G DATA

Security Software

Sommario

Primi passi

Siamo lieti che Lei abbia deciso di acquistare il nostro prodotto e speriamo che resterà pienamente soddisfatto del suo nuovo software. In caso di problemi nel funzionamento del software in questa guida potrete trovare alcune informazioni utili. In caso di domande di tipo tecnico, La preghiamo di contattare i nostri esperti del **Service Center**.

> **Nota**: È possibile richiamare in qualsiasi momento la Guida all'interno del programma e ottenere immediatamente le informazioni necessarie. Basta semplicemente fare clic nel programma sull'icona della Guida.

ServiceCenter

L'installazione e l'utilizzo del software G DATA sono semplici e ricchi di spiegazioni. Tuttavia, in caso di problemi, potete contattare i nostri esperti del ServiceCenter:

G DATA Italia	www.gdata.it
G DATA Svizzera	www.gdata.ch

Installazione

Nel caso in cui il computer fosse nuovo o fosse già stato protetto da un software antivirus, potete installare il software come spiegato di seguito. Nel caso in cui si sospettasse la presenza di un virus, prima dell'installazione del software è consigliabile eseguire un **BootScan**.

> **Attenzione**: prima di installare il programma, rimuovere eventuali programmi antivirus installati sul computer. Poiché questi programmi tendono a penetrare profondamente nel sistema, per disinstallarli vi consigliamo di non affidarvi solo alla normale disinstallazione, bensì di utilizzare, se possibile, anche gli strumenti di pulizia che il produttore mette a disposizione sul proprio sito del Supporto tecnico.

Passo 1: Avvio dell'installazione

Avviare l'installazione nel modo seguente:

- **Installazione da CD/DVD**: per iniziare l'installazione, inserire nel lettore il CD o il DVD del programma.
- **Download del software**: per installare una versione del software scaricata da Internet, fare semplicemente doppio clic sul file scaricato.

Ora si apre automaticamente la finestra di installazione.

> **Nota**: Se l'installazione non si avvia: può accadere che la funzione Autostart del computer non sia stata impostata in modo adeguato. In questo caso, dopo l'inserimento del CD del programma, la procedura di installazione non si avvia automaticamente e non compare nessuna finestra che permetta di installare il software G DATA.
>
> - Se invece si apre una finestra di selezione per la riproduzione automatica, fare clic sull'opzione **Esegui AUTOSTRT.EXE**.
> - Se non si apre nessuna finestra di selezione, cercare in Esplora risorse di Windows il supporto dati che contiene il software G DATA e avviare il file **Setup** o **Setup.exe**.

Passo 2: Scelta della lingua

Selezionare ora la lingua di installazione del nuovo software G DATA.

Passo 3: Metodi di installazione

Una procedura guidata vi aiuterà ad installare il software sul computer. Scegliere ora se si desidera eseguire l'installazione standard o un'installazione personalizzata. Si consiglia di scegliere l'installazione standard.

Raccolta di informazioni sul malware: gli specialisti dei G DATA Security Labs studiano costantemente nuove procedure per proteggere i clienti G DATA dal malware (virus, worm e programmi dannosi). Più sono le informazioni disponibili e maggiori saranno le possibilità di sviluppare meccanismi di protezione efficaci. Tuttavia, molte informazioni si possono reperire soltanto dai sistemi che sono già stati attaccati o infettati. Per inserire anche queste informazioni nelle analisi, G DATA ha ideato la raccolta di informazioni sul malware. In questo contesto, le informazioni sul malware vengono inviate ai G DATA Security Labs. Partecipando a quest'iniziativa, anche voi potrete contribuire ad aumentare la protezione dei clienti G DATA nell'utilizzo di Internet. Durante l'installazione del software G DATA è possibile scegliere se mettere le informazioni a disposizione dei Security Labs o no.

Nota: Nell'installazione personalizzata è possibile scegliere la cartella di archiviazione dei dati del programma e selezionare o deselezionare i moduli del software da installare (ad es. la protezione AntiSpam).

Passo 4: Accordo di licenza

Leggere attentamente l'accordo di licenza e accettare le condizioni.

Passo 5 - Installazione personalizzata (facoltativo)

Se è stata scelta l'installazione personalizzata, compaiono due finestre di una procedura guidata che permettono rispettivamente di scegliere la directory di installazione e i moduli da installare. Se invece è stata scelta l'installazione standard, si può ignorare questo passaggio.

- **Definita dall'utente**: permette di decidere il tipo di installazione selezionando con un segno di spunta i vari moduli software (ad es. antispam ecc.).
- **Completa**: vengono installati tutti i moduli software della versione usata.
- **Minima**: con il modulo AntiVirus viene installata solo la protezione di base del software G DATA.

Aggiornamenti: tramite il programma di installazione è possibile anche in un secondo tempo installare i moduli software o aggiornare il programma. Per aggiungere o ridurre i moduli del programma, riavviare l'installazione e selezionare **Personalizza installazione**. Se si possiede una nuova versione del programma e si desidera aggiornare la versione, è possibile scegliere **Aggiornamento definito da utente** e stabilire i moduli da aggiungere o deselezionare.

Passo 6: Versione del software

Ora è possibile decidere se installare il software come versione completa o come versione di prova. Se avete acquistato il software e possedete un numero di registrazione, installate il software come **Versione completa**. Per testare il software G DATA gratuitamente, è possibile utilizzare la versione di prova, limitata nel tempo.

Passo 7: Attivazione del prodotto

Durante l'installazione viene eseguita l'attivazione del prodotto. Qui è possibile attivare il vostro software.

- **Inserire nuovo numero di registrazione**: se il software G DATA è stato installato per la prima volta, selezionare questa opzione e inserire il numero di registrazione fornito con il prodotto. In base al tipo di prodotto, il codice di registrazione si trova sul retro della copertina del manuale d'uso, nella email di conferma in caso di download del programma o sulla confezione del prodotto.

  Nota: Dopo aver effettuato la registrazione del prodotto, i dati di accesso verranno inviati all'indirizzo e-mail indicato al momento della registrazione.

- **Inserire dati di accesso**: nel caso in cui il software G DATA fosse già stato registrato, avete già ricevuto i dati di accesso (nome utente e password). Per reinstallare il software o per registrare altri computer in caso di multilicenza, inserire semplicemente i propri dati di accesso.

  Nota: i dati di accesso si ricevono soltanto per e-mail. I dati di accesso non vengono forniti con il prodotto.

  Nel caso di smarrimento dei dati sarà possibile recuperarli facendo clic nella finestra di registrazione su **Dati di accesso dimenticati?** Si aprirà una pagina web in cui verrà richiesto il numero di registrazione. Una volta inserito il codice, vi verrà spedita una e-mail con i dati di accesso. Nel caso l'indirizzo email non fosse più lo stesso, rivolgersi al **Service Center**.

- **Attiva più tardi**: se si volesse solo vedere come funziona il software, è possibile installare il programma senza registrarlo. In questo caso però non sarà possibile scaricare gli aggiornamenti del software via Internet e il PC non sarà protetto efficacemente dai programmi nocivi. Il software può essere attivato in un secondo tempo, inserendo il numero di registrazione o i dati di accesso.

Passo 8: Fine dell'installazione

Per attivare il software G DATA, dopo l'installazione sarà necessario riavviare il PC in modo da attivare il software G DATA.

Dopo l'installazione

Dopo l'installazione, per avviare il software G DATA appena installato fare clic sull'icona del programma presente nella barra delle applicazioni. Sul computer sono ora disponibili ulteriori funzioni di sicurezza:

Icona di sicurezza: Il software G DATA protegge in modo permanente il computer da software dannosi e da attacchi. Un'icona nella barra delle applicazioni del computer indica che il programma ritiene necessario un intervento da parte dell'utente. Facendo clic sull'icona con il tasto destro del mouse, si apre l'interfaccia del programma G DATA. Per ulteriori informazioni, consultare il capitolo **Icona di sicurezza**.

Shredder: se durante l'installazione è stato selezionato lo Shredder (non integrato in G DATA Antivirus), questa icona sarà disponibile sul desktop. I dati spostati nello Shredder vengono eliminati in modo tale che non possano essere più recuperati, neppure con strumenti professionali di recupero dei dati. Tutti i dati vengono infatti sottoposti a una quantità di passaggi definibile liberamente. Per accedere alle impostazioni, fare clic con il tasto destro del mouse sull'icona dello Shredder e scegliere le proprietà.

Scansione rapida: la scansione rapida permette di controllare in modo semplice un file o una cartella senza avviare il software. Selezionare semplicemente con il mouse i file o le cartelle in Esplora risorse. Ora fare clic con il tasto destro del mouse e selezionare **Cerca virus**. A questo punto si avvia la scansione antivirus del file.

Dopo l'installazione del software, il computer si avvia in modo diverso dal solito: è possibile che il CD del programma sia rimasto nell'unità CD. Rimuovere il CD e il computer si avvierà come di consueto.

SecurityCenter

È necessario aprire SecurityCenter soltanto quando si desidera accedere attivamente a una delle numerose funzioni supplementari. L'effettiva protezione del computer da virus e altre minacce avviene costantemente in background. Nei casi in cui il programma necessiti di un vostro intervento, verrete avvisati automaticamente dalle informazioni visualizzate nella barra delle applicazioni.

Stato di protezione

Se compare ovunque un segno di spunta, significa che il sistema è protetto.

Un punto esclamativo rosso indica che il sistema è esposto a gravi rischi ed è dunque necessario intervenire affinché possa essere nuovamente garantita la protezione dei propri dati.

Quando viene visualizzato il segnaposto, significa che non è stata attivata la rispettiva funzione di protezione, ad esempio la Protezione da spam.

L'icona gialla indica che presto sarà necessario un intervento dell'utente, ad esempio quando è disponibile un aggiornamento del programma software.

Tutte le altre funzioni e le aree del software (ad es. **Scansione antivirus** o **Impostazioni**) possono essere utilizzate quando ci si vuole occupare attivamente della protezione del sistema, ma non è obbligatorio! L'utente può decidere liberamente quanto tempo dedicare al tema della protezione antivirus e del salvataggio dei dati. È disponibile per la consultazione una guida completa del software.

Ulteriori funzioni

Le seguenti icone indicano lo stato di sicurezza delle relative aree.

Impostazioni: questo pulsante in alto a destra permette di accedere a tutte le finestre di impostazione delle diverse aree del programma. Anche in ciascuna area è possibile selezionare direttamente un'altra finestra di impostazione.

Protocolli: il programma elenca qui i log attuali di tutte le azioni eseguite (scansione antivirus, aggiornamento, virus rilevati ecc).

In altro a destro nell'intestazione del software sono disponibili anche le seguenti funzioni:

Mostra Guida: è possibile richiamare in qualsiasi momento la Guida all'interno del programma. Basta premere semplicemente nel programma il pulsante della guida.

Aggiorna programma: quando sono disponibili nuove versioni del software, si può procedere con l'aggiornamento semplicemente con un clic del mouse, come nel caso delle informazioni sui virus. Pertanto, quando si riceve un messaggio sulla disponibilità di un aggiornamento, fare clic sulla voce Aggiorna programma. Per maggiori informazioni, consultare il capitolo: Aggiornamenti.

Informazioni: qui vengono fornite le informazioni relative alla versione del programma. Conoscere il numero di versione può essere utile, ad esempio quando si contatta il ServiceCenter.

Indicazioni di stato

Le seguenti indicazioni di stato informano l'utente sullo stato di sicurezza del sistema. Quando si seleziona una di queste opzioni, è possibile avviare immediatamente alcune azioni per ottimizzare lo stato della sicurezza:

Protezione in tempo reale

La funzione Protezione in tempo reale del Guardiano AntiVirus controlla ininterrottamente l'eventuale presenza di virus sul computer, controlla i processi di scrittura e di lettura e blocca i programmi che intendono eseguire delle funzioni dannose o diffondere file nocivi. Il Guardiano AntiVirus è la protezione più importante e per questo non dovrebbe mai essere disattivato!

- **Disattiva Guardiano**: se comunque si desidera disattivare il Guardiano, selezionare questa opzione. Se si desidera disattivare il Guardiano per ottimizzare le prestazioni del computer, si consiglia di provare prima a modificare altre impostazioni del Guardiano AntiVirus per vedere se si riesce a ottenere lo stesso risultato di efficienza. Per questo motivo, quando si disattiva il Guardiano AntiVirus è possibile modificare alcune impostazioni. Fare clic sul pulsante Modifica protezione / rendimento e seguire le istruzioni fornite nell'argomento corrispondente della Guida. In alternativa è possibile anche disattivare completamente il Guardiano AntiVirus.

- **Disattiva monitoraggio del comportamento**: la funzione Monitoraggio del comportamento offre un riconoscimento intelligente dei software dannosi sconosciuti e fornisce una protezione aggiuntiva oltre ai database antivirus. Si consiglia di tenere sempre attivata la funzione Monitoraggio del comportamento.

- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | AntiVirus | Protezione in tempo reale**.

Ultima scansione in modo inattivo

Qui viene indicato quando è stato effettuato l'ultimo controllo antivirus completo del computer. Se questa voce è evidenziata in rosso, è consigliabile eseguire al più presto una scansione antivirus.

- **Verifica il computer**: se avete tempo e non dovete utilizzare il computer per alcune ore, questa opzione permette di avviare direttamente una verifica completa del computer. Si può continuare a usare comunque il computer, tuttavia, poiché con questa impostazione la Scansione antivirus verrà eseguita con le massime prestazioni, è possibile che altre applicazioni vengano rallentate. Per ulteriori informazioni, consultare il capitolo **Scansione antivirus**.

- **Avvia ora scansione in modo inattivo**: la Scansione in modo inattivo si avvia automaticamente nelle fasi in cui il computer non è attivo ed esegue ad intervalli stabiliti una verifica dell'intero PC. Per avviare una scansione in modo inattivo prima del termine automatico predefinito, selezionare **Avvia ora scansione in modo inattivo**. Se non si desidera che il programma G DATA avvii automaticamente la scansione in modo inattivo durante le pause di lavoro, è possibile anche disattivare questa funzione scegliendo **Disattiva scansione in modo inattivo** (sconsigliato).

Firewall

Un firewall protegge il computer dall'essere *spiato*. Controlla infatti quali dati e quali programmi provenienti da Internet o dalla rete accedono al computer e quali dati vengono trasmessi dal computer. Non appena ha il sospetto che i dati sul computer vengano riprodotti o scaricati senza alcuna autorizzazione, il firewall emette un allarme e blocca lo scambio di dati non autorizzato. Questo modulo software è disponibile nelle versioni G DATA Internet Security e G DATA Total Security.

- **Disattiva il firewall**: in caso di necessità, è anche possibile disattivare il firewall. Il computer resta collegato ad Internet e alle altre reti, tuttavia non è più protetto dal firewall contro attacchi e azioni di spionaggio (sconsigliato).

- **Disattivare pilota automatico**: generalmente è consigliabile utilizzare il firewall con la modalità **Pilota automatico**. Con questa opzione, il firewall funziona quasi in background e protegge senza dover effettuare impostazioni complicate. Quando si utilizza il firewall senza il Pilota automatico, nei casi di dubbio viene visualizzata una finestra di dialogo in cui è possibile ottimizzare il firewall di volta in volta in base alle condizioni del sistema. Per gli utenti esperti, si tratta di una funzione utile. Tuttavia, normalmente non è necessario disattivare il Pilota automatico.

- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | Firewall | Pilota automatico**.

Protezione Web

Quando è attivata la funzione Protezione Web, i contenuti Internet vengono controllati per l'eventuale presenza di software dannosi già in fase di navigazione. Serve come supporto al Guardiano AntiVirus e blocca i siti Web e i download pericolosi prima ancora che possano essere richiamati.

Quando un sito Internet viene individuato come pericoloso e bloccato dal software G DATA, anziché il sito Web l'utente visualizzerà nel browser una pagina informativa di G DATA.

- **Disattiva protezione Web**: quando si esegue un download di grandi dimensioni da una fonte sicura, può essere utile disattivare la protezione Web per velocizzare l'operazione. Fondamentalmente, anche senza protezione Web il computer è protetto dal Guardiano AntiVirus. Tuttavia, è opportuno disattivare la protezione Web solo in casi eccezionali.

- **Definisci eccezioni**: La funzione Protezione Web serve per non cadere vittima di pagine Web infette o fraudolente in Internet. In rari casi, tuttavia, può accadere che una pagina Internet non venga rappresentata correttamente anche se proviene da una fonte sicura. In questi casi è sufficiente inserire l'indirizzo Internet nella Whitelist, ossia definirlo come eccezione, e in seguito questa pagina Web non verrà più bloccata dalla Protezione Web. Per ulteriori informazioni, consultare il capitolo **Definisci eccezioni**.

- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | AntiVirus | Protezione Web**.

Verifica e-mail

La funzione Verifica E-Mail permette di controllare l'eventuale presenza di virus nelle e-mail in entrata e in uscita e nei relativi allegati e di bloccare le possibili infezioni direttamente all'origine. Se viene rilevato un virus, il software è in grado di eliminare direttamente gli allegati ai file o di riparare i file infetti.

- **Disattiva verifica e-mail**: selezionare questa opzione se non si desidera che il software G DATA controlli le e-mail. Tuttavia, disattivando questa opzione il rischio per la sicurezza è elevato e pertanto si dovrebbe attuare solo in casi eccezionali.

- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | AntiVirus | Verifica e-mail**.

Microsoft Outlook: qui la verifica delle e-mail viene effettuata tramite un plugin che offre la stessa protezione della funzione per POP3/ IMAP disponibile tra le opzioni dell'AntiVirus. Dopo l'installazione del plugin, nel menu Extra di Outlook è disponibile la funzione **Verificare la presenza di virus nella cartella** che permette di controllare l'eventuale presenza di virus nelle cartelle di posta elettronica.

Protezione da spam

Offerte speciali, pubblicità, newsletter: il flusso di e-mail indesiderate è in continua crescita. La tua posta in entrata è sovraccarica a causa di e-mail indesiderate? Il software G DATA offre una protezione contro la posta indesiderata, blocca in modo efficiente i mittenti di e-mail di spam ed evita identificazioni errate, grazie alla combinazione dei più moderni criteri di controllo antispam. Questo modulo software è disponibile nelle versioni G DATA Internet Security e G DATA Total Security.

- **Log: spam**: qui viene mostrato un riepilogo esauriente di tutti i messaggi classificati dal software G DATA come spam. Il pulsante **Aggiorna** consente di richiamare lo stato attuale dei dati del software, mentre il pulsante **Elimina** permette di cancellare tutte le voci finora evidenziate. I messaggi veri e propri contenuti nel programma di posta elettronica non vengono ovviamente cancellati. Il pulsante **Nella whitelist** consente di inserire nella Whitelist un'e-mail selezionata e di escludere così in generale l'indirizzo e-mail corrispondente da un'altra verifica antispam. Il pulsante **Nella blacklist** consente di inserire un'e-mail selezionata nella Blacklist e di eseguire quindi una verifica particolare antispam dell'indirizzo e-mail corrispondente.

- **Log: Nessuno spam**: qui viene mostrato un riepilogo esauriente di tutti i messaggi non classificati dal software G DATA come spam. Il pulsante **Aggiorna** consente di richiamare lo stato attuale dei dati del software, mentre il pulsante **Elimina** permette di cancellare tutte le voci finora evidenziate. I messaggi veri e propri contenuti nel programma di posta elettronica non vengono ovviamente cancellati. Il pulsante **Nella whitelist** consente di inserire nella Whitelist un'e-mail selezionata e di escludere così in generale l'indirizzo e-mail corrispondente da un'altra verifica antispam. Il pulsante **Nella blacklist** consente di inserire un'e-mail selezionata nella Blacklist e di eseguire quindi una verifica particolare antispam dell'indirizzo e-mail corrispondente.

- **Modifica Whitelist**: la whitelist permette di escludere esplicitamente determinati indirizzi mittente o domini dal sospetto di spam. Fare clic sul pulsante **Nuovo** e inserire nel campo **Mittente/Dominio mittente** l'indirizzo e-mail desiderato (ad es. newsletter@informationsseite.de) oppure il dominio (ad es. informationsseite.de) che deve essere eliminato dal sospetto spam in modo tale che il software G DATA non consideri le e-mail provenienti da questo mittente o da questo dominio mittente come spam. Con il pulsante Importa è inoltre possibile inserire nella whitelist alcune liste predefinite di indirizzi e-mail o domini. In questa lista gli indirizzi e i domini devono essere riportati in righe distinte, l'uno sotto l'altro. Come formato viene utilizzato un semplice file txt che può essere generato anche con Blocco Note di Windows. Con il pulsante **Esporta** le whitelist di questo tipo possono essere esportate come file di testo.

- **Modifica Blacklist**: mediante la blacklist è possibile definire esplicitamente determinati indirizzi di mittenti o domini come sospetto spam. Fare clic sul pulsante **Nuovo** e inserire nel campo **Mittente/Dominio mittente** l'indirizzo e-mail desiderato (ad es. newsletter@megaspam.de.vu) oppure il dominio (ad es. megaspam.de.vu) che deve essere incluso nel sospetto di spam in modo tale che il software G DATA consideri le e-mail provenienti da questo mittente o da questo dominio mittente generalmente come e-mail con elevata probabilità di spam. Con il pulsante **Importa** è inoltre possibile inserire nella blacklist alcune liste predefinite di indirizzi e-mail o domini. In questa lista gli indirizzi e i domini devono essere riportati in righe distinte, l'uno sotto l'altro. Come formato viene utilizzato un semplice file txt che può essere generato anche con Blocco Note di Windows. Mediante il pulsante **Esporta**, una blacklist di questo tipo può essere esportata come file di testo.

- **Disattiva protezione da spam**: in caso di necessità, qui è possibile disattivare la protezione da spam sul computer, ad esempio quando sul PC non è installato alcun programma di posta elettronica.

- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | AntiSpam | Filtro antispam**.

Ultimo aggiornamento

Qui viene indicata l'ultima volta in cui il computer ha ricevuto da Internet il database antivirus aggiornato. Se questa voce è evidenziata in rosso, è consigliabile eseguire al più presto un aggiornamento antivirus. Fare clic sulla voce e scegliere l'opzione **Aggiorna database antivirus**.

- **Aggiorna database antivirus**: normalmente gli aggiornamenti dei database antivirus vengono eseguiti in automatico. Per effettuare immediatamente un aggiornamento, fare clic su questo pulsante.

- **Disattiva aggiornamento automatico**: se non si desidera che il software G DATA esegua automaticamente l'aggiornamento dei database antivirus, deselezionare questa opzione. Tuttavia, disattivando questa opzione il rischio per la sicurezza è elevato e pertanto si dovrebbe attuare solo in casi eccezionali.

- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | AntiVirus | Aggiornamenti**.

Prossimo aggiornamento

Qui è indicato quando avrà luogo il prossimo aggiornamento. Per effettuare immediatamente un aggiornamento, fare clic su questa voce e scegliere l'opzione **Aggiorna database antivirus**.

- **Aggiorna database antivirus**: normalmente gli aggiornamenti dei database antivirus vengono eseguiti in automatico. Per effettuare immediatamente un aggiornamento, fare clic su questo pulsante.
- **Disattiva aggiornamento automatico**: se non si desidera che il software G DATA esegua automaticamente l'aggiornamento dei database antivirus, deselezionare questa opzione. Tuttavia, disattivando questa opzione il rischio per la sicurezza è elevato e pertanto si dovrebbe attuare solo in casi eccezionali.
- **Altre impostazioni**: per informazioni consultare il capitolo **Impostazioni | AntiVirus | Aggiornamenti**.

BankGuard

I trojan bancari sono una minaccia in costante crescita. I cybercriminali sviluppano ogni ora nuove tipologie di virus (come ZeuS, SpyEye) con lo scopo di sottrarvi del denaro. Le banche proteggono il traffico dati in Internet, tuttavia i dati vengono decodificati nel browser e qui vengono attaccati dai trojan bancari. La tecnologia all'avanguardia di G DATA BankGuard protegge le transazioni bancarie fin dall'inizio ed esattamente nel punto in cui avviene l'aggressione. Verificando in tempo reale l'integrità delle DLL di rete interessate, G DATA BankGuard garantisce che il vostro browser non verrà manipolato da un trojan bancario. È consigliabile lasciare sempre attivata la protezione di G DATA BankGuard.

Protezione da keylogger

In maniera indipendente dai database antivirus, la Protezione da keylogger monitora se le immissioni da tastiera vengono spiate nel sistema e impedisce agli aggressori di registrare le immissioni delle password. Questa funzione dovrebbe rimanere sempre attiva.

Exploit Protection

Un cosiddetto exploit sfrutta i punti deboli dei più comuni programmi utente e nel peggiore dei casi può assumere il controllo del computer attraverso tali falle. Gli exploit possono accedere perfino durante gli aggiornamenti periodici delle applicazioni, come un visualizzatore per PDF, un browser ecc. Exploit Protection protegge da questi tipi di accessi, anche in modo proattivo contro attacchi sconosciuti.

Licenza

Sotto la voce **Licenza** sul lato sinistro dell'interfaccia del programma è indicata la data di scadenza della licenza. In nessun altro programma gli aggiornamenti sono di tale importanza. Prima della scadenza, il programma segnala automaticamente che occorre prolungare la licenza, anche in modo semplice e comodo via Internet.

Dati di accesso

Cliccando sulla voce **Dati di accessi** si aprirà una finestra di dialogo dove sarà possibile visualizzare il proprio nome utente e numero di registrazione. Per informazioni consultare il capitolo **Impostazioni | AntiVirus | Aggiornamenti**. Per eventuali domande sulla licenza, nel **G DATA ServiceCenter** potremo fornirvi informazioni specifiche. Nel caso abbiate dimenticato la password, questa finestra consente di generarne una nuova in modo semplice e veloce.

