ai tentativi dell'applicazione di criptare i file utente.

9.2. Analisi comportamentale

Il componente Analisi comportamentale consente di configurare la reazione di Dr.Web alle azioni di applicazioni di terzi non incluse tra quelle affidabili, che possono portare all'infezione del computer, per esempio, i tentativi di modifica del file HOSTS o dei rami critici del registro di sistema. Quando è attivato il componente Analisi comportamentale, il programma proibisce la modifica automatica degli oggetti di sistema, la cui modifica indica chiaramente un tentativo di impatto malevolo sul sistema operativo. L'analisi comportamentale protegge il sistema dai programmi malevoli precedentemente sconosciuti che sono capaci di evitare il rilevamento tramite i maccanismi tradizionali di firme antivirali e analisi euristica.

Per attivare o disattivare il componente Analisi comportamentale

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Protezione preventiva**.
3. Attivare o disattivare il componente Analisi comportamentale utilizzando l'interruttore .

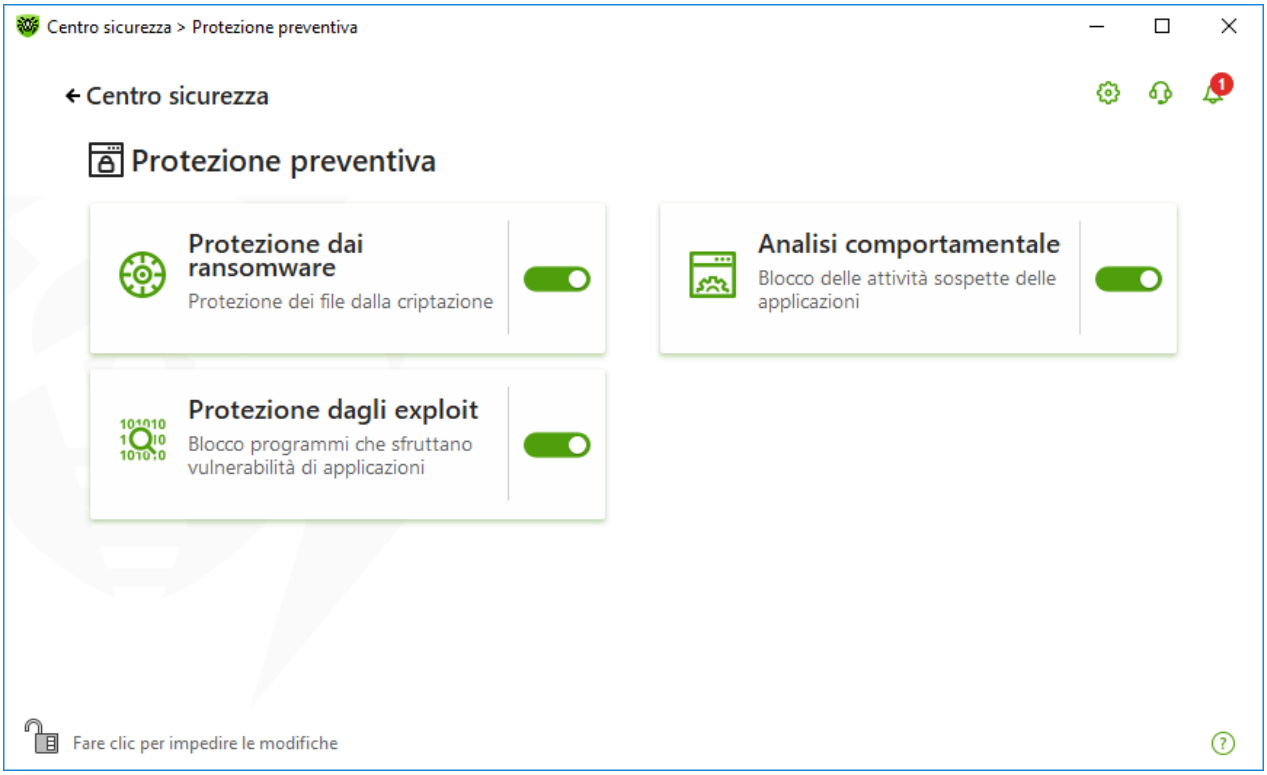

Immagine 61. Attivazione/disattivazione del componente Analisi comportamentale

La modifica dei parametri del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

In questa sezione:

- Modalità di funzionamento del componente
- Creazione e modifica di singole regole per applicazioni
- Descrizione degli oggetti protetti

Parametri di Analisi comportamentale

Le impostazioni predefinite del programma sono ottimali nella maggior parte dei casi, non dovrebbero essere modificate senza necessità.

Per andare ai parametri del componente Analisi comportamentale

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella **Analisi comportamentale**. Si aprirà la finestra dei parametri del componente.

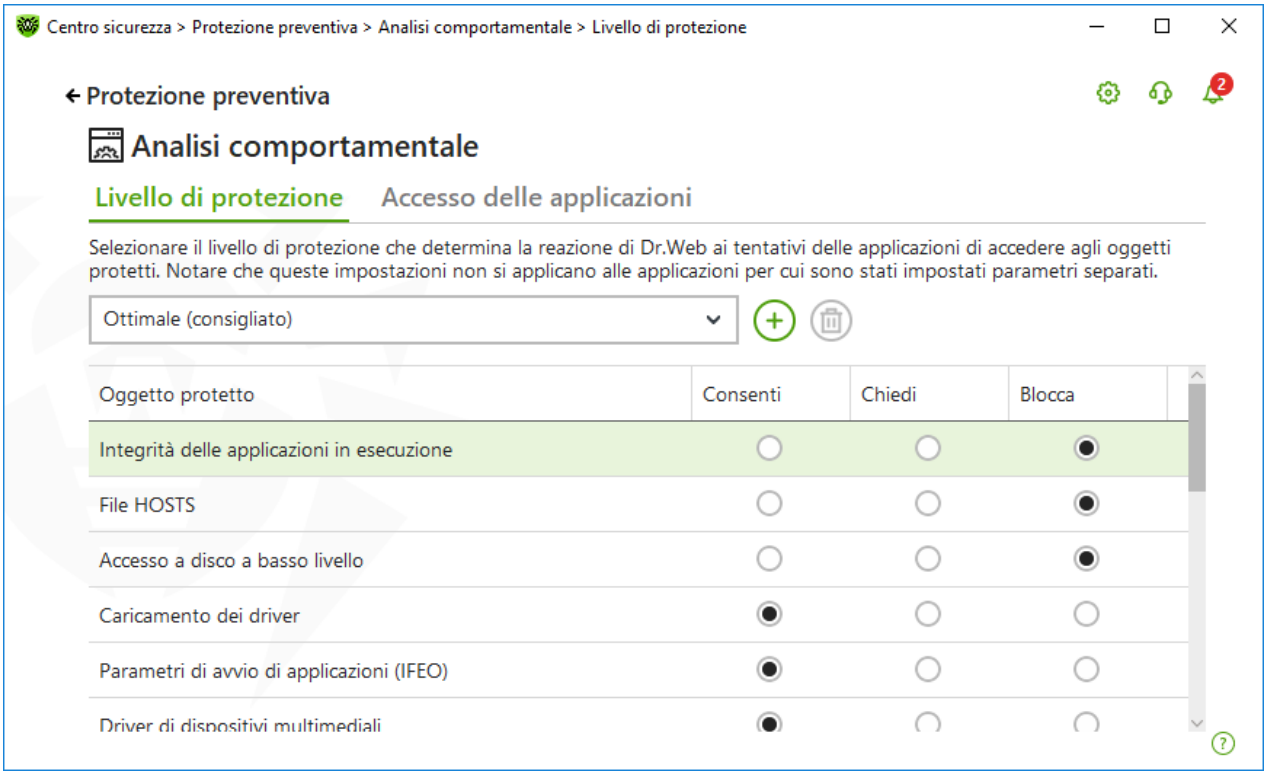

Immagine 62. Parametri di Analisi comportamentale

È possibile impostare un livello di protezione separato per oggetti e processi specifici e un livello generale le cui impostazioni verranno applicate a tutti gli altri processi. Per impostare il livello di protezione generale, nella scheda **Livello di protezione** selezionare il livello richiesto dalla lista a cascata.

Livelli di protezione

Livello di protezione	Descrizione
Ottimale (consigliato)	Dr.Web proibisce la modifica automatica degli oggetti di sistema la cui modifica indica chiaramente un tentativo di impatto malevolo sul sistema operativo. Inoltre, vengono proibiti l'accesso al disco a basso livello e la modifica del file HOSTS da parte di applicazioni le cui attività vengono inequivocabilmente definite come tentativo di impatto malevolo sul sistema operativo.

Livello di protezione	Descrizione
	 Vengono bloccate solo le azioni delle applicazioni che non sono affidabili.
Medio	Questo livello di protezione può essere impostato nel caso di aumentato rischio di infezione. In questa modalità viene proibito addizionalmente l'accesso agli oggetti critici che possono potenzialmente essere utilizzati dai programmi malevoli.  In questa modalità di protezione sono possibili conflitti di compatibilità con programmi di terzi che utilizzano i rami di registro protetti.
Paranoicale	Questo livello di protezione è necessario per il pieno controllo degli accessi agli oggetti critici di Windows. In questo modalità sarà inoltre disponibile il controllo interattivo del caricamento dei driver e dell'esecuzione automatica dei programmi.
Personalizzato	In questa modalità di operazione è possibile selezionare a propria discrezione i livelli di protezione per ciascun oggetto.

Modalità personalizzata

Tutte le modifiche alle impostazioni vengono salvate in modalità di funzionamento Personalizzato. In questa finestra è inoltre possibile creare un nuovo livello di protezione per salvare le impostazioni richieste. Con tutte le impostazioni del componente gli oggetti protetti saranno disponibili per la lettura.

È possibile selezionare una delle reazioni Dr.Web ai tentativi di modifica degli oggetti protetti da parte delle applicazioni:

- **Consenti** — l'accesso all'oggetto protetto sarà consentito per tutte le applicazioni.

- **Chiedi** — quando un'applicazione tenta di modificare un oggetto protetto, verrà visualizzato un avviso:

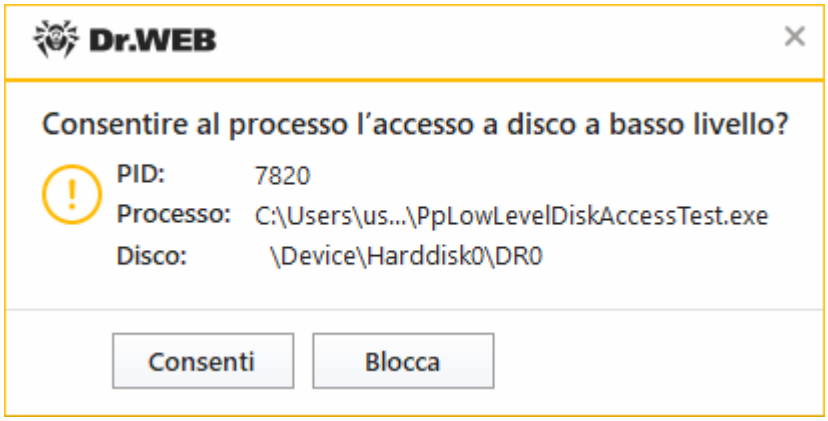

Immagine 63. Esempio di avviso con la richiesta di accesso all'oggetto protetto

- **Blocca** — quando un'applicazione tenta di modificare un oggetto protetto, l'accesso dell'applicazione sarà negato. Verrà visualizzato un avviso:

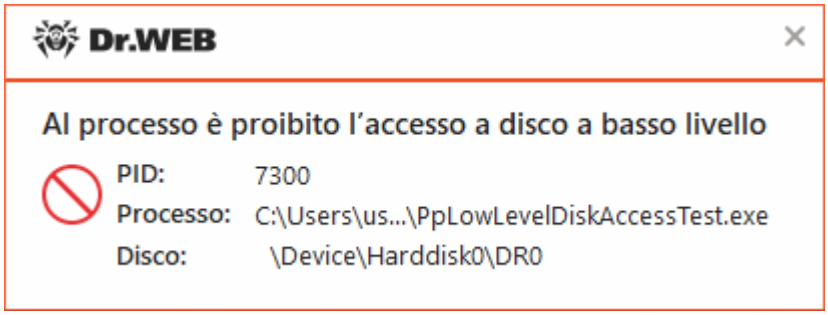

Immagine 64. Esempio di avviso sul divieto di accesso all'oggetto protetto

Per creare un nuovo livello di protezione

1. Visualizzare le impostazioni di protezione di default e, se necessario, modificarle.
2. Premere il pulsante ⊕.
3. Nella finestra che si è aperta indicare il nome per il nuovo profilo.
4. Premere **OK**.

Per rimuovere un livello di protezione

1. Dalla lista a cascata selezionare il livello di protezione creato che si vuole rimuovere.
2. Premere il pulsante 🗑. I profili predefiniti non possono essere rimossi.
3. Premere **OK** per confermare la rimozione.

Ricezione degli avvisi

È possibile configurare la visualizzazione sullo schermo degli avvisi sulle attività del componente Analisi comportamentale.

Vedi inoltre:

- Avvisi

Accesso delle applicazioni

Per configurare i singoli parametri di accesso per applicazioni specifiche, andare alla scheda **Accesso delle applicazioni**. Qui è possibile aggiungere una nuova regola per un'applicazione, modificare una regola già creata o rimuoverne una non richiesta.

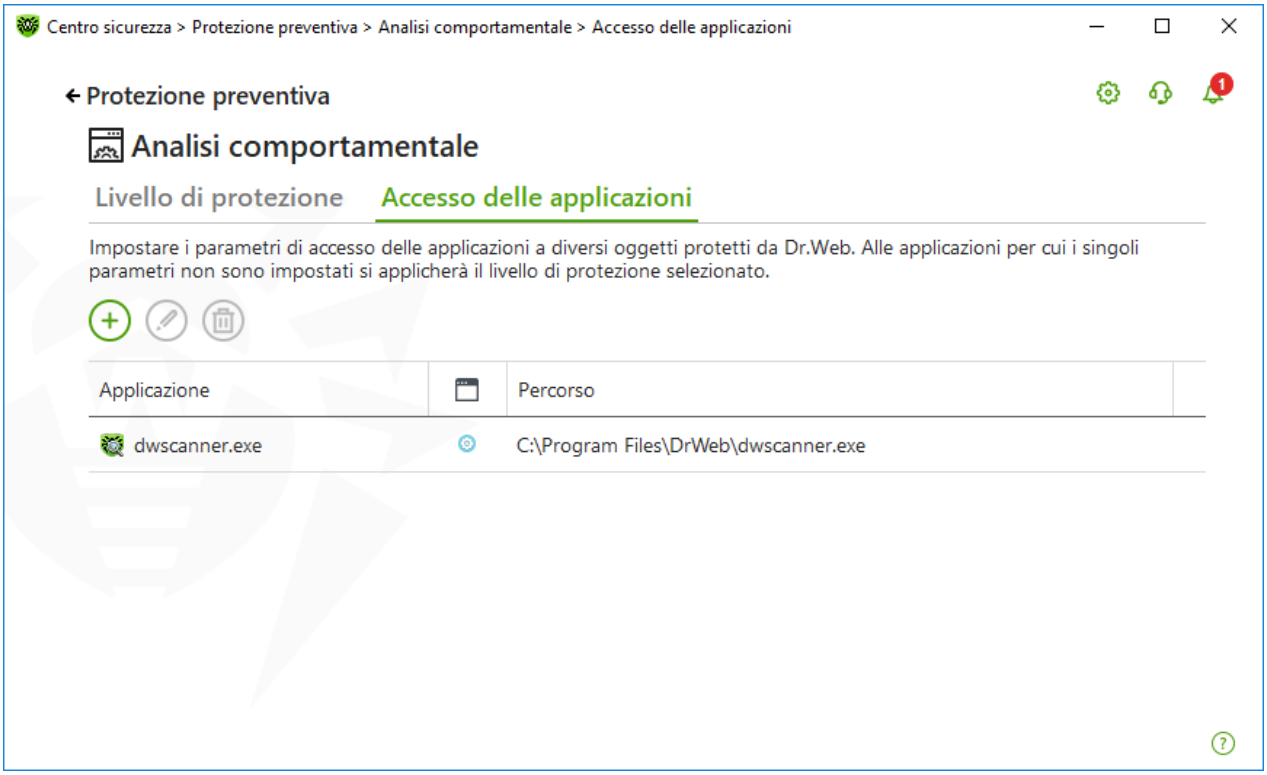

Immagine 65. Parametri di accesso delle applicazioni

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — aggiunta di un set di regole per un'applicazione.
- Pulsante ✎ — modifica dei set di regole esistenti.
- Pulsante 🗑 — rimozione di un set di regole.

Nella colonna (**Tipo di regola**) possono essere visualizzati tre tipi di regole:

- ✔ — è impostata la regola **Consenti tutto** per tutti gli oggetti protetti.
- ⚙ — sono impostate regole diverse per oggetti protetti.
- ⛔ — è impostata la regola **Blocca tutto** per tutti gli oggetti protetti.

Per aggiungere una regola per un'applicazione

1. Premere il pulsante ⊕.

2. Nella finestra che si è aperta premere il pulsante **Sfoglia** e indicare il percorso del file eseguibile dell'applicazione.

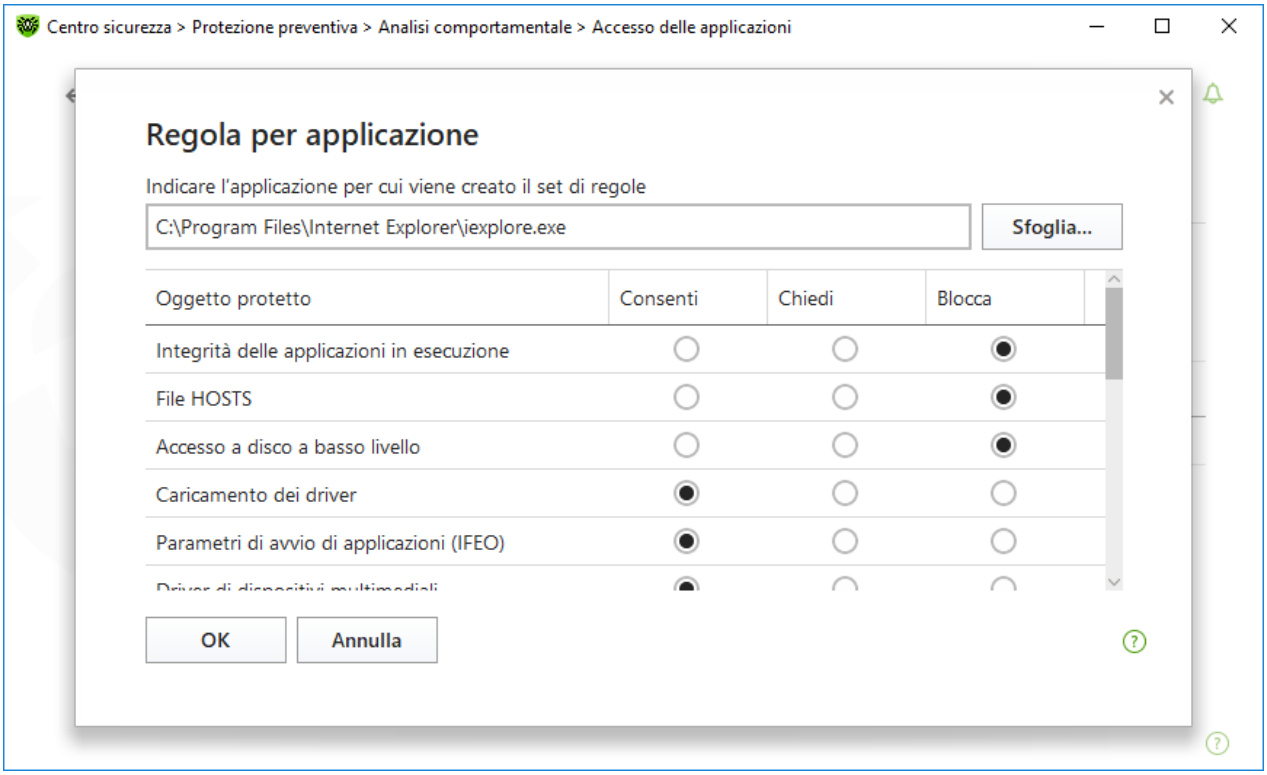

Immagine 66. Aggiunta di un set di regole per un'applicazione

3. Visualizzare le impostazioni di protezione di default e, se necessario, modificarle.
4. Premere **OK**.

Oggetti protetti

Oggetto protetto	Descrizione
Integrità delle applicazioni in esecuzione	Questa impostazione consente di monitorare i processi che si incorporano nelle applicazioni in esecuzione, il che costituisce una minaccia per la sicurezza del computer.
File HOSTS	Il file HOSTS viene utilizzato dal sistema operativo per semplificare l'accesso a internet. Modifiche a questo file possono essere risultato del funzionamento di un virus o di un altro programma malevolo.
Accesso al disco a basso livello	Questa impostazione consente di proibire alle applicazioni di registrare informazioni su disco settore per settore senza utilizzare il file system.
Caricamento dei driver	Questa impostazione consente di proibire alle applicazioni di caricare driver nuovi o sconosciuti.
Aree critiche di Windows	Le altre impostazioni consentono di proteggere i rami di registro contro le modifiche (sia nel profilo di sistema che nei profili di tutti gli utenti).

Oggetto protetto	Descrizione
	Accesso ai parametri di avvio applicazioni (IFEO): • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Driver di dispositivi multimediali: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Parametri della shell Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Notifiche di Winlogon: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Avvio automatico della shell di Windows: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Associazione dei file eseguibili: • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (chiavi) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (chiavi) Criteri restrizione software (SRP): • Software\Policies\Microsoft\Windows\Safer Plugin di Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Esecuzione automatica programmi: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Esecuzione automatica criteri: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Configurazione della modalità provvisoria: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network

Oggetto protetto	Descrizione
	Parametri di Gestione sessioni: • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows Servizi di sistema: • System\CurrentControlXXX\Services

Se si riscontrano problemi durante l'installazione di aggiornamenti importanti Microsoft o l'installazione e il funzionamento di programmi (compresi i programmi di deframmentazione), disattivare temporaneamente Analisi comportamentale.

9.3. Protezione dagli exploit

Il componente Protezione dagli exploit permette di bloccare gli oggetti malevoli che sfruttano le vulnerabilità di applicazioni più diffuse.

Per attivare o disattivare il componente Protezione dagli exploit

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Protezione preventiva**.
3. Attivare o disattivare il componente Protezione dagli exploit utilizzando l'interruttore .

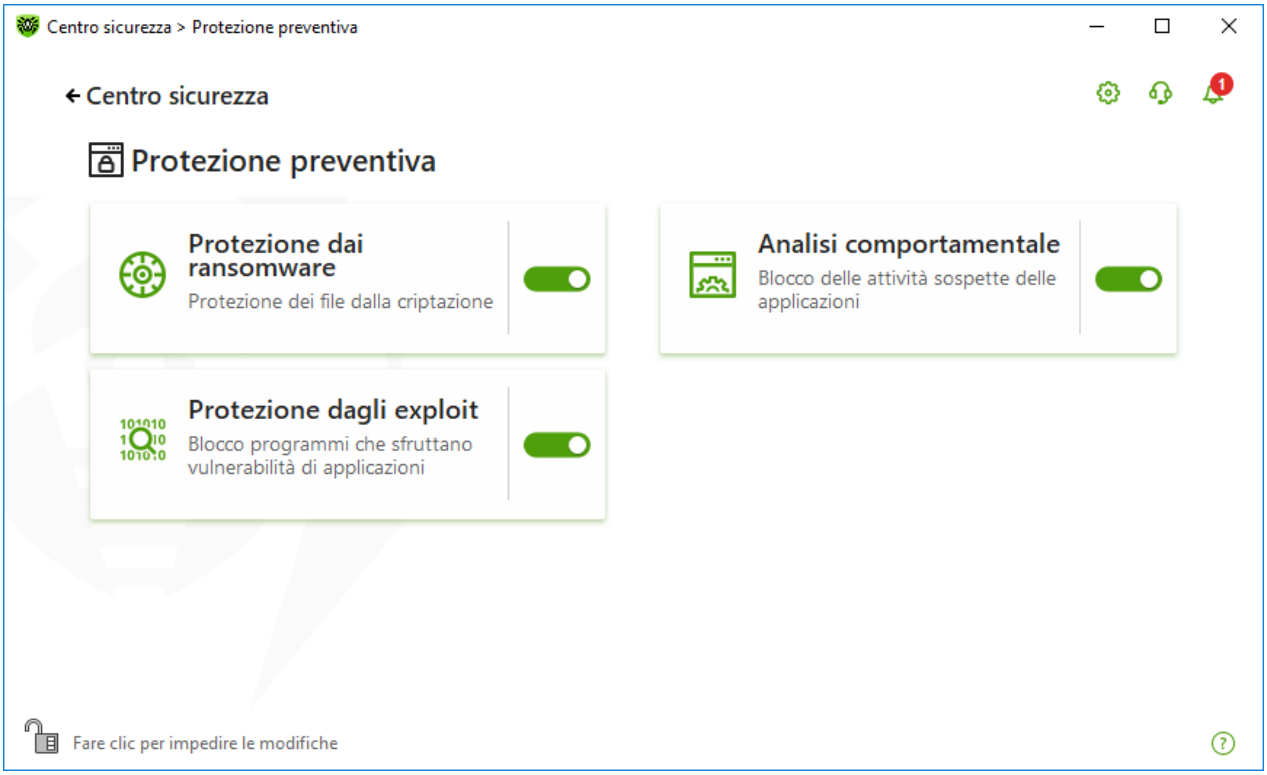

Immagine 67. Attivazione/disattivazione del componente Protezione dagli exploit

Per andare ai parametri del componente Protezione dagli exploit

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella **Protezione dagli exploit**. Si aprirà la finestra dei parametri del componente.

> La modifica dei parametri del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Dalla lista a cascata corrispondente nella finestra dei parametri del componente selezionare il livello di protezione dagli exploit adatto.

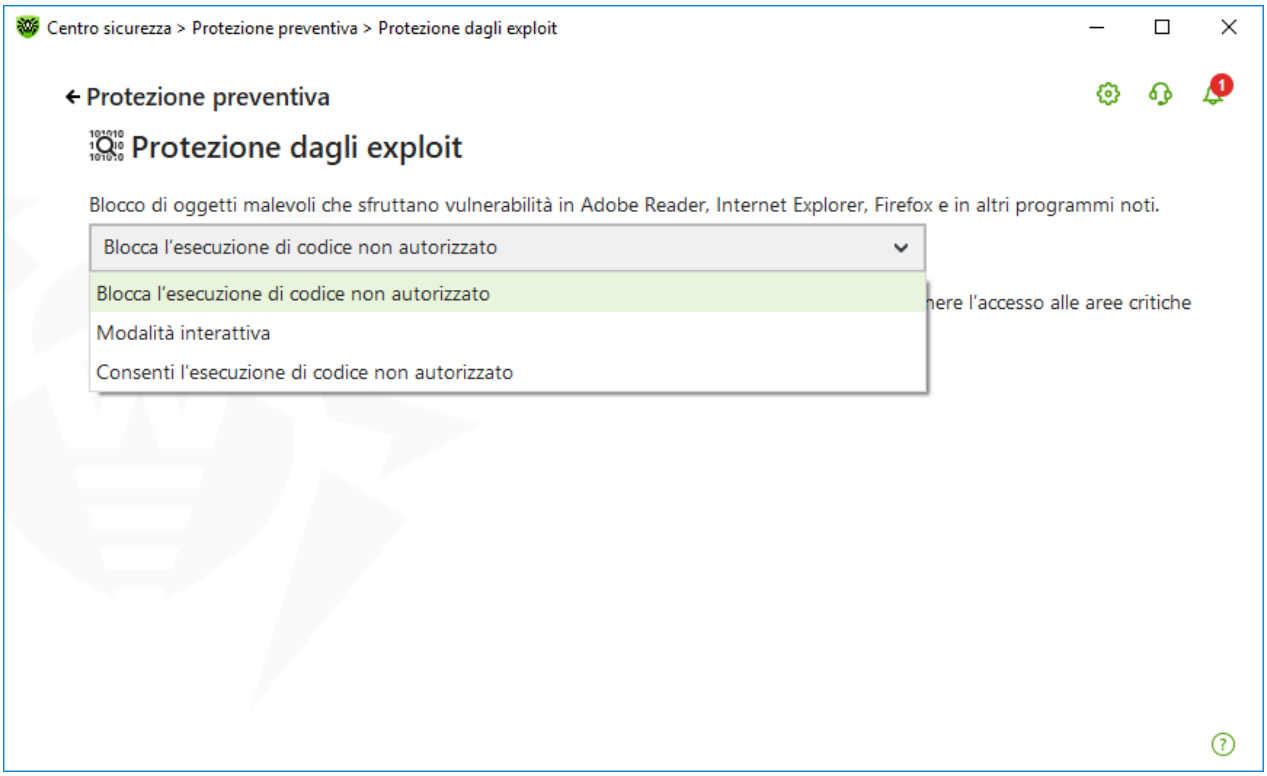

Immagine 68. Selezione del livello di protezione

Livelli di protezione

Livello di protezione	Descrizione
Blocca l'esecuzione di codice non autorizzato	Verrà bloccato automaticamente il tentativo da parte di un oggetto malevolo di sfruttare le vulnerabilità nei software per ottenere l'accesso alle aree critiche del sistema operativo.
Modalità interattiva	Se un oggetto malevolo cercherà di sfruttare le vulnerabilità nei software per ottenere l'accesso alle aree critiche del sistema operativo, Dr.Web

Livello di protezione	Descrizione
	visualizzerà un avviso corrispondente. Leggere le informazioni e selezionare l'azione richiesta.
Consenti l'esecuzione di codice non autenticato	Verrà consentito automaticamente un tentativo da parte di un oggetto malevolo di sfruttare le vulnerabilità nei software per ottenere l'accesso alle aree critiche del sistema operativo.

Ricezione degli avvisi

È possibile configurare la visualizzazione sullo schermo degli avvisi sulle attività del componente Protezione dagli exploit.

Vedi inoltre:

- Avvisi

10. Dispositivi

Nella finestra **Dispositivi** è possibile limitare l'accesso a determinati dispositivi o bus di dispositivo e configurare una lista di dispositivi consentiti.

> I parametri di accesso ai dispositivi si applicano a tutti gli account Windows.

Per andare alla finestra Dispositivi

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
3. Fare clic sulla piastrella **Dispositivi**.

Immagine 69. Accesso alla finestra Dispositivi

In questa sezione:

- Parametri di blocco principali
- Blocco di bus e classi di dispositivi
- Creazione della lista dei dispositivi consentiti

Parametri principali

È possibile attivare le opzioni corrispondenti per:

- bloccare la trasmissione di task a stampanti;
- bloccare la trasmissione di dati attraverso le reti locali e internet.

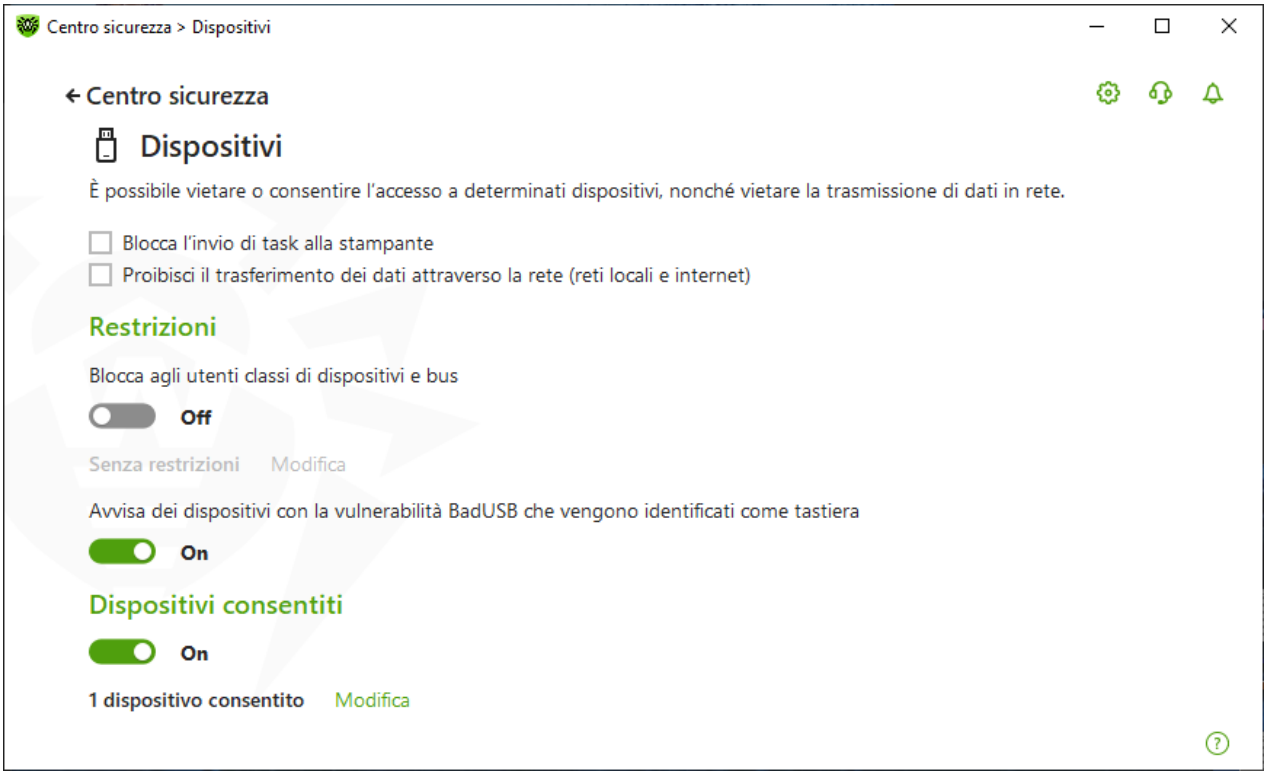

Immagine 70. Parametri di blocco dei dispositivi

Di default tutte le opzioni sono disattivate.

L'opzione **Blocca supporti rimovibili** è disponibile solo per gli utenti che l'avevano attivata prima dell'aggiornamento componenti prodotto del 02.02.2022. Se questa opzione non veniva utilizzata o il prodotto viene installato per la prima volta, utilizzare l'opzione **Blocca classi e bus di dispositivi per utenti** per vietare l'accesso ai dati su supporti rimovibili.

Limitazioni

Parametri di blocco dei dispositivi

La funzione di blocco dispositivi permette sia di bloccare una o più classi di dispositivi su tutti i bus e sia di bloccare tutti i dispositivi collegati a uno o più bus. Le *classi di dispositivi* sono dispositivi che svolgono funzioni uguali (per esempio, i dispositivi per la stampa). I *bus* — sottosistemi di trasmissione di dati tra i blocchi funzionali del computer (per esempio, il bus USB).

Per bloccare l'accesso alle classi di dispositivi e ai bus selezionati

1. Attivare l'opzione **Blocca classi e bus di dispositivi per utenti** utilizzando l'interruttore corrispondente.
2. Fare clic sul link **Modifica**.
3. Nella finestra che si è aperta è possibile selezionare le classi di dispositivi o i bus, l'accesso a cui si vuole bloccare.

Avviso sui dispositivi con la vulnerabilità BadUSB

Alcuni dispositivi USB infetti possono essere riconosciuti dal computer come una tastiera. Affinché il programma Dr.Web verifichi se un dispositivo collegato è veramente una tastiera, attivare l'opzione **Avvisa dei dispositivi con la vulnerabilità BadUSB che vengono identificati come tastiera**. In tale caso, se viene collegata una tastiera, si aprirà una finestra di sblocco. È necessario premere i tasti specificati sulla tastiera.

Immagine 71. Finestra di sblocco della tastiera

Cliccando sul link **Informazioni tecniche**, si aprirà una finestra con informazioni dettagliate sul dispositivo.

Dispositivi consentiti

Se è stato limitato l'accesso a qualche classe di dispositivi o bus, è possibile consentire separatamente l'accesso a determinati dispositivi aggiungendoli alla lista dei dispositivi

consentiti. Inoltre, è possibile aggiungere alla lista un dispositivo specifico per non verificare la presenza della vulnerabilità BadUSB su di esso.

Per aggiungere dispositivi alla lista dei consentiti

1. Attivare l'opzione **Dispositivi consentiti** utilizzando l'interruttore corrispondente .
2. Premere il pulsante **Modifica** (il pulsante diventa attivo se sono impostate limitazioni).
3. Nella finestra che si è aperta è possibile creare una lista di dispositivi a cui non si applicano le limitazioni di accesso.

10.1. Blocco di bus e classi

Per andare alla finestra Classi e bus di dispositivi

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Dispositivi**.
3. Nel gruppo di impostazioni **Limitazioni** attivare l'opzione **Blocca classi e bus di dispositivi per utenti** utilizzando l'interruttore .
4. Fare clic sul link **Modifica**.
5. Nella finestra che si è aperta è possibile selezionare i bus o le classi di dispositivi a cui si desidera bloccare l'accesso.

La finestra contiene una tabella con informazioni sui bus e sulle classi di dispositivi bloccati. Di default la tabella è vuota. Ci saranno visualizzati i bus e le classi quando vengono aggiunti alla lista degli oggetti bloccati. In una riga con un bus bloccato vengono visualizzate tutte le classi di dispositivi che sono bloccate su questo bus.

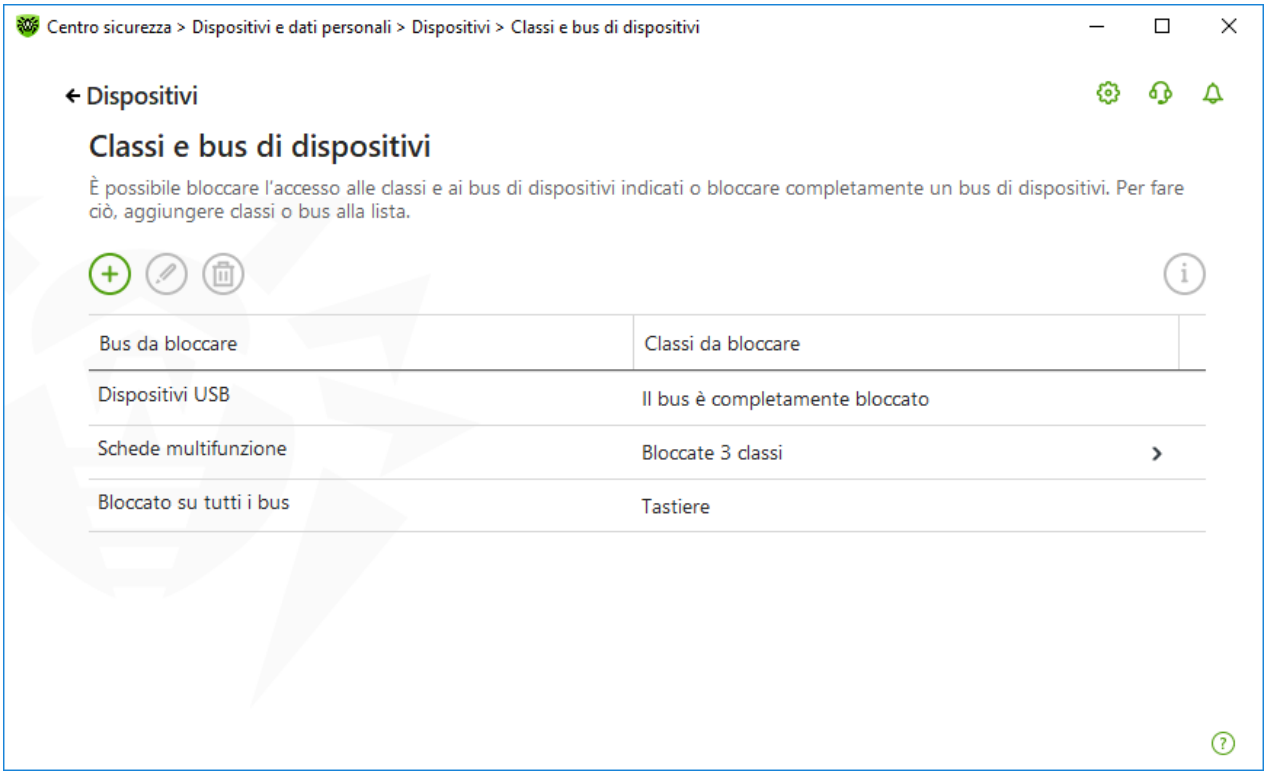

Immagine 72. Bus e classi bloccati

La colonna **Classi da bloccare** visualizza il numero di classi bloccate sul bus corrispondente. Se più classi sono bloccate su un bus, vengono visualizzate in una lista a cascata.

È evidenziata in grigio una classe bloccata su tutti i bus.

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — aggiunta di un oggetto alla lista di oggetti bloccati.
- Pulsante ✎ — modifica delle impostazioni di blocco per l'oggetto selezionato nella tabella.
- Pulsante 🗑 — rimozione dell'oggetto selezionato dalla lista di oggetti bloccati.

È possibile visualizzare informazioni dettagliate su un bus bloccato e sulle classi di dispositivi bloccate su di esso. Per fare ciò, selezionare la riga richiesta e premere ⓘ.

Blocco del bus

1. Per bloccare un bus completamente o alcuni dispositivi su un determinato bus, premere il pulsante ⊕.
2. Dalla lista a cascata selezionare l'oggetto che si vuole bloccare: **Bus**. Premere **Avanti**.

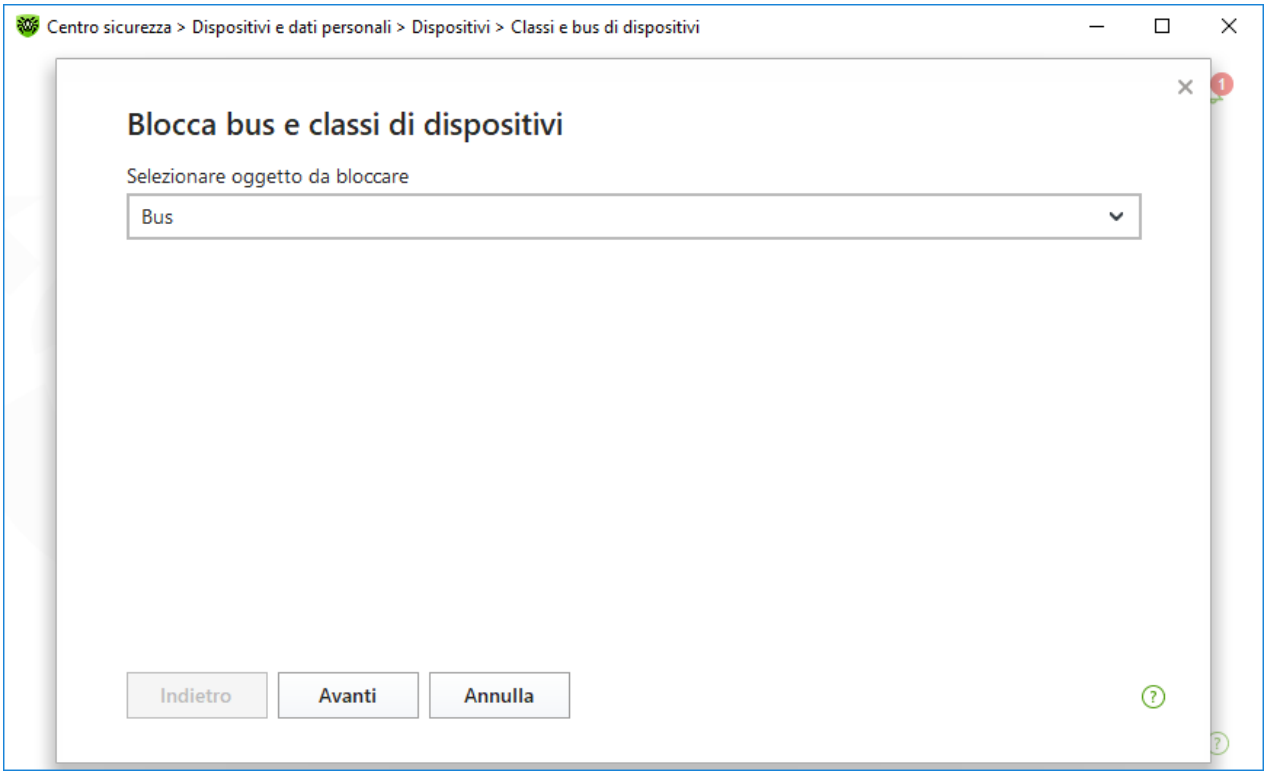

Immagine 73. Selezione dell'oggetto da bloccare

3. Selezionare il tipo di bus. Premere **Avanti**.

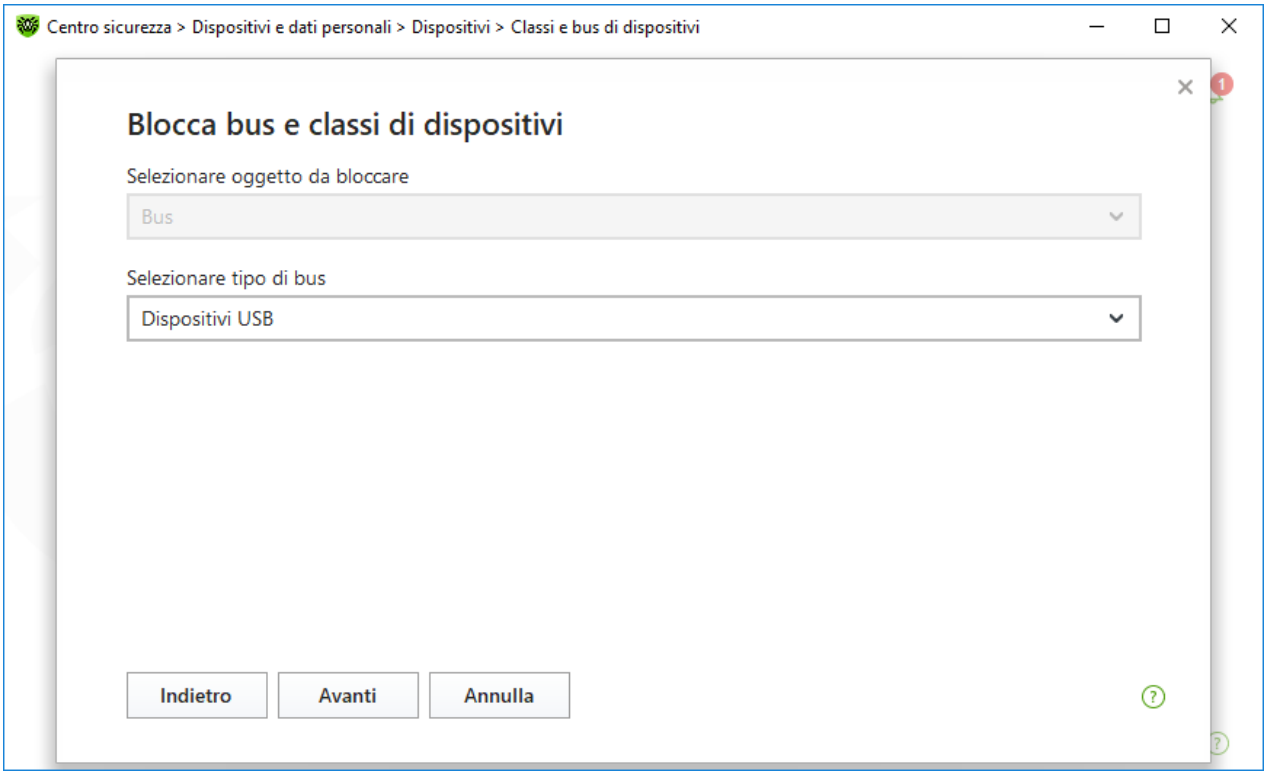

Immagine 74. Selezione del tipo di bus

4. Selezionare il tipo di blocco e premere **Avanti**:
   - **Completamente** — tutte le classi di dispositivi su questo bus saranno bloccate;

- **Parzialmente** — si aprirà una finestra per selezionare le classi di dispositivi da bloccare su questo bus.

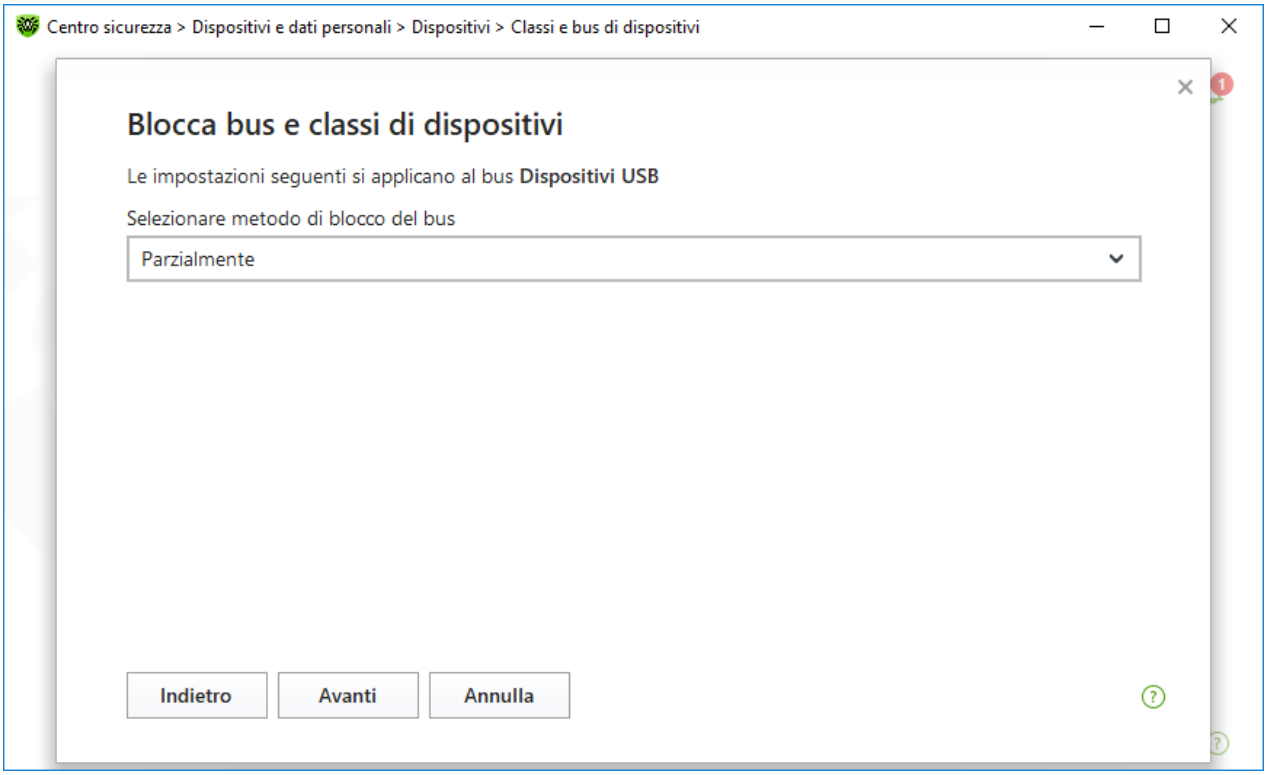

Immagine 75. Selezione del metodo di blocco del bus

5. Se è stata selezionata l'opzione **Parzialmente**, nella finestra che si è aperta contrassegnare con flag le classi dalla lista che si vogliono bloccare. Premere **Blocca**.

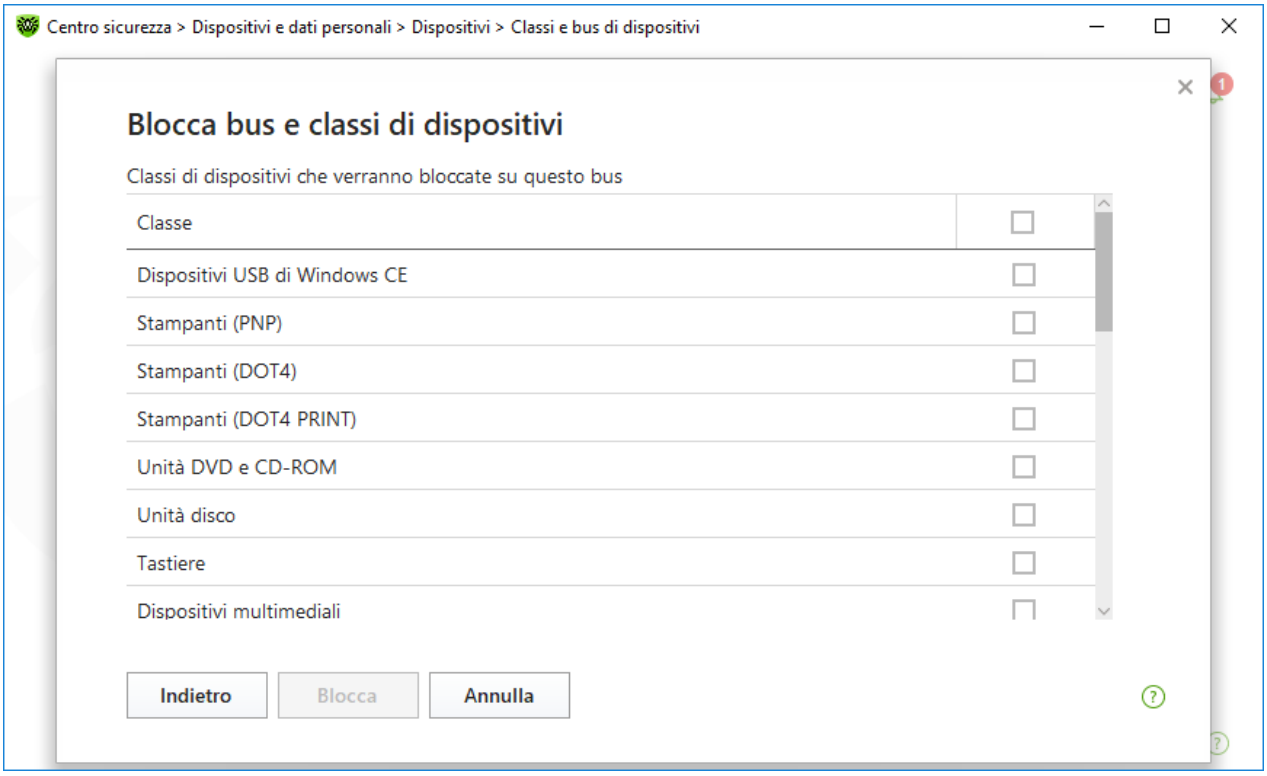

Immagine 76. Selezione delle classi di dispositivi su un bus

Blocco della classe di dispositivi

1. Per bloccare una o più classi di dispositivi, premere il pulsante ⊕.
2. Dalla lista a cascata selezionare l'oggetto che si vuole bloccare: **Classe**. Premere **Avanti**.

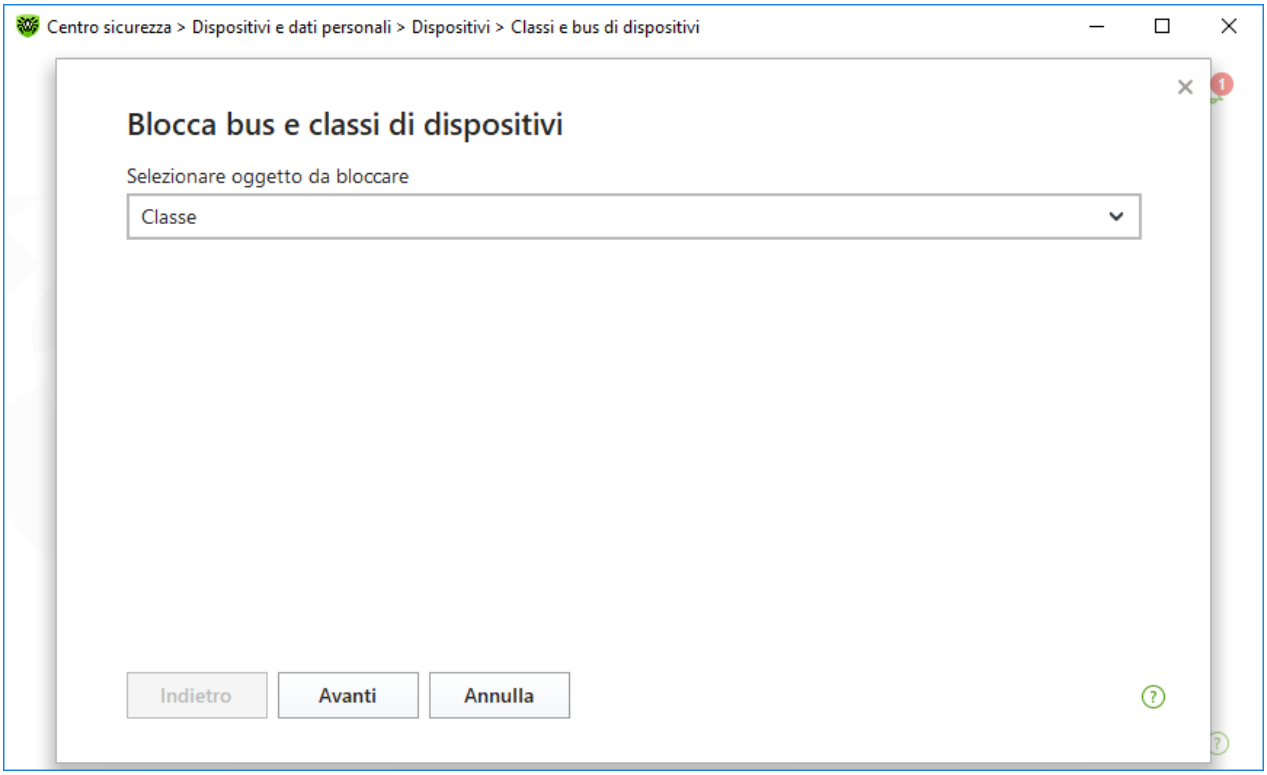

Immagine 77. Selezione dell'oggetto da bloccare

3. Contrassegnare con flag le classi dalla lista che si vogliono bloccare. Premere **Blocca**.

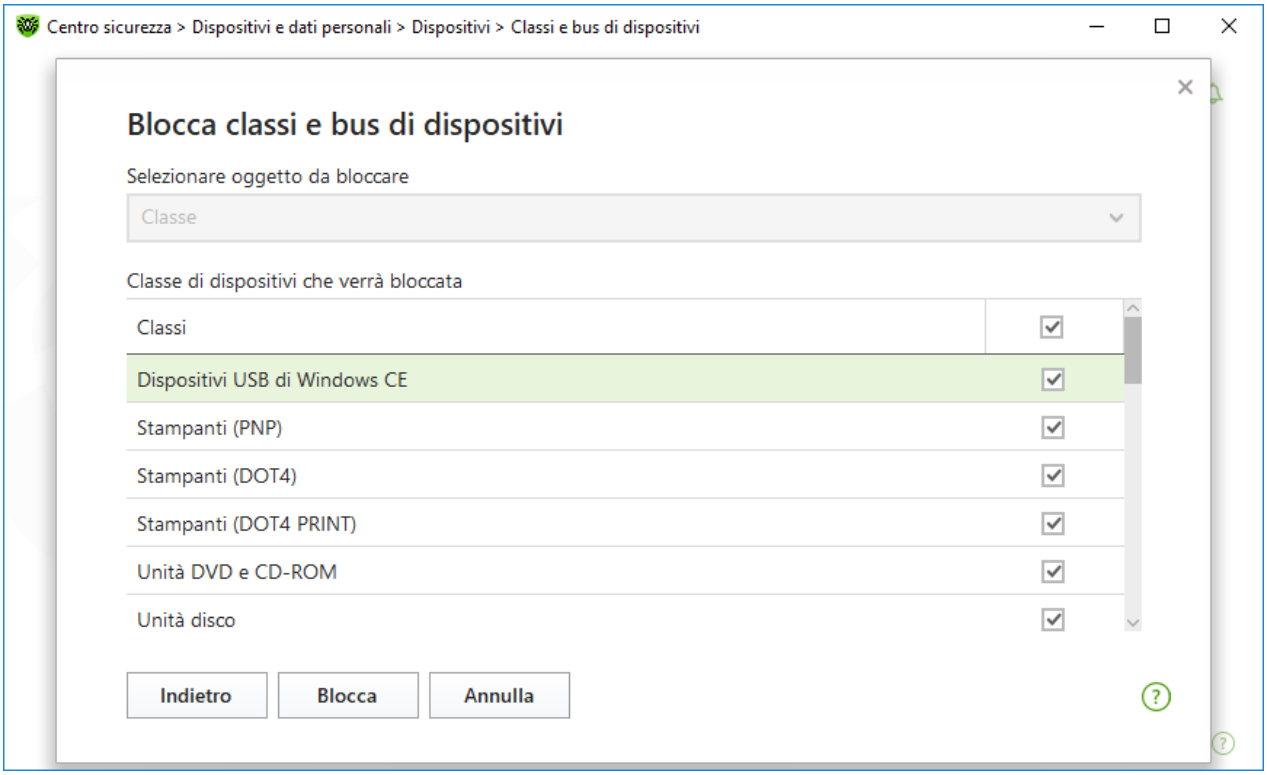

Immagine 78. Selezione delle classi di dispositivi

Quando viene attivato il blocco di un dispositivo già collegato, è necessario o collegare il dispositivo nuovamente, o riavviare il computer. Il blocco funziona solo per i dispositivi che vengono collegati dopo l'attivazione della funzione.