Moduli software

In base alla versione software installata, sono disponibili i seguenti moduli software:

SecurityCenter: è il vostro centro di protezione personale. Qui sono fornite tutte le informazioni necessarie per la protezione del computer e per reagire in modo mirato alle minacce.

Protezione antivirus: in quest'area viene indicato quando è stato effettuato l'ultimo controllo antivirus completo del computer e se attualmente il Guardiano AntiVirus protegge attivamente il sistema da eventuali infezioni. Inoltre, qui è possibile verificare direttamente l'eventuale presenza di software dannosi sul computer o sui supporti dati, modificare i file in quarantena e creare un supporto di boot.

Firewall: un firewall protegge il computer dall'essere "spiato". Controlla infatti quali dati e quali programmi provenienti da Internet o dalla rete accedono al computer e quali dati vengono trasmessi dal computer. Non appena ha il sospetto che i dati sul computer vengano riprodotti o scaricati senza alcuna autorizzazione, il firewall emette un allarme e blocca lo scambio di dati non autorizzato. Questo modulo software è disponibile nelle versioni G DATA Internet Security e G DATA Total Security.

Backup: con la crescente digitalizzazione delle attività quotidiane, l'uso di servizi musicali online, fotocamere digitali e posta elettronica, la protezione dei dati personali diventa sempre più importante. Che si tratti di un errore hardware, una svista o un danno provocato da un virus o dall'attacco di un hacker, i vostri documenti privati devono essere salvati regolarmente. Il modulo Backup svolge questo compito e protegge i documenti e i dati importanti senza che l'utente debba più preoccuparsi. Questo modulo software è disponibile nella versione G DATA Total Security.

Gestione password: la Gestione password permette di gestire comodamente le password e può essere utilizzata come plugin nel browser. Questo modulo software è disponibile nella versione G DATA Total Security.

Tuner: il Tuner è uno strumento che velocizza e semplifica l'uso di Windows, dall'avvio automatico di Windows Update alla deframmentazione periodica ad intervalli predefiniti, fino alla regolare rimozione delle voci di registro superflue e dei file temporanei. Questo modulo software è disponibile nella versione G DATA Total Security.

Protezione minori: la funzione Protezione minori consente di stabilire le regole per la navigazione e l'utilizzo del computer per i propri bambini. Questo modulo software è disponibile nelle versioni G DATA Internet Security e G DATA Total Security.

Crittografia: il modulo di crittografia è come la cassaforte di una banca e serve per proteggere i dati riservati. Una cassaforte può, ad esempio, essere usata come partizione supplementare del disco rigido ed è semplice da gestire. Questo modulo software è disponibile nella versione G DATA Total Security.

Autostart Manager: Autostart Manager permette di gestire i programmi che vengono avviati automaticamente all'avvio di Windows. Normalmente questi programmi si avviano direttamente all'avvio del sistema. Quando i programmi sono gestiti da Autostart Manager, è possibile impostarne anche l'avvio ritardato o in base al sovraccarico del sistema o del disco fisso. Ciò permette un avvio più rapido del sistema e quindi migliori prestazioni del computer.

Controllo dispositivi: questa funzione consente di limitare l'uso di dispositivi, come supporti dati rimovibili, unità CD/DVD e unità a dischetti, a determinati utenti del computer per impedire ad es. l'esportazione o l'importazione non desiderata di dati o l'installazione di programmi. Ora anche con USB KeyboardGuard. Per maggiori informazioni, consultare il capitolo Controllo dispositivi.

Protezione antivirus

Questo modulo permette di verificare in modo mirato l'eventuale presenza di infezioni sul computer o sul supporto dati selezionato. Questa verifica è consigliata soprattutto quando si ricevono CD o chiavette USB da amici, parenti o colleghi. Anche quando si installa un nuovo software o si esegue un download da Internet si consiglia di eseguire una scansione antivirus.

> **Attenzione**: la verifica del computer o del supporto selezionato serve come protezione aggiuntiva. Generalmente la protezione ottimale da software dannosi è già garantita dalla Scansione in modo inattivo e dal Guardiano AntiVirus di G DATA, sempre attivo in background. Una scansione antivirus è in grado di trovare i virus copiati sul computer prima di installare il software G DATA o ricevuti mentre il guardiano AntiVirus era disattivato.

Scansione antivirus

Permette di selezionare le aree del computer o i supporti dati da verificare in modo mirato:

Verifica computer (tutti i dischi fissi locali): per controllare il computer in maniera indipendente dalla scansione automatica, ad esempio quando si sospetta la presenza di un virus, fare clic su questa opzione. Si avvierà la scansione antivirus che controllerà la presenza di virus nel PC. Per ulteriori informazioni, consultare anche il capitolo: **Esecuzione della scansione antivirus**.

Analisi programmate: Questa funzione attiva il controllo automatico dei virus. Per ulteriori informazioni, consultare anche il capitolo: **Verifica automatica virus**.

Verifica memoria e avvio automatico: permette di controllare i file di programma di tutti i processi in corso e le rispettive DLL (librerie di programma). In questo modo è possibile rimuovere i programmi dannosi direttamente dalla memoria e dall'area di avvio automatico. Anche i virus attivi possono essere rimossi direttamente, senza eseguire la scansione dell'intero disco fisso. Questa funzione non sostituisce i controlli periodici antivirus sui dati salvati, ma ne è soltanto un'integrazione.

Verifica directory/file: permette di controllare l'eventuale presenza di virus nelle unità, nelle directory o nei file. Facendo doppio clic su questa opzione si apre una finestra di selezione di directory e file, nella quale è possibile controllare singoli file e intere directory. Nella struttura delle directory, a sinistra, è possibile con un clic del mouse sul simbolo "Plus" aprire e selezionare le directory e visualizzarne il contenuto nella vista dei file. Ogni directory o file provvisto di un segno di spunta viene controllato dal programma.

Se in una directory non vengono controllati tutti i file, tale directory presenta un segno di spunta di colore grigio.

Verifica supporti removibili: con questa funzione è possibile verificare CD-ROM o DVD-ROM, schede di memoria e chiavette USB per rilevare eventuali virus. Selezionando questa opzione, vengono controllati tutti i supporti rimovibili collegati al computer (quindi anche CD inseriti, schede di memoria inserite o dischi fissi collegati tramite la porta USB o chiavette USB). Ricordare che naturalmente il software non può rimuovere i virus dai supporti che non consentono l'accesso in scrittura (ad es. i CD-ROM masterizzati). In questi casi, il virus rilevato viene registrato nel log.

Verifica la presenza di rootkit: i rootkit cercano di sfuggire ai comuni metodi di riconoscimento dei virus. Mediante questa funzione è possibile cercare in modo mirato i rootkit, senza controllare tutto il disco fisso e i dati memorizzati.

File in quarantena

Durante la scansione virus è possibile procedere in modi diversi con i virus rilevati, Un'opzione è costituita dallo spostamento del file infetto in quarantena. La quarantena è un'area protetta all'interno del software nella quale i file infetti vengono salvati in un formato criptato, impedendo in questo modo al virus di diffondersi in altri file.

Mostra Quarantena: facendo clic su questo pulsante, verrà aperta l'area della Quarantena.

I file in quarantena restano conservati nello stato in cui sono stati rilevati dal software G DATA e l'utente può decidere come procedere in seguito.

- **Aggiorna**: se la finestra di dialogo della quarantena è rimasta aperta a lungo e nel frattempo è stato rilevato e spostato in quarantena un virus (ad esempio automaticamente tramite il Guardiano AntiVirus), questo pulsante permette di aggiornare la finestra di dialogo.
- **Permetti in futuro**: nel caso in cui il monitoraggio del comportamento avesse messo erroneamente un file in quarantena, è possibile aggiungerlo alla whitelist, così che in futuro il monitoraggio del comportamento non lo riconosca più come pericoloso.

- **Disinfetta**: in molti casi è possibile recuperare i file infetti. Il software rimuove i componenti del virus presenti nel file infetto e ricostruisce in questo modo il file originale non infetto. Se l'azione avviene correttamente, il file viene ripristinato automaticamente nella posizione in cui era stato archiviato prima dell'analisi antivirus ed è accessibile senza limitazioni.

- **Ripristina**: alcune volte potrebbe essere necessario trasferire un file infetto, impossibile da disinfettare, dalla quarantena alla sua posizione originaria. Ciò potrebbe avvenire, ad esempio, per motivi di salvataggio dati. Usare questa funzione solo in casi eccezionali e con severe misure di sicurezza (ad es. scollegare il computer dalla rete/Internet, effettuare precedentemente un backup dei dati non infetti ecc.).

- **Elimina**: quando il file infetto non è più necessario, è possibile cancellarlo direttamente dalla quarantena.

Supporto di boot

Il supporto di boot rappresenta un utile strumento per ripulire dai virus i computer già infetti. L'utilizzo di un supporto di boot è particolarmente consigliato per quei computer che non avevano alcun tipo di protezione antivirus prima dell'installazione del software G DATA. Per creare un **supporto di boot**, consultare il capitolo **BootScan**.

Per creare un supporto di boot, fare clic sul pulsante **Crea supporto di boot** e seguire le istruzioni fornite dalla procedura guidata. Per avere un supporto di boot aggiornato, è possibile scaricare i database antivirus più recenti. Inoltre, qui è possibile scegliere se masterizzare come supporto di boot un CD/DVD o utilizzare una chiavetta USB.

Se si utilizza la versione del programma G DATA Total Security, un supporto di boot permette di ripristinare il backup di un'unità anche sul volume sul quale si trova attualmente il sistema. È possibile inoltre ripristinare il backup di un'unità o di un file anche su altre destinazioni. Inserire il supporto di boot e selezionare la funzione **Avvia ripristino**.

Firewall

Un firewall protegge il computer dall'essere *spiato*. Controlla infatti quali dati e quali programmi provenienti da Internet o dalla rete accedono al computer e quali dati vengono trasmessi dal computer.

In modalità Firewall sono disponibili tre aree:

- **Stato**: nell' area Stato del firewall sono riportate le informazioni di base sullo stato attuale del proprio sistema e del firewall.
- **Reti**: nell'area Reti sono elencate le unità (ad es. LAN, WAN ecc.) alle quali è collegato il computer.
- **Serie di regole**: in quest'area è possibile creare regole speciali per diverse reti, ottimizzando così il comportamento del firewall.

Non appena ha il sospetto che i dati sul computer vengano riprodotti o scaricati senza alcuna autorizzazione, il firewall emette un allarme e blocca lo scambio di dati non autorizzato.

 **Impostazioni:** questo pulsante in alto a destra permette di accedere ad altre finestre di impostazione del firewall.

Stato

Nell' area Stato del firewall sono riportate le informazioni di base sullo stato attuale del proprio sistema e del firewall. Queste informazioni sono riportate sotto forma di testo numerico o indicazione numerica a destra dalla relativa voce. Lo stato dei componenti è visualizzato anche graficamente: Facendo doppio clic su ciascuna voce è possibile eseguire le azioni direttamente qui o passare alla rispettiva area del programma.

Non appena vengono ottimizzate le impostazioni di un componente che presenta l'icona di avvertenza, l'icona nell'area Stato cambia nuovamente nel segno di spunta verde.

- **Protezione**: mentre si usa il computer per il lavoro quotidiano, il firewall impara progressivamente a conoscere i programmi utilizzati per l'accesso a Internet, i programmi che non vengono utilizzati mai e i programmi che rappresentano un rischio per la sicurezza. In base al livello di conoscenza della tecnologia del firewall, è possibile configurare il firewall in modo da ottenere un'ottima protezione di base, senza frequenti richieste di intervento dell'utente, oppure una protezione professionale, orientata esattamente al tipo di utilizzo del computer, ma che richiede anche conoscenze specifiche in materia. Per impostare il Livello di protezione, selezionare: **Impostazioni | Firewall | Pilota automatico**.
- **Modo**: qui sono descritte le impostazioni di base per l'esecuzione del proprio firewall. È possibile dunque scegliere tra Creazione manuale delle regole e Automatico (pilota automatico).

  Pilota automatico: Il firewall funziona in modo autonomo e protegge automaticamente il PC da qualsiasi pericolo. Questa impostazione garantisce una protezione completa ed è consigliabile per la maggior parte degli utilizzi. Si consiglia di tenere sempre attivato il Pilota automatico.

  Altre impostazioni: se si desidera configurare individualmente il firewall o evitare che determinate applicazioni funzionino con la modalità Pilota automatico, è possibile adattare la protezione firewall alle proprie esigenze utilizzando l'opzione di creazione manuale delle regole. Per maggiori informazioni, consultare il capitolo: **Impostazioni | Firewall | Pilota automatico**.
- **Reti**: qui è possibile visualizzare le reti in cui si trova il computer. Per maggiori informazioni, consultare il capitolo: **Firewall | Reti**.
- **Attacchi respinti**: non appena il firewall rileva un attacco al computer, questo viene bloccato e registrato in un log. Selezionando le voci di menu è possibile ottenere maggiori informazioni.
- **Radar applicazioni**: nella finestra di dialogo sono mostrati i programmi momentaneamente bloccati dal firewall. Nel caso si intenda permettere di utilizzare la rete ad una delle applicazioni bloccate, selezionarla e fare clic sul pulsante **Autorizza**.

Reti

Nell'area Reti sono elencate le unità (ad es. LAN, WAN ecc.) alle quali è collegato il computer. In questa finestra è anche indicata la Serie di regole (consultare il capitolo **Serie di regole**) applicata per la protezione della rete. Se si rimuove il segno di spunta dall'unità di rete, la rete verrà esclusa dalla protezione del firewall. È opportuno, tuttavia, rimuovere la protezione solo in casi eccezionali e per validi motivi. Quando si seleziona con il mouse un'unità di rete e quindi si fa clic sul pulsante **Modifica**, è possibile visualizzare e modificare le impostazioni del firewall specifiche per questa rete.

Modifica rete

In questa finestra riepilogativa sono riportate le seguenti informazioni e opzioni di impostazione per la rete selezionata:

- **Informazioni sulla rete**: in questa sezione sono riportate le informazioni sull'unità di rete (se presenti), così come le indicazioni su indirizzo IP, subnet mask, gateway standard, server DNS e server WINS.
- **Firewall attivo, su questa rete**: qui è possibile disattivare il firewall dell'unità di rete, ma si consiglia di farlo solo in casi eccezionali e per validi motivi.
- **Utilizzo condiviso del collegamento Internet**: in presenza di connessioni dirette con Internet, questa opzione permette di definire se tutti i computer collegati a una rete possono accedere ad Internet tramite un computer collegato. In genere la condivisione della connessione a Internet (ICS) può essere attivata per una rete domestica.
- **Permetti configurazione automatica (DHCP)**: per la connessione del computer all'unità di rete viene assegnato un indirizzo IP dinamico (tramite il protocollo DHCP = Dynamic Host Configuration Protocol). Se si è collegati alla rete tramite questa configurazione standard, questa opzione deve rimanere selezionata.
- **Serie di regole**: questa opzione permette di scegliere rapidamente tra diverse serie di regole predefinite e di stabilire in questo modo i criteri di monitoraggio del firewall se si tratta, ad esempio, di una rete affidabile, non affidabile o da bloccare. Il pulsante **Modifica serie di regole** permette di configurare singole serie di regole. Per ulteriori informazioni, consultare il capitolo **Creare serie di regole**.

Serie di regole

In questa area è possibile creare regole speciali per diverse reti. Tali regole vengono raggruppate in una serie di regole. Sono preimpostate le serie di regole per la connessione diretta a Internet, le reti non affidabili, le reti affidabili e le reti da bloccare. Nel riepilogo viene visualizzata la relativa serie di regole con i nomi. I pulsanti **Nuova**, **Elimina** e **Modifica** permettono di modificare le serie di regole esistenti e di aggiungerne altre.

Non è possibile eliminare le tre serie di regole preimpostate per la **connessione diretta a Internet**, **reti affidabili**, **reti non affidabili** e **reti da bloccare**. Le serie di regole aggiuntive create dall'utente possono invece essere eliminate in qualsiasi momento.

Creare serie di regole

A ciascuna rete è possibile assegnare una serie di regole personalizzata, ovvero una raccolta di regole specifiche per il contesto. Questa possibilità consente di proteggere in modo differenziato le reti soggette a livelli di rischio diversi, utilizzando il firewall. Ad esempio, una rete privata richiede una protezione inferiore (e quindi una gestione meno complessa) di una rete con connessione remota che è a contatto diretto con Internet.

Utilizzando il pulsante **Nuova**, è possibile creare alcune serie di regole specifiche per la rete. Nel riquadro Serie di regole, fare clic sul pulsante **Nuova** e nella finestra di dialogo che si apre definire quanto segue:

- **Nome serie di regole**: inserire un nome identificativo per la serie di regole.
- **Creare una serie di regole vuota**: consente di creare una serie di regole completamente vuota che potrà poi essere completata con regole personalizzate.
- **Creare una serie di regole che contiene alcune regole sensate**: selezionando questa opzione è possibile decidere se la nuova serie di regole che si crea deve contenere delle regole di base predefinite per le reti non affidabili, affidabili o da bloccare. In base a questa predisposizione sarà possibile poi apportare delle modifiche personalizzate.

Il firewall presenta alcune serie di regole predefinite per i seguenti tipi di rete:

- **Connessione diretta a Internet**: Qui si trovano le regole concernenti l'accesso diretto a internet.
- **Reti non affidabili**: Qui si trovano le regole concernenti reti aperte, come ad esempio reti di connessione remota che hanno accesso a Internet.
- **Reti affidabili**: Reti affidabili sono di solito le reti casalinghe o aziendali.
- **Alle reti da bloccare**: Se si desidera bloccare temporaneamente o in modo permanente il contatto tra il computer e una determinata rete, utilizzare questa impostazione. Ciò è utile, ad esempio, durante il collegamento con reti esterne delle quali non si conoscono gli standard di sicurezza (ad esempio nei LAN-Party, nelle reti di aziende sconosciute, nelle postazioni di lavoro pubbliche per i notebook ecc.)

La nuova serie di regole viene ora visualizzata nel riquadro Serie di regole sotto al rispettivo nome (ad esempio *Nuova serie di regole)* nell'elenco. Facendo ora clic su **Modifica**, in base alle impostazioni effettuate in **Impostazioni | Varie** (si veda il capitolo con questo nome), si apre Assistente regole oppure lamodalità di elaborazione avanzata in cui è possibile modificare le singole regole di questa serie. Se nella serie di regole si assegnano delle regole nuove, consultare il capitolo **Uso dell'Assistente regole** oppure **Uso della modalità di elaborazione avanzata**.

Le nuove regole possono essere create, oltre che inserendole direttamente, anche mediante la finestra informativa dell'allarme del firewall. Questo processo di apprendimento del firewall è descritto al capitolo **Allarme del firewall**.

Uso dell'Assistente regole

L'Assistente regole permette di definire alcune regole aggiuntive per una determinata serie di regole oppure di modificare le regole esistenti. Per gli utenti che non sono molto pratici della tecnologia firewall, è preferibile utilizzare l'Assistente regole piuttosto che la modalità di elaborazione avanzata.

L'Assistente regole permette di modificare una o più regole nella serie di regole selezionata. Viene sempre creata una regola all'interno di una serie che ne contiene diverse.

Indipendentemente da quale serie di regole sia stata definita per la relativa rete, un'applicazione può essere bloccata in una serie di regole (ad es. per reti non affidabili), mentre può avere pieno accesso alla rete in un'altra serie di regole (ad es. per reti affidabili). In tale modo è possibile, ad esempio, applicare diverse regole a un browser di modo che possa accedere alle pagine che sono disponibili nella propria rete domestica ma non abbia accesso ai contenuti provenienti dalla rete remota.

Nell'Assistente regole sono disponibili le seguenti regole di base:

- **Autorizza o blocca applicazioni**: In tale modo è possibile selezionare in maniera mirata un'applicazione (un programma) presente nel disco fisso e consentirle o negarle esplicitamente l'accesso alla rete definita mediante la serie di regole. Nell'Assistente, selezionare il programma prescelto (**percorso del programma**) e in **Direzione** specificare se il programma debba essere bloccato per le connessioni in entrata, in uscita o per entrambe. In questo modo è possibile, ad esempio, impedire al software del proprio lettore MP3 di trasmettere dati sulle proprie abitudini di ascolto (connessioni in uscita) o impedire che gli aggiornamenti vengano eseguiti automaticamente (connessioni in entrata).

- **Autorizza o blocca servizi di rete**: come **Porta** vengono definite determinate aree di indirizzo speciali che inoltrano automaticamente mediante una rete i dati trasmessi a un protocollo e quindi a un determinato software. Così si svolgono, ad esempio, la trasmissione di siti Web regolari attraverso la porta 80, la spedizione di e-mail attraverso la porta 25, la ricezione di e-mail attraverso la porta 110 ecc. Senza Firewall tutte le porte del computer sono aperte anche se la maggior parte di esse è superflua per i normali utenti. Bloccando una o più porte è possibile chiudere velocemente delle falle che altrimenti potrebbero essere sfruttate dagli hacker per attaccare il computer. Nell'Assistente è possibile decidere di bloccare le porte per tutte le applicazioni o solamente per una determinata applicazione (ad es. il software di riproduzione dei file MP3).

- **Condividi file/stampante**: se si autorizza l'accesso, è possibile utilizzare in rete le cartelle e le stampanti condivise. Inoltre, altri computer e utenti collegati in rete possono accedere alle condivisioni (se tale opzione è configurata).

- **Autorizza o blocca servizi di dominio**: un dominio è un tipo di directory di classificazione per i computer di una rete e permette una gestione centralizzata dei computer che fanno parte della rete. Le condivisioni per i servizi di dominio dovrebbero essere di norma negate alle reti non affidabili.

- **Utilizzo condiviso del collegamento Internet**: in presenza di connessioni dirette con Internet, questa opzione permette di definire se tutti i computer collegati a una rete possono accedere ad Internet tramite un computer collegato. In genere la condivisione della connessione a Internet può essere attivata per una rete domestica.

- **Autorizza o blocca servizi VPN**: VPN è l'abbreviazione di Virtual Private Network (rete privata virtuale) e definisce la possibilità per i computer di associarsi in modo esclusivo tramite una connessione diretta tra di essi. Per utilizzare i servizi VPN, questi devono essere autorizzati dal firewall.

- **Editor avanzato regole (modalità esperto)**: qui è possibile passare dall'Assistente regole alla modalità di elaborazione avanzata. Per informazioni sulla modalità di elaborazione avanzata, consultare il capitolo **Uso della modalità di elaborazione avanzata**.

Uso della modalità di elaborazione avanzata

Ammesso che si possiedano determinate conoscenze nel campo della sicurezza della rete, la modalità di elaborazione avanzata consente di definire delle regole particolari per una determinata rete. È possibile non solo creare tutte le regole che possono essere generate mediante l'Assistente regole, ma anche effettuare ulteriori impostazioni.

Sono disponibili le seguenti impostazioni:

- **Nome**: qui è possibile eventualmente modificare il nome dell'attuale serie di regole. Il sistema utilizza successivamente questo nome per visualizzare la serie di regole nell'elenco contenuto nell'area Serie di regolee potrà essere combinata con le reti qui identificate dal Firewall.
- **Modo Stealth**: con il modo Stealth (ing.: nascosto, segreto) le query al computer che servono a verificare l'accessibilità delle relative porte non ottengono nessuna risposta. Ciò rende più difficile per gli hacker ottenere informazioni tramite il sistema.
- **Azione, nel caso non vi siano regole corrispondenti**: qui è possibile determinare in linea generale se consentire, rifiutare o concedere su richiesta l'accesso alla rete. Se fosse necessario definire regole speciali per i singoli programmi mediante la funzione di apprendimento del firewall, il sistema le terrà in considerazione.
- **Modo adattivo**: Il modo adattivo supporta le applicazioni che utilizzano la cosiddetta tecnologia con canale di ritorno (ad es. FTP e molti giochi online). Le applicazioni di questo tipo si connettono a un computer remoto con cui negoziano un canale di ritorno che il computer impiega per *ricollegarsi* all'applicazione stessa. Se il modo adattivo è attivo, il firewall riconosce questo canale di ritorno e lo accetta senza presentare ulteriori richieste.

Regole

Nell'elenco delle regole sono presenti tutte le regole che sono state definite per questa serie di regole. Qui è possibile, ad esempio, autorizzare numerosi accessi a determinati programmi, anche quando la rete è stata definita come non affidabile. Le regole incluse nell'elenco possono essere generate in diversi modi:

- mediante il pulsante **Assistente regole**
- direttamente nella **modalità di elaborazione avanzata** tramite il pulsante **Nuovo**
- tramite la finestra informativa che viene aperta in caso di **Allarme del firewall**.

Ogni serie di regole contiene naturalmente un proprio elenco di regole.

Poiché le regole per il firewall sono parzialmente nidificate in modo gerarchico, in alcuni casi è importante rispettare l'ordine gerarchico delle regole. Può accadere, ad esempio, che l'autorizzazione per una porta venga bloccata poiché è negato l'accesso a un determinato protocollo. È possibile modificare il grado di una regola nella sequenza, selezionandolo con il mouse e spostandolo verso l'alto o verso il basso tramite i tasti freccia in **Grado**.

Quando si crea una nuova regola nella modalità di elaborazione avanzata o quando si modifica un regola esistente tramite la finestra di dialogo **Modifica**, viene aperta la finestra di dialogo **Modifica regola**, in cui sono disponibili le seguenti impostazioni:

- **Nome**: per le regole predefinite e per quelle generate automaticamente viene mostrato qui il nome del programma a cui si riferisce la rispettiva regola.
- **Regola attiva**: è possibile disattivare una regola rimuovendo il segno di spunta, senza eliminarla.
- **Commento**: consente di specificare come è stata creata la regola. Per le regole predefinite per la serie di regole compare il commento Regola predefinita, per le regole che derivano dalla finestra di dialogo **Allarme del firewall** compare il commento Creata su richiesta, infine per le regole generate utilizzando la modalità di elaborazione avanzata è possibile aggiungere un commento personalizzato.
- **Direzione collegamento**: con la direzione si definisce se la regola riguarda le connessioni in entrata, in uscita o in entrambe le direzioni.
- **Accesso**: consente di impostare se per ciascun programma contenuto in questa serie di regole debba essere autorizzato o negato l'accesso.
- **Protocollo**: consente di scegliere per quali protocolli di collegamento autorizzare o negare l'accesso. È possibile bloccare o consentire i protocolli a livello generale oppure associare l'utilizzo del protocollo all'uso di una o più applicazioni specifiche (**Assegna applicazioni**). Allo stesso modo è possibile specificare con precisione le porte preferite o non desiderate premendo il tasto **Assegna servizio Internet**.

- **Finestra temporale**: è possibile anche impostare l'accesso alle risorse di rete con delle limitazioni temporali, ad esempio autorizzando l'accesso solo durante gli orari di lavoro.

- **Range indirizzo IP**: è particolarmente utile regolare l'uso delle reti con indirizzi IP predefiniti, limitando il range dell'indirizzo IP. Un range indirizzo IP ben definito riduce notevolmente il rischio di attacchi hacker.

Backup

Con la crescente digitalizzazione delle attività quotidiane, l'uso di servizi musicali online, fotocamere digitali e posta elettronica, la protezione dei dati personali diventa sempre più importante. Che si tratti di un errore hardware, una svista o un danno provocato da un virus o dall'attacco di un hacker, i vostri documenti privati devono essere salvati regolarmente. Il software G DATA svolge questo compito e protegge i documenti e i dati importanti senza che l'utente debba più preoccuparsi.

Salvataggio e ripristino

Non appena si crea un nuovo processo di backup tramite la funzione **Nuovo processo**, le seguenti icone permettono di gestire e modificare tale processo:

Ripristino: consente di ripristinare nel sistema i dati archiviati nel backup. Lo svolgimento dell'attività di ripristino è spiegata nel capitolo **Backup (Ripristina)**.

Backup: consente di avviare immediatamente il processo di backup per un backup specifico, indipendentemente dalla pianificazione impostata per questo backup.

Impostazioni: consente di modificare le impostazioni di un processo di backup specificate al momento della creazione di tale processo di backup in **Nuovo processo di backup**.

Log: fornisce una panoramica di tutte le attività che si svolgono durante questo processo di backup. Sono indicati i processi di backup eseguiti manualmente o pianificati, informazioni su eventuali ripristini e messaggi di errore, ad es. se una directory di destinazione non dispone di spazio sufficiente per completare il backup.

Nuovo processo di backup

Per assegnare un nuovo processo di backup, fare clic sul pulsante **Nuovo processo**.

Selezione file / Disco fisso / Partizione

Ora l'assistente del backup vi chiederà che tipo di backup eseguire.

Backup dei file: si tratta del salvataggio in un file di archivio di cartelle e file specifici scelti dall'utente.

Nella struttura delle directory, selezionare i file e le cartelle da archiviare. Per un backup dei file, in genere si consiglia di archiviare i dati personali e non i file di programma installati. Nella struttura delle directory, a sinistra, è possibile con un clic del mouse sul simbolo + aprire e selezionare le directory e visualizzarne il contenuto nella vista dei file. Ogni directory o file provvisto di un segno di spunta viene controllato dal programma e utilizzato per il backup. Se in una directory non vengono controllati tutti i file e le cartelle utilizzati per il backup, tale directory presenta un segno di spunta di colore grigio.

Backup dell'unità: si tratta di un backup completo di dischi fissi o partizioni in un file di archivio.

Selezione destinazione

Consente di determinare la destinazione, ovvero la posizione in cui il software G DATA dovrà creare la copia di backup dei file e delle cartelle o dei dischi fissi e delle partizioni. Questa può essere un'unità CD-ROM o DVD-ROM, un altro disco fisso, una chiavetta USB, altri supporti rimovibili oppure una directory in rete.

Nome dell'archivio: assegnare qui un nome significativo al file di archivio da creare, ad es. *Backup settimanale dati personali*, *Backup MP3* e così via.

Nuova cartella: se si desidera creare una nuova cartella per il backup, selezionare nella struttura delle directory la posizione desiderata e fare clic sul pulsante **Nuova cartella**.

> **Nota**: fare attenzione a non eseguire il backup sullo stesso disco fisso sul quale si trovano anche i dati originali. Infatti, se dovesse subentrare un problema sul disco rigido, i dati originali e di backup andrebbero persi. Si consiglia di conservare un backup dei dati in un luogo separato dai file originali, ad esempio in un'altra stanza su un disco fisso USB, oppure di masterizzarli su un CD-ROM/DVD-ROM.

Crea archivio nel cloud: per salvare il backup nel cloud, è possibile utilizzare i servizi cloud più comuni, come Dropbox, Microsoft OneDrive*, TeamDrive** o Google Drive. Connettersi semplicemente con i dati di accesso del servizio cloud e l'archivio di backup verrà subito collegato al server cloud.

> **Nota**: Quando si copia un backup nel cloud, verificare che i dati del backup siano crittografati. Nell'area **Opzioni** sotto **Nuovo processo di backup** è possibile attivare e disattivare la crittografia dei dati.
>
> **(*) Nota su OneDrive**: è possibile usare OneDrive se questo servizio è stato integrato come disco virtuale in Esplora risorse. In questo caso l'archivio verrà creato come di consueto tramite la directory dei file e non tramite la funzione **Crea archivio nel cloud**.
>
> **(**) Nota sul TeamDrive**: puoi scegliere TeamDrive dopo aver installato sul tuo PC il software TeamDrive e aver configurato e scelto un TeamDrive Space.

Pianificazione

Consente di definire la frequenza con cui salvare in un backup i dati selezionati e di specificare il tipo di backup da eseguire. È possibile impostare un backup completo, in cui vengano archiviati tutti i dati selezionati, ma anche dei backup parziali, in cui vengano archiviate solo le modifiche subentrate dall'ultimo backup eseguito.

Se si seleziona **Manualmente**, il backup non verrà eseguito automaticamente, bensì dovrà essere avviato dall'utente tramite l'interfaccia del programma. L'opzione **Giornalmente** consente, mediante l'indicazione dei giorni della settimana, di stabilire ad es. che il computer esegua la regolazione solo nei giorni feriali oppure solo ogni due giorni oppure solo nei fine settimana quando non viene utilizzato. Si possono inoltre impostare backup con frequenza settimanale e mensile.

Non eseguire con funzionamento a batteria: Per evitare che in un notebook un processo di backup si interrompa all'improvviso quando si scarica la batteria, è possibile stabilire che i backup vengano eseguiti solo quando il notebook è collegato alla rete elettrica.

Esegui backup completo

Alla voce **Esegui backup completo** specificare la frequenza, i giorni e l'ora in cui dovrà essere eseguito il backup. In questo modo, nella fascia oraria indicata, verrà creato automaticamente un backup di tutti i dati selezionati in **Selezione file / Disco fisso / Partizione**.

> **Attenzione**: il backup automatico non funziona con CD-ROM o DVD-ROM poiché può richiedere l'intervento dell'utente in caso di sostituzione del CD.

Nella sezione **Elimina tutti gli archivi precedenti** è possibile stabilire come il software G DATA dovrà comportarsi con i backup già esistenti. Il software G DATA archivia i dati dell'utente in un unico file con l'estensione ARC. I backup esistenti che non vengono sovrascritti aumentano ulteriormente la sicurezza dei dati poiché, anche nel caso in cui l'archivio attuale dovesse essere danneggiato, sarebbe disponibile un archivio più vecchio, pertanto i file non andrebbero tutti perduti. In linea generale, gli archivi necessitano tuttavia di molto spazio sui supporti dati, pertanto occorre assicurarsi che non si accumulino troppi file di archivio. Si consiglia di indicare nell'area **Conservare backup completi** un numero massimo di backup da salvare sul proprio supporto di salvataggio. L'archivio più vecchio verrà sostituito con l'archivio attuale.

Quando si seleziona l'opzione **Crea backup parziali**, dopo un primo backup completo il programma eseguirà i backup successivi solo in forma parziale, che sono processi di archiviazione molto più veloci, ma che richiedono più tempo quando occorre ripristinare da essi un backup completo. Un altro svantaggio del backup parziale consiste nel fatto che richiede un maggiore spazio di memoria poiché i dati non più necessari nel backup completo non vengono cancellati direttamente. Dopo il successivo backup completo, i dati del backup completo e di quello parziale vengono tuttavia riuniti e la quantità dei dati torna identica a quella che risulterebbe da un backup completo.

Esegui backup parziali

I backup parziali consentono di effettuare il salvataggio dei dati più rapidamente. Anziché utilizzare tutti i dati per un backup, il backup parziale si basa su un backup completo già esistente e salva solo i dati che sono stati modificati dall'ultimo backup completo. In questo modo si avrà comunque un salvataggio completo dei propri dati, ma il processo di backup risulterà chiaramente più veloce.

Differenziale / Incrementale: nel backup differenziale vengono salvati tutti i dati che sono stati aggiunti come nuovi o modificati dopo l'ultimo backup completo. La procedura, quindi, si basa sempre sull'ultimo backup completo eseguito. Rispetto a un backup completo, si risparmia così tempo e spazio in memoria. Il backup incrementale va oltre e salva in due backup parziali i file che risultano modificati tra un backup parziale e un altro. Lo svantaggio di questo tipo di backup è che, in caso di ripristino dei dati, sono necessari più archivi.

Opzioni

L'area Opzioni consente di modificare le opzioni generali impostate per il backup. Di regola non è necessario apportare alcuna modifica in quest'area, poiché le opzioni standard di G DATA si adattano alla maggior parte degli utilizzi.

Opzioni archivio generali

Nelle Opzioni archivio generali sono disponibili le seguenti impostazioni:

- **Limita dimensioni file dell'archivio**: se gli archivi vengono memorizzati su CD, DVD-ROM o altri supporti scrivibili, è importante che il software G DATA limiti le dimensioni dei file di archivio. È possibile scegliere tra dimensioni predefinite che permettono la memorizzazione successiva dei dati di archivio su CD, DVD oppure dischi Blu-ray. L'archivio, una volta raggiunta la dimensione massima qui indicata, viene suddiviso e le informazioni di backup vengono distribuite in due o più file di archivio.

- **Crea CD/DVD multisessione**: selezionando questa opzione vengono creati CD o DVD di backup riscrivibili più volte. Tuttavia, il contenuto archiviato in precedenza non viene cancellato, bensì viene solo aggiunto il nuovo contenuto.

- **Elimina archivio temporaneo**: questa opzione dovrebbe rimanere generalmente attiva. Gli archivi temporanei, dopo un preciso numero di processi di backup, occupano molto spazio sul disco fisso e dopo il loro impiego temporaneo non sono più necessari.

- **Copia file del programma di ripristino**: se viene attivata questa funzione, oltre ai dati di archivio, nella posizione di salvataggio dei dati viene caricato un programma con il quale i dati vengono ripristinati anche senza avere installato il software G DATA. Avviare dal CD/DVD-ROM il programma *AVKBackup* oppure *AVKBackup.exe*.

  Il programma di ripristino viene solo copiato su CD/DVD-ROM ma non sulle copie di sicurezza eseguite su supporti rimovibili (chiavetta USB, disco fisso rimovibile).

  Se il software G DATA è stato installato sul computer in cui dovrebbe aver luogo il ripristino, non eseguirlo con l'apposito programma su CD/DVD-ROM, ma tramite la funzione **Importa archivio**.

- **Scansione antivirus dei file prima dell'archiviazione**: se è stato installato il modulo AntiVirus, è possibile verificare la presenza di virus nei file prima che vengano memorizzati nell'archivio di backup.

- **Verifica archivio dopo la creazione**: questa funzione è utile per verificare dopo la creazione dell'archivio l'eventuale presenza di inconsistenze ed errori.

- **Cifra archivio**: per proteggere i file archiviati da un accesso non autorizzato, è possibile assegnare una password. Il ripristino dei dati può in tal caso avvenire solo con la password. È necessario ricordarla o annotarla in un posto sicuro. Senza password i dati dell'archivio non possono essere ripristinati.

- **Test di integrità con backup differenziale**: questa funzione è utile per verificare dopo la creazione di un backup parziale l'eventuale presenza di incoerenze ed errori.

- **Test di integrità al ripristino del disco rigido**: questa funzione serve per controllare se i dati sono stati recuperati correttamente dopo un ripristino. La **Directory per file temporanei** è una posizione di archiviazione dei dati che vengono scritti dal software G DATA solo temporaneamente sul disco fisso. Se nella partizione standard lo spazio non dovesse essere sufficiente, qui è possibile cambiare partizione e posizione di memorizzazione temporanea di questi file.

- **Usa copia shadow del volume di Windows**: quando questa opzione è attivata, non è possibile creare alcuna immagine della partizione del sistema mentre il sistema è in funzione.

Dati utente

Per poter eseguire dei backup pianificati, è necessario selezionare l'opzione **Esegui processo come** e specificare i dati di accesso per il proprio account di Windows. Questi dati sono necessari per poter eseguire il backup programmato anche se non si è registrati come utente.

Compressione

Nell'area Compressione si può indicare il livello di compressione degli archivi.

- **Buona compressione**: i dati vengono fortemente compressi per il backup. In questo modo si risparmia spazio durante il backup, ma la procedura di backup dura di più.

- **Compressione equilibrata**: il backup non viene compresso eccessivamente, ma in compenso la procedura è più rapida.

- **Esecuzione rapida**: non avviene la compressione dei dati, quindi il backup è rapido.

Escludi file

In genere il software G DATA salva i file in base al rispettivo formato. Sul computer si trovano formati di file anche in aree che vengono gestite automaticamente e che non sono rilevanti per il backup, poiché si tratta di dati che vengono salvati solo temporaneamente (ad es. per una più rapida visualizzazione delle pagine Internet). Per accertarsi che il software G DATA non archivi inutilmente anche questi dati, è possibile escluderli selezionando la casella corrispondente.

- **Directory temporanea con file**: se si seleziona questa opzione, le cartelle temporanee, con i relativi file e sottocartelle, non verranno incluse nel backup dei dati.
- **Directory Internet temporanee con file**: se si seleziona questa opzione, le cartelle per il salvataggio dei siti Internet, con i relativi file e sottocartelle, non verranno incluse nel backup dei dati.
- **Thumbs.db**: selezionando questa opzione, i file thumbs.db creati automaticamente da Windows Explorer non vengono inclusi nel salvataggio dei dati. Questi file servono ad es. a gestire le anteprime delle presentazioni e vengono creati automaticamente dalle immagini originali.
- **File temporanei (attributo file)**: selezionando questa opzione, i file a cui il sistema ha assegnato l'attributo di temporaneo non vengono inclusi nel salvataggio dei dati.
- **File di sistema (attributo file)**: selezionando questa opzione, i file a cui il sistema ha assegnato l'attributo di file di sistema non vengono inclusi nel salvataggio dei dati.
- **Escludi tipi di file**: questa funzione permette di definire le estensioni dei file che non devono essere considerate nel backup. Procedere nel seguente modo: Inserire in **Tipo di file** (ad es. *.txt) l'estensione del file o il nome del file da escludere. Quindi fare clic su **OK**. Ripetere l'operazione per tutti i tipi di file e nomi di file da escludere, ad es. picasa.ini, *.ini, *bak ecc. Il simbolo di asterisco e il punto interrogativo possono essere utilizzati come caratteri jolly. La modalità di funzionamento dei caratteri jolly è la seguente:

  Un punto interrogativo (?) rappresenta un singolo carattere.

  L'asterisco (*) rappresenta un'intera stringa di caratteri.

  Ad esempio, per verificare la presenza di virus in tutti i file con estensione .exe, specificare *.exe. Per verificare file con diversi formati di tabella di calcolo (ad es. *.xlr, *.xls), specificare "*.xl?". Per verificare file di tipo diverso il cui nome inizia con le stesse lettere, specificare ad esempio testo*.*.

Ripristina opzioni standard attuali

Selezionando questo pulsante vengono applicate le opzioni standard del software G DATA. Se per la creazione dei backup sono state impostate alcune opzioni in maniera erronea, fare clic su **Ripristina opzioni standard attuali**.

Backup (Ripristina)

Qui è possibile ripristinare, sulla base dei dati di backup salvati, i propri dati originali dopo una perdita di dati. Fare clic sul pulsante **Ripristina**.

Viene visualizzata una finestra di dialogo in cui sono indicati tutti i backup archiviati per il processo di backup specificato.

Selezionare il backup prescelto (ad es. l'ultimo backup eseguito, nel caso si desideri ripristinare dei documenti eliminati di recente per sbaglio) e premere il pulsante **Ripristina**.

Ora si può scegliere la forma di ripristino desiderata:

- **Ripristina backup completo**: vengono ripristinati tutti i file e le cartelle archiviate in questo backup.
- **Ripristina solo partizioni/file selezionati**: viene visualizzata la struttura delle directory presenti nel backup in cui è possibile selezionare in modo mirato i file, le cartelle e le partizioni da ripristinare. Nella struttura delle directory, a sinistra, è possibile con un clic del mouse sul simbolo + aprire e selezionare le directory e visualizzarne il contenuto nella vista dei file. Ogni directory o file provvisto di un segno di spunta viene ripristinato dal backup. Se in una directory non vengono controllati tutti i file, tale directory presenta un segno di spunta di colore grigio.

Infine è possibile stabilire se i file debbano essere ripristinati nelle loro directory originali. Se invece si preferisce ripristinarli in un'altra posizione, in **Nuova cartella** selezionare un cartella in cui archiviare i file. Indicare in **Password** la password di accesso se il backup è stato compresso e protetto da password.

Quando si ripristinano i file nelle directory originali, è possibile copiare in modo mirato solo i file che sono stati modificati:

- **sovrascrivi sempre**: con questa impostazione i file del backup dei dati vengono sempre trattati come più importanti dei dati che si trovano nella directory originaria. Se si attiva questa funzione, i file già esistenti presenti in archivio verranno sovrascritti.
- **se la dimensione è cambiata**: con questa impostazione i dati esistenti nella directory originaria vengono sovrascritti solo se il file originario è stato modificato. Vengono ignorati i file la cui dimensione non si è modificata. In questo modo la procedura del recupero file sarà più veloce.
- **se data/ora di "Modificato il" nell'archivio è precedente**: con questa opzione i file della directory originaria vengono sempre sostituiti dalla copia dell'archivio se sono più recenti dei dati presenti nell'archivio. Anche in questo caso il ripristino dei dati è più veloce, in quanto non sempre è necessario ripristinare tutti i file ma solo alcuni.
- **se data/ora di "Modificato il" è cambiata**: in questo caso i dati della directory originale vengono sostituiti solo se la data di modifica è diversa da quella dei dati archiviati.

Infine, fare clic sul pulsante **Fine** per eseguire il ripristino secondo le impostazioni specificate.

Azioni

In quest'area è possibile eseguire operazioni di aggiornamento e manutenzione dei backup dei dati.

Sono disponibili i seguenti programmi di utilità:

Masterizzare l'archivio successivamente su CD/DVD

I file di backup possono essere masterizzati su CD o DVD anche in un secondo tempo. È sufficiente scegliere il progetto che si desidera masterizzare nella finestra di dialogo visualizzata, quindi fare clic sul pulsante **Avanti**.

Selezionare a questo punto l'unità in cui si intende masterizzare il backup dei dati.

Sono disponibili le seguenti opzioni:

- **Verificare i dati dopo la masterizzazione**: spuntando questa casella, i dati masterizzati verranno ricontrollati dopo la masterizzazione. Richiede dei tempi maggiori rispetto alla masterizzazione senza verifica ma è comunque generalmente consigliata.
- **Copia file del programma di ripristino**: se viene attivata questa funzione, oltre ai dati di archivio, nella posizione di salvataggio dei dati viene caricato un programma con il quale i dati vengono ripristinati anche senza avere installato il software G DATA. Avviare dal CD/DVD-ROM il programma *AVKBackup* oppure *AVKBackup.exe*.

Fare clic sul pulsante **Masterizza** per avviare la masterizzazione. Dopo la masterizzazione il CD/DVD di backup viene espulso automaticamente.

> **Nota**: ovviamente dopo la masterizzazione i dati di backup non verranno cancellati dal supporto dati originale. La masterizzazione successiva su CD/DVD è una misura di sicurezza supplementare.

Importa archivio

Per ripristinare gli archivi e i backup dei dati che non si trovano in un'unità gestita dal programma G DATA, utilizzare la funzione **Importa archivio**. Si apre una finestra di dialogo in cui è possibile cercare i file di archivio con estensione *ARC*, ad es. su un CD, un DVD o in rete. Una volta trovato l'archivio, contrassegnarlo con un segno di spunta e fare clic sul pulsante **OK**. Una finestra informativa comunica che l'archivio è stato importato correttamente. Se a questo punto l'archivio deve essere utilizzato per il ripristino dei dati, accedere all'area **Ripristina** del software G DATA, selezionare il backup prescelto e avviare il ripristino.

> Nota: I file di archivio creati con il software G DATA hanno l'estensione ARC.

Crea supporto di boot

Per ripristinare i backup anche senza avere installato il software G DATA, è possibile creare un CD/DVD o una chiavetta USB che contenga un programma specifico in grado di eseguire il ripristino dei dati. Per poter ripristinare i backup in questo modo, avviare il supporto di boot e selezionare il programma *AVKBackup* o il file *AVKBackup.exe*. Ora è possibile selezionare i backup prescelti e avviare il ripristino.

> **Nota**: la creazione di un supporto di boot viene spiegata nel capitolo **Supporto di boot**. Nel software G DATA il supporto di boot svolge un doppio ruolo: permette di ripristinare i backup e tramite BootScan permette di verificare la presenza di virus sul computer prima dell'avvio di Windows.

Gestione password

La Gestione password permette di gestire comodamente le password e può essere utilizzata come plugin nel browser.

La Gestione password supporta i seguenti browser delle ultime generazioni:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

Nota: in base alle impostazioni del browser (ad es. le impostazioni per la protezione dei dati), la funzionalità di Gestione password può risultare limitata.

Creare dapprima una cassaforte delle password, quindi installare il plugin per il browser prescelto. Naturalmente la cassaforte delle password può essere installata su tutti i browser compatibili.

Creazione di una nuova cassaforte e installazione del plugin

Fare clic sulla voce **Cassaforte password**. Si apre una finestra di dialogo che permette di creare una nuova cassaforte scegliendo **Crea nuova cassaforte**.

Digitare una password, confermarla, fare clic su **Crea cassaforte** e la cassaforte verrà creata. La frase promemoria può aiutare a ricordare una password dimenticata.

Ora la cassaforte è stata creata e nella parte destra della finestra del programma si può scegliere in quale browser installare il plugin Gestione password. Fare semplicemente clic sul nome del browser per installare il plugin.

Aprendo ora il browser, è possibile che all'utente venga chiesto se desidera utilizzare il nuovo plugin. Confermare per Gestione password di G DATA.

Ora nella barra applicazioni del browser sarà visualizzata la seguente icona. Facendo clic sull'icona, è possibile utilizzare Gestione password.

Nella finestra di dialogo relativa, immettere la password e fare clic su **Sblocca**. L'uso del plugin del browser viene spiegato nel seguente capitolo.

Utilizzo del plugin del browser

Facendo clic sulla seguente icona nella barra delle applicazioni del browser, è possibile utilizzare la Gestione password.

Nota: in base all'impostazione della privacy (ad es. archiviazione della procedura), l'uso del plugin non è consentito. In caso di problemi con il plugin, controllare per prima cosa le impostazioni del browser.

Nella finestra di dialogo relativa, immettere la password e fare clic su **Sblocca**. Sono disponibili le seguenti opzioni:

Preferiti: questa funzione permette di richiamare rapidamente i siti web protetti da password utilizzati regolarmente.

Login: qui vengono gestiti i dati d'accesso per i siti web protetti da password.

Contatti: tramite i dati dei contatti inseriti, è possibile compilare automaticamente i moduli, ad es. gli indirizzi di consegna.

Note: qui è possibile memorizzare ulteriori annotazioni protette da password.

Impostazioni: per chiudere la Gestione password, fare clic qui su **Blocca**. Facendo clic sulle Impostazioni, si possono gestire

comodamente nelle finestre di dialogo Preferiti, Login, Contatti e Note. Il generatore di password permette di generare automaticamente una password sicura e riutilizzarla direttamente tramite gli Appunti.

La Gestione password permette di aggiungere, modificare ed eliminare le voci.

Nuova voce: facendo clic su questo pulsante è possibile creare una nuova voce e inserire tutti i dati necessari nelle rispettive finestre di dialogo per Login, Contatti o Note.

Salva voce: facendo clic su questo pulsante, la voce viene salvata e in seguito compare nella selezione rapida del plugin del browser.

Elimina voce: permette di eliminare le voci non più necessarie

Tuner

Il Tuner è uno strumento che velocizza e semplifica l'uso di Windows, dall'avvio automatico di Windows Update alla deframmentazione periodica ad intervalli predefiniti, fino alla regolare rimozione delle voci di registro superflue e dei file temporanei.