Quando il bus USB è bloccato, la tastiera e il mouse vengono inseriti in eccezioni.

Ricezione degli avvisi

È possibile configurare la visualizzazione sullo schermo degli avvisi sul blocco di dispositivi.

10.2. Dispositivi consentiti

Per andare alla finestra Dispositivi consentiti

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Dispositivi**.
3. Nel gruppo di impostazioni **Dispositivi consentiti** fare clic sul link **Modifica**.

La finestra **Dispositivi consentiti** contiene informazioni su tutti i dispositivi aggiunti alla lista dei consentiti. Queste informazioni sono presentate sotto forma di una tabella:

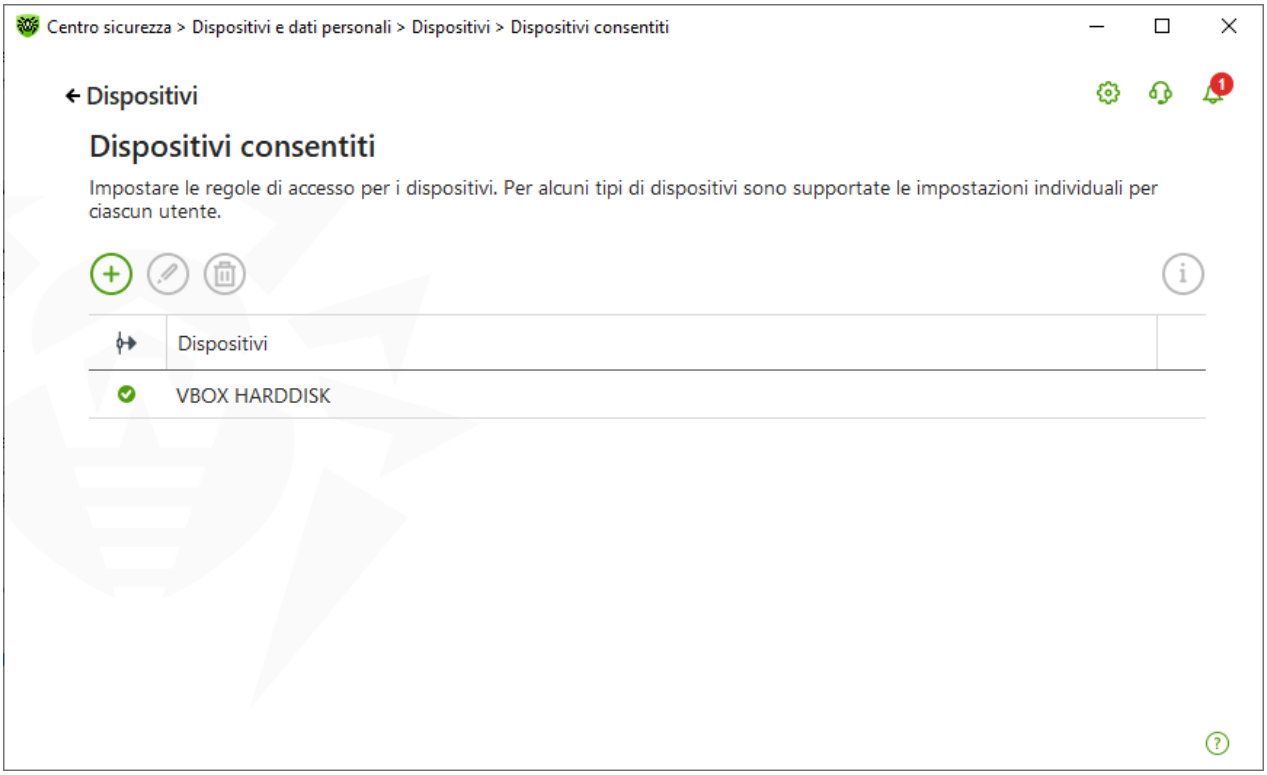

Immagine 79. Dispositivi consentiti

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — aggiunta di un set di regole per il dispositivo;
- Pulsante ✎ — modifica di un set di regole per il dispositivo;
- Pulsante 🗑 — rimozione di un set di regole per il dispositivo.

È possibile visualizzare informazioni dettagliate su un dispositivo aggiunto alla lista dei consentiti. Per fare ciò, selezionare la riga richiesta e premere ⓘ.

Nella colonna (**Tipo di regola**) sono visualizzati due tipi di regole:

- ✔ — è impostata la regola **Consenti tutto**.
- ⚙ — è impostata la regola **Sola lettura**.

Per aggiungere un dispositivo alla lista dei consentiti

1. Assicurarsi che il dispositivo sia collegato al computer.
2. Premere il pulsante ⊕. Nella finestra che si è aperta premere il pulsante **Sfoglia** e selezionare il dispositivo richiesto. Utilizzare un filtro affinché nella tabella vengano visualizzati solo i dispositivi collegati o solo quelli scollegati. Premere il pulsante **OK**.

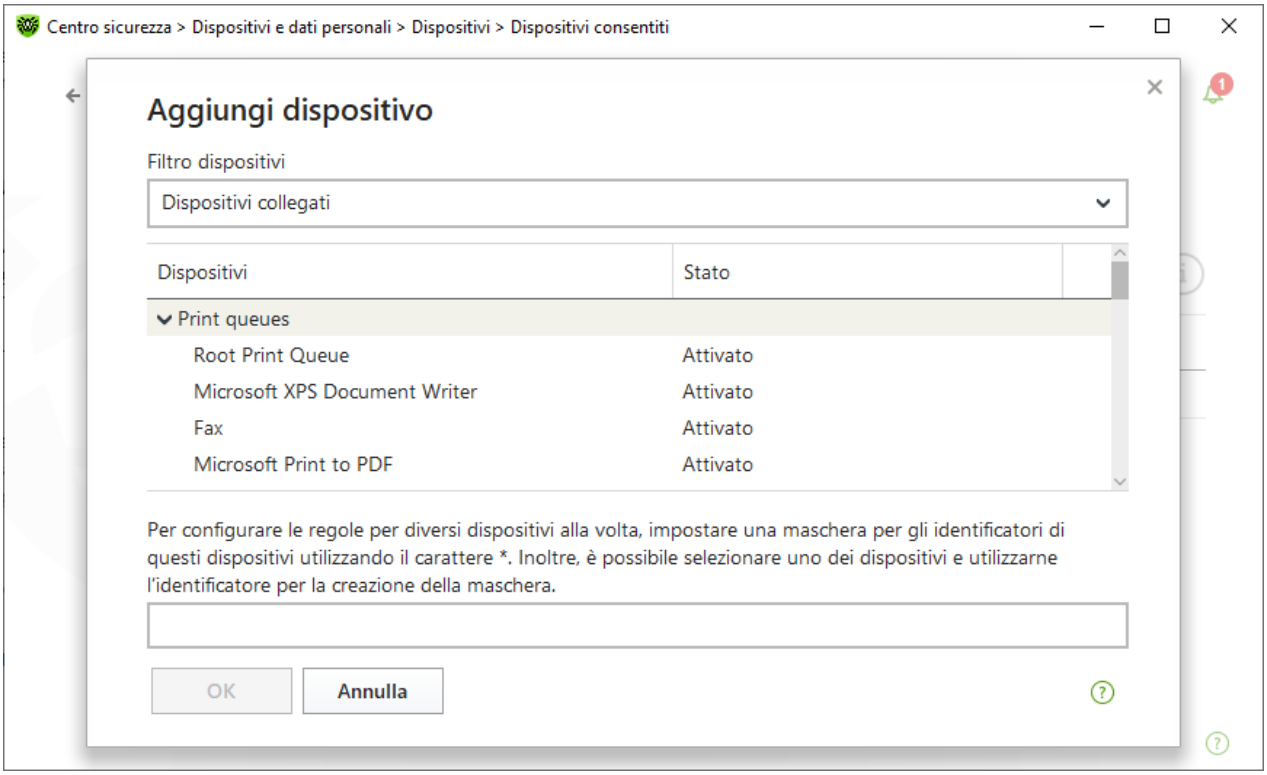

Immagine 80. Aggiunta di un dispositivo alla lista dei consentiti

3. Per i dispositivi con un file system è possibile configurare regole di accesso. Per farlo, nella colonna **Regola** selezionare una delle modalità: **Consenti tutto** o **Sola lettura**. Per aggiungere una nuova regola per uno specifico utente, premere il pulsante ⊕. Per eliminare una regola, premere 🗑.

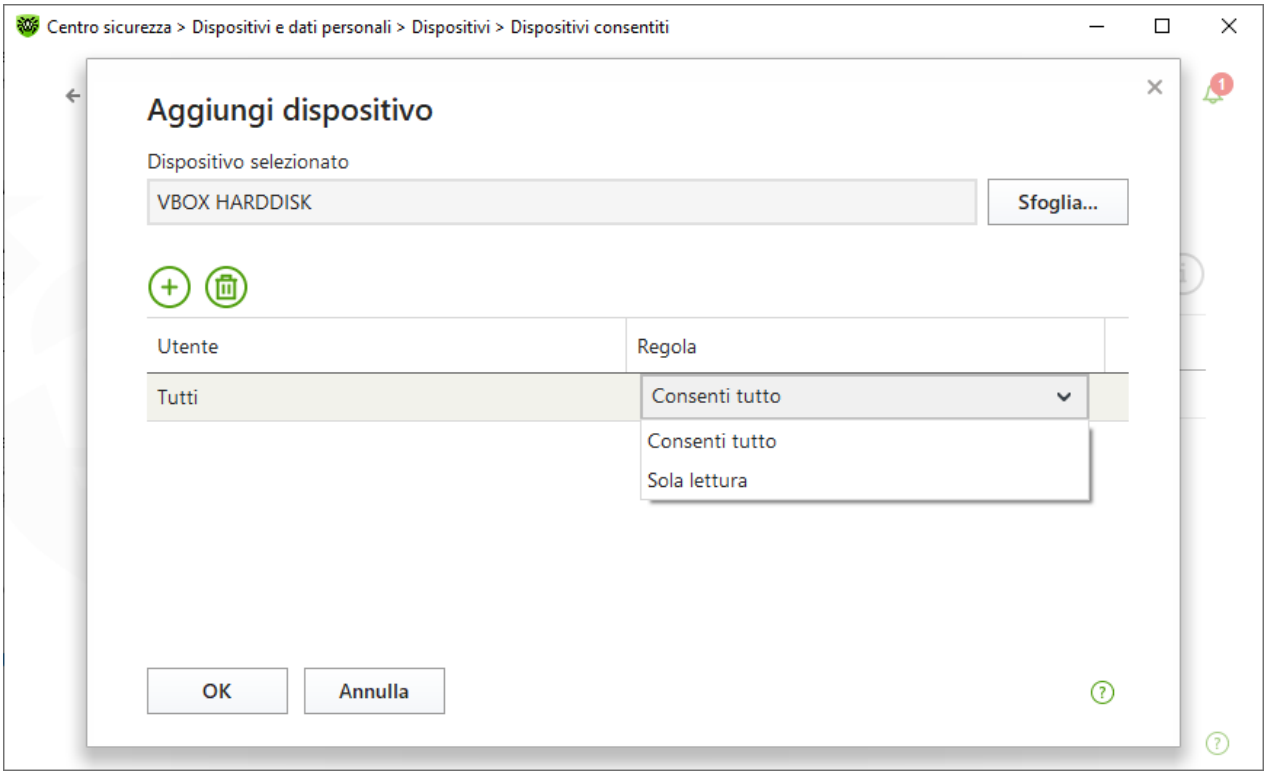

Immagine 81. Selezione della regola per un determinato utente

4. Per salvare le modifiche, premere **OK**. Per uscire dalla finestra senza salvare le modifiche, premere **Annulla** Si ritornerà alla lista dei dispositivi consentiti.

11. Office control

Tramite il componente Office control è possibile gestire l'accesso degli utenti a siti, file e cartelle, e inoltre controllare il tempo di utilizzo di internet e del computer.

Di default Office control è attivato e funziona in modalità **Senza restrizioni**.

Per attivare o disattivare Office control

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Office control**. Si aprirà la finestra **Office control**.

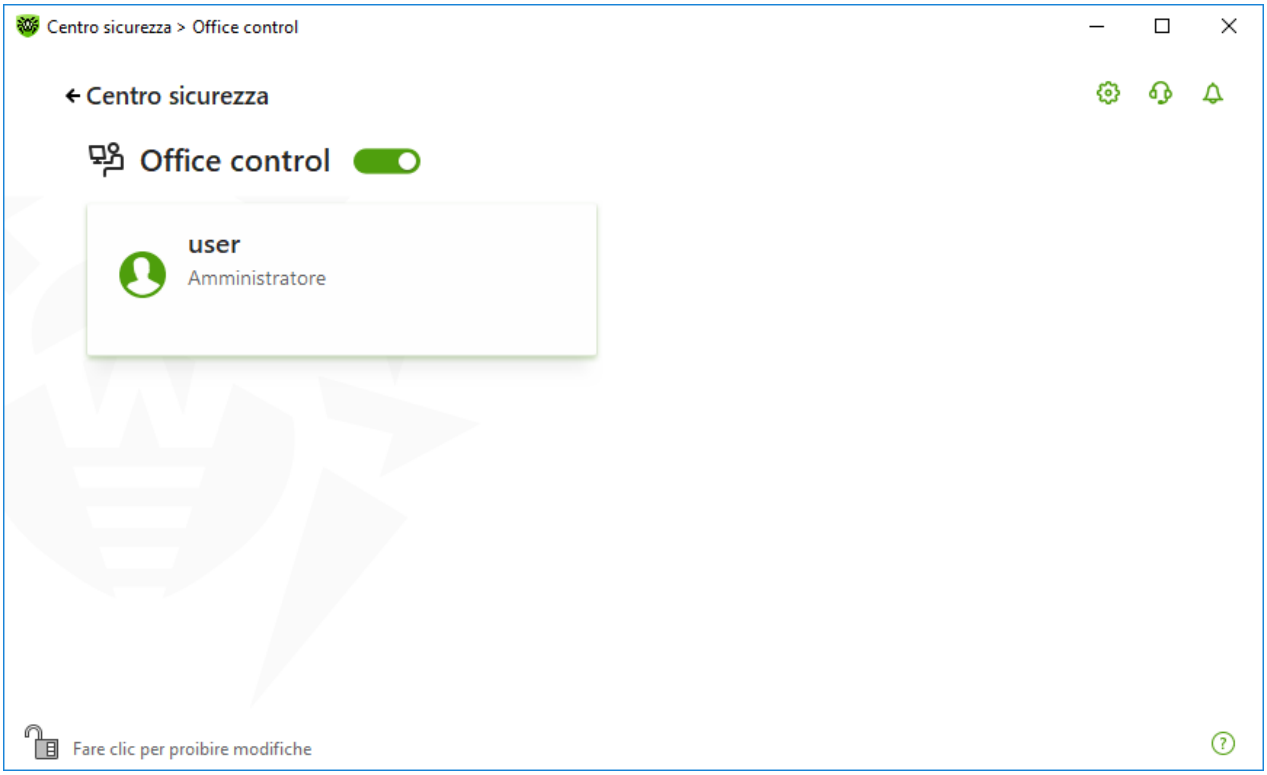

Immagine 82. Office control

3. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
4. Attivare o disattivare Office control utilizzando l'interruttore corrispondente .

I nuovi utenti vengono visualizzati nella lista solo dopo aver eseguito il primo accesso al loro account.

Parametri di Office control per un singolo utente

Prima di impostare limitazioni per un utente, assicurarsi che questo utente non disponga dei permessi di amministratore. Altrimenti, l'utente potrà modificare i parametri del componente Office control e disattivare le limitazioni di accesso.

> La modifica dei parametri del componente è possibile se è stata autorizzata dall'amministratore del server di protezione centralizzata a cui Dr.Web si connette.

Per andare ai parametri di Office control

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Nella finestra di Office control (vedi immagine Office control) fare clic sulla piastrella con il nome dell'utente per cui si vuole configurare Office control. Si aprirà la finestra dei parametri di Office control per l'utente selezionato.

Immagine 83. Parametri di Office control

3. Selezionare la scheda richiesta per modificare i parametri di Office control:
   - **Internet** — parametri di accesso alle risorse internet. Consente di proteggere gli utenti da visite a siti indesiderati (siti dedicati alla violenza, giochi d'azzardo ecc.), e inoltre autorizzare visite a siti indicati. Vedi sezione Accesso alle risorse internet.

- **Tempo** — parametri di accesso al computer e a internet. Consente di limitare per l'utente il tempo di utilizzo a determinati orari e giorni della settimana. Vedi sezione Limitazione di tempo.
- **File e cartelle** — parametri di accesso alle risorse del file system. Consente di limitare l'accesso a singoli file e cartelle interamente (su dischi locali e supporti rimovibili). Vedi sezione Accesso a file e cartelle.

Se l'utente utilizza un account Windows con i permessi di amministratore, è necessario cambiare il tipo di account in utente standard.

Modifica del tipo di account utente

Su Windows XP

1. Aprire il menu **Start**, quindi premere il pulsante **Pannello di controllo** e selezionare **Account utente**.
2. Selezionare l'account di cui si vuole cambiare il tipo e premere **Cambia tipo di account**.
3. Selezionare il tipo di account **Limitato**.
4. Premere **Cambia tipo di account** per salvare le modifiche.

Su Windows Vista e Windows 7

1. Aprire il menu **Start**, quindi premere il pulsante **Pannello di controllo** e selezionare **Account utente**.
2. Per modificare il tipo di account utente, premere **Gestisci un altro account**.
3. Selezionare l'account di cui si vuole cambiare il tipo e premere **Cambia tipo di account**.
4. Selezionare il tipo di account **Utente standard**.
5. Premere **Cambia tipo di account** per salvare le modifiche.

Su Windows 8

1. Aprire il **Pannello di controllo** e selezionare **Account utente e protezione famiglia**.
2. Premere il pulsante **Gestisci un altro account**.
3. Selezionare l'account di cui si vuole cambiare il tipo e premere **Cambia tipo di account**.
4. Selezionare il tipo di account **Utente standard**.
5. Premere **Cambia tipo di account** per salvare le modifiche.

Su Windows 8.1

1. Spostare il puntatore del mouse nell'angolo in basso a destra dello schermo, quindi verso l'alto e premere il pulsante **Impostazioni**, quindi selezionare **Cambia impostazioni computer**.
2. Selezionare l'elemento **Account**, quindi — **Altri account**.
3. Selezionare l'account di cui si vuole cambiare il tipo e premere **Cambia tipo di account**.
4. Selezionare il tipo di account **Utente standard**.
5. Premere **OK**.

Su Windows 10

1. Premere il pulsante **Start**, quindi premere il pulsante **Impostazioni**.
2. Nella finestra che si è aperta selezionare **Account**.
3. Nella parte sinistra della finestra selezionare **Famiglia e altri utenti**.
4. Fare clic sull'icona dell'account di cui si vuole cambiare il tipo e premere **Cambia tipo di account**.
5. Selezionare il tipo di account **Utente standard**.
6. Premere **OK**.

Su Windows 11

1. Premere il pulsante **Start**, quindi premere il pulsante **Impostazioni**.
2. Nella finestra che si è aperta selezionare **Account**.
3. Nella parte centrale della finestra selezionare **Famiglia e altri utenti**.
4. Fare clic sull'icona dell'account di cui si vuole cambiare il tipo e premere **Cambia tipo di account**.
5. Selezionare il tipo di account **Utente standard**.
6. Premere **OK**.

Se sul computer è presente un solo account, non è possibile cambiarne il tipo in utente standard. Maggiori informazioni possono essere trovate sul sito del servizio di supporto tecnico dell'azienda Microsoft.

Ricezione degli avvisi

È possibile configurare la visualizzazione sullo schermo degli avvisi sulle attività del componente Office control.

11.1. Accesso alle risorse internet

Nella scheda **Internet** è possibile limitare per l'utente la visita a siti indesiderati (siti dedicati alla violenza, giochi d'azzardo ecc.), e inoltre autorizzare la visita a siti indicati. Di default per tutti gli utenti è impostata la modalità **Senza restrizioni**. Sono inoltre disponibili le seguenti modalità:

- **Limita l'accesso in base alle categorie**
- **Consenti l'accesso solo per i siti dalla white list**

Il traffico cifrato non viene controllato. Il blocco di risorse in browser è possibile solo in base al nome di host.

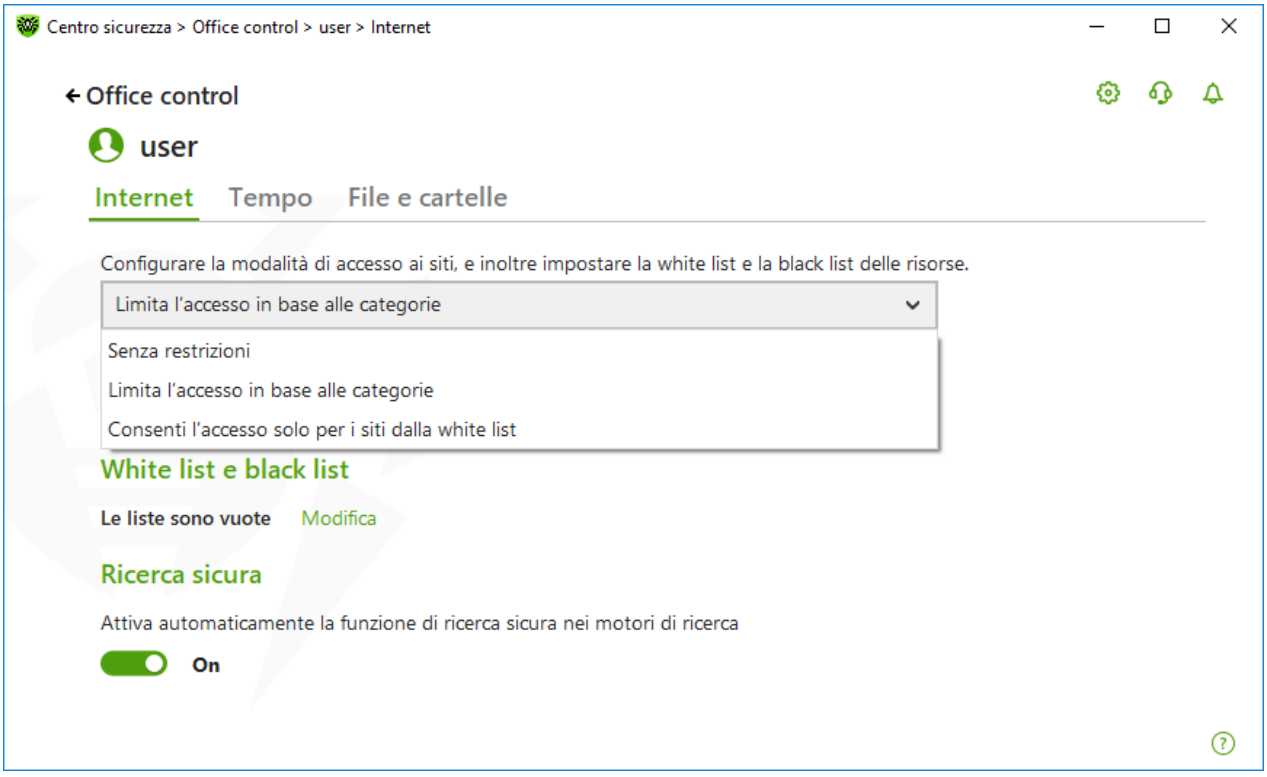

Immagine 84. Selezione della modalità di funzionamento di Office control

La modalità Limita l'accesso in base alle categorie

In questa modalità è possibile indicare le categorie di risorse, l'accesso a cui si vuole limitare. Uno stesso sito può essere classificato contemporaneamente in più categorie diverse. In questo caso Office control blocca l'accesso al sito se rientra in almeno una delle categorie vietate.

Inoltre, in questa modalità è possibile indicare in autonomo i siti l'accesso a cui sarà vietato o consentito a prescindere da altre restrizioni. Per fare questo, utilizzare la white list e black list di siti.

> Prima di attivare la limitazione per categoria, è necessario ripulire la cache del browser.

Per vietare o consentire l'accesso alle risorse web della categoria richiesta

1. Nel gruppo di impostazioni **Categorie di siti** cliccare sul link **Modifica**. Si aprirà la finestra dei parametri delle categorie bloccate.

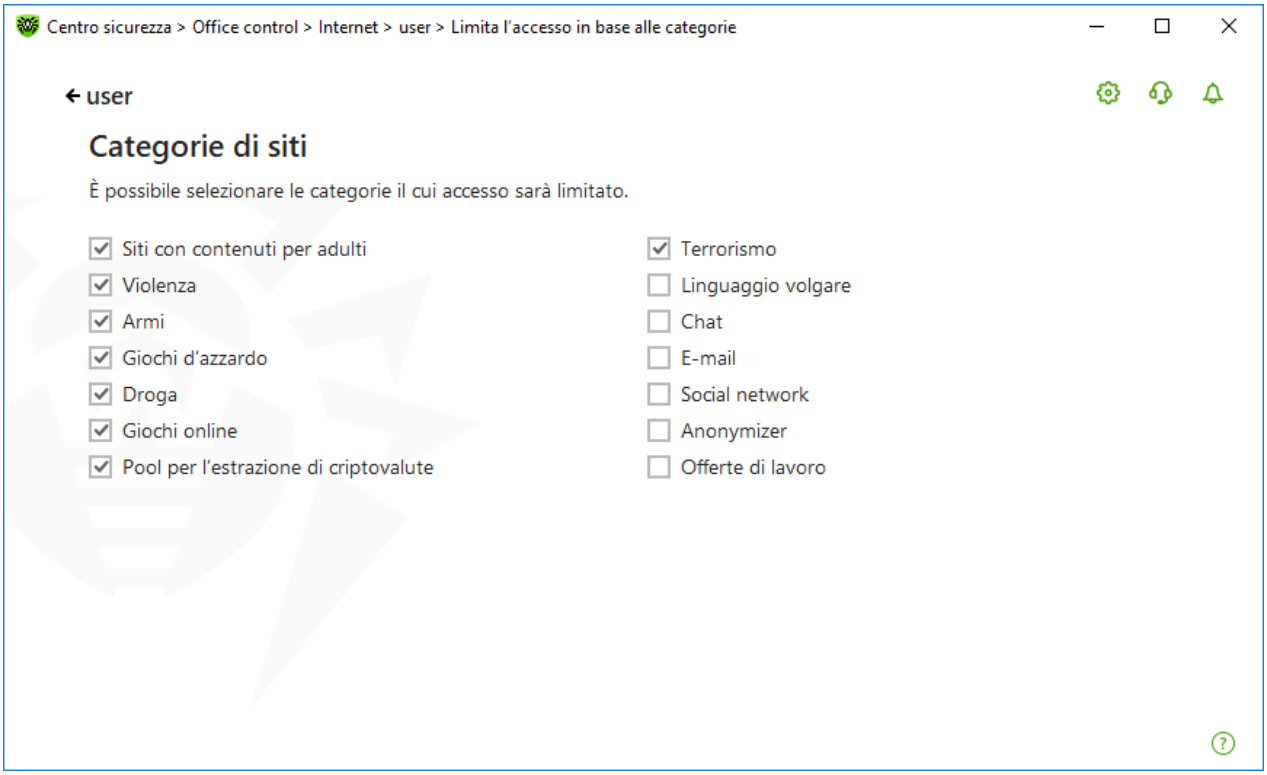

Immagine 85. Categorie di siti bloccati

2. Spuntare o togliere il flag per vietare o consentire l'accesso alle risorse web della categoria richiesta.

Categorie di risorse internet

Categoria	Descrizione
Siti con contenuti per adulti	Siti contenenti materiali di carattere pornografico o erotico, siti di incontri, ecc.
Violenza	Siti contenenti richiami alla violenza, materiali su vari incidenti con perdita di vite umane ecc.
Armi	Siti dedicati alle armi e agli esplosivi, nonché materiali che descrivono la loro fabbricazione ecc.
Giochi d'azzardo	Siti che ospitano giochi online per soldi, casinò online, aste, e inoltre siti di scommesse ecc.
Droga	Siti che promuovono l'uso, la fabbricazione o la distribuzione di sostanze stupefacenti ecc.
Giochi online	Siti che ospitano giochi che utilizzano una connessione Internet permanente.
Terrorismo	Siti contenti materiali di carattere propagandistico e aggressivo, descrizioni di attentati ecc.
Linguaggio volgare	Siti che contengono linguaggio volgare (nei titoli di sezioni, articoli e così via).
Chat	Siti per lo scambio di messaggi in tempo reale.
Posta elettronica	Siti che forniscono la possibilità di registrazione gratuita di caselle email.
Social network	Social network di carattere generale, social network d'affari, aziendali, dedicati a un determinato argomento, nonché siti di incontri dedicati a un determinato argomento.
Anonymizer	Siti che consentono all'utente di nascondere le proprie informazioni personali e forniscono accesso a siti bloccati.
Pool per l'estrazione di criptovalute	Siti che forniscono accesso a servizi che riuniscono gli utenti con lo scopo di estrazione di criptovalute (mining).
Offerte di lavoro	Siti che vengono utilizzati per pubblicare offerte di lavoro e cercare lavoro.

La modalità Consenti l'accesso solo per i siti dalla white list

In questa modalità viene vietato l'accesso a tutte le risorse web eccetto quelle indicate nella white list di siti.

Se è selezionata la modalità **Consenti l'accesso solo per i siti dalla white list**, tali siti possono non essere visualizzati correttamente. Non saranno visualizzati banner e altri

elementi del sito integrati con risorse esterne.

White list e black list di siti

È possibile impostare una white list e una black list di siti l'accesso a cui viene consentito o bloccato a prescindere da altri parametri di Office control.

Prima di aggiungere un sito alla black list o white list, è necessario ripulire la cache del browser, se il sito veniva precedentemente aperto in questo browser.

Configurazione della white list e black list di siti di Office control

1. Nel gruppo di impostazioni **White list e black list** cliccare sul link **Modifica**. Si aprirà la finestra di configurazione della white list e black list.

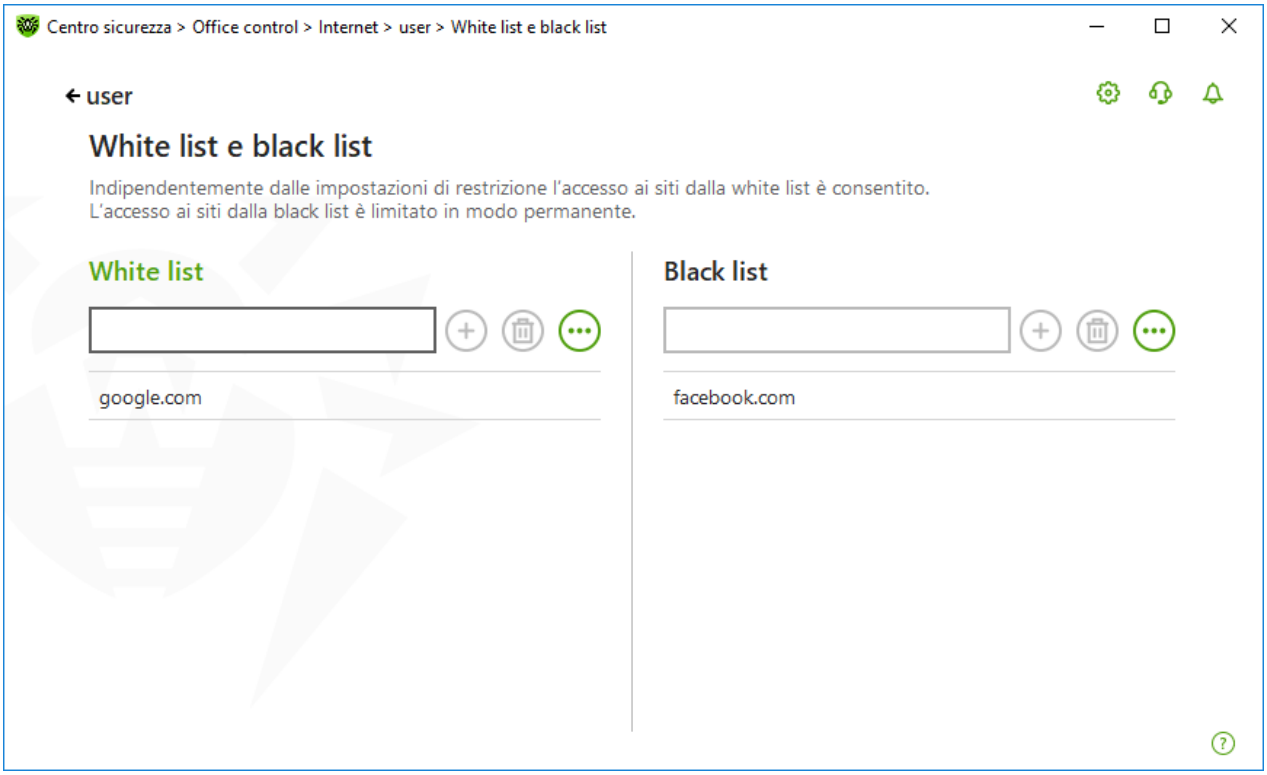

Immagine 86. Configurazione della white list e black list di Office control

2. Inserire un oggetto nel campo **White list** per consentire l'accesso alla risorsa web. Inserire un oggetto nel campo **Black list** per vietare l'accesso alla risorsa web. L'inserimento dell'oggetto nella white list e black list è possibile nel formato di maschera, dominio o indirizzo (a livello di URL):
   - Per aggiungere alla lista determinati siti, inserire nel campo di input una maschera che li definisce. È ammesso l'utilizzo di lettere, cifre, dei caratteri ":", "/", "-", "?" e "*". Le maschere vengono aggiunte nel formato: `mask://...`

La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:

- il carattere "*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
- il carattere "?" sostituisce qualsiasi carattere, anche uno vuoto, ma uno solo.

Esempi:

- `mask://*.it/` — verranno elaborati tutti i siti nella zona `.it`;
- `mask://mail` — verranno elaborati tutti i siti in cui è contenuta la parola "mail";
- `mask://???.it/` — verranno elaborati tutti i siti della zona `.it`, di cui i nomi sono costituiti da tre caratteri o meno.

- Per aggiungere alla lista un dominio specifico, indicare il nome del dominio con o senza il simbolo "." alla fine dell'indirizzo. È ammesso l'utilizzo di lettere, cifre e del carattere "/".

  Esempi:

  - `example.com` — verrà elaborato `example.com` stesso, nonché i suoi sottodomini `*example.com`;
  - `example.` — verranno elaborati i sottodomini `*example.com`, ma non `example.com` stesso;
  - `it.` — verranno elaborati tutti i sottodomini della zona `.it` (per esempio, `example.it` o `www.test.it`).

- Per aggiungere alla lista siti nel cui indirizzo è contenuto un testo specifico, inserire nel campo questo testo. È ammesso l'utilizzo di lettere, cifre, dei caratteri "/" e "-".

  Esempi:

  - `example` — verranno elaborati indirizzi come `example.com`, `test.example222.com` ecc.

La stringa inserita al momento dell'aggiunta alla lista può essere convertita in forma universale. Per esempio, l'indirizzo `https://www.example.com` verrà convertito nel record `example.com`.

L'inserimento di maschera, dominio e indirizzo non tiene conto delle differenze tra maiuscole e minuscole. Questo significa che i record `example.com` e `ExAMple.COM` verranno elaborati allo stesso modo.

3. Premere il pulsante  per aggiungere l'indirizzo alla lista.
4. Per cancellare un indirizzo dalla lista, selezionarlo nella lista e premere il pulsante  .
5. Se necessario, ripetere i passi 2 e 3 per aggiungere altre risorse.

Ricerca sicura

L'opzione **Ricerca sicura** influisce sull'output dei risultati dei motori di ricerca. Questa funzione consente di escludere risorse indesiderate dai risultati di una ricerca, utilizzando le funzionalità dei motori di ricerca.

Il traffico cifrato non viene controllato.

Per attivare la funzione **Ricerca sicura**, impostare l'interruttore sullo stato **On**.

11.2. Limitazione del tempo di utilizzo del computer e di internet

Nella scheda **Tempo** è possibile limitare il tempo di utilizzo del computer e di internet da parte degli utenti. Di default per tutti gli utenti è impostata la modalità **Senza restrizioni**.

È possibile limitare il tempo di utilizzo per gli utenti utilizzando una tabella con quadrati di tempo.

Quando vengono attivate le limitazioni al tempo di utilizzo del computer o di internet, viene automaticamente attivata l'opzione **Proibisci la modifica della data e dell'ora di sistema** nella finestra Auto-protezione delle impostazioni principali.

Tabella della limitazione del tempo di utilizzo del computer e di internet

La tabella è disponibile nella modalità di Office control **Senza restrizioni**. Quando vengono apportate modifiche alla tabella, il profilo **Senza restrizioni** sarà automaticamente sostituito con **Personalizzato**.

Utilizzando la tabella, è possibile specificare i giorni della settimana e le ore in cui un utente può utilizzare il computer, nonché internet. Quando arriverà il momento di limitare l'accesso al computer, verrà automaticamente effettuato il logout dal sistema. Fino a quando sono attive le limitazioni per un account specifico, non è possibile eseguire l'accesso a tale account. Durante il periodo di limitazione dell'utilizzo di internet è interrotto il caricamento di tutti i contenuti internet.

Il tempo mancante all'attivazione delle restrizioni di accesso può essere visualizzato nel menu Dr.Web facendo clic sulla piastrella **Limitazione di tempo**.

Per limitare il tempo di utilizzo in modalità tabella

1. Selezionare i giorni della settimana e le ore in cui occorre vietare all'utente l'accesso a internet ed evidenziare in blue le celle di tempo corrispondenti:
   - per selezionare una cella, farci clic una volta con il pulsante sinistro del mouse;
   - per selezionare contemporaneamente diverse celle situate una accanto alle altre, fare clic una volta con il pulsante sinistro del mouse sulla prima cella e tenendo premuto il pulsante selezionare il periodo richiesto.
2. Selezionare i giorni della settimana e le ore in cui occorre vietare all'utente l'utilizzo del computer ed evidenziare in rosso le celle di tempo corrispondenti:
   - per selezionare una cella, farci doppio clic con il pulsante sinistro del mouse;
   - per selezionare contemporaneamente diverse celle situate una accanto alle altre, fare doppio clic con il pulsante sinistro del mouse sulla prima cella e tenendo premuto il pulsante selezionare il periodo richiesto.

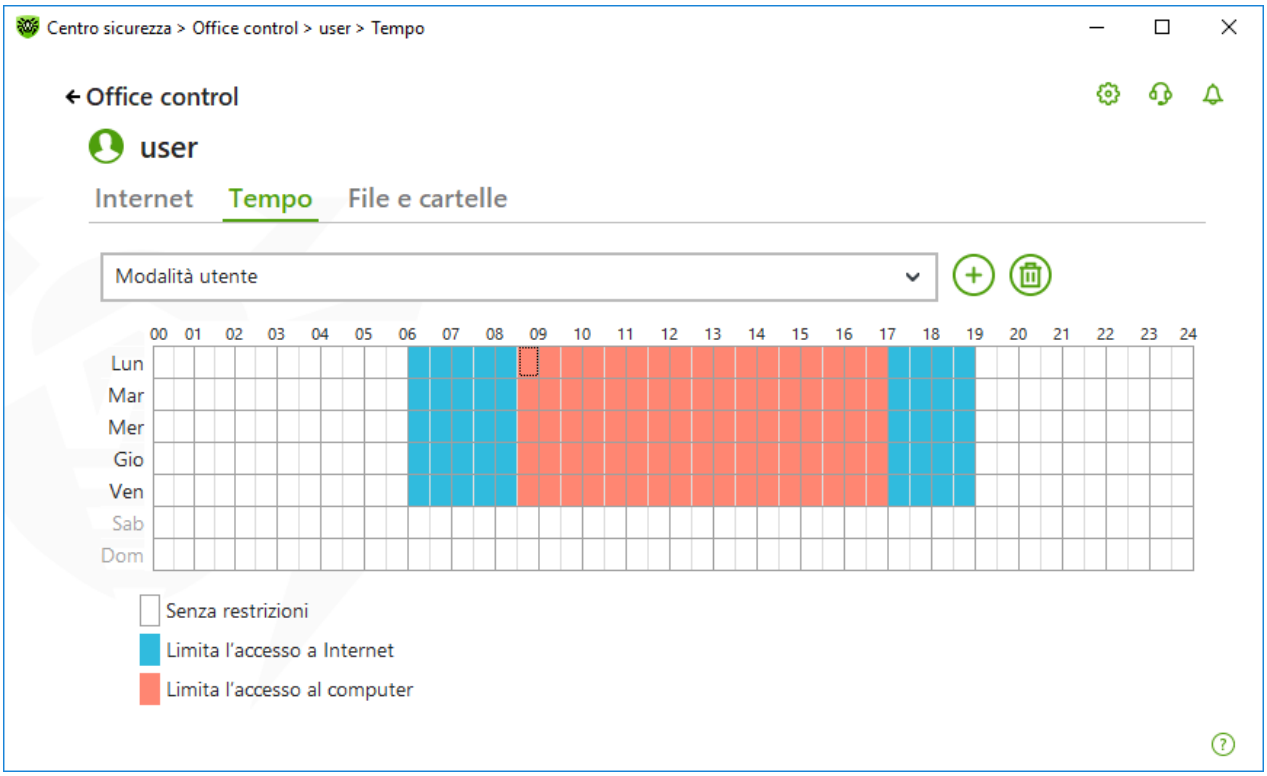

Immagine 87. Tabella del tempo di utilizzo del computer e di internet

Inoltre, è possibile creare diverse impostazioni per lo stesso utente salvandole in profili. Questa opzione sarà comoda se sarà necessario cambiare periodicamente le impostazioni con altri valori memorizzati.

Salvataggio e rimozione di un profilo delle impostazioni

- Per creare un profilo delle impostazioni, premere il pulsante ⊕. Nel profilo verranno salvate le impostazioni della tabella correnti. In futuro quando si modificano le impostazioni del profilo, verranno automaticamente salvate.
- Per rimuovere un profilo delle impostazioni, premere il pulsante 🗑.

11.3. Accesso a file e cartelle

Nella scheda **File e cartelle** è possibile limitare l'accesso degli utenti a file e cartelle. Di default non ci sono limitazioni all'accesso a file e cartelle.

Per attivare o disattivare la limitazione dell'accesso dell'utente a file e cartelle, utilizzare l'interruttore ⬤.

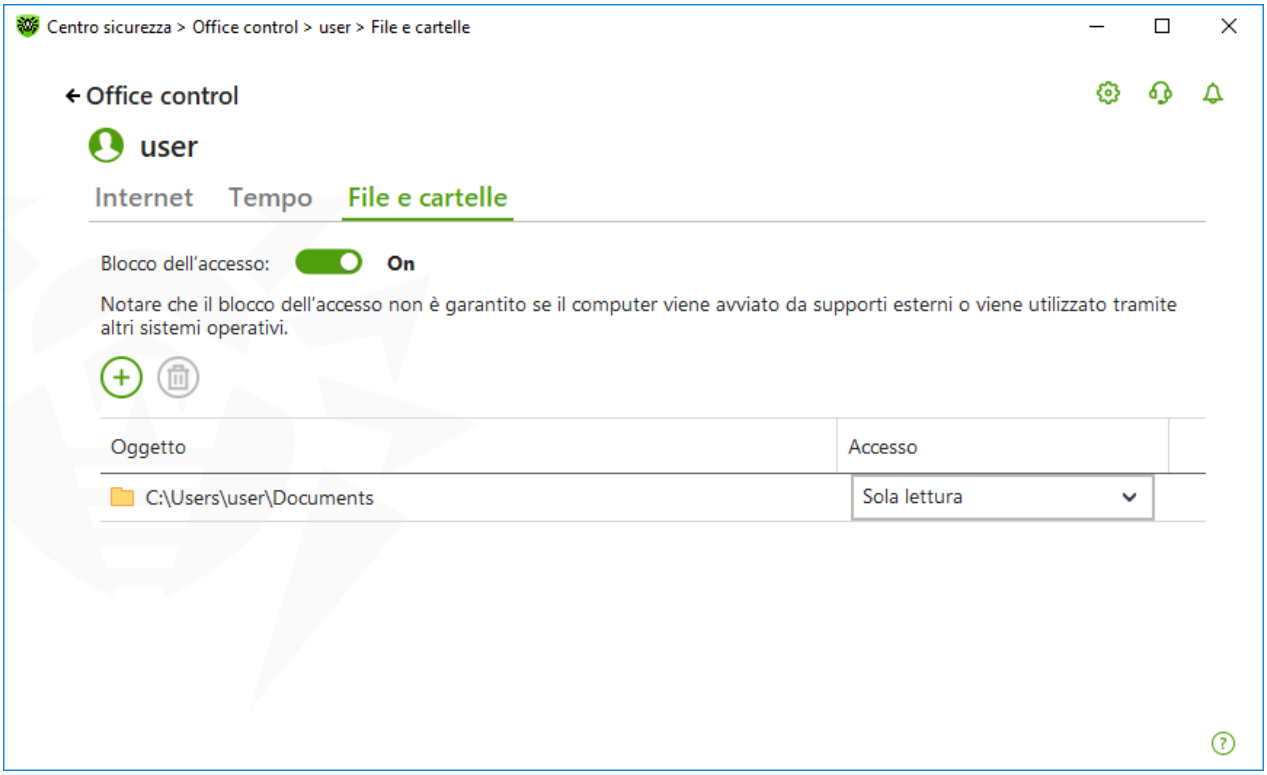

Immagine 88. Gestione dell'accesso a file e cartelle

⚠ La limitazione di accesso non è garantita se il computer viene avviato da supporti rimovibili o se si accede agli oggetti impostati da altri sistemi operativi installati sul computer.

Per limitare l'accesso a file e cartelle

1. Attivare il blocco dell'accesso a file e cartelle utilizzando l'interruttore ⬤.

2. Per aggiungere un oggetto alla lista, premere il pulsante e selezionare il file o la cartella richiesta.
3. Selezionare la modalità di accesso per l'oggetto aggiunto:
   - **Bloccato** per bloccare completamente l'accesso all'oggetto selezionato.
   - **Sola lettura** (selezionata di default) per consentire la lettura dell'oggetto selezionato (per esempio, la visualizzazione di un documento, di un'immagine, l'avvio di un file eseguibile), l'oggetto selezionato non potrà essere spostato, rimosso o il suo contenuto non potrà essere modificato.

Per rimuovere un oggetto, selezionarlo dalla lista e premere il pulsante .

12. Gestione quarantena

Gestione quarantena — strumento che consente di gestire i file isolati. Quarantena contiene file in cui sono stati rilevati oggetti malevoli. Inoltre, in quarantena vengono messe le copie di backup dei file elaborati da Dr.Web. Gestione quarantena fornisce la possibilità di rimuovere, ricontrollare e ripristinare i file isolati.

Per andare alla finestra Gestione quarantena

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Fare clic sulla piastrella **Gestione quarantena**.

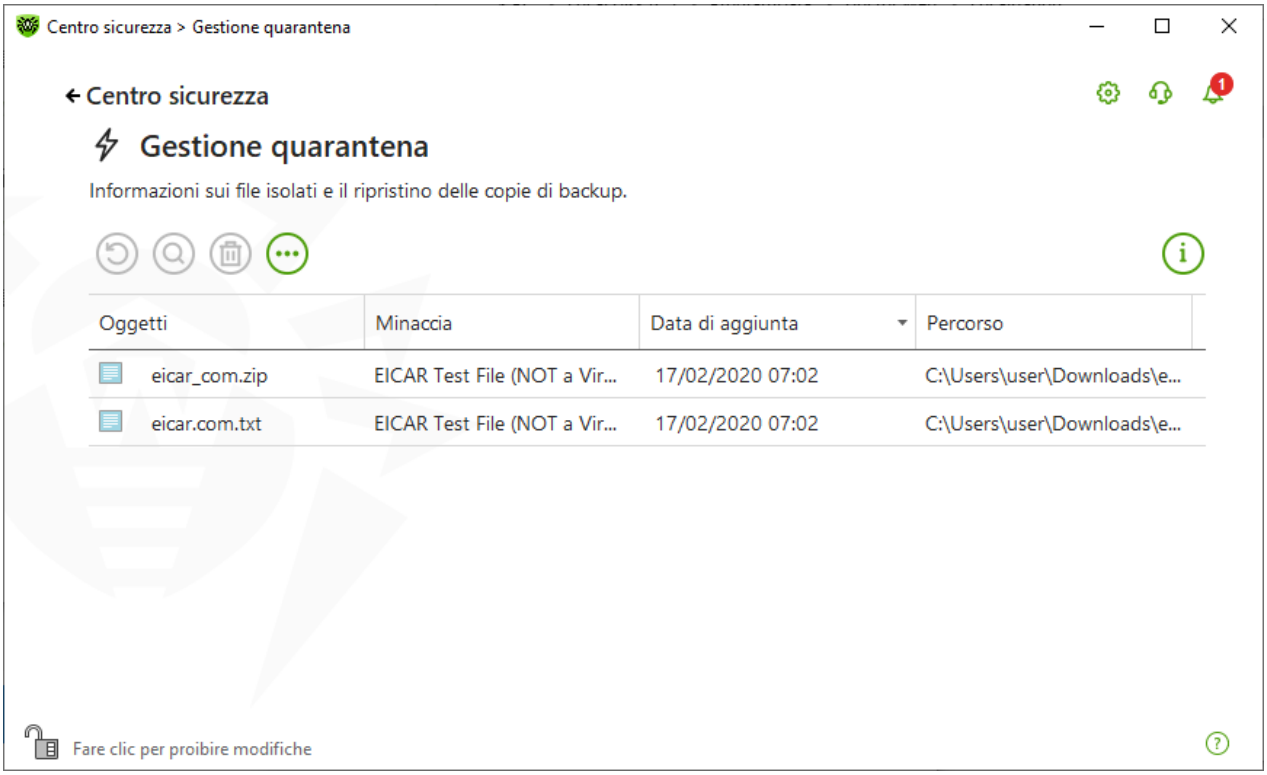

Immagine 89. Oggetti in quarantena

Nella parte centrale della finestra viene visualizzata una tabella con le informazioni sullo stato della quarantena che comprende i seguenti campi:

- **Oggetti** — una lista dei nomi degli oggetti messi in quarantena;
- **Minaccia** — la classificazione del programma malevolo che viene determinata da Dr.Web allo spostamento in quarantena automatico dell'oggetto;
- **Data di aggiunta** — la data in cui l'oggetto è stato spostato in quarantena;
- **Percorso** — il percorso completo in cui si trovava l'oggetto prima dello spostamento in quarantena.

Nella finestra Gestione quarantena i file sono visibili solo agli utenti che hanno accesso ad essi. Per visualizzare oggetti nascosti, è necessario avere i privilegi di amministratore.

Le copie di backup messe in quarantena di default non vengono visualizzate nella tabella. Per vederle nella lista degli oggetti, premere il pulsante e dalla lista a cascata selezionare la voce **Mostra le copie di backup**.

Gestione degli oggetti in quarantena

In modalità amministratore per ciascun oggetto sono disponibili i seguenti pulsanti di gestione:

- Pulsante (**Ripristina**) — per spostare uno o più oggetti selezionati nella cartella richiesta.

  Utilizzare questa funzione solo se si è certi che l'oggetto è sicuro.

- Pulsante (**Ricontrolla**) — per scansionare nuovamente un oggetto messo in quarantena.
- Pulsante (**Rimuovi**) — per rimuovere uno o più oggetti selezionati dalla quarantena e dal sistema.

Queste azioni sono disponibili anche nel menu contestuale quando si fa clic con il pulsante destro del mouse su uno o più oggetti selezionati.

Per rimuovere tutti gli oggetti dalla quarantena, premere il pulsante e dalla lista a cascata selezionare la voce **Rimuovi tutto**.

Avanzate

Per impostare le opzioni di conservazione e di rimozione automatica dei record in quarantena, andare alle impostazioni di Gestione quarantena.

13. Eccezioni

In questo gruppo di impostazioni è possibile impostare le eccezioni al controllo da parte dei componenti SpIDer Guard, SpIDer Gate, SpIDer Mail e Scanner, e inoltre aggiungere indirizzi mittente alla black list o alla white list in modo che le relative email non vengano controllate per la presenza di spam.

Per andare al gruppo di impostazioni Eccezioni

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Eccezioni**.

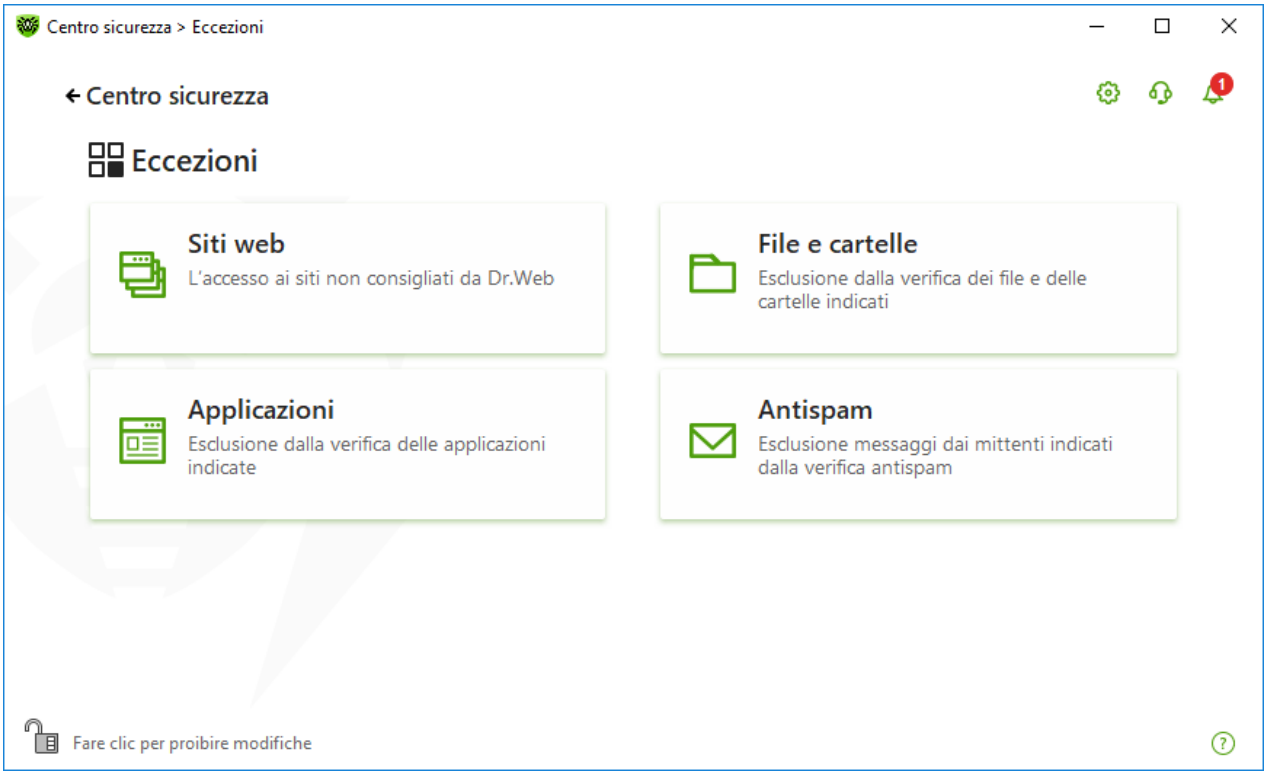

Immagine 90. Finestra Eccezioni

Per andare ai parametri delle eccezioni

1. Assicurarsi che Dr.Web funzioni in modalità amministratore (il lucchetto nella parte inferiore del programma è "aperto"). Altrimenti, cliccare sul lucchetto .
2. Fare clic sulla piastrella della sezione corrispondente.

> Notare che le modifiche in questo gruppo di impostazioni possono essere bloccate da parte dell'amministratore della rete antivirus.

In questa sezione:

- Siti web — parametri di accesso ai siti non raccomandati dall'azienda Doctor Web.
- File e cartelle — esclusione di determinati file e cartelle dalla scansione tramite i componenti SpIDer Guard e Scanner.
- Applicazioni — esclusione di determinati processi dalla scansione tramite i componenti SpIDer Guard, SpIDer Gate e SpIDer Mail.
- Antispam — parametri di scansione antispam delle email tramite il componente SpIDer Mail.