È possibile regolare il computer manualmente premendo un pulsante o programmare l'esecuzione periodica dei processi di regolazione.

Ultima regolazione: qui viene indicata l'ultima volta che è stata eseguita una regolazione del computer. Per avviare una nuova regolazione, selezionare qui la voce **Esegui ora regolazione**. Non appena si avvia il processo di regolazione, lo stato del processo viene indicato da una barra di avanzamento.

Regolazione automatica: se si desidera automatizzare la regolazione del computer, selezionare l'opzione **Attiva regolazione automatica** e creare un processo con una programmazione temporale. Per impostare il processo di regolazione automatico, selezionare l'opzione **Altre impostazioni**.

Configurazione: in questa Area è possibile selezionare tutti i moduli che il Tuner deve utilizzare per il processo di regolazione. I moduli selezionati vengono avviati o tramite un'azione automatica pianificata (consultare il capitolo Pianificazione) o manuale. Per attivare un modulo, fare doppio clic su di esso. È possibile ottimizzare singolarmente le seguenti aree di regolazione:

- *Protezione*: Le varie funzioni che consentono di scaricare automaticamente i dati da Internet sono utili ai provider ma non agli utenti. Spesso queste funzioni aprono la strada a software dannosi. Questi moduli consentono all'utente di proteggere il sistema e di mantenerlo sempre aggiornato.
- *Prestazioni*: I file temporanei, ad esempio le copie di riserva non più utili, i file di registro o i dati di installazione che occupano spazio sul disco rigido una volta terminata l'installazione rallentano il disco rigido e occupano spazio prezioso. I processi e i collegamenti a file non più necessari rallentano considerevolmente il sistema. I moduli elencati qui di seguito consentono di liberare il computer da questi file inutili migliorandone così le prestazioni.
- *Protezione dati*: Raccogli i moduli riguardanti la protezione dei dati. Qui vengono eliminate le tracce lasciate involontariamente mentre si naviga in Internet o si usa il computer che possono fornire molte informazioni sulle abitudini d'uso oppure rivelare password o dati importanti.

Ripristino: per ogni modifica eseguita, il software crea un punto di ripristino. Se una delle azioni di impostazione eseguite ha causato risultati indesiderati, è possibile annullare tale azione e ripristinare lo stato del sistema a prima della rispettiva modifica. Per ulteriori informazioni, vedere anche il capitolo Ripristino.

Browser Cleaner: G DATA Browser Cleaner è in grado di bloccare o rimuovere i componenti dei programmi indesiderati e i programmi supplementari. Questi programmi vengono spesso installati insieme ai software gratuiti e possono modificare le impostazioni del browser o perfino spiare i dati. Per ulteriori informazioni, vedere anche il capitolo Browser Cleaner.

Ripristino

per ogni modifica eseguita, il software crea un punto di ripristino. Se una delle azioni di impostazione eseguite ha causato risultati indesiderati, è possibile annullare tale azione e ripristinare lo stato del sistema a prima della rispettiva modifica.

Seleziona tutto: per annullare tutte le modifiche effettuate dalla regolazione, selezionare qui tutti i punti di ripristino, quindi fare clic sul pulsante **Ripristina**.

Ripristina: per annullare solo alcune modifiche specifiche subentrate con la regolazione, selezionare qui il punto di ripristino prescelto, quindi fare clic sul pulsante **Ripristina**.

Elimina selezionati: questo pulsante permette di eliminare i punti di ripristino che non sono più necessari.

Browser Cleaner

G DATA Browser Cleaner è in grado di bloccare o rimuovere i componenti dei programmi indesiderati e i programmi supplementari. Questi programmi vengono spesso installati insieme ai software gratuiti e possono modificare le impostazioni del browser o perfino spiare i dati. Browser Cleaner permette di visualizzare questi programmi potenzialmente indesiderati ("PUP" = Potentially Unwanted Programs) nei browser Internet Explorer, Firefox e Google Chrome e di decidere se disattivarli soltanto o se rimuoverli definitivamente. Le estensioni disattivate possono essere ripristinate in qualsiasi momento.

> **Nota:** G DATA Browser Cleaner opera con Microsoft Internet Explorer, Mozilla Firefox e Google Chrome insieme e permette di gestire con estrema facilità tutte le estensioni del browser installate. Con un clic del mouse è possibile disattivare o rimuovere tutti i plugin inclusi nell'elenco e liberare il browser da estensioni indesiderate. Lo strumento indica per opzione tutti i plugin classificati come sicuri per distinguerli in modo semplice e rapido dalle estensioni non sicure o indesiderate. G DATA Browser Cleaner è incluso nella soluzione completa per la sicurezza G DATA Total Security ed è sempre disponibile per gli utenti che ne fanno uso.

Protezione minori

La funzione Protezione minori consente di stabilire le regole per la navigazione e l'utilizzo del computer per i propri bambini.

In **Utente** selezionare un utente registrato sul computer e impostare qui le limitazioni per tale utente. Con il pulsante **Crea nuovo utente** è possibile configurare direttamente nuovi account sul computer, ad es. per i bambini.

- **Protezione minori per questo utente**: permette di attivare o disattivare la Protezione minori per l'utente selezionato in precedenza.
- **Contenuti proibiti**: in quest'area viene aperta una finestra di dialogo che permette di bloccare per l'utente attualmente visualizzato alcuni contenuti specifici in Internet. Fare clic su **Modifica** per stabilire i contenuti proibiti per il rispettivo utente.
- **Contenuti autorizzati**: in quest'area viene aperta una finestra di dialogo che permette di autorizzare contenuti speciali di Internet all'utente attualmente visualizzato. Fare clic su **Modifica** per stabilire i contenuti autorizzati per il rispettivo utente.
- **Monitorare il tempo di utilizzo di Internet**: permette di definire per quanto tempo e in quali orari l'utente selezionato può accedere a Internet. Fare clic su **Modifica** per stabilire gli orari di utilizzo per il rispettivo utente.
- **Monitorare il tempo di uso del computer**: permette di definire per quanto tempo e in quali orari l'utente selezionato potrà utilizzare il computer. Fare clic su **Modifica** per stabilire gli orari di utilizzo per il rispettivo utente.

Impostazioni: permette di modificare e di adattare alle proprie esigenze le impostazioni di base per la Protezione minori.

Crea nuovo utente

Fare clic sul pulsante **Crea nuovo utente**. Si apre una finestra di dialogo che permette di inserire il Nome utente e la Password per questo utente.

> **Nota**: Per motivi di sicurezza una password dovrebbe essere lunga almeno otto caratteri e contenere lettere maiuscole, minuscole e numeri.

Ora in **Utente** è riportato il nome del nuovo utente, per il quale viene contemporaneamente creato anche un Account utente di Windows. Ciò significa che la Protezione minori è attivata automaticamente con le relative impostazioni per la persona che all'avvio di Windows accede con questo nome utente. Fare doppio clic con il mouse sull'area delle impostazioni da definire per questo utente. È possibile, ad esempio, vietare i **Contenuti proibiti** o specificare i **Contenuti autorizzati** oppure stabilire che per questo utente venga monitorato il **Tempo di utilizzo di Internet** oppure **Tempo di uso del computer**.

Contenuti proibiti

In quest'area viene aperta una finestra di dialogo in cui è possibile bloccare per l'utente attualmente visualizzato alcuni contenuti specifici in Internet. Selezionare le categorie da bloccare apponendo un segno di spunta. Fare clic su **OK** e verranno bloccate le pagine Internet che corrispondono ai criteri di blocco.

Facendo clic sul tasto **Nuovo**, si apre una finestra di dialogo che permette di definire i criteri di blocco personalizzati (detti anche Blacklist: liste nere). Per ciascun filtro creato, specificare il nome ed eventualmente un testo informativo.

Facendo clic su **OK** viene aperta un'ulteriore finestra nella quale si possono riepilogare i contenuti che dovranno essere soppressi da questo filtro.

In **Filtro** specificare un termine che dovrà essere bloccato e in **Luogo per la ricerca** l'area di un sito web in cui eseguire la ricerca.

Sono disponibili le seguenti opzioni:

- **URL**: se si seleziona URL, il testo da bloccare verrà cercato nell'indirizzo web. Per vietare alcune pagine, ad esempio *www.chatcity.no*, *www.crazychat.co.uk* o altre simili, è sufficiente specificare come **Filtro** *chat*, selezionare **URL**, quindi fare clic sul pulsante **Aggiungi**. Ora verranno bloccate tutte le pagine che utilizzano nel nome del dominio, ovvero nell'indirizzo Internet, la sequenza di caratteri *chat*.
- **Titolo**: se si seleziona URL, il testo da bloccare verrà cercato nel titolo del sito web, ossia nell'area che è visibile quando si desidera contrassegnare una pagina nella lista dei preferiti inserendo un segnalibro. Per vietare alcune pagine, ad esempio *Chat City Detroit*, *Teenage Chat 2005* o altre simili, è sufficiente specificare **chat** come *Filtro*, selezionare **Titolo**, quindi fare clic sul tasto **Aggiungi**. Ora verranno bloccate tutte le pagine che utilizzano nel titolo la sequenza di caratteri *chat*.
- **Meta**: i cosiddetti metatag sono stringhe di testo incorporate nei siti web che servono per elencare tali siti nei motori di ricerca con maggiore efficienza o semplicemente più di frequente. Per incrementare gli accessi alle pagine, vengono spesso utilizzati termini

come *sesso* o *chat*. Per vietare le pagine che contengono nel metatag il termine *chat*, è sufficiente specificare **chat** come *Filtro*, selezionare **Meta**, quindi fare clic sul pulsante **Aggiungi**. Ora verranno bloccate tutte le pagine che utilizzano nei metatag la sequenza di caratteri *chat*.

- **Nel testo complessivo**: Per controllare direttamente l'eventuale presenza di termini da bloccare nel contenuto testuale di una pagina, specificare il termine da bloccare, ad es. *chat*, selezionare l'opzione **Nel testo complessivo**, quindi fare clic sul tasto **Aggiungi**. Ora verranno bloccate tutte le pagine che utilizzano nel testo della pagina visualizzata la sequenza di caratteri *chat*.

Per sbloccare le pagine che rientrano per errore nell'ambito del filtro, utilizzare la funzione Eccezioni. Fare clic sul pulsante **Eccezioni** e specificare qui la pagina desiderata.

> **Nota**: I filtri creati dall'utente possono essere modificati ed eventualmente eliminati nell'area **Filtri personalizzati**. Per ulteriori informazioni, consultare il capitolo **Filtri personalizzati**.

Contenuti autorizzati

In quest'area viene aperta una finestra di dialogo in cui è possibile consentire contenuti speciali di Internet all'utente attualmente visualizzato. Selezionare le categorie da autorizzare, facendo clic sulla casella di spunta relativa. Fare clic ora su **OK** per autorizzare le pagine Internet che corrispondono ai criteri desiderati.

Facendo clic sul tasto **Nuovo**, si apre una finestra di dialogo che permette di definire i contenuti autorizzati (detti anche Whitelist: liste bianche). Per ciascun filtro creato, specificare il nome ed eventualmente un testo informativo.

Fare quindi clic su **OK**. Si apre una finestra di dialogo in cui è possibile inserire la Whitelist con le pagine Web che possono essere visualizzate, ad es. dai bambini.

Indicare in **Filtro**, quali componenti del nome del dominio debbano essere autorizzati. Se ad es. si desidera autorizzare il sito Web per bambini "Trebisonda", è possibile inserire qui *www.trebisonda.rai.it* e autorizzare così l'accesso a tale sito. In **Descrizione**, specificare il contenuto della pagina Web in questione, ad esempio *Trebisonda - sito adatto ai bambini* e in **Collegamento all'offerta** digitare l'indirizzo Web esatto della pagina. La descrizione e il collegamento all'offerta diventeranno importanti se il bambino dovesse effettivamente digitare un indirizzo di una pagina che non è consentita. Invece di un messaggio di errore, nel browser viene visualizzata una pagina HTML che elenca tutti i siti Web inseriti nella whitelist, comprensivi di descrizione. In tal modo il bambino potrà accedere alle pagine che sono state autorizzate. Una volta effettuati tutti gli inserimenti, fare clic su **Aggiungi** e nella whitelist verranno inseriti i dati.

> **Nota**: Il filtro ricerca i segmenti nel nome del dominio. Per ogni indicazione nel filtro, è possibile distinguere i risultati gli uni dagli altri. Ogni ulteriore restrizione può essere utile a seconda del sito Web.

Monitorare il tempo di utilizzo di Internet

Qui è possibile definire per quanto tempo e in quali orari l'utente selezionato può accedere a Internet. A questo scopo, selezionare l'opzione **Monitorare il tempo di utilizzo di Internet**. È possibile anche stabilire per quanto tempo nell'arco di un mese l'utente potrà accedere ad Internet, quanto tempo ha a disposizione ogni settimana e per quante ore in determinati giorni della settimana. In questo modo è possibile, ad esempio, gestire i fine settimana per i ragazzi in età scolastica in modo diverso rispetto ai giorni infrasettimanali. I rispettivi intervalli temporali vengono specificati in **giorni/hh:mm**, quindi l'impostazione *04/20:05* indica un tempo di utilizzo di Internet pari a 4 giorni, 20 ore e 5 minuti.

> **Nota**: In presenza di indicazioni temporali diverse per l'utilizzo di Internet, ha sempre priorità il valore più piccolo. Perciò, se per il mese è stato stabilito un limite di quattro giorni, ma per la settimana sono ammessi, ad esempio, cinque giorni, il programma imposterà automaticamente per l'utente un tempo di utilizzo di Internet di quattro giorni.

Una volta esaurita la quantità di tempo, se l'utente prova ad accedere ad Internet, comparirà un avviso che informa che il tempo a disposizione è stato superato.

Blocco orari

Premendo il pulsante **Blocco orari** si apre la finestra di dialogo in cui, oltre a una limitazione quantitativa dell'utilizzo di Internet, è possibile bloccare categoricamente determinati periodi di tempo nel corso della settimana. Gli archi temporali bloccati sono indicati in rosso mentre quelli liberi sono indicati in verde. Per liberare o bloccare un periodo di tempo, selezionarlo con il mouse. Accanto al cursore del mouse compare un menu contestuale con due opzioni: **Sblocca orario** e **Blocca orario**. Quando un utente tenta di accedere a Internet durante gli orari di blocco, nel browser viene visualizzata una schermata di informazioni in cui viene specificato che in quel momento non è consentito l'accesso a Internet.

Monitorare il tempo di uso del computer

Qui è possibile definire per quanto tempo e in quali orari l'utente selezionato potrà utilizzare il computer. A questo scopo, selezionare l'opzione **Monitorare il tempo di uso del computer**. Ora è possibile stabilire per quanto tempo nell'arco di un mese l'utente potrà accedere ad Internet, quanto tempo ha a disposizione ogni settimana e per quante ore in determinati giorni della settimana. In questo modo è possibile, ad esempio, gestire i fine settimana per i ragazzi in età scolastica in modo diverso rispetto ai giorni infrasettimanali. I rispettivi intervalli temporali vengono specificati in **giorni/hh:mm**, quindi l'impostazione *04/20:05* indica un tempo di utilizzo del computer pari a 4 giorni, 20 ore e 5 minuti. Il pulsante **Visualizzare un messaggio di avvertenza prima dello scadere del tempo** consente di informare l'utente poco prima dello spegnimento del computer affinché possa salvare i propri dati. Lo spegnimento del computer senza avvertimento potrebbe causare una perdita dei dati.

> **Nota**: Insieme all'indicazione sull'utilizzo del computer viene considerato sempre il valore inferiore. Perciò, se per il mese è stato stabilito un limite di quattro giorni, ma per la settimana sono ammessi, ad esempio, cinque giorni, il programma imposterà automaticamente per l'utente un tempo di utilizzo del computer di quattro giorni.

Blocco orari

Premendo il tasto **Blocco orari** si apre la finestra di dialogo in cui, oltre a una limitazione quantitativa dell'utilizzo del computer, è possibile bloccare categoricamente determinati periodi di tempo nel corso della settimana. Gli archi temporali bloccati sono indicati in rosso mentre quelli liberi sono indicati in verde. Per liberare o bloccare un periodo di tempo, selezionarlo con il mouse. Accanto al cursore del mouse compare un menu contestuale con due opzioni: **Sblocca orario** e **Blocca orario**.

Filtri personalizzati

In quest'area è possibile modificare le whitelist (quindi contenuti autorizzati) e le blacklist (quindi contenuti proibiti) create in proprio, nonché creare manualmente elenchi completamente nuovi.

I seguenti tipi di elenchi si distinguono fondamentalmente gli uni dagli altri:

- **Contenuti autorizzati**: se per uno degli utenti selezionati in precedenza viene selezionata una whitelist, questi potrà visualizzare esclusivamente pagine Web incluse nella whitelist. In qualità di amministratore è possibile configurare la presente whitelist a proprio piacimento oppure selezionare dalle whitelist predefinite l'elenco adatto per un utente. Una whitelist è particolarmente indicata per autorizzare ai bambini più piccoli un accesso ad Internet molto limitato e per dare loro la possibilità di accedere ai siti Web con contenuti pedagogici raccomandabili, ma niente più di questo.

- **Contenuti proibiti**: Con una blacklist è possibile bloccare le pagine Web selezionate per un utente. In caso contrario l'utente avrà un accesso illimitato ad Internet. È bene tenere conto del fatto che tale funzione permette di bloccare alcune pagine, ma che contenuti analoghi possono trovarsi su altre pagine Web. Una blacklist di indirizzi Internet non fornisce mai una protezione completa dai contenuti indesiderati.

Mediante i seguenti pulsanti è possibile modificare gli elenchi di esclusione:

- **Elimina**: la funzione **Elimina** permette di eliminare con il mouse gli elenchi selezionati.

- **Nuovo**: permette di creare una blacklist o una whitelist completamente nuova. La procedura da seguire è la stessa descritta nel capitolo **Contenuti proibiti** e dei **Contenuti autorizzati**.

- **Modifica**: Permette di modificare il contenuto di un elenco esistente.

Impostazioni: Log

Questa scheda consente di modificare le impostazioni di base per le informazioni nell'area Log. È possibile stabilire se registrare gli accessi a contenuti permessi e/o proibiti. Se i contenuti vengono registrati, è possibile permetterne la visione ai vari utenti nell'area Log.

I file di log, in caso di utilizzo regolare, hanno la tendenza ad occupare molto spazio, pertanto è possibile impostare la Protezione minori in **Mostrare il messaggio quando il file raggiunge____ KB** in modo da ricevere un messaggio in caso di superamento di una certa dimensione. In questo caso, nella scheda **Log** eliminare manualmente tali file di log in **Elimina log**.

Crittografia

Il modulo di crittografia è come la cassaforte di una banca e serve per proteggere i dati riservati. Una cassaforte può, ad esempio, essere usata come partizione supplementare del disco rigido ed è semplice da gestire.

Per la creazione e la gestione di una cassaforte, sono disponibili le seguenti opzioni:

- **Aggiorna**: se avete aperto o chiuso la cassaforte al di fuori del modulo Crittografia, si consiglia di fare clic su **Aggiorna** per aggiornare i dati contenuti nella cassaforte allo stato più recente.
- **Apri/Chiudi**: qui potete aprire e chiudere le casseforti presenti sul computer e sui supporti collegati. Ricordare che per aprire una cassaforte è necessario fornire la relativa password, impostata durante la creazione della cassaforte. Qui è possibile chiudere le casseforti senza fornire una password.
- **Crea nuova crittografia**: questa funzione permette di creare una nuova cassaforte. Si apre una procedura guidata (Assistente) che vi aiuta a creare la cassaforte. Per ulteriori informazioni, consultare il capitolo **Crea nuova cassaforte**.
- **Crea cassaforte portatile**: dopo avere creato una cassaforte, è possibile impostarla come cassaforte portatile, ossia è possibile configurarla in modo da utilizzarla su una chiavette USB o spedirla per posta elettronica. Per ulteriori informazioni, consultare il capitolo **Crea cassaforte portatile**.
- **Elimina**: l'area Gestione casseforti offre un riepilogo di tutte le casseforti presenti nel computer e nei supporti collegati. Qui è possibile anche eliminare le casseforti obsolete. Ricordare che qui si possono eliminare le casseforti anche senza conoscerne la password. Perciò, prima di cancellare una cassaforte, controllare con attenzione che il suo contenuto non vi serva più.

Crea nuova cassaforte

Quando si desidera creare una nuova cassaforte, si è assistiti da una finestra di dialogo interattiva. Fare clic sul pulsante **Avanti** per continuare.

Posizione di salvataggio e dimensioni della cassaforte

Indicare ora il percorso dove si desidera salvare la cassaforte e specificarne le dimensioni.

> **Nota**: La cassaforte è in realtà un file protetto, che, al momento dell'apertura, si comporta come una partizione di disco rigido. Questo vuol dire che durante la collocazione vengono creati dei file sicuri nella posizione desiderata del disco rigido. Qui i dati vengono archiviati in formato cifrato. Quando si apre e si utilizza la cassaforte, è possibile modificare, eliminare, copiare e spostare i file e le cartelle in essa contenuti come in un normale disco fisso o in una partizione del disco.

Posizione di salvataggio

Seleziona qui, su quale unità (ad esempio Disco locale (C:)) deve essere creata la cassaforte.

> **Nota**: Le casseforti create in una directory protetta sono visibili sul computer soltanto se il software G DATA è installato sul PC. Se si disinstalla questo programma, le casseforti create non saranno più visibili.

Dimensione della cassaforte

Scegliere infine le dimensioni della cassaforte, spostando il cursore di scorrimento secondo le esigenze. Lo spazio a disposizione corrisponderà allo spazio disponibile nella posizione di salvataggio. È opportuno scegliere una grandezza inferiore di almeno 2 GB rispetto alla grandezza massima, in modo da non rallentare le prestazioni del computer in altri ambiti a causa di spazio insufficiente.

> **Nota**: Per una selezione rapida delle dimensioni della cassaforte, utilizzare i pulsanti alla sinistra del cursore di scorrimento. È possibile definire le dimensioni della cassaforte con estrema precisione oppure impostarle in modo che sia possibile masterizzare la cassaforte su un CD, un DVD o un disco Blu-Ray.

Fare clic ora sul pulsante **Avanti**.

Parametri della cassaforte

In questa finestra di dialogo è possibile definire le seguenti impostazioni per la cassaforte:

- **Nome cassaforte**: il nome con cui la cassaforte verrà gestita dal software G DATA.
- **Descrizione**: un breve descrizione supplementare, ad es. alcune informazioni sul contenuto della cassaforte.
- **File system**: permette di definire se l'unità virtuale creata dalla cassaforte debba utilizzare il file system FAT o NTFS. Di norma è opportuno lasciare l'impostazione **Selezione automatica**.
- **Selezione automatica unità cassaforte**: la cassaforte viene rappresentata sul computer come un'unità disco rigido. È possibile definire una lettera per l'unità oppure lasciare che il sistema ne scelga una automaticamente. Di solito si consiglia l'assegnazione automatica.
- **Assegna unità**: questa opzione è disponibile soltanto quando si preferisce che l'unità della cassaforte non venga scelta automaticamente.

Fare clic ora sul pulsante **Avanti**.

Accesso alla cassaforte

Qui è possibile impostare una password per la cassaforte. Fare clic sul pulsante **Aggiungi**.

Nella finestra di dialogo visualizzata, in **Password** e in **Ripeti password** specificare la password prescelta. Se le due password coincidono, la password verrà accettata. La ripetizione serve ad evitare che, a causa di un errore ortografico, venga assegnata inavvertitamente una password che neppure l'utente è in grado di ripristinare.

Fare clic su **Aggiungi** per attivare la password, quindi su **Avanti** per terminare la configurazione della cassaforte.

> **Nota**: quando si crea una cassaforte, è possibile assegnarvi più password diverse ed associarle a tipi di autorizzazione differenti. Si può, ad esempio, creare una cassaforte per se stessi, in cui copiare e modificare i file, e assegnare una password diversa agli altri utenti, che consenta loro di leggere il contenuto della cassaforte, ma non di modificarlo.

Una volta creata la cassaforte, è possibile selezionarla e fare clic sul pulsante **Autorizzazione** per scegliere le seguenti opzioni di impostazione:

- **Modifica Autostart**: in ogni cassaforte è presente una cartella chiamata Autostart. Se questa opzione rimane impostata su Sì, all'apertura della cassaforte verranno avviati automaticamente tutti i file eseguibili presenti.
- **Apri in modalità "Solo lettura"**: un utente che effettua il login con il metodo di accesso in sola lettura non potrà né salvare né modificare i file presenti nella cassaforte. In ogni caso potrà leggerli.
- **Apri come supporto rimovibile**: il software G DATA apre le casseforti dati in Esplora risorse come dischi rigidi locali. Se si desidera che la cassaforte venga visualizzata come supporto dati rimovibile, nel sistema è necessario selezionare questa opzione.
- **Utilizzo condiviso**: la selezione di questa opzione consente l'utilizzo condiviso della directory della cassaforte con altri computer in rete. Avvertenza: Con questa impostazione, l'accesso alla cassaforte non necessita dell'immissione di una password. Consigliamo pertanto di essere cauti e convinti nel voler utilizzare la cassaforte in modo condiviso. L'utilizzo condiviso della cassaforte per tutti gli utenti della rete non ha senso poiché in questo caso i dati sono accessibili a tutti.
- **Chiudi cassaforte dopo logout utente**: questa opzione dovrebbe essere attivata sempre poiché se la cassaforte resta aperta anche dopo il logout dell'utente, altri utenti potrebbero consultare il contenuto della cassaforte.
- **Cassaforte automatica**: tutte le casseforti con questa proprietà possono essere aperte con un singolo comando.