13.1. Siti

È possibile configurare una lista di siti l'accesso a cui sarà consentito indipendentemente dai parametri di scansione del traffico HTTP tramite il componente SpIDer Gate. Se nei parametri di SpIDer Gate è attivata l'opzione **Blocca l'accesso ai siti sconsigliati**, è possibile consentire l'accesso a determinati siti aggiungendoli alla lista delle eccezioni. L'accesso ai siti dalla lista sarà consentito, però la scansione antivirus di questi siti si mantiene.

Per impostare la lista dei siti a cui sarà consentito l'accesso

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Eccezioni**.
3. Fare clic sulla piastrella **Siti web**.

Immagine 91. Lista di siti esclusi

Di default la lista è vuota. Se l'indirizzo di un sito è aggiunto alla lista delle eccezioni, l'accesso ad esso verrà fornito indipendentemente dagli altri parametri di SplDer Gate. Notare che se tale sito è aggiunto contemporaneamente alla black list del modulo Office control e alle eccezioni, l'accesso ad esso sarà bloccato.

Per aggiungere indirizzi di dominio alla lista delle eccezioni

1. Nel campo di immissione indicare il nome a dominio o una parte del nome a dominio di un sito, l'accesso a cui si vuole consentire a prescindere dalle altre restrizioni:
   - per aggiungere alla lista un determinato sito, immettere il suo indirizzo (per esempio `www.example.com`). Sarà consentito l'accesso a tutte le risorse situate su questo sito;
   - per consentire l'accesso ai siti nei cui indirizzi è contenuto un determinato testo, immettere questo testo nel campo. Esempio: se si immette il testo `example`, sarà consentito l'accesso agli indirizzi `example.com`, `example.test.com`, `test.com/example`, `test.example222.it` e così via;
   - per consentire l'accesso a un determinato dominio, indicare il nome del dominio con il carattere ".". In tale caso sarà consentito l'accesso a tutte le risorse situate in questo dominio. Se per indicare il dominio si usa il carattere "/", allora la parte della sottostringa a sinistra del carattere "/" verrà considerata il nome a dominio e le parti a destra del carattere verranno considerate la parte dell'indirizzo consentito in questo dominio. Esempio: se si immette il testo `example.com/test`, saranno consentiti gli indirizzi `example.com/test11`, `template.example.com/test22` e così via;
   - per aggiungere alle eccezioni determinati siti, immettere nel campo di immissione una maschera che li definisce. Le maschere vengono aggiunte nel formato: `mask://...`

     La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:

     - il carattere "*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
     - il carattere "?" sostituisce qualsiasi carattere, anche uno vuoto, ma uno solo.

     Esempi:

     - `mask://*.it/` — si apriranno tutti i siti nella zona `.it`;
     - `mask://mail` — si apriranno tutti i siti in cui è contenuta la parola "mail";
     - `mask://???.it/` — si apriranno tutti i siti della zona `.it`, di cui i nomi sono costituiti da tre caratteri o meno.

   La stringa immessa al momento dell'aggiunta alla lista può essere trasformata in forma universale. Per esempio, l'indirizzo `http://www.example.com` verrà trasformato nel record `www.example.com`.
2. Premere il pulsante ⊕ o il tasto INVIO sulla tastiera. L'indirizzo indicato apparirà nella lista.
3. Se necessario, ripetere i passi 1 e 2 per aggiungere altri indirizzi.

Gestione degli oggetti nella lista

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante — aggiunta dell'indirizzo di un sito alla lista delle eccezioni. Diventa disponibile se viene inserito un valore nel campo di testo.
- Pulsante — modifica dell'indirizzo di sito selezionato nella lista delle eccezioni.
- Pulsante — rimozione dell'indirizzo di sito selezionato dalla lista delle eccezioni.
- Attraverso il pulsante sono disponibili le seguenti azioni:
  - **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
  - **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
  - **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

Le azioni di rimozione o modifica dell'oggetto sono disponibili anche nel menu contestuale quando si fa clic con il pulsante destro del mouse su uno o più oggetti selezionati.

13.2. File e cartelle

È possibile configurare una lista di file e cartelle esclusi dalla scansione antivirus del sistema tramite i componenti SpIDer Guard e Scanner. Come tali possono essere le cartelle di quarantena dell'antivirus, le cartelle di lavoro di alcuni programmi, i file temporanei (file di swap) ecc.

Per configurare la lista di file e cartelle esclusi

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Eccezioni**.
3. Fare clic sulla piastrella **File e cartelle**.

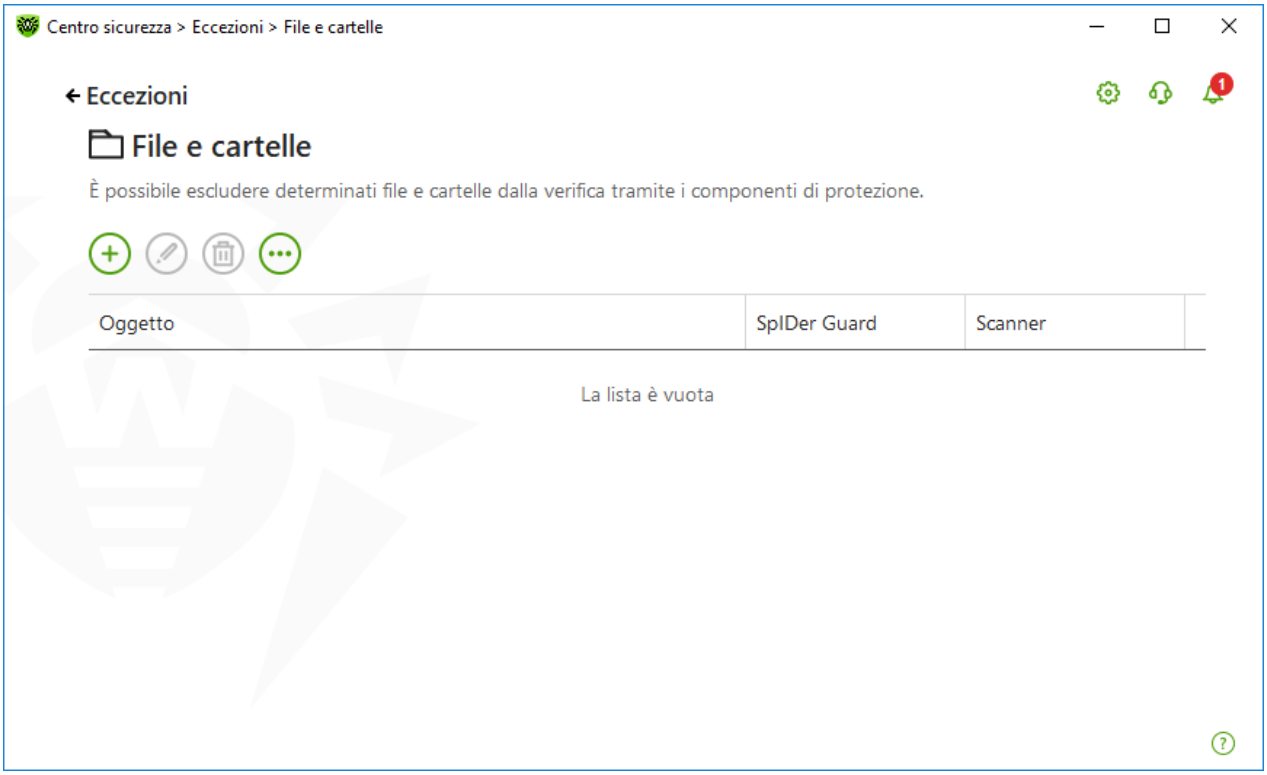

Immagine 92. Lista di file e cartelle esclusi

Di default la lista è vuota. Aggiungere alle eccezioni cartelle e file specifici o utilizzare maschere per vietare la scansione di un determinato gruppo di file. Ciascun oggetto che viene aggiunto può essere escluso dalla scansione eseguita tramite entrambi i componenti o tramite ciascun componente separatamente.

Per aggiungere file e cartelle alla lista delle eccezioni

1. Per aggiungere una cartella o un file alla lista delle eccezioni, eseguire una delle seguenti azioni:
   - per indicare un file o cartella specifica esistente, premere il pulsante ⊕. Nella finestra che si è aperta premere il pulsante **Sfoglia** per selezionare una cartella o un file. Si può immettere manualmente il percorso completo del file o della cartella nel campo di immissione, nonché modificare la stringa nel campo di immissione prima di aggiungerla alla lista. Esempio:
     - `C:\folder\file.txt` — si esclude dalla scansione il `file.txt` nella cartella `C:\folder`.
     - `C:\folder` — si escludono dalla scansione tutte le sottocartelle e i file nella cartella `C:\folder`.
   - per escludere dalla scansione un file con un determinato nome, immettere il nome del file con l'estensione nel campo di immissione. In questo caso non è necessario specificare il percorso del file. Esempio:
     - `file.txt` — si escludono dalla scansione tutti i file con il nome `file` e l'estensione `.txt` in tutte le cartelle.

- `file` — si escludono dalla scansione tutti i file con il nome `file` senza estensione in tutte le cartelle.

- per escludere dalla scansione un determinato tipo di file o cartelle, immettere nel campo di immissione una maschera che lo definisce.

  La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:

  - il carattere "*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
  - il carattere "?" sostituisce qualsiasi carattere, ma uno solo;

  Esempi:

  - `resoconto*.doc` — una maschera che imposta tutti i documenti Microsoft Word di cui il nome inizia con la sottostringa "resoconto", per esempio i file `resoconto-febbraio.doc`, `resoconto121209.doc` e così via;
  - `*.exe` — una maschera che imposta tutti i file eseguibili con l'estensione EXE, per esempio `setup.exe`, `iTunes.exe` e così via;
  - `photo????09.jpg` — una maschera che imposta tutti i file delle immagini del formato JPG di cui il nome inizia con la sottostringa "photo" e finisce con la sottostringa "09" e tra queste due sottostringhe nel nome di file ci sono esattamente quattro caratteri casuali, per esempio `photo121209.jpg`, `photopapà09.jpg` o `photo----09.jpg`.
  - `file*` — si escludono dalla scansione tutti i file con qualsiasi estensione di cui il nome inizia con `file` in tutte le cartelle.
  - `file.*` — si escludono dalla scansione tutti i file con il nome `file` e qualsiasi estensione in tutte le cartelle.
  - `C:\folder\**` — si escludono dalla scansione tutte le sottocartelle e i file nella cartella `C:\folder`. I file nelle sottocartelle verranno scansionati.
  - `C:\folder\*` — si escludono dalla scansione tutti i file nella cartella `C:\folder` e in tutte le sottocartelle a qualsiasi livello di nidificazione.
  - `C:\folder\*.txt` — si escludono dalla scansione i file `*.txt` nella cartella `C:\folder`. I file `*.txt` nelle sottocartelle verranno scansionati.
  - `C:\folder\*\*.txt` — si escludono dalla scansione i file `*.txt` solo nelle sottocartelle del primo livello di nidificazione della cartella `C:\folder`.
  - `C:\folder\**\*.txt` — si escludono dalla scansione i file `*.txt` nelle sottocartelle di qualsiasi livello di nidificazione della cartella `C:\folder`. Nella cartella stessa `C:\folder` i file `*.txt` verranno scansionati.

2. Nella finestra di aggiunta di un file o una cartella indicare i componenti che non devono eseguire la scansione dell'oggetto selezionato.
3. Premere il pulsante **OK**. Il file o la cartella selezionata apparirà nella lista.
4. Se necessario, ripetere i passi 1–3 per aggiungere altri file o cartelle.

Gestione degli oggetti nella lista

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante — aggiunta di un oggetto alla lista delle eccezioni.
- Pulsante — modifica dell'oggetto selezionato nella lista delle eccezioni.
- Pulsante — rimozione dell'oggetto selezionato dalla lista delle eccezioni.

  Queste azioni sono disponibili anche nel menu contestuale quando si fa clic con il pulsante destro del mouse su uno o più oggetti selezionati.
- Attraverso il pulsante sono disponibili le seguenti azioni:
  - **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
  - **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
  - **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

13.3. Applicazioni

È possibile configurare una lista di programmi e processi la cui attività è esclusa dalla scansione tramite il monitoraggio dei file SpIDer Guard, il monitoraggio di internet SpIDer Gate e l'antivirus della posta SpIDer Mail. Sono esclusi dalla scansione gli oggetti che sono modificati a seguito dell'operazione di queste applicazioni.

Per configurare la lista di applicazioni escluse

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta fare clic sulla piastrella **Eccezioni**.
3. Fare clic sulla piastrella **Applicazioni**.

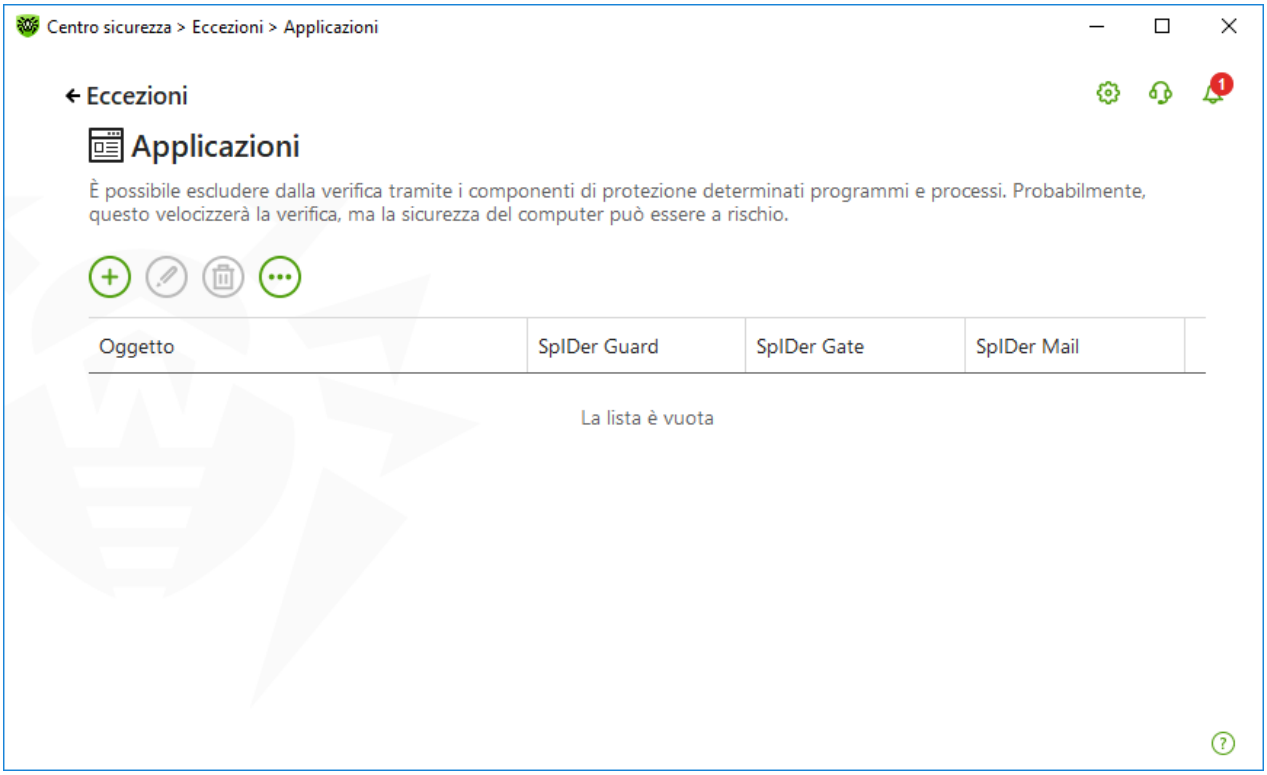

Immagine 93. Lista di applicazioni escluse

Di default la lista è vuota.

Per aggiungere applicazioni alle eccezioni

1. Per aggiungere un programma o processo alla lista delle eccezioni, premere ⊕. Eseguire una delle seguenti azioni:
   - nella finestra che si è aperta premere il pulsante **Sfoglia** per selezionare un'applicazione. È possibile immettere manualmente il percorso completo dell'applicazione nel campo di immissione. Per esempio:

     ```
     C:\Program Files\folder\example.exe
     ```
   - per escludere un'applicazione dalla scansione, immettere il suo nome nel campo di immissione. In questo caso non è necessario specificare il percorso completo dell'applicazione. Per esempio:

     ```
     example.exe
     ```
   - per escludere dalla scansione un determinato tipo di applicazioni, immettere nel campo di immissione una maschera che lo definisce.

     La maschera imposta la parte generale del nome di un oggetto, notare in particolare che:

     - il carattere "*" sostituisce qualsiasi sequenza di caratteri, anche una vuota;
     - il carattere "?" sostituisce qualsiasi carattere, ma uno solo;

Esempio di come si impostano le eccezioni:

- `C:\Program Files\folder\*.exe` — esclude dalla scansione le applicazioni nella cartella `C:\Program Files\folder`. Nelle sottocartelle le applicazioni verranno scansionate.
- `C:\Program Files\*\*.exe` — esclude dalla scansione le applicazioni solo nelle sottocartelle del primo livello di nidificazione della cartella `C:\Program Files`.
- `C:\Program Files\**\*.exe` — esclude dalla scansione le applicazioni nelle sottocartelle di qualsiasi livello di nidificazione della cartella `C:\Program Files`. Nella cartella stessa `C:\Program Files` le applicazioni verranno scansionate.
- `C:\Program Files\folder\exam*.exe` — esclude dalla scansione qualsiasi applicazione nella cartella `C:\Program Files\folder`, di cui il nome inizi con exam. Nelle sottocartelle queste applicazioni verranno scansionate.
- `example.exe` — esclude dalla scansione tutte le applicazioni con il nome `example` e l'estensione `.exe` in tutte le cartelle.
- `example*` — esclude dalla scansione qualsiasi tipo di applicazioni di cui i nomi iniziano con `example` in tutte le cartelle.
- `example.*` — esclude dalla scansione tutte le applicazioni con il nome `example` e qualsiasi estensione in tutte le cartelle.

- è possibile escludere dalla scansione un'applicazione in base al nome di una variabile, se il nome e il valore di questa variabile sono specificati nelle impostazioni delle variabili di sistema. Per esempio:

  `%EXAMPLE_PATH%\example.exe` — esclude dalla scansione un'applicazione in base al nome di una variabile di sistema. Il nome e il valore della variabile di sistema possono essere definiti nelle impostazioni del sistema operativo.

  In caso del sistema operativo Windows 7 e versioni successive: **Pannello di controllo** → **Sistema** → **Impostazioni di sistema avanzate** → **Avanzate** → **Variabili d'ambiente** → **Variabili di sistema**.

  Il nome della variabile nell'esempio: `EXAMPLE_PATH`.

  Il valore della variabile nell'esempio: `C:\Program Files\folder`.

2. Nella finestra di configurazione indicare quali componenti non devono eseguire la scansione dell'applicazione selezionata.

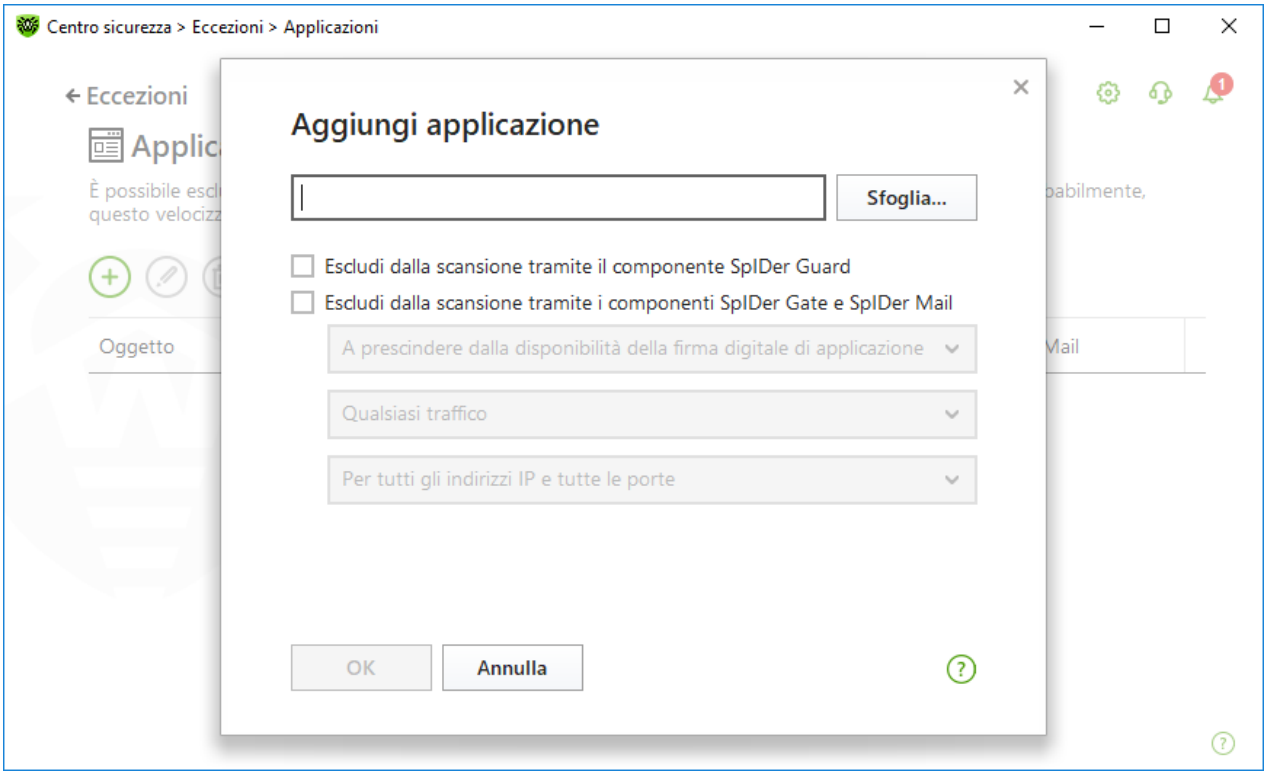

Immagine 94. Aggiunta di applicazioni alle eccezioni

3. In caso di oggetti che vengono esclusi dalla scansione tramite i componenti SpIDer Gate e SpIDer Mail,, indicare le condizioni aggiuntive.

Parametro	Descrizione
A prescindere dalla disponibilità della firma digitale di applicazione	Selezionare questa opzione se l'applicazione deve essere esclusa dalla scansione a prescindere dalla disponibilità di una firma digitale valida.
Se è disponibile una firma digitale valida di applicazione	Selezionare questa opzione se l'applicazione deve essere esclusa dalla scansione soltanto se ha una firma digitale valida. Altrimenti l'applicazione verrà controllata dai componenti.
Qualsiasi traffico	Selezionare questa opzione per escludere dalla scansione sia il traffico cifrato dell'applicazione che quello non cifrato.
Traffico cifrato	Selezionare questa opzione per escludere dalla scansione soltanto il traffico cifrato dell'applicazione.
Per tutti gli indirizzi IP e tutte le porte	Selezionare questa opzione per escludere dalla scansione il traffico trasmesso su qualsiasi indirizzo IP e porta.
Per gli indirizzi IP e le porte indicate	Selezionare questa opzione per indicare gli indirizzi IP o le porte in modo da escludere dalla scansione il traffico che ne viene trasmesso. Il traffico trasmesso

Parametro	Descrizione
	da altri indirizzi IP o porte verrà controllato (se non è escluso dalle altre impostazioni).
Impostazione di indirizzi e porte	Per la messa a punto delle eccezioni, utilizzare i seguenti suggerimenti: • per escludere dalla scansione un determinato dominio su una determinata porta, indicare, per esempio `site.com:80`; • per escludere dalla scansione il traffico su una porta non standard (per esempio 1111), è necessario indicare: `*:1111`; • per escludere dalla scansione il traffico da un dominio su qualsiasi porta, indicare: `site:*`

4. Premere il pulsante **OK**. L'applicazione selezionata apparirà nella lista.
5. Se necessario, ripetere le azioni per aggiungere altri programmi.

Gestione degli oggetti nella lista

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — aggiunta di un oggetto alla lista delle eccezioni.
- Pulsante ✎ — modifica dell'oggetto selezionato nella lista delle eccezioni.
- Pulsante 🗑 — rimozione dell'oggetto selezionato dalla lista delle eccezioni.

  Queste azioni sono disponibili anche nel menu contestuale quando si fa clic con il pulsante destro del mouse su uno o più oggetti selezionati.
- Attraverso il pulsante ⋯ sono disponibili le seguenti azioni:
  - **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
  - **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
  - **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

13.4. Antispam

È possibile configurare liste di mittenti le cui email saranno escluse dalla scansione antispam. La scansione antivirus di tali email si mantiene.

Per configurare la black list e la white list di indirizzi

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.

2. Nella finestra che si è aperta fare clic sulla piastrella **Eccezioni**.
3. Fare clic sulla piastrella **Antispam**.

La reazione del componente SpIDer Mail alle email dei mittenti dalla black list e dalla white list:

- Se l'indirizzo di un mittente è aggiunto alla white list, l'email è considerata sicura e non viene analizzata dal punto di vista del contenuto di spam.
- Se l'indirizzo di un mittente è aggiunto alla black list, lo status di spam viene attribuito alla relativa email senza ulteriori analisi.

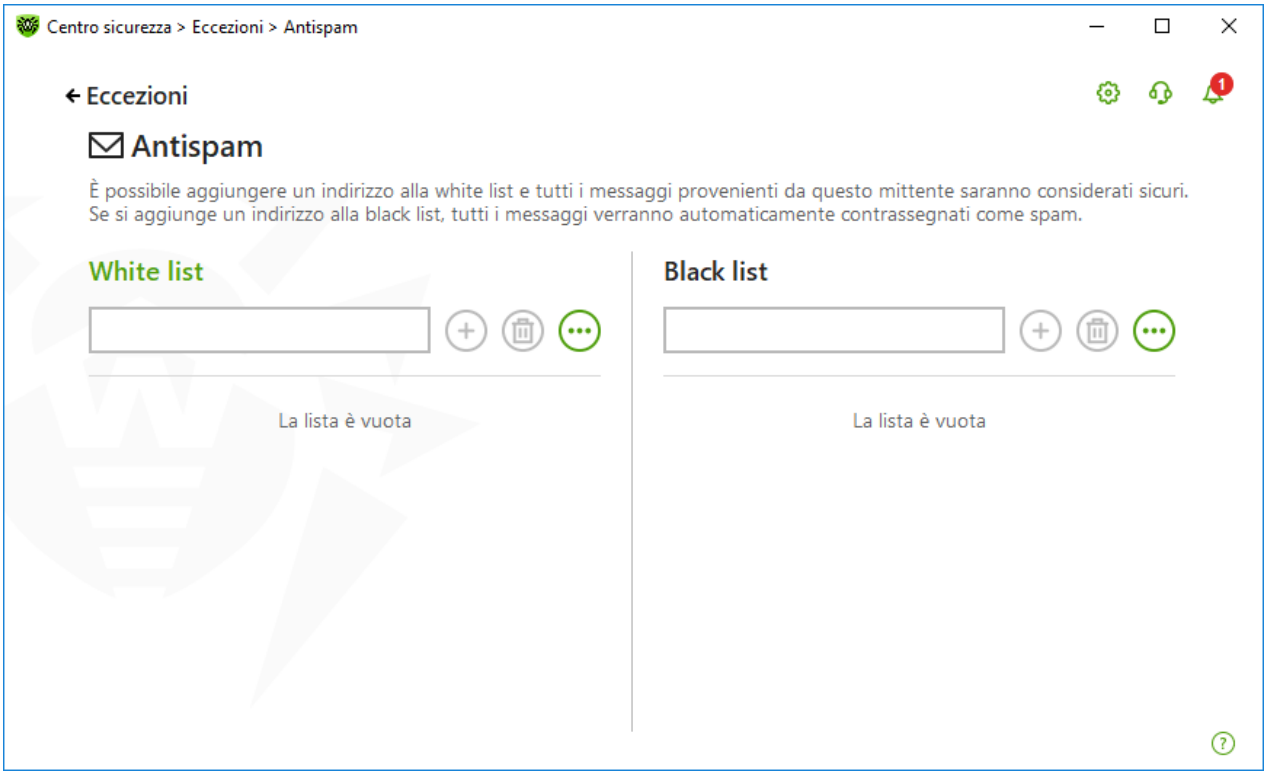

Immagine 95. Black list e white list di indirizzi

Di default entrambe le liste sono vuote.

Per aggiungere indirizzi email alle eccezioni

1. Immettere nel rispettivo campo di immissione l'indirizzo email del mittente o una maschera che definisce gli indirizzi email dei mittenti di cui le email si vogliono processare automaticamente senza analisi. Metodi di immissione:

- per aggiungere alla lista un determinato mittente, immettere il suo indirizzo email completo (per esempio `name@pochta.ru`). Tutte le email ricevute da questo indirizzo verranno processate senza analisi;
- per aggiungere alla lista mittenti che utilizzano indirizzi email simili, utilizzare i caratteri "`*`" e "`?`" per sostituire la parte differente dell'indirizzo. In particolare, il carattere "`*`" sostituisce qualsiasi sequenza di caratteri, e il carattere "`?`" sostituisce un carattere (qualsiasi). Esempio: se si inserisce l'indirizzo `name*@pochta.ru`, le email dai mittenti con gli indirizzi come

`name@pochta.ru`, `name1@pochta.ru`, `name_moj@pochta.ru` ecc. verranno processate senza analisi;

- per assicurarsi di ricevere o bloccare le email dagli indirizzi email in uno specifico dominio, utilizzare il carattere "`*`" invece del nome utente. Esempio: per impostare tutte le email dai mittenti dal dominio pochta.ru, immettere `*@pochta.ru`.

2. Per aggiungere alla lista l'indirizzo immesso, premere il pulsante ⊕ o il tasto INVIO sulla tastiera.
3. Se necessario, ripetere i passi 1 e 2 per aggiungere altri indirizzi.

Gestione degli oggetti nella lista

Per la gestione degli oggetti nella tabella, sono disponibili i seguenti elementi di gestione:

- Pulsante ⊕ — aggiunta di un indirizzo email alla lista. Diventa disponibile se viene inserito un valore nel campo di testo.
- Pulsante 🗑 — rimozione dell'indirizzo email selezionato dalla lista.
- Attraverso il pulsante ⋯ sono disponibili le seguenti azioni:
  - **Modifica** — questa opzione consente di modificare l'indirizzo email selezionato dalla lista.
  - **Esportazione** — questa opzione consente di salvare la lista delle eccezioni creata per utilizzarla su un altro computer su cui è installato Dr.Web.
  - **Importazione** — questa opzione consente di utilizzare una lista delle eccezioni creata su un altro computer.
  - **Pulisci tutto** — questa opzione consente di cancellare tutti gli oggetti dalla lista delle eccezioni.

Le azioni di rimozione o modifica dell'oggetto sono disponibili anche nel menu contestuale quando si fa clic con il pulsante destro del mouse su uno o più oggetti selezionati.

14. Statistiche di funzionamento dei componenti

Si ha la possibilità di visualizzare statistiche sul funzionamento dei componenti principali Dr.Web.

Per andare alla visualizzazione delle statistiche su eventi importanti nel funzionamento dei componenti di protezione

1. Aprire il menu Dr.Web e selezionare la voce **Centro sicurezza**.
2. Nella finestra che si è aperta selezionare la scheda **Statistiche**.
3. Si aprirà la finestra di visualizzazione delle statistiche da cui sono disponibili i report per i seguenti gruppi:
   - Report dettagliato
   - Office control
   - Minacce
   - Firewall

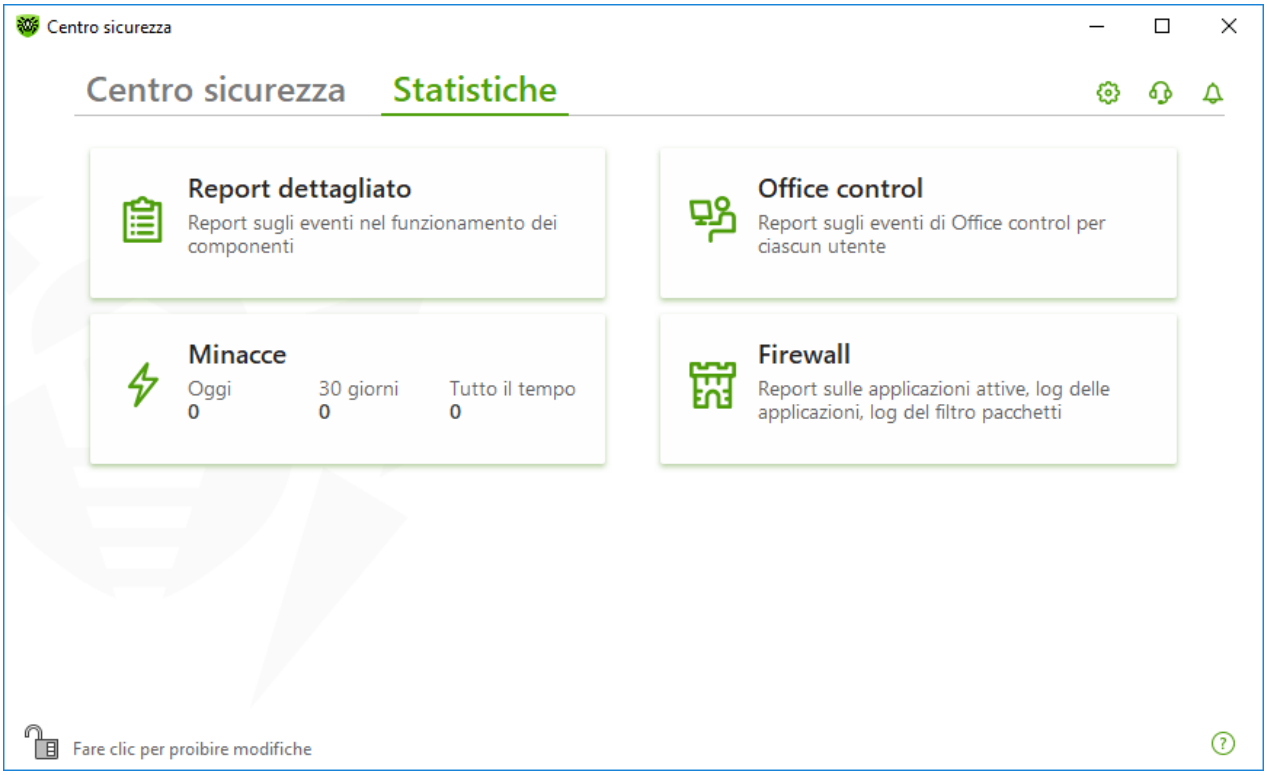

Immagine 96. Statistiche di funzionamento dei componenti

4. Selezionare un gruppo per visualizzare i report.

Report dettagliato

In questa finestra vengono raccolte informazioni dettagliate su tutti gli eventi per tutto il tempo di funzionamento.

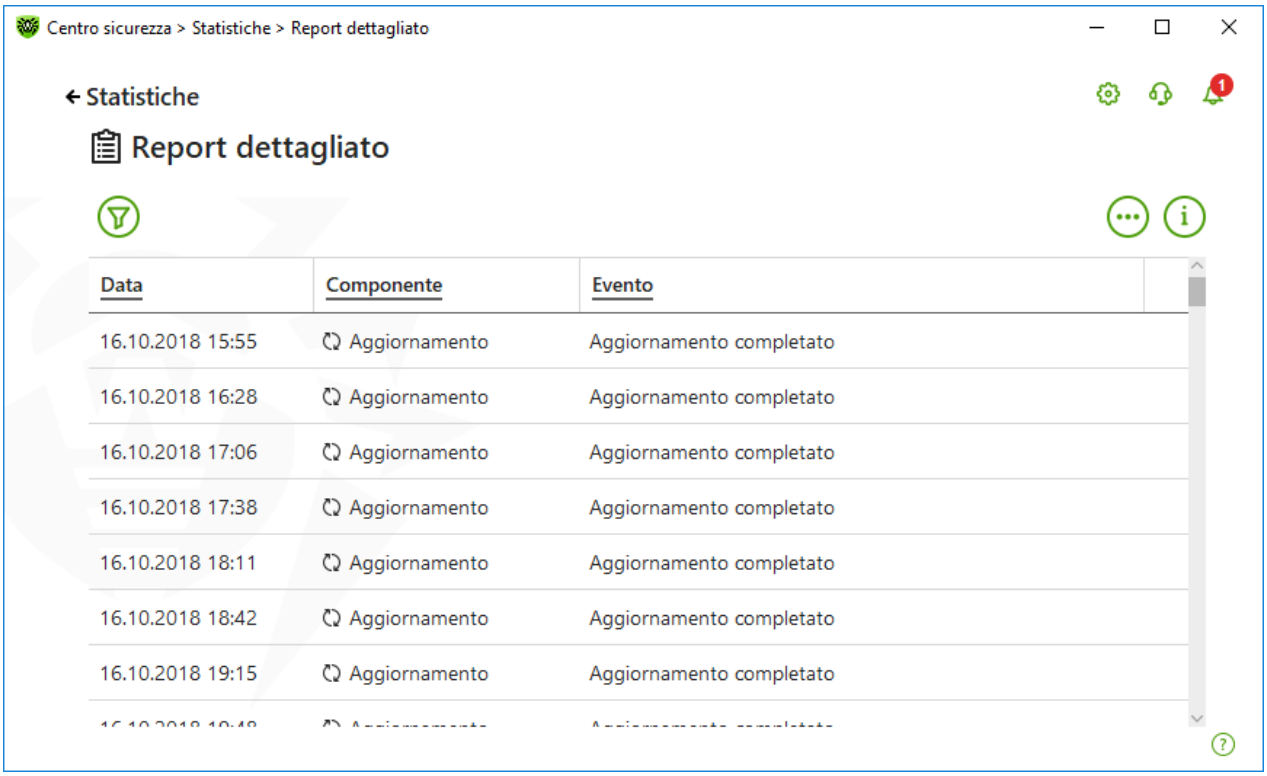

Immagine 97. Finestra del report dettagliato

Nel report vengono registrate le seguenti informazioni:

- **Data** — data e ora dell'evento;
- **Componente** — componente o modulo a cui appartiene l'evento;
- **Evento** — breve descrizione dell'evento.

Di default vengono visualizzati tutti gli eventi per tutto il tempo.

Per la gestione degli oggetti nella tabella vengono utilizzati gli elementi di gestione , , .

Per la selezione di eventi è possibile utilizzare filtri aggiuntivi.

Office control

Nel gruppo **Office control** vengono visualizzate le statistiche delle URL bloccate per ciascun account.

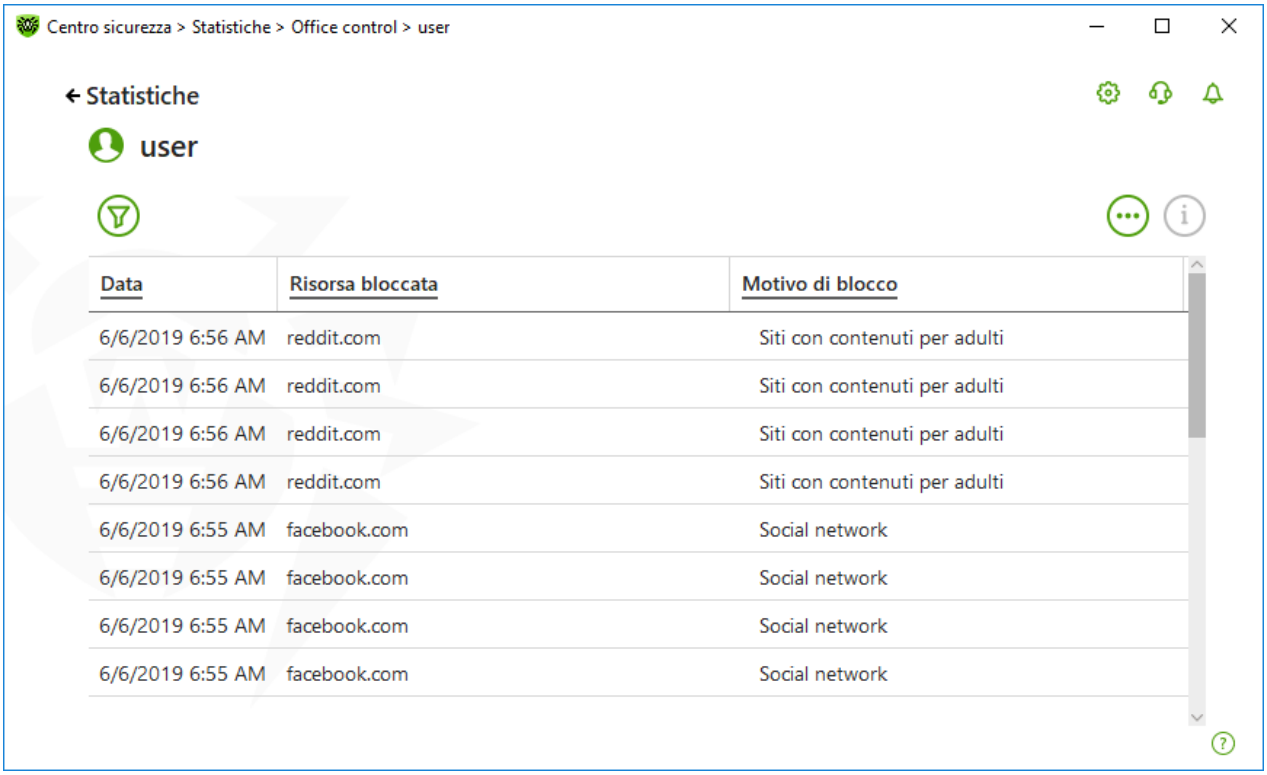

Immagine 98. Finestra delle statistiche di Office control

Nel report vengono registrate le seguenti informazioni:

- **Data** — data e ora di blocco;
- **Risorsa bloccata** — link della risorsa bloccata;
- **Motivo di blocco** — categoria o lista di eccezioni a cui appartiene la risorsa bloccata.

Di default vengono visualizzati tutti gli eventi per tutto il tempo.

Per la gestione degli oggetti nella tabella vengono utilizzati gli elementi di gestione, , .

Per la selezione di eventi è possibile utilizzare filtri aggiuntivi.

Le statistiche includono anche risorse esterne integrate con altre pagine, per esempio widget incorporati. La loro inclusine nelle statistiche non significa che l'utente ha cercato intenzionalmente di visitare questi siti.

Minacce

Nella finestra principale di visualizzazione delle statistiche sulla piastrella **Minacce** sono raccolte informazioni sul numero di minacce per un determinato periodo di tempo.

Quando viene selezionata questa opzione, si aprirà la finestra **Report dettagliato** con filtri predefiniti di tutte le minacce.

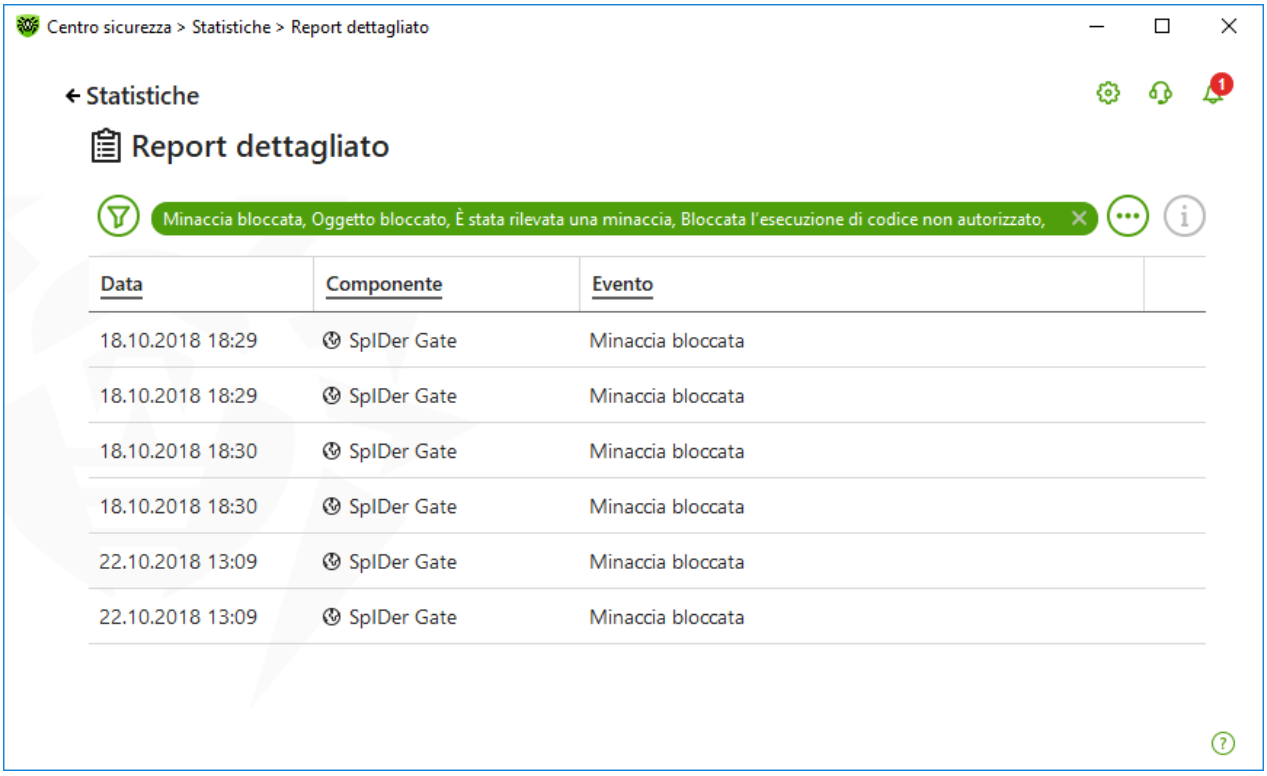

Immagine 99. Finestra delle statistiche delle minacce

Nel report vengono registrate le seguenti informazioni:

- **Data** — data e ora di rilevamento della minaccia;
- **Componente** — componente che ha rilevato la minaccia;
- **Evento** — breve descrizione dell'evento.

Di default vengono visualizzati tutti gli eventi per tutto il tempo.

Per la gestione degli oggetti nella tabella vengono utilizzati gli elementi di gestione , , .

Per la selezione di eventi è possibile utilizzare filtri aggiuntivi.

Attività di rete

Se è installato Firewall Dr.Web, è disponibile un report sulle attività di rete.

È possibile visualizzare i dati per le applicazioni attive, un log delle applicazioni, un log del filtro pacchetti. A questo scopo, selezionare l'oggetto richiesto dalla lista a cascata.

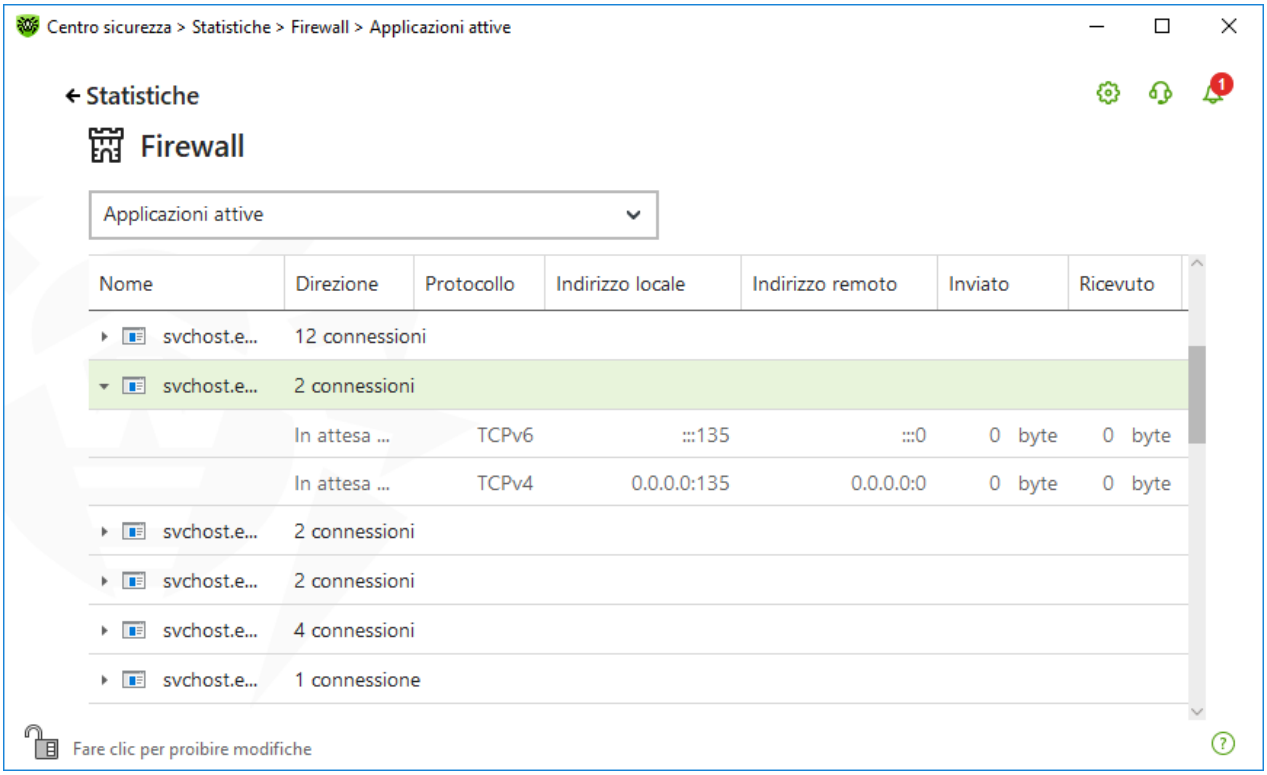

Immagine 100. Finestra delle statistiche delle attività di rete

Per ciascuna applicazione attiva vengono visualizzati i seguenti dati:

- direzione della trasmissione dei dati;
- log di funzionamento;
- indirizzo locale;
- indirizzo remoto;
- dimensione di un pacchetto dati inviato;
- dimensione di un pacchetto dati ricevuto.

È possibile bloccare una delle connessioni correnti o consentire una connessione precedentemente bloccata. Per fare ciò, selezionare la connessione richiesta e fare clic con il tasto destro del mouse. È disponibile solo una opzione a seconda dello stato della connessione.

Nel log delle applicazioni vengono visualizzati i seguenti dati:

- ora di inizio del funzionamento di un'applicazione;
- nome dell'applicazione;
- nome della regola di processamento dell'applicazione;
- direzione della trasmissione dei dati;
- azione;
- indirizzo di destinazione.

È possibile attivare la registrazione del log delle applicazioni nella finestra di aggiunta o modifica di una regola per un'applicazione nella sezione **Firewall**. Per dettagli vedi sezione Configurazione dei parametri della regola per applicazioni.

Nel log del filtro pacchetti vengono visualizzati i seguenti dati:

- ora di inizio del processamento di un pacchetto dati;
- direzione della trasmissione del pacchetto dati;
- nome della regola di processamento;
- interfaccia;
- contenuto del pacchetto.

È possibile attivare la registrazione del log del filtro pacchetti nella finestra di aggiunta o modifica di una regola di pacchetto nella sezione **Firewall**. Per dettagli vedi sezione Set di regole di filtraggio pacchetti.

Quando si fa clic su una delle colonne, gli eventi vengono ordinati nella colonna in ordine decrescente o crescente.

Filtri

Per visualizzare nella lista solo gli eventi che corrispondono a determinati parametri, utilizzare i filtri. Per tutti i report sono disponibili filtri predefiniti a cui si accede facendo clic su . Inoltre, si possono creare filtri di eventi personalizzati.

Pulsanti di gestione degli elementi nella tabella:

- Attraverso il pulsante sono disponibili le seguenti azioni:
  - Selezione di un filtro predefinito per il periodo di tempo impostato o di un filtro per un evento di aggiornamento.
  - Salvataggio del filtro personalizzato corrente. È inoltre possibile rimuovere un filtro personalizzato già creato.
  - Rimozione di tutti i filtri attualmente impostati.
- Attraverso il pulsante sono disponibili le seguenti azioni:
  - **Copia selezione** — consente di copiare la riga selezionata (più righe selezionate) negli Appunti.
  - **Esporta selezione** — consente di esportare la riga selezionata (più righe selezionate) in una cartella specificata in formato .csv.
  - **Esporta tutto** — consente di esportare tutte le righe della tabella in una cartella specificata in formato .csv.
  - **Rimuovi selezione** — consente di rimuovere l'evento selezionato (più eventi selezionati).
  - **Rimuovi tutto** — consente di rimuovere tutti gli eventi dalla tabella delle statistiche.

- Attraverso il pulsante ⓘ vengono visualizzate informazioni dettagliate sull'evento. È disponibile quando è selezionata una riga. Quando si preme di nuovo questo pulsante, i dati dettagliati sull'evento vengono nascosti.

Per impostare un filtro personalizzato

1. Per ordinare secondo un parametro specifico, fare clic sull'intestazione della colonna richiesta:
   - Ordinamento per data. È possibile selezionare uno dei periodi predefiniti specificati nella parte sinistra della finestra o impostare un periodo personalizzato. Per impostare il periodo richiesto, selezionare nel calendario la data di inizio e la data di fine del periodo o indicare le date nella riga **Periodo**. Inoltre, è disponibile l'ordinamento per data in ordine crescente o decrescente.

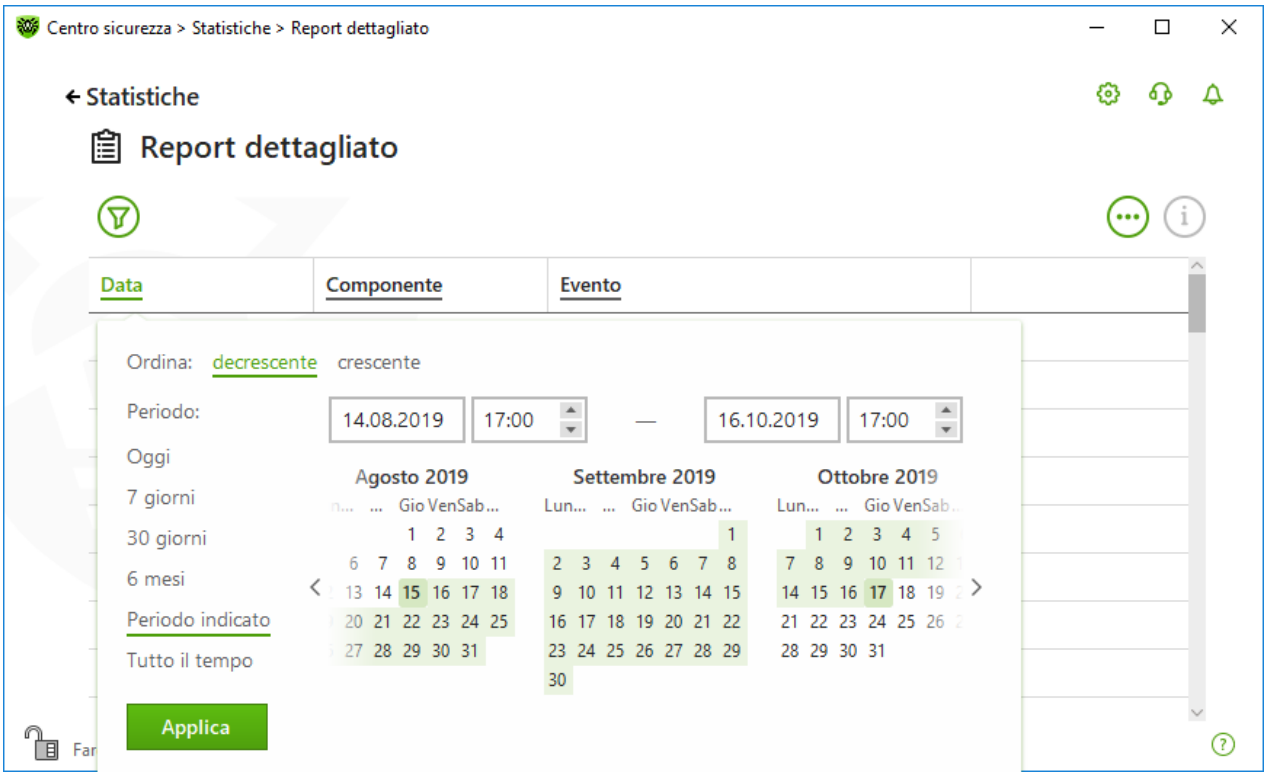

Immagine 101. Ordinamento per data

   - Ordinamento per componente. È possibile contrassegnare i componenti, le informazioni da cui verranno visualizzate nel report, od ordinare i record in ordine crescente o decrescente.
   - Ordinamento per evento. È possibile contrassegnare gli eventi da visualizzare nel report, od ordinare i record in ordine crescente o decrescente.

   Per le statistiche di Office control sono disponibili, oltre all'ordinamento per data, i seguenti parametri:

   - Ordinamento per risorsa bloccata. È possibile ordinare i record solo in ordine crescente o decrescente.

- Ordinamento per motivo di blocco. È possibile contrassegnare i motivi di blocco da visualizzare nel report, od ordinare i record in ordine crescente o decrescente.

2. Dopo aver selezionato i parametri di filtraggio, premere **Applica**. Gli elementi selezionati verranno visualizzati sopra la tabella.
3. Per salvare il filtro, premere  e selezionare **Salva filtro**.
4. Nella finestra che si è aperta indicare il nome del nuovo filtro. Premere **Salva**.

15. Avvisi del server

L'amministratore della rete ha la possibilità di configurare l'invio degli avvisi server su qualsiasi delle postazioni. Questa funzione è utile per ricevere gli avvisi dal server quando l'amministratore della rete lavora su una delle postazioni.

Per andare alla finestra Avvisi del server

1. Aprire il menu Dr.Web.
2. Selezionare la voce **Avvisi del server**.

Immagine 102. Finestra Avvisi del server

Tutti gli avvisi ricevuti vengono visualizzati in una lista nella parte superiore della finestra. Per visualizzare ulteriori informazioni, fare clic su un avviso.

Filtri

Per visualizzare nella lista solo gli avvisi che corrispondono a determinati parametri, utilizzare i filtri. Al clic su è disponibile il filtro predefinito. Le sue impostazioni sono uguali a quelle sul server. Inoltre, si possono creare filtri di avviso personalizzati.

Pulsanti di gestione degli elementi nella tabella:

- Attraverso il pulsante  sono disponibili le seguenti azioni:
  - Selezione del filtro predefinito.
  - Salvataggio del filtro personalizzato corrente. È inoltre possibile rimuovere un filtro personalizzato già creato.
  - Rimozione di tutti i filtri attualmente impostati.
- Attraverso il pulsante  sono disponibili le seguenti azioni:
  - **Copia selezione** — consente di copiare la riga selezionata (più righe selezionate) negli Appunti.
  - **Esporta selezione** — consente di esportare la riga selezionata (più righe selezionate) in una cartella specificata in formato .csv.
  - **Esporta tutto** — consente di esportare tutte le righe della tabella in una cartella specificata in formato .csv.
  - **Rimuovi selezione** — consente di rimuovere l'avviso selezionato (più avvisi selezionati).
  - **Segna come già letto** — consente di contrassegnare come letti gli avvisi selezionati.
  - **Rimuovi tutto** — consente di rimuovere tutti gli avvisi dalla tabella.
- Attraverso il pulsante  è disponibile una finestra di ricerca tra tutti gli avvisi.