Configurazione della cassaforte

La procedura guidata di creazione della cassaforte nell'ultima fase informa l'utente sui parametri di impostazione. Se si desidera modificare queste impostazioni è necessario fare clic sul tasto **Indietro**. Quando si è soddisfatti delle impostazioni, fare clic su **Crea**.

La cassaforte dati virtuale e crittografata viene creata sul disco fisso del proprio computer. Con un ultimo clic sul pulsante **Fine** la cassaforte verrà creata e aperta direttamente, se lo si desidera.

Crea cassaforte portatile

Dopo avere creato una cassaforte, è possibile impostarla come cassaforte portatile, ossia è possibile configurarla in modo da utilizzarla su una chiavette USB o spedirla per posta elettronica.

Selezionare il riepilogo di una cassaforte esistente e fare clic sul pulsante **Crea cassaforte portatile**. Si apre una finestra di dialogo per assistere l'utente nella creazione di una cassaforte portatile. Fare clic su **Avanti** per avviare la procedura.

Parametri della cassaforte

Come per l'impostazione dei parametri di una cassaforte standard, qui è possibile modificare i parametri della cassaforte. Tuttavia, per le casseforti portatili sono disponibili solo alcune impostazioni:

- **Selezione automatica unità cassaforte**: quando è aperta, la cassaforte viene rappresentata come un'unità disco fisso. È possibile definire una lettera per l'unità oppure lasciare che il sistema ne scelga una automaticamente. Di solito si consiglia l'assegnazione automatica.
- **Collega cassaforte al supporto dati**: qui è possibile stabilire che la cassaforte portatile verrà utilizzata, ad esempio, esclusivamente con la chiavetta USB o con l'unità disco fisso in cui viene creata. Quando la cassaforte dati non è collegata al supporto dati, è possibile inviare il file cassaforte (riconoscibile dall'estensione **tsnxg**) anche come allegato di una e-mail o spostare/copiare il file cassaforte su un altro supporto dati.

Supporto

Qui è possibile definire il supporto sul quale archiviare la cassaforte portatile. Può essere ad es. una chiavetta USB, un disco fisso esterno o un CD/DVD.

> **Nota**: quando si archivia una cassaforte su un CD o un DVD, quest'ultimo può solo essere aperto e letto. Su questo tipo di supporto dati non è possibile modificare i file e le directory contenuti nella cassaforte.

Dimensione della cassaforte

Qui è indicata la quantità di spazio in memoria necessario per la cassaforte dati sul supporto di destinazione. Se la quantità necessaria è troppo grande, qui è possibile interrompere la creazione della cassaforte portatile.

> **Nota**: oltre alle dimensioni della cassaforte, occorre calcolare 6 MB aggiuntivi per i dati del driver, necessari per aprire la cassaforte anche in un sistema Windows in cui non è installato il software G DATA.

Fine

Terminare ora la creazione della cassaforte portatile facendo clic sul pulsante **Fine**. Se lo si desidera, nella struttura dei file è possibile visualizzare il file in cui si trova la cassaforte portatile sul supporto dati prescelto.

Apri cassaforte portatile

Per aprire una cassaforte portatile su un computer Windows sul quale non è installato il modulo Cassaforte dati G DATA, è possibile accedere ai dati selezionando su una chiavetta USB, sul disco fisso o su un CD/DVD il file di programma **start.exe** o **start** presente nella cartella **TSNxG_4**. Facendo clic su questo file verrà aperta una finestra di dialogo che permette di aprire o chiudere (se già aperta) la cassaforte.

> **Attenzione**: al primo utilizzo di Cassaforte dati G DATA, sul computer verranno caricati i relativi dati del driver e gli elementi del programma. Successivamente sarà necessario riavviare il computer. Dopo il riavvio del computer, selezionare nuovamente la voce **Start** o **Start.exe**.

Inserire la password oppure utilizzare uno degli altri metodi di accesso alla cassaforte.

La cassaforte viene aperta e sarà possibile utilizzarne il contenuto.

Dopo avere effettuato il login nella cassaforte, in Esplora risorse compare accanto alle unità locali anche l'icona della cassaforte come unità supplementare contrassegnata da una lettera corrispondente. Ogni utente mobile della cassaforte può copiare i dati dalla cassaforte sul computer. Quando si utilizza una cassaforte mobile su un supporto dati USB oppure una memoria Flash, l'utente autorizzato può copiare i dati dalla cassaforte del computer nella cassaforte.

Le operazioni di chiusura della cassaforte mobile sono simili alle operazioni di apertura. Fare doppio clic sulla lettera dell'unità della

cassaforte o selezionare il relativo comando con il tasto destro del mouse nel menu contestuale.

Attenzione: dopo aver eseguito le operazioni appena descritte, si consiglia di chiudere la cassaforte prima di rimuovere il supporto dati portatile. A questo scopo è necessario accedere al supporto dati portatile, aprire la directory G DATA e fare clic su Start.exe. Verrà quindi visualizzata una finestra di dialogo che permette di chiudere la cassaforte.

Autostart Manager

Autostart Manager permette di gestire i programmi che vengono avviati automaticamente all'avvio di Windows. Normalmente questi programmi si avviano direttamente all'avvio del sistema. Quando i programmi sono gestiti da Autostart Manager, è possibile impostarne anche l'avvio ritardato o in base al sovraccarico del sistema o del disco fisso. Ciò permette un avvio più rapido del sistema e quindi migliori prestazioni del computer.

Quando si apre Autostart Manager, sulla sinistra è visualizzato un elenco di tutti i programmi con avvio automatico installati sul computer. In genere questi programmi si avviano direttamente all'avvio di Windows e possono contribuire a rallentare l'avvio del computer.

Utilizzando l'icona di freccia, selezionare i programmi con avvio automatico per i quali si desidera posticipare l'avvio, ingannando in questo modo la procedura di avvio di Windows. Il sistema operativo Windows si avvierà più velocemente e sarà pronto prima per l'utilizzo.

Se invece non si desidera posticipare l'avvio automatico di un programma, tornare semplicemente dalla cartella **Autostart con ritardo** alla cartella **Autostart senza ritardo**.

Imposta ritardo

Quando un programma si trova nella cartella Autostart con ritardo, è possibile determinare di quanti minuti dovrà essere posticipato il suo avvio. A questo scopo, fare clic sul programma e nella colonna Ritardo selezionare il periodo di tempo desiderato.

Sono disponibili le seguenti opzioni:

- **Non avviare**: L'applicazione viene gestita dall'Autostart Manager, ma non viene riavviato al successivo riavvio di sistema. Rimane inattivo.
- **1 - 10 minuti**: l'applicazione si avvia dopo i minuti di ritardo specificati.
- **Avvio automatico**: l'applicazione viene avviata automaticamente in base al carico della CPU/disco fisso. Ciò significa che un'applicazione con avvio automatico verrà avviata solo quando si sarà risolto il sovraccarico del sistema, causato dall'avvio di altre applicazioni o altri processi con avvio automatico.

Proprietà

Facendo doppio clic sulla voce di un programma negli elenchi di Autostart Manager, verranno visualizzate numerose informazioni sul software gestito.

Controllo dispositivi

La funzione Controllo dispositivi permette di definire per il vostro computer quali supporti di memoria sono autorizzati per la lettura e/o la scrittura dei dati. È possibile, ad esempio, vietare che i dati privati vengano copiati su una chiavetta USB o masterizzati su un CD. È possibile inoltre stabilire quali supporti dati rimovibili, ossia quali chiavette USB o dischi fissi USB, siano autorizzati a copiare i dati. Si può, ad es., utilizzare il proprio disco fisso USB per eseguire il backup dei dati e contemporaneamente vietare l'accesso ad altri dischi fissi.

Questo riepilogo mostra gli effetti delle impostazioni di Controllo dispositivi per il rispettivo utente. Tramite il pulsante "Modifica regole" è possibile adattare alle proprie esigenze le impostazioni per il dispositivo e per l'utente.

> **USB Keyboard Guard:** da ora il nostro software vi protegge anche da una nuova minaccia: le chiavette USB infette che si presentano al sistema operativo come tastiera per poter introdurre programmi dannosi. Quando si collega un dispositivo USB, il software avvisa l'utente quando il sistema crede si tratti di una nuova tastiera e tramite l'inserimento di un PIN è possibile confermare o smentire. Naturalmente il software memorizza tutte le tastiere già autorizzate e non chiede di nuovo l'autorizzazione.

Impostazioni

L'area **Impostazioni** permette di configurare il rispettivo modulo di programma in base alle proprie esigenze. Generalmente non è necessario apportare alcuna modifica, poiché il software G DATA è già stato configurato in modo ottimale durante l'installazione sul vostro sistema. Nell'area Impostazioni sono disponibili le seguenti funzioni aggiuntive:

Salva impostazioni: permette di salvare le impostazioni effettuate in un file di impostazioni di G DATA. Quando si utilizza il software G DATA su più computer, questa opzione permette di eseguire le impostazioni su un computer, salvarle e caricare il file con le impostazioni su altri computer.

Carica impostazioni: permette di caricare il file delle impostazioni G DATA su un altro computer.

Ripristina impostazioni: in caso di errore nelle impostazioni del software G DATA, questo pulsante permette di ripristinare tutte le impostazioni del programma allo stato predefinito. Potete scegliere se ripristinare tutte o solo alcune impostazioni. Selezionare con un segno di spunta le impostazioni da ripristinare.

Generale

Protezione / Rendimento

Per utilizzare la protezione antivirus su un computer lento, è possibile ottimizzare il livello di protezione per migliorare le prestazioni, ossia la velocità operativa, del computer. Nel grafico riportato di seguito si possono comprendere gli effetti di un'ottimizzazione delle impostazioni.

- **Computer standard (consigliato)**: permette di impostare la protezione ottimale per il software G DATA. Entrambi i motori antivirus del programma lavorano in contemporanea. Tutti gli accessi in lettura e scrittura sul computer vengono controllati per rilevare l'eventuale presenza di codici dannosi.

  Motori: il software G DATA funziona con due motori antivirus. In linea di principio, l'utilizzo dei due motori garantisce risultati ottimali durante la profilassi antivirus.

- **Computer lenti**: per non compromettere la velocità operativa dei computer lenti, il software G DATA può funzionare anche con un solo motore. Questa protezione è disponibile in molti programmi antivirus reperibili in commercio, che operano sempre con un solo motore. La protezione è comunque sempre a un buon livello. Si noterà che in Modalità Guardiano verranno controllate solo le operazioni di scrittura. Verranno controllati soltanto i nuovi dati salvati, migliorando in questo modo le prestazioni.

- **Definita dall'utente**: permette di scegliere se utilizzare entrambi o solo un motore e di impostare il Guardiano come attivo per le azioni di lettura e scrittura, solo per la scrittura (esecuzione) o totalmente disattivato (impostazione sconsigliata).

Password

La definizione di una password protegge le impostazioni del software G DATA. In questo modo un altro utente del medesimo computer non potrà, ad es., disattivare le funzioni Guardiano AntiVirus o Scansione in modo inattivo.

Per impostare una password, digitarla prima in "Password" e poi ripetere l'inserimento in "Ripetere la password" per evitare errori di ortografia. Inoltre, in "Nota sulla password", è possibile aggiungere un'annotazione alla password.

Nota: la nota sulla password viene visualizzata quando si inserisce una password errata. Pertanto la nota sulla password serve solo a voi per trarre deduzioni sulla password.

Nota: la protezione tramite password rappresenta una protezione supplementare del programma. La massima protezione si ottiene utilizzando più account utente. In qualità di amministratore, si dovrebbe gestire nel proprio account la protezione antivirus e permettere ad altri utenti (ad es. figli, amici e parenti) solo diritti di accesso limitati per i loro account utente, senza la possibilità di effettuare modifiche.

Nota: se dopo la creazione di vari account utente non si necessita più di una password per il software G DATA, è possibile rimuovere l'obbligo di immissione della password utilizzando il pulsante "Rimuovi password".

Antivirus

Protezione in tempo reale

La funzione Protezione in tempo reale del Guardiano AntiVirus controlla ininterrottamente l'eventuale presenza di virus sul computer, controlla i processi di scrittura e di lettura e blocca i programmi che intendono eseguire delle funzioni dannose o diffondere file nocivi. Il Guardiano AntiVirus è la protezione più importante e per questo non dovrebbe mai essere disattivato!

Sono disponibili le seguenti opzioni:

- **Stato del guardiano**: qui è possibile definire se il Guardiano dovrà essere attivato o disattivato.
- **Usa motori**: Il software utilizza due motori, ossia due programmi di scansione antivirus indipendenti l'uno dall'altro. Ciascun motore è in grado di proteggere da solo in maniera efficace il PC dai virus. Tuttavia, proprio l'uso congiunto dei due motori fornisce risultati ottimali. Nei computer di vecchia generazione, l'uso di un solo motore di scansione antivirus può velocizzare le prestazioni. Di regola, però, si consiglia di mantenere l'impostazione **Entrambi i motori**.
- **File infetti**: nell'impostazione predefinita, in caso di virus rilevati il sistema chiede come si desidera procedere con il virus e con il file infetto. Se si desidera eseguire sempre la stessa azione, la si può impostare qui. La sicurezza massima per i dati offre in questo caso l'impostazione **Disinfettare (se non è possibile: in quarantena)**.
- **Archivi infetti**: Qui è possibile decidere se i dati di archivio (quindi ad es. i file con estensione RAR, ZIP o PST) debbano essere trattati diversamente rispetto ai file normali. Tenere presente, tuttavia, che lo spostamento di un archivio in quarantena potrebbe danneggiarlo al punto tale da non poterlo più utilizzare, neppure se lo si ripristina dalla **Quarantena** nella posizione originaria.
- **Monitoraggio del comportamento**: quando è attivato il monitoraggio del comportamento, vengono monitorate tutte le attività del sistema, indipendentemente dal Guardiano AntiVirus. In questo modo vengono rilevati anche i virus ancora sconosciuti.
- **AntiRansomware**: Protezione contro i Trojan di crittografia.
- **Exploit Protection**: un cosiddetto exploit sfrutta i punti deboli dei più comuni programmi utente e nel peggiore dei casi può assumere il controllo del computer attraverso tali falle. Gli exploit possono accedere perfino durante gli aggiornamenti periodici delle applicazioni, come un visualizzatore per PDF, un browser ecc. Exploit Protection protegge da questi tipi di accessi, anche in modo proattivo contro attacchi sconosciuti.

Eccezioni

Facendo clic sul pulsante Eccezioni è possibile escludere determinate unità, directory e file dalla verifica, accelerando pertanto il riconoscimento antivirus.

Procedere nel modo seguente:

1. Fare clic sul pulsante **Eccezioni**.
2. Fare clic nella finestra **Eccezioni guardiano** su **Nuova**.
3. Scegliere se si desidera escludere un'unità, una directory oppure un file e/o un tipo di file.
4. Selezionare quindi la directory o l'unità che si desidera proteggere. Per proteggere singoli file, inserire il nome file completo nel campo di immissione sotto la maschera file. In questo campo è possibile utilizzare i segnaposto.

   Nota: la modalità di funzionamento dei caratteri jolly è la seguente:

   - Un punto interrogativo (?) rappresenta un singolo carattere.
   - L'asterisco (*) rappresenta un'intera stringa di caratteri.

   Ad esempio, per proteggere tutti i file con estensione ".sav", inserire *.sav. Per proteggere una selezione specifica di file con il nome progressivo (ad es. text1.doc, text2.doc, text3.doc), specificare ad esempio text?.doc.

È possibile ripetere questa procedura un numero qualsiasi di volte ed eliminare o modificare di nuovo le eccezioni presenti.

Avanzate

Facendo clic sul tasto **Esteso** stabilire inoltre quali altri controlli supplementari devono essere eseguiti dal Guardiano AntiVirus.

Solitamente qui non è necessario eseguire ulteriori impostazioni.

- **Modo**: qui è possibile definire se i file dovranno essere verificati solo in lettura o sia in lettura che in scrittura. Se la verifica è stata eseguita sulla scrittura di un file, al momento della creazione di un nuovo file o di una nuova versione del file verrà controllato se eventualmente un processo sconosciuto ha infettato questo file. Altrimenti i file vengono controllati soltanto quando vengono letti dai programmi.

- **Monitoraggio speciale cartelle critiche**: questa funzione consente di controllare in modo approfondito le cartelle particolarmente critiche, ad es. le cartelle condivise in rete, i dati personali o i servizi cloud (come Microsoft Dropbox OneDrive, Google Drive ecc.). Dopo avere selezionato gli elementi nella finestra di dialogo, questi verranno sempre monitorati nella modalità **Verifica durante la lettura e la scrittura**, indipendentemente dalle impostazioni applicate ad altri file, cartelle e directory. Se la modalità **Verifica durante la lettura e la scrittura** è stata selezionata per tutti i file, l'opzione di impostazione delle cartelle critiche appare disattivata.

- **Verifica degli accessi alla rete**: quando il computer è collegato in rete a computer non protetti (es. portatili sconosciuti), è utile verificare anche l'eventuale trasmissione di malware in seguito all'accesso alla rete. Se il computer viene usato come postazione di lavoro singola senza collegamento ad una rete, non è necessario attivare questa opzione. Anche qualora sia stata installata una protezione antivirus su tutti i computer della rete, si consiglia di disattivare l'opzione, poiché altrimenti alcuni file verrebbero controllati due volte, influenzando negativamente la velocità del PC.

- **Euristica**: con l'analisi euristica i virus non vengono rilevati solo sulla base del database antivirus aggiornato, distribuito da noi regolarmente online, bensì anche in base a determinate caratteristiche tipiche dei virus. Questo metodo fornisce un ulteriore livello di sicurezza, ma in taluni casi può generare falsi allarmi.

- **Controlla archivi**: la verifica dei dati compressi negli archivi (riconoscibili dall'estensione di file ZIP, RAR o anche PST) richiede molto tempo e può essere tralasciata quando il Guardiano AntiVirus è stato attivato in tutto il sistema. Per aumentare la velocità della scansione antivirus, è possibile limitare le dimensioni dei file di archivio da esaminare specificando un valore in kilobyte.

- **Verifica archivi e-mail**: poiché il software controlla già i messaggi e-mail in entrata e in uscita, nella maggioranza dei casi può essere utile tralasciare il periodico controllo degli archivi di posta poiché questa procedura può durare molti minuti in base alle dimensioni di tali file.

- **Scansione delle aree di sistema all'avvio**: solitamente è consigliabile includere le aree di sistema (ad es. i settori di avvio) del computer nel controllo antivirus. Questa opzione consente di determinare se queste aree devono essere controllate all'avvio del sistema oppure quando viene inserito un nuovo supporto (ad es. un nuovo CD-ROM). In genere, deve essere attivata almeno una di queste due funzioni.

- **Verifica le aree di sistema con cambio supporto**: solitamente è consigliabile includere le aree di sistema (ad es. i settori di avvio) del computer nel controllo antivirus. Questa opzione consente di determinare se queste aree devono essere controllate all'avvio del sistema oppure in caso di cambio di supporto (ad es. un nuovo CD-ROM). In genere, deve essere attivata almeno una di queste due funzioni.

- **Verifica la presenza di dialer/spyware/adware/riskware**: il software permette di verificare la presenza sul sistema di dialer e di altro malware. Si tratta di programmi che effettuano costose connessioni indesiderate a Internet e che per quanto riguarda il danno economico potenziale non hanno niente da invidiare ai virus, poiché registrano di nascosto i siti Internet visitati dall'utente o i dati immessi da tastiera (quindi anche le password) trasmettendoli alla prima occasione a terzi tramite Internet.

- **Controlla solo file nuovi o modificati**: attivando questa funzione, i file che non sono stati modificati da lungo tempo e che in precedenza risultavano privi di infezioni verranno ignorati. In questo modo si incrementano le prestazioni senza alcun rischio per la sicurezza.

Scansione antivirus manuale

Qui vengono definite le impostazioni di base per la Scansione antivirus.

Ciò non è necessario durante il normale utilizzo.

- **Usa motori**: il software utilizza due motori, ossia due programmi di scansione antivirus ottimizzati l'uno con l'altro. Nei computer di vecchia generazione, l'uso di un solo motore di scansione antivirus può velocizzare le prestazioni. Di regola, però, si consiglia di mantenere l'impostazione **Entrambi i motori**.

- **File infetti**: il software ha trovato un virus? A questo punto, nella configurazione standard, il programma chiede come si intende procedere con il virus e il file infetto. Se si desidera eseguire sempre la stessa azione, la si può impostare qui. La sicurezza massima

per i dati offre in questo caso l'impostazione **Disinfettare (se non è possibile: in quarantena)**.

- **Archivi infetti**: Qui è possibile decidere se i dati di archivio (quindi ad es. i file con estensione RAR, ZIP o PST) debbano essere trattati diversamente rispetto ai file normali. Tenere presente, tuttavia, che lo spostamento di un archivio in quarantena potrebbe danneggiarlo al punto tale da non poterlo più utilizzare, neppure se lo si ripristina dalla **Quarantena** nella posizione originaria.
- **In caso di carico del sistema, sospendere la scansione**: si consiglia di effettuare la scansione antivirus quando il computer non viene utilizzato. Nel caso non fosse possibile, selezionando questa voce, nel caso di carico del sistema la scansione antivirus resta in sospeso per lasciare il computer a disposizione dell'utente. La scansione antivirus riprende poi durante le pause di lavoro.

Eccezioni

Facendo clic sul pulsante Eccezioni è possibile escludere determinate unità, directory e file dalla verifica, accelerando pertanto il riconoscimento antivirus.

Procedere nel modo seguente:

1. Fare clic sul pulsante **Eccezioni**.
2. Fare clic nella finestra **Eccezioni per la scansione manuale del computer** su **Nuovo**.
3. Scegliere se si desidera escludere un'unità, una directory oppure un file e/o un tipo di file.
4. Selezionare quindi la directory o l'unità che si desidera proteggere. Per proteggere singoli file, inserire il nome file completo nel campo di immissione sotto la maschera file. In questo campo è possibile utilizzare i segnaposto.

   Nota: la modalità di funzionamento dei caratteri jolly è la seguente:

   - Un punto interrogativo (?) rappresenta un singolo carattere.
   - L'asterisco (*) rappresenta un'intera stringa di caratteri.

   Ad esempio, per proteggere tutti i file con estensione ".sav", inserire *.sav. Per proteggere una selezione specifica di file con il nome progressivo (ad es. text1.doc, text2.doc, text3.doc), specificare ad esempio text?.doc.

È possibile ripetere questa procedura un numero qualsiasi di volte ed eliminare o modificare di nuovo le eccezioni presenti.

Usa eccezioni anche per la scansione in modo inattivo: durante una scansione antivirus manuale il computer viene analizzato in modo mirato alla ricerca di virus e non dovrebbe essere utilizzato per altre attività. La Scansione in modo inattivo è una scansione antivirus intelligente che controlla costantemente l'eventuale presenza di virus in tutti i file del computer. La scansione in modo inattivo funziona come uno screensaver, ossia quando l'utente non usa il computer per un po' di tempo, e si interrompe immediatamente appena l'utente riprende a lavorare, per garantire prestazioni ottimali. Qui è possibile definire le eccezioni per file e directory anche per la scansione in modo inattivo.

Avanzate

Facendo clic sul pulsante "Avanzate" è possibile eseguire ulteriori impostazioni per la scansione antivirus.

Nella maggior parte dei casi, comunque, è sufficiente utilizzare le impostazioni predefinite.

- **Tipi di file**: consente di stabilire in quali tipi di file il software dovrà controllare la presenza di virus. L'opzione Solo file di programma e documenti offre alcuni vantaggi in merito alla velocità.
- **Euristica**: con l'analisi euristica i virus non vengono rilevati solo sulla base dei database antivirus, costantemente aggiornati, bensì anche grazie a determinate caratteristiche tipiche dei virus. Questo metodo fornisce un ulteriore livello di sicurezza, ma in taluni casi può generare falsi allarmi.
- **Controlla archivi**: la verifica dei dati compressi negli archivi (riconoscibili dall'estensione di file ZIP, RAR o anche PST) richiede molto tempo e può essere tralasciata quando il Guardiano AntiVirus è stato attivato in tutto il sistema. Per aumentare la velocità della scansione antivirus, è possibile limitare le dimensioni dei file di archivio da esaminare specificando un valore in kilobyte.
- **Verifica archivi e-mail**: permette di definire se eseguire la ricerca di infezioni anche negli archivi della posta elettronica.
- **Verifica aree di sistema**: solitamente è consigliabile includere le aree di sistema (ad es. i settori di avvio) del computer nel controllo antivirus.

- **Verifica la presenza di dialer/spyware/adware/riskware**: questa funzione permette di verificare la presenza sul sistema di dialer e di altro malware. Si tratta di programmi che effettuano costose connessioni indesiderate a Internet e che per quanto riguarda il danno economico potenziale non hanno niente da invidiare ai virus, poiché registrano di nascosto i siti Internet visitati dall'utente o i dati immessi da tastiera (quindi anche le password) trasmettendoli alla prima occasione a terzi tramite Internet.

- **Verifica la presenza di rootkit**: i rootkit cercano di sfuggire ai comuni metodi di riconoscimento dei virus. È sempre consigliabile eseguire un controllo supplementare alla ricerca di questi codici nocivi.

- **Controlla solo file nuovi o modificati**: attivando questa funzione, i file che non sono stati modificati da lungo tempo e che in precedenza risultavano privi di infezioni verranno ignorati. In questo modo si incrementano le prestazioni senza alcun rischio per la sicurezza.