Per impostare un filtro personalizzato

1. Per ordinare secondo un parametro specifico, fare clic sull'intestazione della colonna richiesta:
   - Ordinamento per postazione. È possibile ordinare i record solo in ordine crescente o decrescente.
   - Ordinamento per categoria. È possibile contrassegnare le categorie, le informazioni da cui verranno visualizzate nel report, od ordinare i record in ordine crescente o decrescente. È possibile filtrare gli avvisi secondo le seguenti categorie:
     - Amministratori;
     - Postazioni;
     - Licenze;
     - Nuovi arrivi;
     - Repository;
     - Installazioni;
     - Altro.
   - Ordinamento per avviso del server. È possibile ordinare i record solo in ordine crescente o decrescente.
   - Ordinamento per data. È possibile selezionare uno dei periodi predefiniti specificati nella parte sinistra della finestra o impostare un periodo personalizzato. Per impostare il

periodo richiesto, selezionare nel calendario la data di inizio e la data di fine del periodo o indicare le date nella riga **Periodo**. Inoltre, è disponibile l'ordinamento per data in ordine crescente o decrescente.

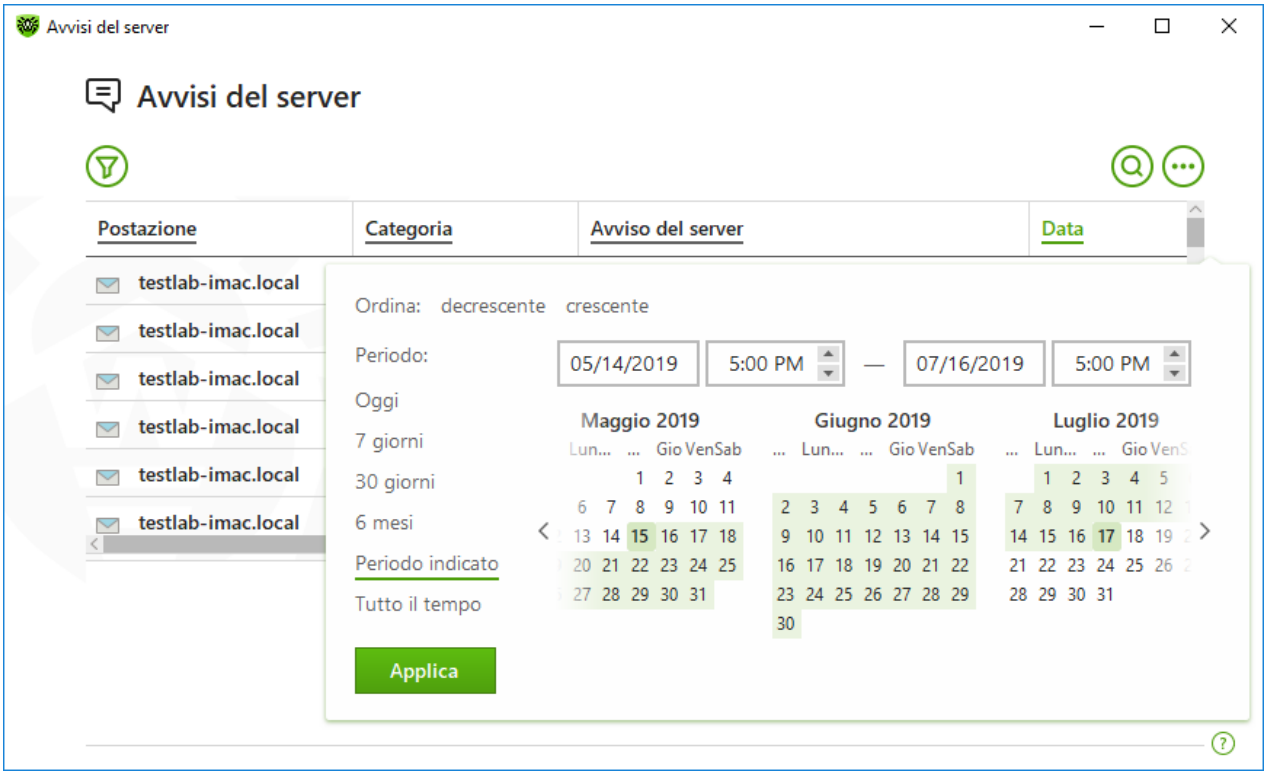

Immagine 103. Ordinamento per data

2. Dopo aver selezionato i parametri di filtraggio, premere **Applica**. Gli elementi selezionati verranno visualizzati sopra la tabella.
3. Per salvare il filtro, premere e selezionare **Salva filtro**.
4. Nella finestra che si è aperta indicare il nome del nuovo filtro. Premere **Salva**.

16. Supporto tecnico

Se si verificano dei problemi con l'installazione o il funzionamento dei prodotti della società, prima di chiedere aiuto al reparto di supporto tecnico, provare a trovare una soluzione nei seguenti modi:

- leggere le ultime versioni delle descrizioni e dei manuali sull'indirizzo https://download.drweb.com/doc/;
- leggere la sezione delle domande ricorrenti sull'indirizzo https://support.drweb.com/show_faq/;
- visitare i forum della società Doctor Web sull'indirizzo https://forum.drweb.com/.

Se provati questi modi, non si è riusciti a risolvere il problema, è possibile utilizzare uno dei seguenti modi per contattare il servizio di supporto tecnico della società Doctor Web:

- compilare il modulo web nella relativa sezione della pagina https://support.drweb.com/;
- chiamare il numero di telefono a Mosca: +7 (495) 789-45-86 o il numero verde per tutta la Russia: 8-800-333-7932.

Le informazioni sulle rappresentanze regionali e sedi della società Doctor Web sono ritrovabili sul sito ufficiale sull'indirizzo https://company.drweb.com/contacts/offices/.

16.1. Aiuto nella risoluzione di problemi

Quando si rivolge all'amministratore della rete antivirus, può essere necessario generare un report sul sistema operativo e sul funzionamento di Dr.Web.

Per creare il report tramite la Creazione report guidata

1. Aprire il menu Dr.Web e selezionare la voce **Supporto**.
2. Nella finestra che si è aperta premere il pulsante **Vai a Creazione report guidata**.

È anche possibile aprire questa finestra facendo clic sul pulsante in alto a destra della finestra **Centro sicurezza**.

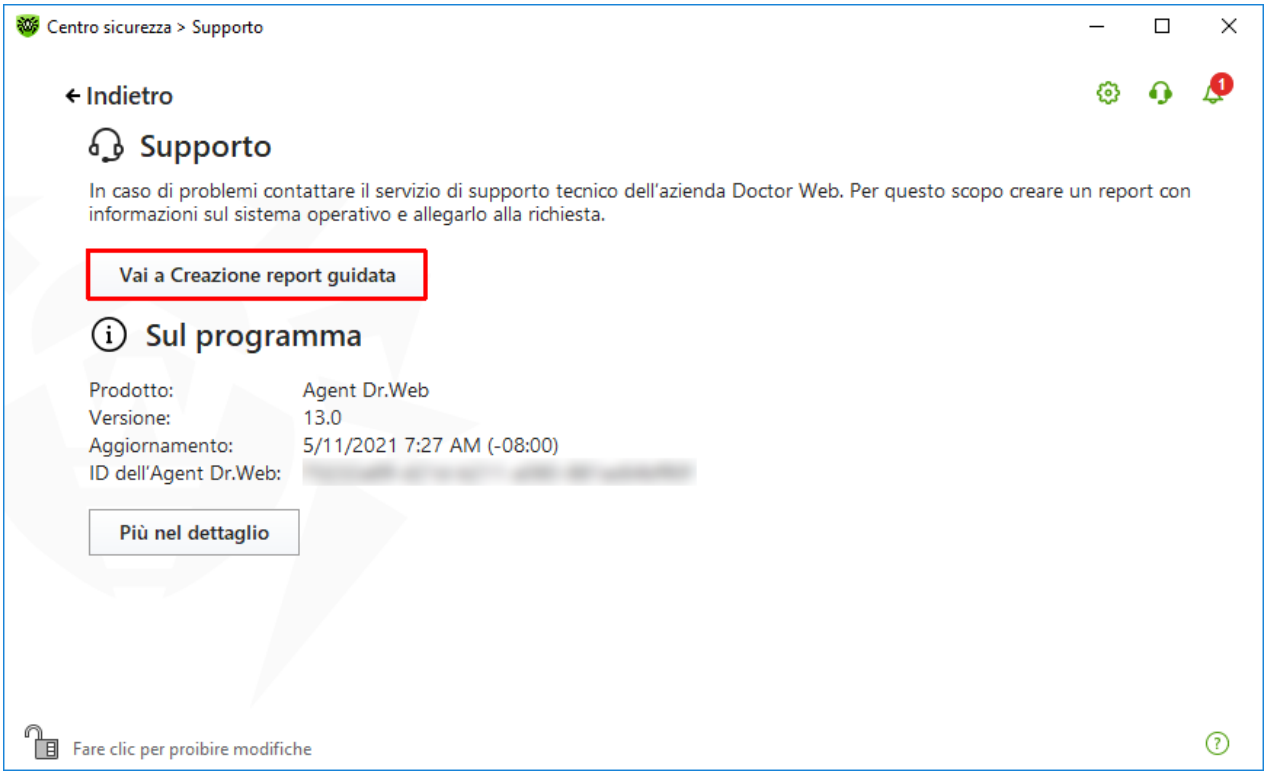

Immagine 104. Supporto

3. Nella finestra che si è aperta premere il pulsante **Crea report**.

Immagine 105. Creazione del report per il supporto tecnico

4. Inizierà la creazione del report.

Creazione del report tramite la riga di comando

Per generare un report, utilizzare il seguente comando:

`/auto`, per esempio: `dwsysinfo.exe /auto`

Inoltre è possibile utilizzare il comando:

`/auto /report:`[<*percorso_completo_del_file_di_report*>], per esempio:
`dwsysinfo.exe /auto /report:C:\report.zip`

Il report verrà salvato come archivio nella cartella Doctor Web situata nella cartella del profilo dell'utente %USERPROFILE%. È possibile accedere all'archivio premendo il pulsante **Apri cartella** al termine della creazione dell'archivio.

Informazioni incluse nel report

Il report include le seguenti informazioni:

1. Informazioni tecniche sul sistema operativo:
   - informazioni generali sul computer,
   - informazioni sui processi in esecuzione,
   - informazioni sui task pianificati,
   - informazioni sui servizi, driver,
   - informazioni sul browser predefinito,
   - informazioni sulle applicazioni installate,
   - informazioni sui criteri di restrizione,
   - informazioni sul file HOSTS,
   - informazioni sui server DNS,
   - record del log degli eventi di sistema;
   - elenco delle directory di sistema;
   - rami del registro;
   - provider Winsock;
   - connessioni di rete;
   - report del programma di debug Dr. Watson;
   - indice di prestazioni.
2. Informazioni sul prodotto Dr.Web installato:
   - tipo e versione del prodotto Dr.Web installato;
   - informazioni sulla lista dei componenti installati; informazioni sui moduli Dr.Web;
   - impostazioni e parametri di configurazione del prodotto Dr.Web;

- informazioni sulla licenza;
- log di funzionamento Dr.Web.

Informazioni sul funzionamento di Dr.Web sono locate nel Log degli eventi del sistema operativo Windows, nella sezione **Log delle applicazioni e dei servizi di → Doctor Web**.

16.2. Sul programma

Il blocco **Sul programma** contiene informazioni sulla:

- versione del prodotto;
- data e ora dell'ultimo aggiornamento;
- numero di identificazione dell'Agent Dr.Web.

Informazioni sulla versione dei componenti installati e sulla data di aggiornamento dei database dei virus sono ritrovabili nella finestra **Sul programma Dr.Web**.

Per andare a questa finestra

1. Aprire il menu principale e selezionare la voce **Supporto**.
2. Nella finestra che si è aperta premere il pulsante **Più nel dettaglio**.

È anche possibile aprire questa finestra facendo clic sul pulsante in alto a destra della finestra **Centro sicurezza**.

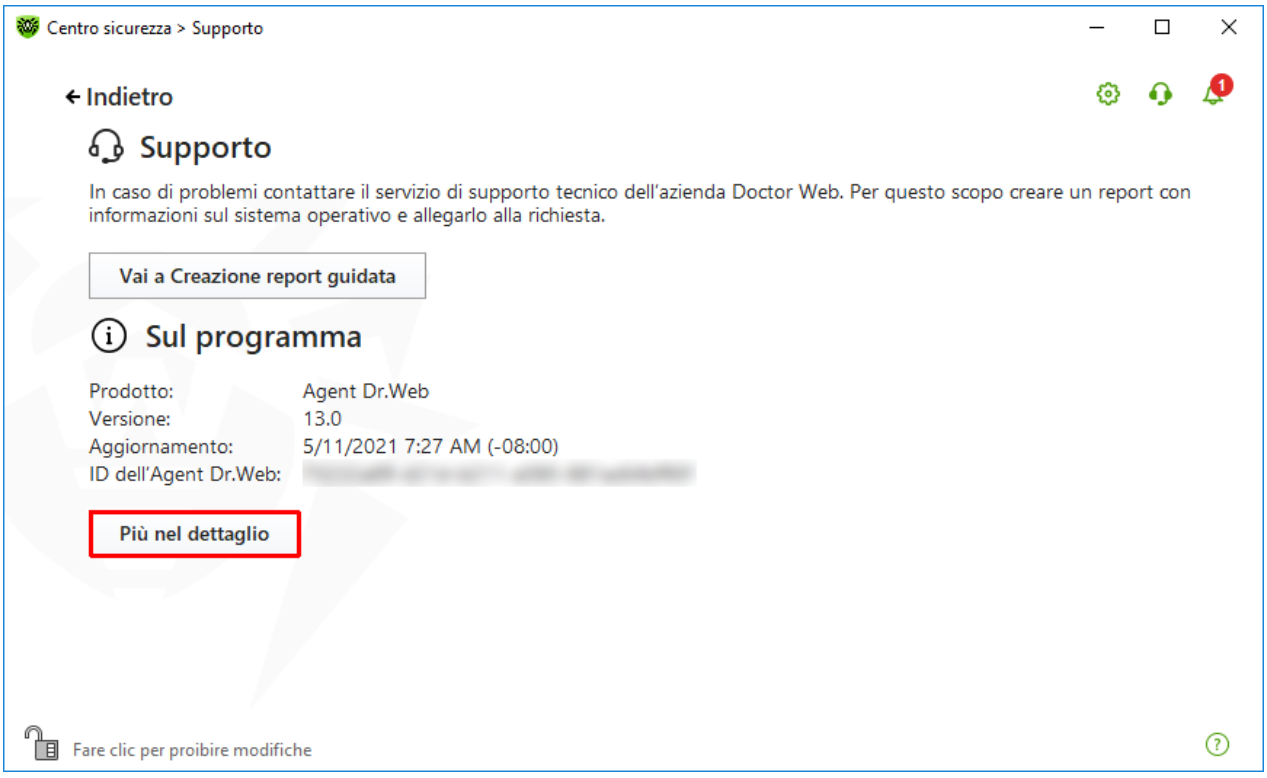

Immagine 106. Accesso alla finestra Sul programma Dr.Web

17. Allegato A. Parametri della riga di comando addizionali

I parametri della riga di comando si usano per configurare programmi che possono essere avviati tramite l'esecuzione di un file eseguibile. Questo vale per Scanner Dr.Web e Scanner console. Le opzioni possono impostare parametri assenti nel file di configurazione e hanno la precedenza sui parametri impostati nel file di configurazione.

Le opzioni iniziano con il carattere "/" e, come gli altri parametri della riga di comando, vengono separate da spazi.

17.1. Parametri per Scanner e Scanner console

Opzione	Descrizione
/AA	Applica automaticamente le azioni alle minacce rilevate. (Solo per Scanner).
/AC	Controlla i pacchetti di installazione. Di default l'opzione è attivata.
/AFS	Utilizza la barra quando si indica la nidificazione all'interno dell'archivio. Di default l'opzione è disattivata.
/AR	Controlla archivi. Di default l'opzione è attivata.
/ARC:<*rapporto_di_compressione*>	Il livello massimo di compressione. Se Scanner determina che il rapporto di compressione dell'archivio eccede il limite indicato, la decompressione e la scansione non vengono eseguite. Di default è senza limitazioni.
/ARL:<*livello_di_nidificazione*>	Il livello massimo di nidificazione dell'archivio controllato. Di default è senza limitazioni.
/ARS:<*dimensione*>	La dimensione massima in kilobyte dell'archivio controllato. Di default è senza limitazioni.
/ART:<*dimensione*>	Il valore soglia in kilobyte del controllo del livello di compressione (la dimensione minima di un file all'interno dell'archivio a partire da cui viene controllato il rapporto di compressione). Di default è senza limitazioni.
/ARX:<*dimensione*>	La dimensione massima in kilobyte degli oggetti in archivi controllati. Di default è senza limitazioni.
/BI	Visualizza informazioni sui database dei virus. Di default l'opzione è attivata.
/CUSTOM	Avvia Scanner sulla pagina di scansione personalizzata. Se vengono impostati parametri addizionali (per esempio, oggetti da

Opzione	Descrizione
	controllare o i parametri /TM, /TB), verrà avviata la scansione personalizzata degli oggetti indicati. (Vale solo per Scanner).
/DCT	Non visualizzare il tempo di scansione stimato. (Vale solo per Scanner console).
/DR	Controlla ricorsivamente le cartelle (controlla le sottocartelle). Di default l'opzione è attivata.
/E:<*numero_di_thread*>	Esegui la scansione con il numero di thread indicato.
/FAST	Esegui la scansione rapida del sistema. Se vengono impostati parametri addizionali (per esempio, oggetti da controllare o i parametri /TM, /TB), gli oggetti indicati anche verranno controllati. (Vale solo per Scanner).
/FL:<*nome_di_file*>	Controlla i percorsi indicati nel file.
/FM:<*maschera*>	Controlla i file in base a una maschera. Di default, tutti i file vengono controllati.
/FR:<*espressione_regolare*>	Controlla i file in base a un'espressione regolare. Di default tutti i file vengono controllati.
/FULL	Esegui la scansione completa di tutti i dischi rigidi e supporti rimovibili (compresi i settori di avvio). Se vengono impostati parametri addizionali (per esempio, gli oggetti da controllare o i parametri /TM, /TB), verrà eseguita la scansione rapida e la scansione degli oggetti indicati. (Vale solo per Scanner).
/FX:<*maschera*>	Non controllare i file che corrispondono alla maschera. (Vale solo per Scanner console).
/GO	Modalità di funzionamento di Scanner in cui vengono saltate le domande che sottintendono l'attesa di una risposta dell'utente; vengono prese in automatico le decisioni che richiedono una scelta. Questa modalità è utile per una verifica di file automatica, per esempio, durante il controllo giornaliero o settimanale del disco rigido. Nella riga di comando deve essere indicato l'oggetto da controllare. Insieme al parametro /GO possono inoltre essere utilizzati i parametri /LITE, /FAST, /FULL. In questa modalità la scansione viene interrotta se il computer passa all'alimentazione a batteria.
/H o /?	Visualizza una breve guida all'utilizzo del programma. (Vale solo per Scanner console).
/HA	Esegui un'analisi euristica dei file e cerca nei file minacce sconosciute. Di default l'opzione è attivata.

Opzione	Descrizione
/LITE	Esegui una scansione iniziale del sistema con cui vengono controllati la memoria operativa e i settori di avvio di tutti i dischi, inoltre esegui una verifica della presenza di rootkit. (Vale solo per Scanner).
/LN	Controlla i file a cui indicano i collegamenti. Di default l'opzione è disattivata.
/LS	Esegui una scansione sotto l'account LocalSystem. Di default l'opzione è disattivata.
/MA	Controlla file di posta. Di default l'opzione è attivata.
/MC:<*numero_di_tentativi*>	Imposta il numero massimo di tentativi di cura del file. Di default è senza limitazioni.
/NB	Non creare copie di backup dei file curati/rimossi. Di default l'opzione è disattivata.
/NI[:X]	Il livello di utilizzo delle risorse di sistema, in percentuale. Definisce la quantità di memoria utilizzata per la scansione e la priorità di sistema della scansione. Di default è senza limitazioni.
/NOREBOOT	Annulla il riavvio e lo spegnimento dopo la scansione. (Vale solo per Scanner).
/NT	Controlla stream NTFS. Di default l'opzione è attivata.
/OK	Visualizza la lista completa degli oggetti controllati, contrassegnando quelli non infetti con OK. Di default l'opzione è disattivata.
/P:<*priorità*>	La priorità del task di verifica avviato nella coda generale dei task di verifica: 0 — minima. L — bassa. N — normale. La priorità predefinita. H — alta. M — massima.
/PAL:<*livello_di_nidificazione*>	Il livello massimo di nidificazione dei packer di un file eseguibile. Se il livello di nidificazione supera quello indicato, la scansione viene eseguita solo fino al livello di nidificazione indicato. Di default, è 1000.
/QL	Visualizza la lista di tutti i file messi in quarantena su tutti i dischi. (Vale solo per Scanner console).

Opzione	Descrizione
/QL:<*nome_del_disco_logico*>	Visualizza la lista di tutti i file messi in quarantena sul disco logico indicato. (Vale solo per Scanner console).
/QNA	Visualizza i percorsi tra virgolette doppie.
/QR[:[d][:p]]	Rimuovi i file dal disco <d> (nome_del_disco_logico) indicato, che si trovano in quarantena per più di <p> (quantità) giorni. Se <d> e <p> non sono impostati, verranno rimossi tutti i file in quarantena da tutti i dischi logici. (Vale solo per Scanner console).
/QUIT	Chiudi Scanner dopo la scansione (a prescindere da quello se le azioni sono state applicate alle minacce rilevate). (Vale solo per Scanner).
/RA:<*nome_di_file*>	Aggiungi il report sul funzionamento del programma al file indicato. Di default la scrittura nel file di log non viene eseguita (con Scanner avviato dalla riga di comando).
/REP	Controlla in base a collegamenti simbolici. Di default l'opzione è disattivata.
/RK	Verifica della presenza di rootkit. Di default l'opzione è disattivata.
/RP:<*nome_di_file*>	Scrivi il report sul funzionamento del programma nel file indicato. Di default la scrittura nel file di log non viene eseguita (con Scanner avviato dalla riga di comando).
/RPC:<*sec*>	Il timeout della connessione con il motore di scansione Scanning Engine, in secondi. Di default è di 30 secondi. (Vale solo per Scanner console).
/RPCD	Utilizza l'identificatore dinamico RPC. (Vale solo per Scanner console).
/RPCE	Utilizza l'indirizzo di destinazione dinamico RPC. (Vale solo per Scanner console).
/RPCE:<*indirizzo_di_destinazione*>	Utilizza l'indirizzo di destinazione RPC indicato. (Vale solo per Scanner console).
/RPCH:<*nome_di_host*>	Utilizza il nome di host indicato per le chiamate RPC. (Vale solo per Scanner console).
/RPCP:<*protocollo*>	Utilizza il protocollo RPC indicato. È possibile utilizzare i protocolli: lpc, np, tcp. (Vale solo per Scanner console).
/SCC	Visualizza il contenuto degli oggetti composti. Di default l'opzione è disattivata.

Opzione	Descrizione
/SCN	Visualizza il nome del pacchetto di installazione. Di default l'opzione è disattivata.
/SLS	Visualizza i log sullo schermo. Di default l'opzione è attivata. (Vale solo per Scanner console).
/SPN	Visualizza il nome del packer. Di default l'opzione è disattivata.
/SPS	Visualizza l'avanzamento della scansione. Di default l'opzione è attivata. (Vale solo per Scanner console).
/SST	Visualizza il tempo di verifica dell'oggetto. Di default l'opzione è disattivata.
/ST	Avvio di Scanner in background. Se il parametro /GO non è impostato, la modalità grafica viene visualizzata solo quando vengono rilevate minacce. In questa modalità la scansione viene interrotta se il computer passa all'alimentazione a batteria.
/TB	Controlla i settori di avvio e i settori di avvio principali (MBR) del disco rigido.
/TM	Cerca minacce nella memoria operativa (compresa l'area di sistema di Windows).
/TR	Controlla i punti di ripristino di sistema.
/W:<*sec*>	Il tempo massimo di scansione in secondi. Di default è senza limitazioni.
/WCL	Output compatibile con drwebwcl. (Vale solo per Scanner console).
/X:S[:R]	A termine della scansione fai passare la macchina in modalità indicata: spegnimento/riavvio/sospensione/ibernazione.

Impostazione delle azioni su diversi oggetti (C — cura, Q — sposta in quarantena, D — elimina, I — ignora, R — informa. L'azione R è possibile solo per Scanner console. Di default è impostata l'azione informa per tutti gli oggetti (anche vale solo per Scanner console)):

Azione	Descrizione
/AAD:<*azione*>	le azioni su adware (le azioni possibili: DQIR)
/AAR:<*azione*>	le azioni su archivi infetti (le azioni possibili: DQIR)
/ACN:<*azione*>	le azioni su pacchetti di installazione infetti (le azioni possibili: DQIR)

Azione	Descrizione
/ADL:<*azione*>	le azioni su dialer (le azioni possibili: DQIR)
/AES:<*azione*>	le azioni su programmi vulnerabili (le azioni possibili: DQIR)
/AHT:<*azione*>	le azioni su hacktool (le azioni possibili: DQIR)
/AIC:<*azione*>	le azioni su file incurabili (le azioni possibili: DQR)
/AIN:<*azione*>	le azioni su file infetti (le azioni possibili: CDQR)
/AJK:<*azione*>	le azioni su joke (le azioni possibili: DQIR)
/AML:<*azione*>	le azioni su file di posta infetti (le azioni possibili: QIR)
/ARW:<*azione*>	le azioni su file potenzialmente pericolosi (le azioni possibili: DQIR)
/ASU:<*azione*>	le azioni su file sospetti (le azioni possibili: DQIR)

Alcune opzioni possono avere modificatori attraverso cui una modalità viene esplicitamente attivata o disattivata. Per esempio:

/AC-	la modalità viene esplicitamente disattivata
/AC, /AC+	la modalità viene esplicitamente attivata

Tale possibilità può essere utile se la modalità è attivata/disattivata di default o secondo le impostazioni precedentemente definite nel file di configurazione. La lista delle opzioni che permettono l'uso dei modificatori:

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.

Per l'opzione /FL il modificatore "–" significa: controlla i percorsi elencati nel file indicato ed elimina il file.

Per le opzioni /ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W il valore di parametro "0" significa che il parametro si usa senza limitazioni.

Un esempio di utilizzo delle opzioni per l'avvio di Scanner console:

[<*percorso_del_programma*>]dwscancl /AR- /AIN:C /AIC:Q C:\

controlla tutti i file ad eccezione degli archivi sul disco C, cura i file infetti, metti in quarantena i file incurabili. Per avviare a un modo analogo Scanner per Windows, è necessario invece di dwscancl digitare il nome del comando dwscanner.

17.2. Parametri per i pacchetti di installazione

`/compression` <*modalità*> — la modalità di compressione dei dati che vengono scambiati con il server di protezione centralizzata. Il parametro <*modalità*> può assumere i seguenti valori:

- `yes` — utilizza la compressione.
- `no` — non utilizzare la compressione.
- `possible` — la compressione è possibile. La decisione finale viene presa a seconda delle impostazioni sul lato server.

Se l'opzione non è impostata, di default si usa il valore `possible`.

`/encryption` <*modalità*> — la modalità di cifratura dei dati che vengono scambiati con il server di protezione centralizzata. Il parametro <*modalità*> può assumere i seguenti valori:

- `yes` — utilizza la cifratura.
- `no` — non utilizzare la cifratura.
- `possible` — la cifratura è possibile. La decisione finale viene presa a seconda delle impostazioni sul lato server.

Se l'opzione non è impostata, di default si usa il valore `possible`.

`/excludeFeatures` <*componenti*> — lista dei componenti che verranno esclusi all'installazione. Se vengono impostati più componenti, utilizzare il carattere "," come separatore. I componenti disponibili:

- `scanner` — Scanner Dr.Web,
- `spider-mail` — SpIDer Mail,
- `spider-g3` — SpIDer Guard,
- `outlook-plugin` — Dr.Web per Microsoft Outlook,
- `firewall` — Firewall Dr.Web,
- `spider-gate` — SpIDer Gate,
- `parental-control` — Office control,
- `antispam-outlook` — Antispam Dr.Web per il componente Dr.Web per Microsoft Outlook,
- `antispam-spidermail` — Antispam Dr.Web per il componente SpIDer Mail.

Per i componenti non direttamente indicati viene mantenuto lo status di installazione impostato per essi di default.

`/id` <*identificatore_della_postazione*> — l'identificatore della postazione su cui viene installato Agent Dr.Web.

Viene impostata insieme alla password (l'opzione `/pwd`) per l'autenticazione manuale sul server. Se i parametri di autenticazione non sono impostati, la decisione circa l'autenticazione viene presa sul lato server.

`/includeFeatures` <*componenti*> — lista dei componenti da installare. Se vengono impostati diversi componenti, utilizzare il carattere "," come separatore. I componenti disponibili:

- `scanner` — Scanner Dr.Web,
- `spider-mail` — SpIDer Mail,
- `spider-g3` — SpIDer Guard,
- `outlook-plugin` — Dr.Web per Microsoft Outlook,
- `firewall` — Firewall Dr.Web,
- `spider-gate` — SpIDer Gate,
- `parental-control` — Office control,
- `antispam-outlook` — Antispam Dr.Web per il componente Dr.Web per Microsoft Outlook,
- `antispam-spidermail` — Antispam Dr.Web per il componente SpIDer Mail.