- **Preparazione log**: selezionando questa casella di controllo, si richiede al programma di preparare un log per ogni sessione di scansione antivirus. Il log può essere visualizzato nell'area Protocolli.

- **Scansione antivirus per verifica supporto dati rimovibile**: selezionando questa casella, quando si collega al computer un supporto dati rimovibile (ossia chiavette USB, dischi fissi esterni ecc.), verrà chiesto se si desidera eseguire una scansione antivirus del dispositivo.

Aggiornamenti

Se non si riesce ad effettuare l'aggiornamento del software o dei database antivirus via Internet, in quest'area è possibile specificare tutti i dati necessari per effettuare un aggiornamento automatico. In Opzioni, inserite i vostri dati d'accesso (nome utente e password) ricevuti all'indirizzo e-mail indicato al momento della registrazione online del software. Tramite questi dati, ci si potrà collegare al server di aggiornamento G DATA e l'aggiornamento del database dei virus potrà avvenire automaticamente.

Se avete richiesto una nuova licenza e desiderate attivarla, selezionare **Attiva licenza**. Nelle **Impostazioni Internet** sono visualizzate opzioni speciali, necessarie solo in alcuni casi eccezionali (server proxy, altra regione). Se si incontrano difficoltà con l'aggiornamento dei database antivirus, disattivare temporaneamente la verifica della versione.

> **Gestione accessi:** Questa opzione permette di scegliere le connessioni Internet da usare per scaricare gli aggiornamenti del programma e altri aggiornamenti. È particolarmente utile quando a volte occorre collegarsi a una rete con trasmissione dati a pagamento, ad es. di piani tariffari per cellulari senza abbonamento flat.
>
> **Importa/Esporta database**: per i computer che non si collegano mai o raramente a Internet o per i quali esistono delle limitazioni sul volume di dati per il download, è possibile aggiornare i database antivirus anche tramite un supporto dati, ad es. una chiavetta USB, ossia si può eseguire un **Aggiornamento offline**. Da un computer collegato a Internet che possiede i diritti necessari, si possono esportare i database antivirus su un supporto dati, quindi importarli sul computer senza connessione Internet tramite la funzione "Importa da". In questo modo anche il sistema di questo computer sarà aggiornato con i database antivirus più recenti. Contrariamente agli aggiornamenti periodici dell'antivirus via Internet, è l'utente responsabile di eseguire gli aggiornamenti dei database il più spesso possibile.

Aggiornamento automatico del database antivirus

Se non si desidera che il software G DATA esegua automaticamente l'aggiornamento dei database antivirus, deselezionare questa opzione. Tuttavia, disattivando questa opzione il rischio per la sicurezza è elevato e pertanto si dovrebbe attuare solo in casi eccezionali. Se la distanza tra un aggiornamento e l'altro è troppo breve, è possibile personalizzarla e specificare, ad es. che gli aggiornamenti vengano eseguiti solo quando si instaura una connessione a Internet. Questa scelta ha senso, ad esempio, nei computer che non sono collegati in modo permanente a Internet.

Preparazione log: selezionando questa opzione, ogni aggiornamento del database antivirus viene registrato nel log, che può essere visualizzato nelle funzioni aggiuntive del software G DATA (in **SecurityCenter** sotto **Protocolli**). Oltre a questi voci, nel log vengono registrate ad es. le informazioni sui virus rilevati e su altre azioni eseguite dal programma.

Attiva licenza

Se non avete ancora registrato il vostro software G DATA, ora è possibile farlo e inserire il vostro numero di registrazione e i vostri dati cliente. In base al tipo di prodotto, il numero di registrazione si trova sul retro della copertina del manuale d'uso, nella e-mail di conferma in caso di download del programma o sulla busta del CD. Il prodotto viene attivato dopo l'inserimento del numero di registrazione.

Fare clic sul pulsante **Registrare** e i dati di accesso verranno generati sul server di aggiornamento. Se la registrazione avviene senza problemi, viene visualizzata una schermata informativa con la nota **La registrazione è stata eseguita correttamente**, che potrà essere chiusa facendo clic sul pulsante Chiudi.

> **Attenzione**: per la documentazione e per eventuali nuove installazioni del software, l'utente riceverà i dati di accesso anche via e-

mail. Verificare pertanto che l'indirizzo e-mail fornito all'atto della registrazione online sia corretto.

Infine, i dati di accesso verranno rilevati automaticamente nella maschera di inserimento originale e da questo momento sarà possibile aggiornare i database antivirus via Internet.

Non riuscite ad attivare la licenza? Se non si riesce ad effettuare la registrazione sul server, potrebbe dipendere dal server proxy. Fare clic sul pulsante **Impostazioni Internet**. Qui è possibile definire le impostazioni per la connessione Internet. Quando si verificano problemi con l'aggiornamento dei database antivirus, è opportuno controllare se si riesce ad accedere a Internet con un browser, ad esempio con Internet Explorer. Se non si riesce ad instaurare una connessione a Internet, è possibile che il problema dipenda dalla connessione e non dalle impostazioni del server proxy.

Impostazioni Internet

Se si utilizza un server proxy, selezionare l'opzione **Usa server proxy**. Questa impostazione deve essere modificata solo se l'aggiornamento Internet non funziona. Per conoscere l'Indirizzo proxy, rivolgersi all'amministratore del sistema oppure al fornitore dell'accesso a Internet. Se necessario, è possibile specificare anche i dati di accesso per il server proxy.

Server proxy: un server proxy riunisce le richieste alle reti e le distribuisce ai computer collegati. Quando, ad esempio, si utilizza il proprio computer in una rete aziendale, può essere opportuno accedere alla rete tramite un server proxy. Generalmente, quando si verificano problemi con l'aggiornamento dei database antivirus, si dovrebbe controllare innanzitutto se si riesce ad accedere a Internet con un browser. Se non si riesce ad instaurare una connessione a Internet, è possibile che il problema dipenda dalla connessione e non dalle impostazioni del server proxy.

Protezione Web

Quando è attivata la funzione Protezione Web, i contenuti Internet vengono controllati per l'eventuale presenza di software dannosi già in fase di navigazione. Sono disponibili le seguenti impostazioni.

- **Verifica contenuti Internet (HTTP)**: nelle opzioni di Protezione Web è possibile decidere che venga controllata la presenza di virus in tutti i contenuti Web HTTP già durante la navigazione. I contenuti Web infetti non vengono aperti e le pagine corrispondenti non vengono visualizzate. A tal fine, selezionare **Verifica contenuti Internet (HTTP)**.

  Se non si intendono verificare i contenuti Internet, il Guardiano AntiVirus interviene naturalmente durante l'esecuzione dei file infetti. proteggendo in questo modo il computer anche senza la verifica dei contenuti Internet.

  È possibile definire alcuni siti Web specifici come eccezioni quando si è certi che si tratta di siti sicuri. Per ulteriori informazioni, consultare il capitolo **Definisci eccezioni**. Selezionando il pulsante **Avanzate** è possibile eseguire ulteriori impostazioni in merito ai contenuti Internet.

- **Protezione da phishing**: con il cosiddetto Phishing gli impostori cercano di indirizzare su Internet i clienti di una determinata banca o di un determinato negozio a un sito web falsificato per rubare i loro dati. È consigliabile mantenere questa protezione da phishing attiva.

- **Invia indirizzi da pagine Internet infette**: tramite questa funzione è possibile segnalare automaticamente - ovviamente in modo anonimo - le pagine Internet valutate dal software come pericolose. In questo modo si ottimizza la sicurezza per tutti gli utenti.

- **Protezione browser BankGuard**: i trojan bancari sono una minaccia in costante crescita. I cybercriminali sviluppano ogni ora nuove tipologie di virus (come ZeuS, SpyEye) con lo scopo di sottrarvi del denaro. Le banche proteggono il traffico dati in Internet, tuttavia i dati vengono decodificati nel browser e qui vengono attaccati dai trojan bancari. La tecnologia all'avanguardia di G DATA BankGuard protegge le transazioni bancarie fin dall'inizio ed esattamente nel punto in cui avviene l'aggressione. Verificando in tempo reale l'integrità delle DLL di rete interessate, G DATA BankGuard garantisce che il vostro browser non verrà manipolato da un trojan bancario. È consigliabile lasciare sempre attivata la protezione di G DATA BankGuard.

  Informazioni: Oltre al metodo "man in the middle", con il quale l'aggressore manipola la comunicazione tra l'utente e il server di destinazione, esiste anche il metodo "man in the browser" (MITB). Con questo metodo l'aggressore infetta direttamente il browser e accede ai dati prima che questi vengano crittografati. Il modulo BankGuard protegge anche da questo tipo di attacchi, confrontando la cosiddetta impronta digitale di un file o di una parte di un sito Internet con un database in Internet. Ciò consente di scoprire immediatamente una truffa e il software G DATA sostituisce automaticamente la connessione fraudolenta con quella originale.

- **Protezione da keylogger**: in maniera indipendente dai database antivirus, la Protezione da keylogger monitora se le immissioni da tastiera vengono spiate nel sistema e impedisce agli aggressori di registrare le immissioni delle password. Questa funzione dovrebbe rimanere sempre attiva.

Definisci eccezioni

Per definire nella Whitelist una pagina Web come eccezione, procedere nel modo seguente:

1. Fare clic sul pulsante **Definisci eccezioni**. Viene aperta la finestra Whitelist. Qui vengono visualizzate le pagine Web già inserite e definite come sicure dall'utente.

2. Per aggiungere un'altra pagina Web, fare clic sul pulsante **Nuovo**. Si apre automaticamente una maschera di immissione. In **URL** specificare il nome del sito Web, ad esempio (www.gdata.de), e in **Osservazione** inserire eventualmente una nota sul motivo dell'eccezione applicata a tale sito. Confermare l'immissione facendo clic su **OK**.

3. Confermare ora con un clic su **OK** le modifiche apportate alla Whitelist.

Per eliminare una pagina Web dalla Whitelist, contrassegnarla con il mouse nell'elenco e fare clic sul pulsante **Elimina**.

Avanzate

Consente di determinare il numero di porta del server che dovrà essere sorvegliato dalla Protezione Web. In genere, per il monitoraggio di un normale browser è sufficiente specificare il numero di porta 80.

- **Evita timeout nel browser**: Poiché il software controlla il contenuto web prima di pubblicarlo nel browser Internet, talvolta a causa del volume elevato di dati tale operazione può richiedere tempi lunghi e di conseguenza il browser Internet, non ottenendo immediatamente i dati (il software non ha ancora concluso la verifica di routine dannose), potrebbe visualizzare un messaggio di errore. Marcando con una spunta la voce **Evita superamento del tempo nel browser**, questo messaggio di errore viene soppresso e, dopo avere verificato l'assenza di virus nei dati, questi vengono inviati normalmente al browser per la visualizzazione.

- **Attivazione di notifica durante il test di Download**: Attiva questa funzione per ricevere una notifica durante i download.

- **Limitare le dimensioni dei download**: Consente di vietare il controllo HTTP dei contenuti Web troppo grandi. I contenuti, in questo caso, vengono controllati dal Guardiano antivirus appena le eventuali routine nocive si attivano. La limitazione delle dimensioni ha il vantaggio di evitare rallentamenti nella navigazione causati dal controllo antivirus.

Verifica e-mail

La funzione Verifica E-Mail permette di controllare l'eventuale presenza di virus nelle e-mail in entrata e in uscita e nei relativi allegati e di bloccare le possibili infezioni direttamente all'origine. Se viene rilevato un virus, il software è in grado di eliminare direttamente gli allegati ai file o di riparare i file infetti.

> **Attenzione**: In Microsoft Outlook la verifica delle e-mail viene effettuata tramite un plugin, che offre la stessa protezione della funzione per POP3/IMAP disponibile tra le opzioni dell'AntiVirus. Dopo l'installazione del plugin, nel menu **Extra** di Outlook è disponibile la funzione **Verificare la presenza di virus nella cartella** che permette di controllare l'eventuale presenza di virus nelle cartelle di posta elettronica.

E-mail in entrata

Per la protezione antivirus delle e-mail in entrata sono disponibili le opzioni seguenti:

- **In caso di infezione**: consente di stabilire come procedere nel caso fosse rilevata una e-mail infetta. A seconda dell'utilizzo che si fa del proprio computer, sono possibili diverse impostazioni. Normalmente, si consiglia l'impostazione **Disinfettare (se non è possibile: eliminare allegato/testo)**.

- **Verificare le e-mail ricevute**: attivando questa opzione, tutte le mail ricevute sul proprio computer durante il lavoro vengono analizzate per controllare l'eventuale presenza di virus.

- **Allega rapporto alle e-mail infette ricevute**: se si è scelto di attivare il rapporto, quando viene rilevato un virus nella riga dell'oggetto della e-mail infetta compare l'avviso **VIRUS** e all'inizio del testo della e-mail la comunicazione **Attenzione! Questa e-mail contiene il seguente virus**, seguita dal nome del virus e dall'informazione se il virus è stato eliminato o se il file è stato o meno riparato.

E-mail in uscita

Per evitare di inviare dei virus accidentalmente, il software offre la possibilità di controllare la presenza di virus nelle e-mail prima dell'invio. Se si sta effettivamente inviando un virus (sebbene involontariamente), compare il messaggio **L'e-mail [riga oggetto] contiene il seguente virus: [nome virus]**. L'e-mail non viene inviata. Per controllare l'eventuale presenza di virus nelle e-mail in uscita, selezionare la casella **Verificare le e-mail prima dell'invio**.

Opzioni di scansione

In questo riquadro è possibile attivare o disattivare le opzioni di base per la Scansione antivirus:

- **Usa motori**: il software utilizza due motori antivirus, ossia due unità di analisi ottimizzate l'una con l'altra. In linea di principio, l'utilizzo dei due motori garantisce risultati ottimali durante la profilassi antivirus.
- **OutbreakShield**: consente di attivare l'OutbreakShield. Nel momento in cui OutbreakShield è attivo, il software genera dei checksum delle e-mail, li confronta con le blacklist antispam costantemente aggiornate in Internet ed è quindi in grado di reagire a un invio di massa, prima che siano disponibili i relativi database dei virus. OutbreakShield scandaglia in Internet le concentrazioni particolari di messaggi sospetti e chiude quasi in tempo reale il gap esistente fra l'inizio di un invio di e-mail di massa e la sua azione di contrasto per mezzo di un database antivirus ad hoc. L'OutbreakShield è integrato nel Antivirus per e-mail.

Connessioni crittografate (SSL)

Molti provider di posta elettronica, ad es. GMX, WEB.DE, T-Online e Freenet, hanno adottato la crittografia SSL. Perciò ora le email e gli account sono molto più sicuri. Tuttavia, è sempre necessario proteggere le email tramite un programma antivirus. G DATA offre a questo scopo il modulo **Connessioni crittografate (SSL)**. È inoltre possibile controllare l'eventuale presenza di virus e malware nelle email crittografate con SSL.

Per verificare con il software G DATA le email crittografate tramite SSL, è necessario importare nel programma di posta un certificato del software G DATA. In questo modo si permette al software G DATA di verificare tutte le email in entrata.

Sono supportati tutti i programmi di posta in grado di importare certificati o in grado di accedere all'archivio dei certificati di Windows, ad es.:

- Outlook 2003 o versione successiva
- Thunderbird
- The Bat
- Pegasusmail

Se il certificato di G DATA non si installa automaticamente, procedere nel modo seguente:

1. Durante l'installazione del certificato, i programmi di posta non devono essere attivi. Chiudere quindi tutti i programmi di posta prima di creare e installare il certificato.
2. Nel software G DATA, selezionare l'opzione Verifica connessioni SSL.
3. Fare clic sul pulsante Esporta certificato. Il software G DATA crea ora un nuovo certificato. Questo file si chiama GDataRootCertificate.crt.
4. Aprire ora il file GDataRootCertificate.crt. Si apre una finestra di dialogo che permette di installare il certificato sul computer.
5. Nella finestra di dialogo, fare clic sul pulsante **Installa certificato** e seguire le istruzioni della procedura di installazione.

Fatto. Ora Outlook e tutti gli altri programmi di posta in grado di accedere all'archivio certificati di Windows contengono il certificato necessario per verificare virus e malware anche nelle email crittografate con SSL.

Nota: Se si utilizza **Thunderbird (portable)** e il certificato non è stato importato automaticamente, è necessario importarlo successivamente e gestire le impostazioni di affidabilità del certificato G DATA creato. Per far ciò, in Thunderbird (portable), in **Impostazioni > Avanzate > Certificati**, selezionare il pulsante **Certificati**. Facendo clic qui vengono visualizzate varie schede. Scegliere la scheda **Creazione certificato**, quindi il pulsante **Importa**. Ora è possibile selezionare il certificato **G DATA Mail Scanner Root**.

Selezionare con un segno di spunta le seguenti opzioni e fare clic su OK. Thunderbird portable verrà ora protetto da G DATA:

- **Considera affidabile questo CA per identificare il sito web.**

- **Considera affidabile questo CA per identificare l'utente email.**
- **Considera affidabile questo CA per identificare lo sviluppatore del software**.

Negli altri programmi di posta esistono funzioni simili per importare i certificati. In caso di dubbi, consultare la guida in merito alla procedura da seguire per il programma di posta utilizzato.

Avanzate

Se durante l'utilizzo dei programmi di posta elettronica non vengono utilizzate le porte standard, è possibile indicare alla voce **Numero porta server** anche la porta utilizzata per le e-mail in entrata o in uscita. Mediante il pulsante **Standard** è possibile ripristinare automaticamente i numeri di porte standard. È anche possibile specificare più porte. Separare le porte con una virgola.

Attenzione: Microsoft Outlook viene protetto tramite un plugin speciale col quale è possibile scansionare direttamente da Outlook le cartelle e i messaggi. Per eseguire in Outlook la scansione antivirus di un messaggio o di una cartella, fare clic sull'icona di G DATA e verrà eseguita una scansione virus della cartella messaggi selezionata.

Dato che il software elabora le e-mail in entrata prima del programma di posta, nel caso di traffico molto alto o connessioni lente può capitare che compaia un messaggio di errore del programma di posta. Questa notifica è dovuta al fatto che il server non riceve immediatamente i dati di posta in quanto questi vengono sottoposti a verifica dal software per rilevare l'eventuale presenza di virus. Selezionando la casella di controllo **Non superare il tempo limite sul Mail Server**, viene eliminato questo messaggio di errore e, dopo aver verificato l'assenza di virus nei dati, questi vengono normalmente inviati dal software al programma di posta.

Verifica automatica virus

Consente di attivare e disattivare la Scansione in modo inattivo. In questo modo, anziché eseguire le verifiche periodiche, è possibile analizzare il computer o specifiche aree del computer alla ricerca di infezioni. Si possono, ad esempio, eseguire queste verifiche quando il computer non è in uso.

Scansioni antivirus pianificate: in molti casi una scansione in modo inattivo del computer è sufficiente. Con il tasto **Nuovo** è possibile creare anche diversi controlli antivirus automatici indipendenti fra loro. Ad esempio, si può controllare quotidianamente la cartella Download, mentre la collezione di MP3 può essere controllata solo una volta al mese.

Nei capitoli successivi verrà spiegato come creare scansioni antivirus personalizzate.

Generale

Qui è possibile definire il nome da assegnare alla nuova scansione antivirus automatica impostata. Per distinguere meglio, si consiglia di usare nomi significativi, ad esempio *Dischi rigidi locali (scansione settimanale)* oppure *Archivi (scansione mensile)*.

Selezionando **Spegnere il computer al termine del processo**, il computer viene spento automaticamente una volta eseguita la scansione antivirus automatica. Questa opzione è utile, ad esempio, quando si desidera eseguire la scansione antivirus in ufficio dopo l'orario lavorativo.

Job: con job si definisce qualsiasi attività automatica di verifica del computer o di determinate aree.

Ampiezza analisi

Questa scheda consente di specificare se la scansione per la ricerca dei virus deve avvenire sulle unità disco rigido locali, se devono essere esaminate le aree di memoria o di avvio automatico o se si desidera verificare soltanto particolari directory e file. In quest'ultimo caso, indicare le directory prescelte mediante il pulsante **Selezione**.

Selezione di directory/file: Nella struttura delle directory, a sinistra, è possibile con un clic del mouse sul simbolo + aprire e selezionare le directory e visualizzarne il contenuto nella vista dei file. Ogni directory o file provvisto di un segno di spunta viene controllato dal programma. Se in una directory non vengono controllati tutti i file, tale directory presenta un segno di spunta di colore grigio.

Pianificazione

Questa scheda permette di definire quando e con quale frequenza debba avere luogo il relativo job. In **Esegui** indicare l'impostazione e indicare in **Data/ora** quando deve venir eseguita. Se si seleziona **All'avvio del sistema** non occorre specificare alcuna indicazione temporale e il software esegue la scansione ogni volta che il computer viene riavviato.

- **Esegui job quando il computer non è acceso all'avvio**: attivando questa opzione, le verifiche automatiche dei virus non riprendono automaticamente ogni volta che si avvia il computer.
- **Non eseguire con funzionamento a batteria**: Per non ridurre inutilmente la durata della batteria, è possibile definire per i notebook che le verifiche automatiche dei virus avvengano soltanto quando il portatile è collegato alla rete elettrica.

Impostazioni di scansione

In quest'area è possibile definire come dovrà avvenire la scansione antivirus automatica.

- **Usa motori**: il software utilizza due motori, ossia due programmi di scansione antivirus ottimizzati l'uno con l'altro. Nei computer di vecchia generazione, l'uso di un solo motore di scansione antivirus può velocizzare le prestazioni. Di regola, però, si consiglia di mantenere l'impostazione **Entrambi i motori**.
- **File infetti**: il software ha trovato un virus? A questo punto, nella configurazione standard, il programma chiede come si intende procedere con il virus e il file infetto. Se si desidera eseguire sempre la stessa azione, la si può impostare qui. La sicurezza massima per i dati offre in questo caso l'impostazione **Disinfettare (se non è possibile: in quarantena)**.
- **Archivi infetti**: qui è possibile decidere se i dati di archivio (quindi ad es. i file con estensione RAR, ZIP o PST) debbano essere trattati diversamente rispetto ai file normali. Tenere presente, tuttavia, che lo spostamento di un archivio in quarantena potrebbe danneggiarlo al punto tale da non poterlo più utilizzare, neppure se lo si ripristina nella posizione originaria.

Facendo clic sul tasto **Avanzate** è possibile stabilire quali altri controlli antivirus supplementari devono essere eseguiti dal Guardiano AntiVirus.

Nella maggior parte dei casi, comunque, è sufficiente utilizzare le impostazioni predefinite.

- **Tipi di file**: consente di stabilire in quali tipi di file il software dovrà controllare la presenza di virus.
- **Euristica**: con l'analisi euristica i virus non vengono rilevati solo sulla base dei database antivirus del software, costantemente aggiornati, bensì anche grazie a determinate caratteristiche tipiche dei virus. Questo metodo fornisce un ulteriore livello di sicurezza, ma in taluni casi può generare falsi allarmi.
- **Controlla archivi**: la verifica dei dati compressi negli archivi (riconoscibili dall'estensione di file ZIP, RAR o anche PST) richiede molto tempo e può essere tralasciata quando il Guardiano AntiVirus è stato attivato in tutto il sistema. Quando si decomprimono gli archivi, il Guardiano antivirus riconosce i virus fino ad allora nascosti e ne impedisce automaticamente la propagazione.
- **Verifica archivi e-mail**: permette di definire se eseguire la ricerca di infezioni anche negli archivi della posta elettronica.
- **Verifica aree di sistema**: solitamente è consigliabile includere le aree di sistema (ad es. i settori di avvio) del computer nel controllo antivirus.
- **Verifica la presenza di dialer/spyware/adware/riskware**: con questa funzione è possibile verificare la presenza nel sistema di dialer e di altri software dannosi (spyware, adware e riskware). Si tratta di programmi che effettuano costose connessioni indesiderate a Internet e registrano di nascosto i siti Internet visitati dall'utente o i dati immessi da tastiera (quindi anche le password), trasmettendoli alla prima occasione a terzi.
- **Verifica la presenza di rootkit**: i rootkit cercano di sfuggire ai comuni metodi di riconoscimento dei virus. È sempre consigliabile eseguire un controllo supplementare alla ricerca di questi codici nocivi.
- **Preparazione log**: selezionando questa casella di controllo, si richiede al programma di preparare un log per ogni sessione di scansione antivirus. Il log può essere visualizzato nell'area **Protocolli**.

Account utente

Qui è possibile definire l'account utente sul computer che si desidera sottoporre alla scansione antivirus. Questo account è necessario per accedere alle unità di rete.

Antispam

Filtro antispam

Il filtro antispam prevede molte possibilità d'impostazione per bloccare in modo efficace messaggi e-mail con contenuti indesiderati oppure da mittenti indesiderati, ad es. nel caso di e-mail di massa. Il programma verifica molti aspetti dei messaggi e-mail tipici dello spam. In base alla caratteristiche corrispondenti, il sistema calcola un valore che riflette la probabilità di spam. Tramite il pulsante **Usa filtro antispam** si attiva o si disattiva il filtro antispam.

Per attivare o disattivare i diversi tipi di filtro antispam, impostare o eliminare semplicemente la spunta dalla relativa voce. Per eseguire delle modifiche nei diversi tipi di filtri, fare clic sulla relativa voce. Verrà aperta una finestra di dialogo per la modifica dei parametri. Sono disponibili le seguenti opzioni di impostazione:

- **Spam OutbreakShield**: OutbreakShield è in grado di riconoscere e combattere i parassiti presenti nella posta elettronica massiva già prima che siano disponibili i database antivirus aggiornati. OutbreakShield scandaglia in Internet le concentrazioni particolari di messaggi sospetti e chiude quasi in tempo reale il gap esistente fra l'inizio di un invio di mail di massa e la sua azione di contrasto per mezzo di un database antivirus ad hoc. Se si utilizza un computer con un server proxy, fare clic sul pulsante **Impostazioni Internet** ed eseguire le modifiche necessarie. Queste impostazioni devono essere modificate solo se OutbreakShield presenta dei problemi.

- **Usa whitelist**: La whitelist permette di escludere esplicitamente determinati indirizzi mittente o domini dal sospetto di spam. Inserire nel campo **Indirizzi/Domini** l'indirizzo e-mail desiderato (ad es. *newsletter@informationsseite.de*) oppure il dominio (ad es. *informationsseite.de*) che deve essere eliminato dal sospetto spam in modo tale che il software G DATA non consideri le e-mail provenienti da questo mittente o da questo dominio mittente come spam.

  Con il pulsante **Importa** è inoltre possibile inserire nella whitelist alcune liste predefinite di indirizzi e-mail o domini. In questa lista gli indirizzi e i domini devono essere riportati in righe distinte, l'uno sotto l'altro. Come formato viene utilizzato un semplice file txt che può essere generato anche con Blocco Note di Windows. Con il pulsante **Esporta** le whitelist di questo tipo possono essere esportate come file di testo.

- **Usa blacklist**: mediante la blacklist è possibile definire esplicitamente determinati indirizzi di mittenti o domini come sospetto spam. Inserire nel campo **Indirizzi/Domini** l'indirizzo e-mail desiderato (ad es. *newsletter@megaspam.de.vu*) oppure il dominio (ad es. *megaspam.de.vu*) che deve essere incluso nel sospetto di spam in modo tale che il software G DATA consideri le e-mail provenienti da questo mittente o da questo dominio mittente generalmente come e-mail con elevata probabilità di spam. Con il pulsante **Importa** è inoltre possibile inserire nella blacklist alcune liste predefinite di indirizzi e-mail o domini. In questa lista gli indirizzi e i domini devono essere riportati in righe distinte, l'uno sotto l'altro. Come formato viene utilizzato un semplice file txt che può essere generato anche con Blocco Note di Windows. Mediante il pulsante **Esporta**, una blacklist di questo tipo può essere esportata come file di testo.

- **Usa Realtime Blacklist (impostazione predefinita)**: in Internet sono disponibili delle liste che contengono gli indirizzi IP dei server tramite i quali viene notoriamente inviato dello spam. Il software G DATA determina tramite query alle Realtime Blacklist se il server del mittente è presente nelle liste. Se la risposta è sì, la probabilità di spam aumenta. Si raccomanda di utilizzare l'impostazione standard; è tuttavia possibile inserire nelle blacklist 1, 2 e 3 degli indirizzi propri per le blacklist.

- **Usa parole chiave (Testo messaggio)**: Mediante l'elenco di parole chiave è possibile classificare i messaggi come sospetto spam anche in base alle parole utilizzate nel testo della e-mail. Se almeno uno dei termini di ricerca appare nel testo del messaggio, aumenta la probabilità di spam. Questa lista può essere modificata a piacere utilizzando i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. Mediante il pulsante **Importa** è possibile inserire delle liste predefinite di parole chiave nella propria lista. In un elenco del genere gli inserimenti devono essere riportati in righe distinte, l'una sotto all'altra. Come formato viene utilizzato un semplice file txt che può essere generato anche con Blocco Note di Windows. Con il pulsante **Esporta** le liste di questo tipo possono essere esportate come file di testo. Inserendo un segno di spunta davanti a **Cerca solo parole complete** è possibile stabilire che il software G DATA cerchi nella riga dell'oggetto di un'e-mail solo parole complete.

- **Usa parole chiave (Oggetto)**: mediante l'elenco di parole chiave è possibile classificare le e-mail come sospetto spam anche sulla base delle parole presenti nella riga dell'oggetto. Se almeno uno dei termini di ricerca appare nella riga dell'oggetto, aumenta la probabilità di spam.

- **Usa filtro contenuti**: il Filtro dei contenuti è un filtro ad autoapprendimento che calcola la probabilità di spam in base alle parole usate nel testo dell'e-mail. Il filtro non opera solo sulla base di elenchi di parole fisse, ma integra la sua conoscenza con ogni e-mail ricevuta. Mediante il pulsante **Interroga i contenuti della tabella** si possono visualizzare gli elenchi di parole che il filtro dei

contenuti utilizza per classificare un'e-mail come spam. Mediante il pulsante **Ripristina tabella** si eliminano tutti i contenuti di tabella appresi e il filtro dei contenuti con autoapprendimento riavvia il processo di apprendimento dall'inizio.

Reazione

Qui è possibile stabilire come il filtro antispam dovrà comportarsi in presenza di e-mail che possono contenere spam. È possibile impostare tre livelli in base ai quali il software G DATA valuterà la probabilità che l'email interessata contenga spam.

- **Sospetto di spam**: consente di definire come dovranno essere trattati i messaggi in cui il software G DATA trova singoli elementi di spam. In questi casi può anche non trattarsi di spam, bensì di e-mail provenienti da newsletter o mailing list che sono gradite al destinatario. In questo caso si raccomanda di avvertire il destinatario del sospetto spam.
- **Alta probabilità di spam**: qui vengono raggruppati i messaggi che riuniscono in sé molte caratteristiche e che molto raramente sono graditi al destinatario.
- **Probabilità di spam molto alta**: qui si trovano i messaggi che corrispondono a tutti i criteri di un messaggio spam. In questo caso non si tratta quasi mai di e-mail desiderate e nella maggior parte dei casi è raccomandabile rifiutare e-mail del genere.

Ognuno di questi tre gradi di reazione può essere configurato individualmente. Fare clic sul pulsante **Modifica** e definire la reazione che verrà adottata dal software G DATA. In questo modo, con l'opzione **Rifiuta messaggio di posta**, si può impedire che l'e-mail arrivi nella casella di posta. L'opzione **Inserisci avviso spam nell'oggetto e nel testo dell'email** permette di contrassegnare come spam i messaggi che sono stati identificati come tali, in modo da poterli ad es. eliminare più facilmente. Se si utilizza **Microsoft Outlook** (Attenzione: non confonderlo con Outlook Express o Windows Mail), è anche prevista la possibilità di spostare le e-mail che hanno suscitato il sospetto di spam in una cartella definita dall'utente all'interno della propria casella di posta (**Sposta la posta nella cartella**). Questa cartella può essere creata direttamente tramite il software G DATA specificandone il nome in **Nome cartella**.

> **Nota**: Anche se non si utilizza Outlook è possibile spostare i messaggi identificati come spam in una cartella. Inserire un avvertimento nella riga dell'oggetto (ad es. "*[Spam]*") e creare nel proprio programma di posta elettronica una regola per spostare in un'altra cartella le e-mail con questo testo nella riga dell'oggetto.

Impostazioni avanzate

In quest'area è possibile modificare in modo dettagliato il riconoscimento spam del software G DATA e adattarlo alle caratteristiche del proprio traffico e-mail. Di regola si raccomanda però di utilizzare le impostazioni standard. Nelle impostazioni avanzate è possibile apportare modifiche soltanto se si ha dimestichezza con l'argomento e si sa esattamente cosa si fa.

Altri filtri

I filtri riportati di seguito sono impostati per default; tuttavia, in caso di necessità, si possono disattivare rimuovendo il segno di spunta.

- **Disattiva script HTML**
- **Filtrare allegati pericolosi**

È possibile creare nuove regole del filtro tramite il pulsante **Nuovo** oppure modificare filtri già esistenti tramite il pulsante **Modifica**. I filtri creati vengono visualizzati nell'elenco dei filtri e possono essere selezionati o deselezionati mediante le caselle a sinistra di ogni voce. Quando una casella di spunta è selezionata, il filtro corrispondente è attivo. Quando una casella di spunta non è selezionata, il filtro corrispondente non è attivo. Per eliminare definitivamente un filtro, selezionarlo facendo clic con il mouse, quindi scegliere il pulsante **Elimina**.

Tra le opzioni sono disponibili filtri aggiuntivi di supporto al filtro antispam vero e proprio del software G DATA che semplificano le impostazioni personalizzate. Il filtro antispam prevede molte possibilità d'impostazione per bloccare in modo efficace messaggi e-mail con contenuti indesiderati oppure da mittenti indesiderati, ad es. nel caso di e-mail di massa. Il programma verifica molti aspetti dei messaggi e-mail tipici dello spam. In base alla caratteristiche corrispondenti, il sistema calcola un valore che riflette la probabilità di spam. Sono pertanto disponibili varie schede che contengono tutte le impostazioni rilevanti suddivise per argomento.

Quando si imposta un nuovo filtro, viene visualizzata una finestra di selezione che consente d'impostare il tipo di filtro base. Tutte le altre indicazioni per la creazione del filtro vengono specificate in una finestra di procedura guidata che varia a seconda del tipo di filtro. In questo modo è possibile creare facilmente filtri per ogni tipo di minaccia prevista.

- **Disattivazione degli script HTML**: Questo filtro disattiva gli script nella parte HTML di un'e-mail. Gli script, utili in una pagina Internet, possono invece essere molto fastidiosi se inseriti nella parte HTML di un'e-mail. In alcuni casi gli script HTML vengono attivamente utilizzati per infettare i computer, poiché possono essere attivati non solo con l'apertura di un allegato infetto ma anche con la sola visione dell'anteprima di un'e-mail.

- **Filtrare allegati pericolosi**: Per filtrare gli allegati delle e-mail (= attachments) sono disponibili numerose opzioni. Gran parte dei virus inclusi nelle e-mail si diffonde tramite questi allegati, che nella maggior parte dei casi contengono file eseguibili più o meno nascosti. Può trattarsi di un classico file EXE che contiene un programma nocivo, ma anche di uno script VB che talvolta può nascondersi in un presunto file sicuro di immagini, filmati o musica. In generale, nell'esecuzione degli allegati di posta si dovrebbe prestare molta attenzione e, in caso di dubbio, si consiglia di chiedere al mittente dell'e-mail prima di aprire un file che non sia stato espressamente richiesto.

  In **Estensione dei file** è possibile elencare i suffissi dei file ai quali si desidera applicare un filtro. È possibile, ad esempio, raccogliere tutti i file eseguibili (file EXE e COM) in un unico filtro, ma è possibile filtrare anche altri formati (ad es. MPEG, AVI, MP3, JPEG, JPG, GIF ecc.) se per le loro dimensioni causano un sovraccarico del server di posta. Naturalmente è possibile applicare un filtro anche ai file di archivio, come i file ZIP, RAR e CAB. Separare le estensioni dei file di un gruppo di filtri tramite punto e virgola.

  La funzione **Filtrare anche allegati nelle e-mail integrate** permette di applicare il filtro specificato per determinate **estensioni dei file** anche agli allegati presenti nelle e-mail. Questa opzione dovrebbe essere generalmente attivata.

  Tramite l'opzione **Rinominare solo gli allegati**, gli allegati da filtrare non vengono eliminati automaticamente, bensì solo rinominati. Ciò è utile, ad esempio, nel caso di file eseguibili come EXE e COM, ma anche per i file di Microsoft Office che potrebbero contenere script eseguibili e macro. La ridenominazione di un allegato fa sì che questo non possa essere aperto inavvertitamente con un clic del mouse, bensì il destinatario deve prima salvare il file ed eventualmente rinominarlo nuovamente prima di poterlo utilizzare. Se non è stata selezionata l'opzione **Rinominare solo gli allegati**, gli allegati verranno eliminati direttamente.

  In **Suffisso**, digitare la stringa di caratteri con la quale estendere il reale suffisso del file (ad esempio .exe_danger). In questo modo si impedisce che il file venga eseguito con un semplice clic del mouse. L'opzione **Inserire il messaggio nel testo della e-mail** permette di avvisare il destinatario dell'e-mail filtrata che un allegato è stato eliminato o rinominato in base ad una regola filtro.

- **Filtro dei contenuti**: il filtro dei contenuti permette di bloccare comodamente i messaggi che contengono determinati argomenti o testo.

  In **Criterio di ricerca** inserire le parole chiave e le espressioni a cui deve reagire il software G DATA. In questo caso il testo può essere liberamente collegato tramite gli operatori logici AND e OR.

  In **Campo di ricerca** indicare in quali aree di un'e-mail devono essere ricercate queste espressioni. Per **Intestazione** si intende quell'area di un messaggio che contiene l'indirizzo e-mail del mittente e del destinatario e le informazioni relative a programmi, protocolli e dati di invio utilizzati. Invece, selezionando il campo **Oggetto**, viene verificata solo la riga dell'oggetto senza ulteriori informazioni testuali dell'intestazione. In **Testo e-mail** è inoltre possibile scegliere se l'area di ricerca si deve limitare ai semplici messaggi di testo o estendersi anche al testo nei messaggi HTML (testo HTML).

  In **E-mail integrate** si può indicare se la ricerca del filtro dei contenuti debba estendersi anche alle e-mail che sono disponibili come allegato delle e-mail ricevute.
  In **Reazione** è possibile specificare come dovranno essere gestite dal software G DATA le e-mail individuate come spam. Tramite **Rifiuta messaggio di posta** l'e-mail non verrà neppure presa in considerazione dal programma di posta.

  Selezionando l'opzione **Inserire un avviso nell'oggetto e nel testo del messaggio**, è possibile inserire un avviso prima del testo vero e proprio della riga dell'oggetto (Prefisso nella riga dell'oggetto), ad es. *Spam* o *Attenzione*. In alternativa è anche possibile specificare un testo che verrà anteposto al testo vero e proprio del messaggio qualora vi sia il sospetto che si tratti di spam (Messaggio nel testo).

  Se si utilizza *Microsoft Outlook* (**Attenzione**: non confonderlo con Outlook Express o Windows Mail), è anche prevista la possibilità di spostare le e-mail che hanno suscitato il sospetto di spam in una cartella definita dall'utente all'interno della propria casella di posta (**Sposta la posta nella cartella**). Questa cartella può essere creata direttamente tramite il software G DATA specificandone il nome in **Nome cartella**.

- **Filtro mittente**: mediante il filtro mittente è possibile bloccare facilmente le e-mail provenienti da determinati mittenti. Specificare in **Mittente/Dominio** gli indirizzi e-mail o i nomi di dominio ai quali dovrà reagire il software G DATA. In presenza di voci multiple, separarle con punto e virgola.

  In **Reazione** è possibile specificare come dovranno essere gestite dal software G DATA le e-mail individuate come spam.

  Tramite **Rifiuta messaggio di posta** l'e-mail non verrà neppure presa in considerazione dal programma di posta.

  Selezionando l'opzione **Inserire un avviso nell'oggetto e nel testo del messaggio**, è possibile inserire un avviso prima del testo vero e proprio della riga dell'oggetto (Prefisso nella riga dell'oggetto), ad es. *Spam* o *Attenzione*. In alternativa è anche possibile specificare un testo che verrà anteposto al testo vero e proprio del messaggio qualora vi sia il sospetto che si tratti di spam (Messaggio nel testo).

  Se si utilizza *Microsoft Outlook* (**Attenzione**: non confonderlo con Outlook Express o Windows Mail), è anche prevista la possibilità di

spostare le e-mail che hanno suscitato il sospetto di spam in una cartella definita dall'utente all'interno della propria casella di posta (**Sposta la posta nella cartella**). Questa cartella può essere creata direttamente tramite il software G DATA specificandone il nome in **Nome cartella**.

- **Filtro lingua**: il Filtro lingua consente di definire automaticamente come spam i messaggi di posta in determinate lingue. Se ad esempio non si hanno solitamente contatti via e-mail con persone che parlano inglese, è possibile filtrare molti messaggi e-mail di spam definendo l'inglese come lingua di spam. Selezionare in questa finestra le lingue per le quali si ritiene di non avere contatti regolari tramite e-mail: il software G DATA considererà con maggiore probabilità queste e-mail come spam.

  In **Reazione** è possibile specificare come dovranno essere gestite dal software G DATA le e-mail individuate come spam.

  Tramite **Rifiuta messaggio di posta** l'e-mail non verrà neppure presa in considerazione dal programma di posta.

  Selezionando l'opzione **Inserire un avviso nell'oggetto e nel testo del messaggio**, è possibile inserire un avviso prima del testo vero e proprio della riga dell'oggetto (Prefisso nella riga dell'oggetto), ad es. *Spam* o *Attenzione*. In alternativa è anche possibile specificare un testo che verrà anteposto al testo vero e proprio del messaggio qualora vi sia il sospetto che si tratti di spam (Messaggio nel testo).

  Se si utilizza *Microsoft Outlook* (**Attenzione**: non confonderlo con Outlook Express o Windows Mail), è anche prevista la possibilità di spostare le e-mail che hanno suscitato il sospetto di spam in una cartella definita dall'utente all'interno della propria casella di posta (**Sposta la posta nella cartella**). Questa cartella può essere creata direttamente tramite il software G DATA specificandone il nome in **Nome cartella**.

Varie

In quest'area è possibile effettuare modifiche aggiuntive.

- **Verificare i messaggi non letti nella cartella di posta in arrivo all'avvio del programma**: *Solo per Microsoft Outlook*: questa opzione consente di controllare offline che le e-mail ricevute non contengano spam. All'avvio di Outlook vengono quindi controllate tutte le e-mail non lette presenti nella cartella Posta in arrivo e nelle rispettive sottocartelle del software G DATA.

- **Altri programmi di posta (utilizzo di POP3)**: le e-mail ricevute tramite POP3 non possono essere eliminate direttamente per motivi tecnici. Quando un filtro deve rifiutare un messaggio di posta, il sistema aggiunge un testo sostitutivo al messaggio. Il testo sostitutivo per i messaggi rifiutati è il seguente: **Messaggio rifiutato**. È possibile inoltre personalizzare il testo di questa funzione di notifica. Nel testo personalizzabile, per l'**Oggetto** e per il **Testo e-mail** sono a disposizione i seguenti segnaposto (definiti con un segno di percentuale e una lettera minuscola associata):

  %s Mittente

  %u Oggetto

Nel programma di posta è possibile definire una regola che elimini automaticamente le e-mail con il testo sostitutivo qui definito.

Firewall

Automatismo

Se non si desidera occuparsi delle impostazioni del firewall, si può lasciare l'impostazione Pilota automatico. Oltre alla modalità Pilota automatico, che per molti utenti rappresenta la scelta migliore, sono disponibili numerose opzioni che permettono di configurare il firewall G DATA nel modo ottimale secondo le proprie esigenze.

Nelle impostazioni del firewall vi sono due aree principali che possono essere configurate singolarmente:

Pilota automatico

Qui è possibile definire se il firewall dovrà agire in autonomia e con autoapprendimento, senza interpellare l'utente sulle decisioni in merito al blocco o all'autorizzazione delle richieste provenienti da Internet, oppure se in caso di dubbio l'utente verrà interpellato.

- **Pilota automatico**: Il firewall funziona in modo autonomo e protegge automaticamente il PC da qualsiasi pericolo. Questa impostazione garantisce una protezione completa ed è consigliabile per la maggior parte degli utilizzi.

- **Creazione manuale della serie di regole**: se si desidera configurare individualmente il proprio firewall, è possibile adattare la protezione firewall alle proprie esigenze usando la creazione manuale delle regole.

- **Modo Pilota automatico quando si avvia un'applicazione a pieno schermo**: proprio con i giochi per computer (e altre applicazioni a pieno schermo) può risultare fastidioso se il firewall interrompe il flusso del gioco chiedendo varie conferme o se ostacola la

visualizzazione. Per giocare indisturbati ma senza compromettere la sicurezza, il pilota automatico è l'impostazione ideale poiché sopprime le richieste del firewall. Se il pilota automatico non è impostato come predefinito, questa funzione permette di attivarlo automaticamente ogni volta che si usa un programma con modalità a pieno schermo.

Impostazioni di sicurezza personalizzate

Mentre si usa il computer per il lavoro quotidiano, il firewall impara progressivamente a conoscere i programmi utilizzati per l'accesso a Internet, i programmi che non vengono utilizzati mai e i programmi che rappresentano un rischio per la sicurezza. Grazie ai gradi di protezione predefiniti, è possibile impostare il firewall in modo da andare incontro alle proprie esigenze, senza tuttavia la necessità di avere competenze specifiche ed eseguire procedure amministrative. Tramite il cursore di scorrimento, impostare il grado di protezione desiderato. Sono disponibili i seguenti gradi di protezione:

- **Massima protezione**: le regole per il firewall vengono create in base a criteri molto sofisticati ed è necessario conoscere i termini tecnici specifici della rete (TCP, UDP, porte ecc.). Il firewall rileva ogni minima variazione e durante la fase di apprendimento richiederà spesso l'intervento dell'utente.
- **Protezione alta**: le regole per il firewall vengono create in base a criteri molto sofisticati ed è necessario conoscere i termini tecnici specifici della rete (TCP, UDP, porte ecc.). In determinate situazioni, durante la fase di apprendimento il firewall richiede spesso l'intervento dell'utente.
- **Protezione normale**: le regole per il firewall vengono create solo a livello di applicazioni e la procedura guidata si occupa dei dettagli specifici della rete. Durante la fase di apprendimento, l'utente deve intervenire in maniera limitata.
- **Protezione bassa**: le regole per il firewall vengono create solo a livello di applicazioni e la procedura guidata si occupa dei dettagli specifici della rete. Durante la fase di apprendimento, l'utente deve intervenire solo raramente. Anche con questo grado, la protezione nei confronti delle richieste di collegamento in entrata resta elevata.
- **Firewall disattivato**: in caso di necessità, è anche possibile disattivare il firewall. Il computer resta collegato ad Internet e alle altre reti, tuttavia non è più protetto dal firewall contro attacchi e azioni di spionaggio.

Se si desidera impostare il firewall in maniera ancora più specifica, selezionare l'opzione **Impostazioni di sicurezza personalizzate**. Per eseguire queste impostazioni, tuttavia, è necessario possedere almeno una conoscenza di base in materia di protezione della rete.

Richieste

Questa scheda consente di specificare quando, come e se il firewall debba richiedere conferma all'utente non appena un programma tenta di stabilire un collegamento a Internet o alla rete.

Crea una regola

Quando il firewall rileva una connessione con la rete, il sistema visualizza una finestra informativa nella quale è possibile stabilire come procedere con la relativa applicazione. Tramite questa funzione è possibile consentire o vietare l'accesso a una rete.

- **Applicazione**: consente di concedere o rifiutare l'accesso alla rete per l'applicazione attualmente visualizzata, generalmente su ciascuna porta e con ciascun protocollo di trasmissione (ad es. TCP o UDP).
- **Protocollo/porta/applicazione**: l'applicazione che richiede l'accesso alla rete riceve l'autorizzazione solo con il protocollo FTP ottenuto e accede online esclusivamente attraverso la porta ottenuta. Se la stessa applicazione richiedesse un altro accesso alla rete su un'altra porta o con un altro protocollo, comparirebbe nuovamente la richiesta ed è possibile creare un'altra regola per questa richiesta.
- **Applicazione, se almeno x richieste**: esistono applicazioni (ad es. Microsoft Outlook) che durante una richiesta di rete inviano contemporaneamente richieste a diverse porte oppure utilizzano contemporaneamente diversi protocolli. Poiché questo, ad esempio con l'impostazione Protocollo/porta/applicazione, comporterebbe diverse richieste, qui è possibile definire se impostare un'autorizzazione o un divieto generale alle applicazioni per l'utilizzo della rete in fase di consenso o di divieto di connessione da parte dell'utente.

Applicazioni server sconosciute

Le applicazioni che non vengono ancora gestite dal firewall in base a una regola possono essere trattate in modi diversi. Il momento della richiesta è collocato in un determinato spazio discrezionale. Quando l'applicazione server si trova in ricezione, significa che attende una richiesta di connessione quasi in standby. Altrimenti la richiesta avviene quando viene effettivamente posta la richiesta di connessione.

Verifica di reti non protette

Naturalmente un firewall può funzionare correttamente solo quando tutte le reti alle quali ha accesso il computer sono riconosciute e controllate. Perciò si dovrebbe lasciare attivata questa verifica di reti non protette.

Ripetizione delle richieste di applicazioni

È possibile associare a un'applicazione le richieste di connessione ripetitive. In questo modo, durante i tentativi di connessione non ancora specificati mediante una regola, non si visualizza continuamente una richiesta, bensì soltanto ad intervalli ad es. di 20 secondi o ad altri intervalli personalizzabili.

Verifica dei riferimenti

La funzione Verifica riferimenti consente di calcolare un checksum sulla base delle dimensioni del file e di altri criteri per le applicazioni il cui l'accesso alla rete è già stato autorizzato nel firewall. Se il checksum del programma si discosta improvvisamente, è possibile che il programma sia stato modificato da un programma dannoso; pertanto viene attivato l'allarme del firewall.

Verifica riferimenti per moduli caricati: vengono monitorati non soltanto le applicazioni, bensì anche i moduli utilizzati da tali applicazioni, ad es. le DLL. Poiché questi variano frequentemente o vengono caricati nuovi moduli, il controllo dei riferimenti modificati e sconosciuti per i moduli può comportare un notevole lavoro di amministrazione. Ogni modulo modificato comporterebbe una corrispondente richiesta di conferma da parte del firewall. Per questo motivo il controllo dei moduli dovrebbe essere utilizzato solo quando è richiesto un livello di sicurezza molto alto.

Varie

Sono disponibili delle impostazioni aggiuntive.

Procedura per l'Assistente regole

Consente di determinare se creare nuove regole tramite Assistente regole o nella modalità di elaborazione avanzata. Agli utenti inesperti in materia di sicurezza delle reti si consiglia l'uso dell'Assistente regole.