Per i componenti non direttamente indicati viene mantenuto lo status di installazione impostato per essi di default.

`/installdir` <*cartella*> — la cartella di installazione.

Se l'opzione non è impostata, di default l'installazione viene eseguita nella directory `Program Files\DrWeb` sul disco di sistema.

`/instMode` <*modalità*> — la modalità di avvio dell'installer. Il parametro <*modalità*> può assumere i seguenti valori:

- `remove` — rimuovi il prodotto installato.

Se l'opzione non è impostata, di default l'installer definisce automaticamente la modalità di avvio.

`/lang` <*codice_di_lingua*> — la lingua dell'installer e del prodotto che viene installato. Viene impostata nel formato ISO-639-1 per il codice di lingua.

Se l'opzione non è impostata, di default si usa la lingua di sistema.

`/pubkey` <*percorso*> — il percorso completo del file del certificato o della chiave pubblica del server.

Se il certificato o la chiave pubblica non sono impostati, di default all'avvio dell'installazione locale l'installer accetta automaticamente il certificato (con l'estensione `.pem`) o la chiave pubblica (`drwcsd.pub`) dalla cartella del suo avvio. Se il certificato o la chiave pubblica si

trovano in una cartella diversa dalla cartella dell'installer, è necessario specificare manualmente il percorso completo del certificato o della chiave pubblica.

Se viene avviato un pacchetto di installazione creato nel Pannello di controllo, il certificato o la chiave pubblica fanno parte del pacchetto di installazione e non è richiesta alcuna indicazione aggiuntiva.

`/pwd` <*password*> — la password di Agent Dr.Web per l'accesso al server.

Viene impostata insieme all'identificatore della postazione (l'opzione `/id`) per l'autenticazione manuale sul server. Se i parametri di autenticazione non sono impostati, la decisione circa l'autenticazione viene presa sul lato server.

`/regagent` <*modalità*> — determina se Agent Dr.Web verrà registrato nella lista dei programmi installati. Il parametro <*modalità*> può assumere i seguenti valori:

- `yes` — registra Agent Dr.Web nella lista delle applicazioni installate.
- `no` — non registrare Agent Dr.Web nella lista delle applicazioni installate.

Se l'opzione non è impostata, di default si usa il valore `no`.

`/retry` <*numero*> — il numero di tentativi di ricerca del server tramite l'invio delle richieste multicast. Se non c'è una risposta dal server dopo il numero di tentativi impostato, si ritiene che il server non è stato trovato.

Se l'opzione non è impostata, di default vengono eseguiti 3 tentativi di ricerca del server.

`/server` "[<*protocollo*>/]<*indirizzo_del_server*>[:<*porta*>]" — l'indirizzo del server da cui verrà effettuata l'installazione di Agent Dr.Web e a cui Agent Dr.Web si connetterà dopo l'installazione.

Se l'opzione non è impostata, di default il server viene cercato tramite l'invio delle richieste multicast.

`/silent` <*modalità*> — determina se l'installer verrà eseguito in modalità silenziosa. Il parametro <*modalità*> può assumere i seguenti valori:

- `yes` — avvia l'installer in modalità silenziosa.
- `no` — avvia l'installer in modalità grafica.

Se l'opzione non è impostata, di default l'installazione di Agent Dr.Web viene eseguita in modalità grafica.

`/timeout` <*tempo*> — il limite di tempo per aspettare ciascuna risposta nel corso della ricerca del server. Viene impostato in secondi. I messaggi di risposta continuano ad essere accettati fino a quando il tempo di attesa della risposta non supererà il valore del time-out.

Se l'opzione non è impostata, di default si usa il valore di 3 secondi.

17.3. Codici di ritorno

I valori possibili del codice di ritorno e gli eventi corrispondenti sono i seguenti:

Codice di ritorno	Evento
0	Non sono stati rilevati virus o casi sospetti di virus.
1	Sono stati rilevati virus conosciuti.
2	Sono state rilevate varianti di virus sconosciuti.
4	Sono stati rilevati oggetti sospetti di virus.
8	Virus conosciuti sono stati rilevati in un archivio, un container o una casella di posta.
16	Varianti di virus conosciuti sono state rilevate in un archivio, un container o una casella di posta.
32	Oggetti sospetti di virus sono stati rilevati in un archivio, un container o una casella di posta.
64	È stata completata con successo la cura di almeno un oggetto infettato da un virus.
128	È stata completata con successo la rimozione/la rinominazione/lo spostamento di almeno un file infetto.

Il codice di ritorno risultante generato al completamento della scansione è uguale alla somma dei codici degli eventi che si sono verificati durante la scansione (e gli addendi possono essere ripristinati da esso in modo univoco).

Per esempio, il codice di ritorno 9 = 1 + 8 indica che uno o più virus conosciuti sono stati rilevati durante la scansione, tra l'altro anche in archivio; la neutralizzazione non veniva eseguita; non c'erano altri eventi di virus.

18. Allegato B. Minacce informatiche e metodi per neutralizzarle

Con l'evoluzione delle tecnologie informatiche e delle soluzioni di rete, diventano sempre più diffusi vari programmi malevoli volti a recare danno agli utenti in un modo o nell'altro. La loro evoluzione iniziò nella lontana epoca della nascita del computer, e durante tutto il periodo si evolvevano anche gli strumenti di protezione da tali programmi. Tuttavia, non esiste ancora un'unica classificazione di tutte le possibili minacce, il che è dovuto, in primo luogo, alla natura imprevedibile della loro evoluzione e al continuo miglioramento delle tecnologie utilizzate.

I programmi malevoli possono diffondersi tramite internet, la rete locale, la posta elettronica e i supporti di archiviazione rimovibili. Alcuni di essi fanno affidamento sulla negligenza e l'inesperienza dell'utente e possono funzionare in modo del tutto autonomo, altri sono solo strumenti controllati da hacker e possono recare danno anche a sistemi protetti in modo sicuro.

Questo capitolo fornisce le descrizioni di tutti i tipi principali e più diffusi di programmi malevoli che le tecnologie dell'azienda Doctor Web sono volti a combattere in primo luogo.

18.1. Tipi di minacce informatiche

In questa classificazione il termine "*minaccia informatica*" significa qualsiasi strumento software che sia indirettamente o direttamente capace di causare un danno al computer, alla rete, alle informazioni o ai diritti dell'utente (cioè programmi malevoli e altri programmi indesiderati). In senso più ampio, il termine "minaccia informatica" può significare qualsiasi potenziale pericolo per il computer o la rete (cioè una vulnerabilità che può essere sfruttata per condurre attacchi hacker).

Tutti i tipi di programmi descritti sotto sono potenzialmente capaci di mettere a rischio i dati dell'utente o la loro riservatezza. Di solito, non vengono categorizzati come minacce i programmi che non nascondono la loro presenza nel sistema (per esempio, alcuni programmi per l'invio dello spam o per l'analisi del traffico dati), sebbene in determinate circostanze anche tali programmi possano causare un danno all'utente.

Virus informatici

Questo tipo di minacce informatiche può incorporare il suo codice eseguibile in altri programmi. Tale incorporazione si chiama *infezione*. Nella maggior parte dei casi il file infetto diventa lui stesso portatore del virus, mentre il codice incorporato non necessariamente del tutto corrisponde all'originale. La maggior parte dei virus viene creata per danneggiare o distruggere dati.

Nell'azienda Doctor Web i virus sono divisi per il tipo di file che loro infettano:

- *I virus di file* infettano i file del sistema operativo (di solito, file eseguibili e librerie dinamiche) e diventano attivati all'accesso a un file infettato.

- *I macro virus* infettano documenti che vengono utilizzati dai programmi dal pacchetto Microsoft Office (e da altri programmi che utilizzano macro scritte, per esempio, nel linguaggio Visual Basic). Le *macro* – programmi incorporati, scritti in un linguaggio di programmazione a pieno titolo che possono avviarsi in determinate condizioni (per esempio, in Microsoft Word le macro possono avviarsi all'apertura, la chiusura o il salvataggio di un documento).
- *I virus di script* sono scritti nei linguaggi di scripting, e nella maggior parte dei casi infettano altri file di script (per esempio, i file di servizio del sistema operativo). Possono infettare anche altri tipi di file che supportano l'esecuzione di script, utilizzando script vulnerabili in applicazioni web.
- *I virus di boot* infettano i settori di avvio di dischi e partizioni, nonché i master boot record di dischi rigidi. Occupano poca memoria e rimangono pronti per svolgere le loro funzioni fino a quando il sistema operativo non verrà scaricato da memoria, riavviato o arrestato.

La maggior parte dei virus possiede alcuni meccanismi di difesa dal rilevamento. I metodi di difesa dal rilevamento vengono migliorati di continuo, perciò per i programmi antivirus vengono sviluppati nuovi metodi per superare questa difesa. I virus possono essere divisi secondo il principio di difesa dal rilevamento:

- *I virus cifrati* criptano il proprio codice a ogni infezione nuova, il che ne ostacola il rilevamento in un file, nella memoria o in un settore di avvio. Ciascuna copia di tale virus contiene solo un breve frammento comune (la procedura di decifratura) che può essere selezionato come firma antivirale.
- *I virus polimorfi* utilizzano, oltre alla cifratura del codice, una procedura di decifratura specifica che cambia sé stessa in ciascuna copia nuova del virus, quindi per tale virus non esistono firme antivirali di byte.
- *I virus stealth* (virus invisibili) intraprendono azioni speciali per mascherare le loro attività al fine di nascondere la loro presenza negli oggetti infetti. Tale virus memorizza le caratteristiche di un oggetto prima dell'infezione e quindi trasmette i vecchi dati quando arriva una richiesta del sistema operativo o di un programma che cerca file modificati.

Inoltre, i virus possono essere classificati secondo il linguaggio in cui sono scritti (la maggior parte è scritta nel linguaggio assembly, ma ci sono anche virus scritti nei linguaggi di programmazione di altro livello, linguaggi di scripting ecc.) e secondo il sistema operativo che viene infettato.

Worm

Recentemente i programmi malevoli del tipo "worm" sono diventati molto più diffusi dei virus e degli altri programmi malevoli. Così come i virus, i worm sono in grado di creare copie di sé, ma non infettano altri oggetti. Un worm si infiltra su un computer dalla rete (il più delle volte come allegato a un'email o attraverso internet) e invia le proprie copie funzionali su altri computer. Per iniziare a diffondersi, i worm possono utilizzare sia le attività dell'utente che una modalità automatica di selezione del computer da attaccare.

I worm non necessariamente sono costituiti per intero da un singolo file (il corpo del worm). Molti worm hanno la cosiddetta parte di infezione (un codice shell) che viene caricata nella memoria operativa del computer e ulteriormente scarica dalla rete il corpo stesso del worm come un file eseguibile. Fino a quando il corpo del worm non c'è nel sistema, è possibile liberarsene riavviando il computer (a riavvio la memoria operativa viene azzerata). Ma se il corpo del worm è già presente nel sistema, soltanto un antivirus può affrontarlo.

Propagandosi intensamente, i worm possono mettere fuori servizio intere reti anche quando non hanno alcun payload (cioè non causano un danno diretto al sistema).

Nell'azienda Doctor Web i worm sono divisi in base al modo (ambiente) di propagazione:

- *I worm di rete* si diffondono tramite vari protocolli di rete e protocolli di condivisione di file.
- *I worm di posta* si diffondono tramite i protocolli di email (POP3, SMTP ecc.).
- *I worm di chat* si diffondono utilizzando i programmi di messaggistica istantanea più comuni (ICQ, IM, IRC ecc.).

Trojan

Questo tipo di programmi malevoli non è in grado di autoreplicarsi. I programmi trojan sostituiscono uno dei programmi frequentemente avviati e svolgono le sue funzioni (o simulano di svolgere queste funzioni) eseguendo contemporaneamente qualche attività malevola (corruzione e cancellazione dei dati, invio di informazioni riservate ecc.) o rendendo possibile l'uso non autorizzato del computer da parte di un malintenzionato, per esempio, per causare danni a terzi.

Questi programmi hanno funzioni malevole e mimetiche simili a quelle dei virus e persino possono essere un modulo dei virus, ma di regola i trojan vengono distribuiti come file eseguibili separati (vengono collocati su file server, registrati su supporti di informazione o inviati in email come allegati) che vengono eseguiti dall'utente stesso o da un determinato processo del sistema.

I trojan sono molto difficili da classificare, in primo luogo, perché spesso vengono distribuiti dai virus e worm, in secondo luogo, le azioni malevole che possono essere eseguite da altri tipi di minacce solitamente vengono imputate solo ai programmi trojan. Di seguito è riportato un elenco di alcuni tipi di programmi trojan che l'azienda Doctor Web classifica in classi separate:

- *I backdoor* – programmi trojan che consentono di ottenere l'accesso privilegiato al sistema aggirando il meccanismo di accesso e protezione esistente. I backdoor non infettano file; si trascrivono nel registro, modificando le chiavi.
- *I rootkit* sono studiati per intercettare le funzioni del sistema operativo al fine di nascondere la propria presenza nel sistema. Inoltre, i rootkit possono nascondere i processi di altri programmi, diverse chiavi del registro, cartelle e file. Un rootkit si diffonde come programma indipendente o come componente aggiuntivo di un altro programma malevolo. In base al principio di funzionamento i rootkit sono convenzionalmente divisi in due gruppi: quelli che funzionano in modalità utente (intercettano le funzioni delle librerie di modalità utente) (*User Mode Rootkits – UMR*) e quelli che funzionano in modalità kernel (intercettano le

funzioni a livello di kernel del sistema, il che rende notevolmente più difficile il rilevamento e la neutralizzazione) (*Kernel Mode Rootkits – KMR*).

- *I keylogger* (*software che catturano eventi della tastiera*) vengono utilizzati per raccogliere i dati che l'utente immette tramite la tastiera. Lo scopo di tali azioni è il furto di informazioni personali (per esempio, password di rete, login, numeri di carte di credito ecc.).
- *I clicker* sostituiscono i link quando si fa clic su di essi e in questo modo reindirizzano l'utente su determinati siti web (probabilmente malevoli). Di solito, il reindirizzamento viene effettuato per aumentare il traffico pubblicitario di siti web o per organizzare attacchi denial of service distribuiti (attacchi DDoS).
- *I trojan proxy* forniscono al malintenzionato l'accesso anonimo a internet attraverso il computer della vittima.

Oltre a quelle elencate, i trojan possono eseguire anche altre funzioni malevole, per esempio cambiare la pagina iniziale nel browser o rimuovere determinati file. Tali azioni però possono essere eseguite anche da altri tipi di minacce (per esempio, dai virus e worm).

Hacktool

Gli hacktool vengono creati per lo scopo di aiutare un intruso. Il tipo più comune di tali programmi sono gli scanner delle porte che consentono di scoprire vulnerabilità nei firewall e in altri componenti di protezione del computer. Oltre agli hacker, anche gli amministratori possono utilizzare questi strumenti per controllare la sicurezza delle loro reti. Talvolta vengono classificati come hacktool i programmi che utilizzano metodi di social engineering (ingegneria sociale).

Adware

Il più delle volte questo termine significa un codice software incorporato in vari programmi gratuiti, utilizzando i quali l'utente è costretto a visualizzare pubblicità. Tuttavia, tale codice può talvolta essere distribuito di nascosto attraverso altri programmi malevoli e può visualizzare pubblicità, per esempio nei browser. Spesso gli adware funzionano sulla base dei dati raccolti dai programmi spyware.

Joke

Questo tipo di programmi malevoli, così come gli adware, non causa alcun danno diretto al sistema. Il più delle volte, gli joke generano avvisi di errori inesistenti e minacciano di azioni che possono portare alla corruzione dei dati. La loro funzione principale è quella di intimidire o infastidire l'utente.

Dialer

Questi sono programmi per computer speciali progettati per scansionare un range di numeri di telefono per trovare un numero su cui risponderà un modem. In seguito, i malintenzionati

utilizzano i numeri trovati per aumentare furtivamente il pagamento per il telefono o per connettere impercettibilmente l'utente tramite il modem a costosi servizi telefonici.

Riskware

Questi programmi non sono stati creati per causare danni, ma in virtù delle loro caratteristiche possono rappresentare un rischio per la sicurezza del sistema. A tali software appartengono non solo quelli che possono danneggiare o cancellare accidentalmente i dati, ma anche quelli che possono essere utilizzati dagli hacker o da altri programmi per causare danni al sistema. Possono essere classificati come riskware diversi programmi di comunicazione e amministrazione in remoto, server FTP ecc.

Oggetti sospetti

Agli oggetti sospetti appartiene qualsiasi potenziale minaccia rilevata tramite l'analisi euristica. Tali oggetti possono essere qualsiasi tipo di minacce informatiche (probabilmente persino un tipo non ancora conosciuto dagli specialisti di sicurezza informatica), o possono essere sicuri in caso di falso positivo. Si consiglia di mettere in quarantena i file contenenti oggetti sospetti, nonché inviarli per l'analisi agli specialisti del laboratorio antivirus dell'azienda Doctor Web.

18.2. Azioni per neutralizzare le minacce

Esistono molti metodi diversi per combattere le minacce informatiche. Per fornire una protezione affidabile dei computer e delle reti, i prodotti dell'azienda Doctor Web combinano in sé questi metodi tramite le impostazioni flessibili e un approccio integrato alla sicurezza. Le principali azioni per neutralizzare i programmi malevoli sono:

1. **Cura** — azione applicabile ai virus, worm e trojan. Sottintende la rimozione del codice malevolo dai file infetti o la rimozione delle copie funzionali dei programmi malevoli, e inoltre, se possibile, il ripristino dell'operatività degli oggetti colpiti (cioè il ripristino della struttura e delle funzionalità di un programma allo stato precedente all'infezione).
2. **Spostamento in quarantena** — azione con cui un oggetto malevolo viene messo in una cartella specifica in cui esso è isolato dal resto del sistema. Questa azione va preferita quando la cura non è possibile, così come per tutti gli oggetti sospetti. È preferibile inviare le copie di simili file per l'analisi al laboratorio antivirus Doctor Web.
3. **Rimozione** — un'azione efficace per combattere le minacce informatiche. È applicabile a qualsiasi tipo di oggetti malevoli. Va notato che talvolta la rimozione verrà applicata ad alcuni file per cui è selezionata l'azione cura. Ciò accade quando l'intero file è costituito da codice malevolo e non contiene alcuna informazione utile. Così, per esempio, sotto la cura di un worm è sottintesa la rimozione di tutte le sue copie funzionali.
4. **Blocco** — anche questa è un'azione che consente di neutralizzare i programmi malevoli, con cui, tuttavia, le loro copie complete rimangono nel file system. Viene bloccato qualsiasi tentativo di accesso da e verso l'oggetto malevolo.

19. Allegato C. Principi di denominazione delle minacce

Se viene rilevato un codice di virus, i componenti Dr.Web ne informano l'utente tramite gli strumenti dell'interfaccia e scrivono nel file di log il nome del virus assegnato ad esso dagli specialisti dell'azienda Doctor Web. Questi nomi si basano su determinati principi e rispecchiano la struttura del virus, le classi di oggetti vulnerabili, l'ambiente di diffusione (sistema operativo e pacchetti applicativi) e una serie di altre caratteristiche. Conoscere questi principi può essere utile per identificare le vulnerabilità di software e organizzative del sistema protetto. Di seguito è riportato un riepilogo dei principi di denominazione dei virus; una versione più completa e costantemente aggiornata della descrizione è disponibile sull'indirizzo https://vms.drweb.com/classification/.

Questa classificazione in alcuni casi è condizionale in quanto tipi specifici di virus possono avere più caratteristiche allo stesso tempo da quelle riportate. Inoltre, essa non può essere considerata esauriente in quanto appaiono costantemente nuovi tipi di virus e, di conseguenza, viene precisata la classificazione.

Il nome completo di un virus è costituito da diversi elementi separati da punti. Alcuni elementi all'inizio del nome completo (prefissi) e alla fine (suffissi) sono tipici secondo la classificazione adottata.

Principali prefissi

Prefissi del sistema operativo

I seguenti prefissi vengono utilizzati per denominare i virus che infettano i file eseguibili di determinate piattaforme (sistemi operativi):

- `Win` — programmi a 16 bit per SO Windows 3.1;
- `Win95` — programmi a 32 bit per SO Windows 95/98/Me;
- `WinNT` — programmi a 32 e 64 bit per SO Windows NT/2000/XP/Vista/7/8/8.1/10;
- `Win32` — programmi a 32 bit per diversi ambienti di SO Windows 95/98/Me ed SO Windows NT/2000/XP/Vista/7/8/8.1/10;
- `Win64` — programmi a 64 bit per SO Windows XP/Vista/7/8/8.1/10/11;
- `Win32.NET` — programmi nel sistema operativo Microsoft .NET Framework;
- `OS2` — programmi per OS/2;
- `Unix` — programmi per diversi sistemi operativi UNIX;
- `Linux` — programmi per il sistema operativo Linux;
- `FreeBSD` — programmi per il sistema operativo FreeBSD;
- `SunOS` — programmi per il sistema operativo SunOS (Solaris);
- `Symbian` — programmi per il sistema operativo Symbian OS (un sistema operativo mobile).

Va notato che alcuni virus possono infettare programmi di un sistema, sebbene essi stessi operino in un altro.

Virus che infettato i file di MS Office

Gruppo di prefissi dei virus che infettano gli oggetti di MS Office (è indicato il linguaggio delle macro che vengono infettate da questo tipo di virus):

- `WM` — Word Basic (MS Word 6.0-7.0);
- `XM` — VBA3 (MS Excel 5.0-7.0);
- `W97M` — VBA5 (MS Word 8.0), VBA6 (MS Word 9.0);
- `X97M` — VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0);
- `A97M` — database MS Access'97/2000;
- `PP97M` — file di presentazione MS PowerPoint;
- `O97M` — VBA5 (MS Office'97), VBA6 (MS Office'2000), il virus infetta i file di più di un componente di MS Office.

Prefissi del linguaggio di sviluppo software

Il gruppo di prefissi `HLL` è usato per denominare virus scritti in linguaggi di programmazione di alto livello, come per esempio C, C++, Pascal, Basic ecc. Sono usati modificatori che indicano l'algoritmo di funzionamento di base, in particolare:

- `HLLW` — worm;
- `HLLM` — worm di email;
- `HLLO` — virus che sovrascrivono il codice del programma vittima;
- `HLLP` — virus parassiti;
- `HLLC` — virus satelliti.

Inoltre, il gruppo di prefissi del linguaggio di sviluppo software può includere:

- `Java` — virus per l'ambiente della macchina virtuale Java.

Trojan

`Trojan` — nome generico di vari programmi trojan. In molti casi i prefissi di questo gruppo sono usati insieme al prefisso Trojan.

- `PWS` — trojan che ruba password;
- `Backdoor` — trojan con la funzionalità RAT (Remote Administration Tool — utility di amministrazione in remoto);
- `IRC` — trojan che utilizza per il suo funzionamento l'ambiente Internet Relayed Chat channels;
- `DownLoader` — trojan che scarica da internet vari file malevoli all'insaputa dell'utente;

- `MulDrop` — trojan che carica di nascosto vari virus che sono contenuti direttamente nel suo corpo;
- `Proxy` — trojan che consente a un malintenzionato di navigare su internet in modo anonimo attraverso il computer infetto;
- `StartPage` (sinonimo: `Seeker`) — trojan che sostituisce in modo non autorizzato l'indirizzo della pagina impostata nel browser come la homepage (pagina iniziale);
- `Click` — trojan che organizza il reindirizzamento delle richieste fatte dall'utente al browser su uno specifico sito (o siti);
- `KeyLogger` — trojan spione; segue e registra le battiture sulla tastiera; può inviare periodicamente i dati raccolti a un malintenzionato;
- `AVKill` — arresta il funzionamento dei programmi di protezione antivirus, firewall ecc.; e inoltre, può rimuovere dal disco questi programmi;
- `KillFiles`, `KillDisk`, `DiskEraser` — rimuovono uno specifico insieme di file (file in determinate directory, file in base a una maschera, tutti i file su un disco ecc.);
- `DelWin` — rimuove i file necessari per il funzionamento del sistema operativo (Windows);
- `FormatC` — formatta il disco C: (sinonimo: `FormatAll` — formatta alcuni o tutti i dischi);
- `KillMBR` — danneggia o cancella il contenuto del settore di avvio principale (MBR);
- `KillCMOS` — danneggia o cancella il contenuto del CMOS.

Strumento per l'utilizzo delle vulnerabilità

- `Exploit` — strumento che utilizza le vulnerabilità conosciute di un sistema operativo o di un'applicazione al fine di introdurre nel sistema un codice malevolo, un virus od eseguire azioni non autorizzate.

Strumenti per gli attacchi di rete

- `Nuke` — strumenti per gli attacchi di rete ad alcune vulnerabilità conosciute dei sistemi operativi al fine di causare un arresto di emergenza del sistema attaccato;
- `DDoS` — programma agent studiato per effettuare gli attacchi di rete distribuiti di "negazione del servizio" (Distributed Denial Of Service);
- `FDOS` (sinonimo: Flooder) — Flooder Denial Of Service — programmi per vari tipi di azioni malevole nella Rete che in un modo o nell'altro utilizzano l'idea di un attacco "negazione del servizio" (denial-of-service); a differenza del DDoS quando molti agent su più computer vengono utilizzati contemporaneamente contro lo stesso bersaglio, l'FDOS funziona come un programma separato "autosufficiente".

Script virus

Prefissi dei virus scritti in diversi linguaggi di scripting:

- `VBS` — Visual Basic Script;
- `JS` — Java Script;

- `Wscript` — Visual Basic Script e/o Java Script;
- `Perl` — Perl;
- `PHP` — PHP;
- `BAT` — linguaggio dell'interprete comandi del sistema operativo MS-DOS.

Programmi malevoli

Prefissi degli oggetti che sono altri programmi malevoli, anziché virus:

- `Adware` — programma di visualizzazione di pubblicità;
- `Dialer` — programma di effettuazione di chiamate del modem (reindirizza una chiamata del modem a un numero o una riscorsa a pagamento che sono impostati nel programma);
- `Joke` — programma scherzo;
- `Program` — programma potenzialmente pericoloso (riskware);
- `Tool` — utility di hacking (hacktool).

Varie

Il prefisso `generic` è usato dopo un altro prefisso che indica l'ambiente o il metodo di sviluppo software per indicare un campione tipico di questo tipo di virus. Tale virus non possiede alcuni tratti distintivi (come per esempio stringhe di testo, effetti speciali ecc.) che avrebbero permesso di attribuirgli un nome specifico.

In precedenza, per denominare i virus più semplici senza volto, veniva utilizzato il prefisso `Silly` con diversi modificatori.

Suffissi

I suffissi vengono utilizzati per denominare alcuni oggetti di virus specifici:

- `generator` — l'oggetto non è un virus, ma è un generatore di virus;
- `based` — il virus è stato sviluppato tramite il generatore di virus specificato o tramite la modifica del virus specificato. In entrambi i casi i nomi di questo tipo sono gentilizi e possono denotare centinaia e talvolta persino migliaia di virus;
- `dropper` — indica che l'oggetto non è un virus, ma è l'installer del virus specificato.

20. Allegato D. Termini e concetti di base

A

Applicazioni affidabili — le applicazioni le cui firme sono aggiunte alla lista di quelle affidabili in drwbase.db. Alle applicazioni affidabili appartengono software popolari, come per esempio Google Chrome, Firefox, le applicazioni Microsoft.

B

Bus di dispositivi — sottosistemi di trasferimento dati tra unità funzionali di un computer (ad esempio, un bus USB).

C

Classi di dispositivi — dispositivi che svolgono le stesse funzioni (ad esempio, dispositivi per la stampa).

E

Emulazione — simulazione del funzionamento di un sistema per mezzo di un altro senza perdita di funzionalità e distorsione dei risultati attraverso l'uso di software speciali.

Euristica — ipotesi la cui significatività statistica è confermata empiricamente.

Exploit — un programma, un frammento di codice o una sequenza di comandi che sfrutta le vulnerabilità dei software e viene utilizzato per attaccare il sistema.

F

Firma antivirale — sequenza di byte continua finita, necessaria e sufficiente per identificare univocamente una minaccia.

Firma digitale elettronica — requisito di un documento elettronico progettato per la protezione di questo documento elettronico da falsificazione. È stato ottenuto a seguito della trasformazione crittografica delle informazioni tramite la chiave privata della firma digitale elettronica e consente di identificare il proprietario del certificato della chiave della firma e anche di stabilire l'assenza di distorsione delle informazioni nel documento elettronico.

H

Hashsum — identificatore univoco di un file, che è una sequenza di numeri e lettere di una determinata lunghezza. Viene utilizzato per verificare l'integrità dei dati.

M

Mirror di aggiornamento — cartella in cui vengono copiati gli aggiornamenti. Il mirror di aggiornamento può essere utilizzato come fonte di aggiornamento Dr.Web per i computer della rete locale che non sono connessi a Internet.

Modalità amministratore — modalità di Dr.Web in cui è fornito l'accesso a tutte le impostazioni dei componenti di protezione e alle impostazioni del programma. Per andare alla modalità amministratore, è necessario fare clic sul lucchetto .

R

Rete antivirus — insieme di computer su cui sono installati i prodotti Dr.Web (Antivirus Dr.Web per Windows, Antivirus Dr.Web per server Windows e Dr.Web Security Space) e che sono connessi alla stessa rete locale.

V

Variante di un virus — codice ottenuto tramite la modifica di un virus conosciuto, in questo caso viene riconosciuto dallo scanner, ma ad esso non possono essere applicati gli algoritmi di cura del virus originale.