Verifica all'avvio del programma

Consente di definire se il firewall dovrà cercare eventuali applicazioni server sconosciute ad ogni avvio del programma. È consigliabile lasciare sempre attivate queste funzioni di ricerca, tranne quando si lavora in una rete chiusa.

Salvataggio del protocollo di connessione

Consente di definire per quanto tempo il firewall debba conservare i dati di connessione. È possibile conservare i dati da una a 60 ore e prenderne visione nell'area di programma dei log.

Tuner

Generale

Qui è possibile effettuare le seguenti modifiche:

- **Elimina i dati di ripristino**: consente di stabilire quando eliminare i dati di ripristino (che il software G DATA crea quando si apportano modifiche).
- **Elimina vecchi dati**: consente di stabilire quando eliminare i dati obsoleti (ad es. le vecchie cartelle TEMP).
- **Elimina i collegamenti del desktop**: consente di stabilire quando eliminare i collegamenti del desktop (quando non vengono utilizzati per uno specifico numero di giorni).
- **Con l'esecuzione di Microsoft Update cercare anche gli aggiornamenti di Office**: qui è possibile stabilire se il regolatore deve automaticamente cercare in Internet gli Aggiornamenti di Office oltre agli attuali Aggiornamenti di Windows. L'aggiornamento di entrambi fa risparmiare tempo e mantiene il sistema allo stato più aggiornato. Gli aggiornamenti di Office vengono cercati solo se Microsoft Office è installato sul computer corrente.
- **Non creare file di log con informazioni dettagliate riguardo agli elementi eliminati**: Il regolatore è concepito in modo da registrare senza interruzioni le informazioni relative alle modifiche effettuate. Se si considera un file di log con le informazioni sulle cancellazioni eseguite dal Tuner come un rischio per la sicurezza, è possibile sopprimere la creazione di un log degli elementi eliminati.

- **Elimina file temporanei in modo permanente**: questa funzione permette di rimuovere i file Web (ad es. cookie, file temporanei di Internet) dall'opzione di ripristino del Tuner, ossia questi file non potranno essere ripristinati. Attivando questa funzione, la quantità di dati che il Tuner deve gestire nell'area Ripristina viene ridotta in modo considerevole, con conseguenti vantaggi sulle prestazioni.

- **Non permettere il riavvio automatico del computer tramite il servizio**: l'opzione impedisce un possibile riavvio del computer che verrebbe effettuato dal Tuner sulla base di un processo di regolazione programmato. Il Tuner riavvia il computer senza chiedere conferma solo quando nessun utente è collegato, pertanto nella maggioranza dei casi è consigliabile non attivare questa opzione.

- **Permettere la creazione dei singoli punti di ripristino**: senza questa funzione, il software G DATA non è in grado di eseguire alcun ripristino.

- **Per la deframmentazione non considerare il tipo di unità**: poiché la maggior parte dei produttori sconsiglia la deframmentazione dei propri dischi SSD, in G DATA Tuner la deframmentazione di questo tipo di unità è esclusa per impostazione predefinita. Potete lasciare spuntata questa casella soltanto nei casi in cui non sia possibile classificare automaticamente i tipi di unità del software G DATA, ma siete assolutamente certi che non vi siano unità SSD. Ad ogni esecuzione il Tuner avvia quindi una deframmentazione di tutti i dischi fissi presenti nel sistema.

Configurazione

In questa Area è possibile selezionare tutti i moduli che il Tuner deve utilizzare per il processo di regolazione. I moduli selezionati vengono avviati o tramite un'azione automatica pianificata (consultare il capitolo **Pianificazione**) o manuale. Per attivare un modulo, fare doppio clic su di esso. È possibile ottimizzare singolarmente le seguenti aree di regolazione:

- *Protezione*: Le varie funzioni che consentono di scaricare automaticamente i dati da Internet sono utili ai provider ma non agli utenti. Spesso queste funzioni aprono la strada a software dannosi. Questi moduli consentono all'utente di proteggere il sistema e di mantenerlo sempre aggiornato.

- *Prestazioni*: I file temporanei, ad esempio le copie di riserva non più utili, i file di registro o i dati di installazione che occupano spazio sul disco rigido una volta terminata l'installazione rallentano il disco rigido e occupano spazio prezioso. I processi e i collegamenti a file non più necessari rallentano considerevolmente il sistema. I moduli elencati qui di seguito consentono di liberare il computer da questi file inutili migliorandone così le prestazioni.

- *Protezione dati*: Raccogli i moduli riguardanti la protezione dei dati. Qui vengono eliminate le tracce lasciate involontariamente mentre si naviga in Internet o si usa il computer che possono fornire molte informazioni sulle abitudini d'uso oppure rivelare password o dati importanti.

Protezione delle cartelle

Con questa scheda è possibile escludere specifiche cartelle (anche la partizione di Windows) dall'eliminazione automatica dei file obsoleti.

Fare clic sull'icona **Aggiungi**, quindi selezionare la cartella o l'unità desiderata.

Per cancellare di nuovo una cartella eccezioni, selezionarla nell'elenco visualizzato e fare clic sul pulsante **Elimina**.

Protezione del file

L'opzione di protezione dei file consente di proteggere file specifici dall'eliminazione da parte del Tuner, ad es. i punteggi di un gioco per computer o file simili che abbiano estensioni di file non usuali, che potrebbero essere considerati come file di backup o temporanei.

Per proteggere specifici file, fare clic sul pulsante **Aggiungi**, quindi inserire il nome del file corrispondente. In questo campo è possibile utilizzare i segnaposto.

la modalità di funzionamento dei caratteri jolly è la seguente:

- Un punto interrogativo (?) rappresenta un singolo carattere.

- L'asterisco (*) rappresenta un'intera stringa di caratteri.

Ad esempio, per proteggere tutti i file con estensione ".sav", inserire quindi *.sav. Per proteggere, ad esempio, file diversi che iniziano con la stessa lettera iniziale, inserire ad esempio testo*.*.

Selezionare la cartella nella quale devono essere protetti i file, facendo clic sul pulsante Avanzate. Quindi selezionare la posizione in memoria in cui si trovano i file da proteggere. Il Tuner protegge solo i file definiti in questa cartella (ad es. i punteggi dei giochi

solo nelle cartelle di gioco).

Per attivare di nuovo una cartella eccezioni, selezionarla nell'elenco visualizzato e fare clic sul pulsante **Elimina**.

Pianificazione

La scheda **Pianificazione** permette di definire quando e con quale frequenza debba avere luogo il processo di regolazione automatica.

L'opzione **Giornalmente** consente, mediante l'indicazione dei giorni della settimana, di stabilire ad es. che il computer esegua la regolazione solo nei giorni feriali oppure solo ogni due giorni oppure solo nei fine settimana quando non viene utilizzato. Per modificare la data e l'ora nell'opzione **Pianificazione**, selezionare con il mouse l'elemento che si desidera modificare (ad es. giorno, ora, mese, anno), quindi usare il tasto freccia o la piccola icona della freccia alla destra del campo d'immissione per modificare cronologicamente l'elemento selezionato.

Se non si desidera che la regolazione avvenga automaticamente, deselezionare la casella **Attivato** per il processo di regolazione automatico.

Controllo dispositivi

La funzione Controllo dispositivi permette di definire per il vostro computer quali supporti di memoria sono autorizzati per la lettura e/o la scrittura dei dati. È possibile, ad esempio, vietare che i dati privati vengano copiati su una chiavetta USB o masterizzati su un CD. È possibile inoltre stabilire quali supporti dati rimovibili, ossia quali chiavette USB o dischi fissi USB, siano autorizzati a copiare i dati. Si può, ad es., utilizzare il proprio disco fisso USB per eseguire il backup dei dati e contemporaneamente vietare l'accesso ad altri dischi fissi.

Per utilizzare la funzione Controllo dispositivi, selezionare **Attiva controllo dispositivi** e scegliere per quali dispositivi impostare delle limitazioni:

- **Supporto dati rimovibile (ad es. chiavette USB)**
- **Unità CD/DVD**
- **Unità a dischetti**

Ora è possibile definire le regole per ogni singolo supporto di memoria.

Regola generale

Permette di definire per un dispositivo se non potrà mai essere utilizzato (**Blocca accesso**), se sarà possibile solo scaricare i dati, senza poter memorizzare altri dati sul dispositivo (**Accesso in lettura**) o se non impostare nessuna limitazione (**Accesso totale**). Questa regola verrà applicata a tutti gli utenti del computer.

Regole specifiche dell'utente

Se si desidera limitare i diritti di accesso solo per alcuni utenti, in quest'area è possibile selezionare il nome di un utente che utilizza il computer oltre a voi, quindi nel riquadro **Regola generale** limitarne l'accesso a determinati supporti di memoria. In qualità di amministratore e proprietario del computer avrete pertanto accesso totale, ma potrete limitare i diritti degli altri utenti.

Selezionare qui l'utente. Facendo clic su OK si apre un'altra finestra di dialogo che permette di definire il tipo di accesso per questo utente e se ai diritti di accesso verranno applicate limitazioni temporali (ad es. due settimane) (**Validità**).

> **Nota**: le regole specifiche dell'utente hanno priorità sulla regola generale, ossia se in generale si imposta il divieto di accesso alle chiavette USB, si può tuttavia consentire l'accesso a un utente specifico tramite una regola personalizzata. Se a un utente sono state applicate determinate limitazioni temporali di accesso tramite la funzione Controllo dispositivi, allo scadere di tali limitazioni verrà nuovamente applicata la regola generale.

Regole specifiche del dispositivo

Per l'uso dei supporti dati rimovibili, come le chiavette USB o i dischi esterni, è possibile stabilire che solo determinati supporti possano accedere al computer. Per questa impostazione, collegare il supporto dati rimovibile al computer e fare clic sul pulsante **Aggiungi**. Si apre una finestra di dialogo che permette di selezionare i supporti dati rimovibili. Facendo clic su OK si apre un'altra finestra di dialogo che permette di definire il tipo di accesso per questo supporto, se all'uso del supporto verranno applicate limitazioni temporali (ad es. due settimane) (**Validità**) e se tutti gli utenti potranno utilizzare questo supporto dati con i propri diritti di accesso.

Backup

Quest'area permette di eseguire le impostazioni generali per la funzionalità del modulo di backup.

- **Directory per file temporanei**: Qui è possibile definire dove dovranno essere archiviati temporaneamente i dati ricevuti dal modulo di backup. Questi file vengono generati al momento della creazione, ma anche del ripristino, di un backup. Tuttavia, vengono eliminati automaticamente dopo il rispettivo processo. Per questo motivo è necessario disporre di spazio sufficiente sul disco fisso altrimenti si ridurrebbe la velocità del backup e del ripristino. Si consiglia di modificare questa impostazione solo nel caso in cui nella directory scelta per i file temporanei non vi sia spazio sufficiente.

- **Controllo unità origine/destinazione sullo stesso disco rigido**: In genere il modulo di backup avvisa l'utente ogni volta che un backup deve essere eseguito sul medesimo supporto dati che contiene i dati originali. Ciò avviene perché, in caso di guasto o perdita del supporto dati, anche il backup non sarebbe più disponibile. Tuttavia, se per determinati motivi si desidera eseguire regolarmente il backup sul supporto dati originale, è possibile qui disattivare questo avviso.

Protocolli

Per ciascun modulo sono disponibili delle funzioni di log che offrono una panoramica sulle azioni eseguite dal software G DATA per proteggere il computer.

Log di Protezione antivirus

Nell'area Log sono elencati i log prodotti dal software. Facendo clic sulle intestazioni delle colonne **Ora di avvio**, **Tipo**, **Titolo** o **Stato**, è possibile ordinare i log esistenti. Tramite i pulsanti **Salva con nome** e **Stampa** è possibile salvare o stampare direttamente i dati di un log come file di testo. Per eliminare un log, selezionare con il mouse la voce della tabella, quindi premere il tasto Canc o il pulsante **Elimina**.

Log del firewall

Per ogni azione del firewall, nell'area dei log viene creato un file di log voluminoso. Qui è possibile aprire le singole azioni facendovi doppio clic e eventualmente stamparle o salvarle come file di testo. Per ulteriori informazioni, vedere anche il capitolo **Impostazioni: Varie**.

Log di backup

Per ogni azione e per ogni processo di backup, nell'area dei log viene creato un file di log voluminoso. Qui è possibile aprire le singole azioni facendovi doppio clic e eventualmente stamparle o salvarle come file di testo. Per ulteriori informazioni, vedere anche il capitolo **Salvataggio e ripristino**.

Log di Protezione da spam

Per ogni azione, nell'area dei log viene creato un file di log voluminoso. Qui è possibile aprire le singole azioni facendovi doppio clic e eventualmente stamparle o salvarle come file di testo.

Log di Protezione minori

Nell'area Log in qualità di amministratore disponete di un riepilogo di tutti i tentativi effettuati dagli altri utenti di richiamare i contenuti bloccati. In alto è possibile selezionare dall'elenco l'utente di cui si desidera visualizzare il log. Per ulteriori informazioni, consultare il capitolo **Impostazioni: Log**.

> **Nota**: i log possono essere eliminati anche premendo il pulsante **Elimina log**.

Log di Controllo dispositivi

Per ogni azione della gestione dispositivi, nell'area dei log viene creato un file di log voluminoso. Per ulteriori informazioni, vedere il capitolo: **Impostazioni: Controllo dispositivi**

FAQ: BootScan

Nel caso in cui il computer fosse nuovo o fosse già stato protetto da un software antivirus, potete installare il software come spiegato di seguito.

Nel caso in cui si sospettasse la presenza di un virus, prima dell'installazione del software è consigliabile eseguire un BootScan.

> **BootScan**: quando si accende il computer, normalmente si avvia automaticamente il sistema operativo Windows. Questa procedura è definita boot (avvio). È possibile inoltre avviare automaticamente altri sistemi operativi e programmi.
>
> Per controllare sul computer l'eventuale presenza di virus prima dell'avvio di Windows, G DATA mette a disposizione, oltre alla versione per Windows, una versione speciale in grado di eseguire un avvio.

Requisiti

Il BootScan è uno strumento pratico per combattere i virus che si sono insediati nel computer prima dell'installazione di un software antivirus.

A questo proposito esiste una versione speciale del software che può essere eseguita prima dell'avvio di Windows.

Avvio dall'unità CD/DVD: se il computer non si avvia automaticamente dall'unità CD/DVD, procedere nel modo seguente:

1. Spegnere il computer.

2. Riavviare il computer. Solitamente è possibile attivare l'impostazione del BIOS quando durante l'accensione (= Boot) del computer si preme il tasto CANC (anche F2 o F10, a seconda del sistema).

3. Come si modificano le singole impostazioni nella configurazione del BIOS dipende dal computer in uso.

   Consultare a questo proposito la documentazione del computer.

   Il risultato dovrebbe corrispondere alla sequenza di avvio **CD/DVD-ROM:, C**, ovvero l'unità CD/DVD-ROM viene impostata come **1st Boot Device** e la partizione del disco rigido del sistema operativo Windows come **2nd Boot Device**.

4. Salvare le modifiche e riavviare il computer. Ora il computer è pronto per un'analisi di base dei virus prima dell'installazione (BootScan).

   Come si può interrompere un BootScan? Se al riavvio si desidera che sul computer non venga visualizzato il consueto ambiente Windows, bensì un'interfaccia speciale del software Bootscan di G DATA, non c'è problema.

   Se non si desidera effettuare un BootScan, selezionare con i tasti freccia la voce **Microsoft Windows** e fare clic su **Invio**. A questo punto si avvia Windows senza essere preceduto da un BootScan.

   Avvio da chiavetta USB: se come supporto di boot si utilizza una chiavetta USB, si può impostarla come 1° dispositivo di boot.

FAQ: Funzioni del programma

Icona di sicurezza

Il software G DATA protegge in modo permanente il computer da virus e software dannosi. Per indicare che la protezione è attiva, è visualizzata un'icona nella barra delle applicazioni, in basso accanto all'ora.

Questa icona di G DATA conferma che tutto è a posto e che sul PC la protezione è attivata.

Se il Guardiano è stato disattivato o se si sono verificati altri problemi, sull'icona di G DATA compare un avvertimento. In questo caso è opportuno avviare al più presto il software G DATA e verificare le impostazioni.

Facendo clic sull'icona con il tasto destro del mouse, viene aperto un menu contestuale che permette di controllare i principali aspetti della protezione.

Sono disponibili le seguenti funzioni:

- **Avvia software G DATA**: questa funzione permette di richiamare SecurityCenter per eseguire ad es. le impostazioni per il Guardiano AntiVirus. Per conoscere le opzioni disponibili nel SecurityCenter, consultare il capitolo: **SecurityCenter**.
- **Disattiva Guardiano**: questa opzione permette in caso di necessità di disattivare il Guardiano AntiVirus e di riattivarlo. Ciò può essere opportuno se ad es. sul disco fisso si intende copiare quantità notevoli di dati da una posizione a un'altra o se si eseguono operazioni di calcolo che richiedono molto spazio in memoria, come la masterizzazione di DVD. Il Guardiano AntiVirus dovrebbe essere disattivato solo per il tempo strettamente necessario e bisogna fare in modo che durante questo periodo il sistema sia possibilmente scollegato da Internet o non abbia accesso a nuovi dati non ancora verificati, ad es. su CD, DVD, schede di memoria o chiavette USB.
- **Disattiva il firewall**: se si utilizza una versione del software G DATA con firewall integrato, è possibile, in caso di necessità, disattivare il firewall dal menu contestuale. Il computer resta collegato ad Internet e alle altre reti, tuttavia non è più protetto dal firewall contro attacchi e azioni di spionaggio.
- **Disattivare il pilota automatico**: il Pilota automatico è un componente del firewall e decide in modo indipendente quali richieste e quali contatti il computer deve accettare dalla rete o da Internet. Per un normale utilizzo il Pilota automatico è una funzione ottimale ed è consigliabile tenerlo sempre attivato. Come il firewall, il Pilota automatico è disponibile per le versioni selezionate del software G DATA.
- **Aggiorna database antivirus**: un software antivirus dovrebbe sempre essere aggiornato. Naturalmente l'aggiornamento dei dati può essere eseguito automaticamente dal software. Tuttavia, nel caso in cui sia necessario effettuare tempestivamente un aggiornamento, è possibile avviarlo tramite il pulsante **Aggiorna database antivirus**. Per informazioni su quando sia necessario eseguire un aggiornamento antivirus, consultare il capitolo: **Scansione antivirus**.
- **Statistiche**: qui è possibile visualizzare le statistiche relative alle operazioni di scansione del Guardiano AntiVirus, ma anche le informazioni sulla scansione in modo inattivo, i messaggi del filtro web e ulteriori parametri.

Esecuzione della scansione antivirus

La scansione antivirus permette di verificare l'eventuale presenza di software dannosi sul proprio computer. Quando viene avviata la scansione, tutti i file presenti nel computer vengono controllati per verificare se sono in grado di infettare o se sono infetti.

Nel caso in cui durante una scansione antivirus venissero rilevati dei virus o altri software dannosi, esistono diverse possibilità per rimuovere o neutralizzare tali virus.

1 Avviare la scansione antivirus. La procedura è descritta nel capitolo: **Protezione antivirus**.

2 A questo punto viene eseguito un controllo sul computer per rilevare l'eventuale presenza di virus. A questo scopo si apre una finestra nella quale si ottengono le informazioni sullo stato della verifica.

Una barra di avanzamento nell'area superiore della finestra mostra di quanto è progredita la scansione del sistema. Già durante la scansione antivirus è possibile intervenire sullo svolgimento della scansione:

- **In caso di carico del sistema, sospendere la scansione**: ponendo un segno di spunta in questo campo, il programma sospende la scansione fino a quando il computer non ha terminato tutte le altre attività.

- **Spegnere il computer dopo la scansione antivirus**: questa funzione si rivela molto utile quando occorre eseguire la scansione antivirus durante la notte o dopo l'orario lavorativo. Non appena il software G DATA termina la scansione antivirus, il computer viene spento.

- **Archivi protetti da password**: finché un archivio è protetto da password, il software G DATA non eseguirà un controllo di tale archivio. Selezionando quest'opzione, il software antivirus fornisce informazioni sugli archivi protetti da password sui quali non è stato possibile eseguire la scansione. Finché tali archivi non vengono decompressi, il virus presente non costituisce alcun rischio per il sistema.

- **Accesso negato**: in generale, in Windows vi sono file che vengono utilizzati esclusivamente dalle applicazioni e per i quali non viene eseguita la scansione finché tali applicazioni sono in esecuzione. Per questo è preferibile che durante una scansione antivirus non vengano utilizzati altri programmi. Selezionando questa casella, vengono visualizzati i dati che non sono stati controllati.

3a Se sul sistema non sono presenti dei virus, al termine della scansione si può uscire dalla finestra della procedura guidata premendo il pulsante **Chiudi**. Il sistema è stato sottoposto a scansione antivirus e non sono presenti virus.

3b Se sono stati rilevati virus e altri programmi dannosi, è possibile decidere come il sistema dovrà procedere con i virus rilevati. Di regola è sufficiente fare clic sul pulsante **Esegui azioni**.

Il software G DATA applica ora un'impostazione standard (se non diversamente configurato in **Impostazioni: Scansione antivirus manuale** per file e archivi infetti) e disinfetta i file colpiti, ossia li ripara in modo che possano essere di nuovo utilizzati senza limitazioni e non rappresentino più un pericolo per il computer.

Se una disinfezione non è possibile, il file viene spostato in quarantena, cioè viene crittografato in un'apposita cartella da cui non potrà più arrecare danni.

Se è necessario usare ancora questo file infetto, è possibile in casi eccezionali estrarlo dall'area di quarantena e riutilizzarlo.

Il sistema è stato sottoposto a scansione antivirus e non sono presenti virus.

3c Se si conoscono i file e gli oggetti infetti e si è in grado di distinguere quelli che non servono più, è possibile rispondere singolarmente ad ogni specifico rilevamento di virus.

Nell'elenco dei virus rilevati, nella colonna Azione, è possibile infatti definire l'azione da intraprendere per ogni singolo file infetto.

- **Solo log**: nella vista **Protocolli** viene indicato il tipo di virus, tuttavia non ha luogo alcuna riparazione o cancellazione dei relativi file. **Attenzione**: Se un virus viene registrato nel log, continua ad essere attivo e pericoloso.

- **Disinfettare (quando non è possibile: solo log)**: se si sceglie questa voce il programma tenterà di rimuovere il virus dal file infetto; nel caso in cui non fosse possibile senza danneggiare il file, il virus viene registrato e si può esaminare in un secondo tempo la voce registrata nel log. Attenzione: Se un virus viene registrato nel log, continua ad essere attivo e pericoloso.

- **Disinfettare (quando non è possibile: spostare in quarantena)**. Questa è un'impostazione standard. Scegliendo questa opzione il programma tenterà prima di rimuovere il virus da un file infetto; nel caso in cui non fosse possibile senza danneggiare il file, questi verrà spostato in **Quarantena**. Per ulteriori informazioni, consultare il capitolo: **File in quarantena**.

- **Disinfettare (quando non è possibile: eliminare il file)**. Il programma tenterà di rimuovere il virus da un file infettato; nel caso non fosse possibile, il file verrà eliminato. Questa funzione deve essere utilizzata solo quando sul computer non sono presenti dati importanti. L'eliminazione di file infetti potrebbe provocare un malfunzionamento di Windows e rendere necessaria una nuova installazione.

- **Spostare il file in quarantena**: I file infetti vengono spostati direttamente in Quarantena. Nella quarantena i file sono salvati in modo cifrato. Qui il virus non può arrecare alcun danno ed il file infetto è disponibile per eventuali tentativi di riparazione. Per ulteriori informazioni, consultare il capitolo: **File in quarantena**

- **Elimina file**: Questa funzione deve essere utilizzata solo quando sul computer non sono presenti dati importanti. L'eliminazione di file infetti potrebbe provocare un malfunzionamento di Windows e rendere necessaria una nuova installazione.

Facendo ora clic sul pulsante **Esegui azioni**, il software G DATA procederà per ogni singolo rilevamento di virus con l'azione definita dall'utente.

Il sistema è stato sottoposto a scansione antivirus. Se tuttavia è stata impostata un'opzione di **Registrazione** nel log, è possibile che il

computer non sia esente da virus.

Allarme virus

Quando il software G DATA rileva un virus o un programma dannoso sul computer, si apre una finestra di avviso su un lato dello schermo.

Sono disponibili le seguenti opzioni per intervenire sui file infetti.

- **Solo log**: nella vista Protocolli viene indicato il tipo di virus, tuttavia non ha luogo alcuna riparazione o cancellazione dei relativi file. Attraverso il log è comunque possibile controllare singolarmente i virus e rimuoverli in modo mirato. Attenzione: Se un virus viene registrato nel log, continua ad essere attivo e pericoloso.

- **Disinfettare (quando non è possibile: spostare in quarantena)**: Scegliendo questa opzione il programma tenterà prima di rimuovere il virus da un file infetto; nel caso in cui non fosse possibile senza danneggiare il file, questi verrà spostato in Quarantena. Per ulteriori informazioni, consultare il capitolo: Come funziona la quarantena?

- **Spostare il file in quarantena**: I file infetti vengono spostati direttamente in Quarantena. Nella quarantena i file sono salvati in modo cifrato. Qui il virus non può arrecare alcun danno ed il file infetto è disponibile per eventuali tentativi di riparazione. Per ulteriori informazioni, consultare il capitolo: **File in quarantena**

- **Eliminare il file infetto**: Questa funzione deve essere utilizzata solo quando sul computer non sono presenti dati importanti. L'eliminazione di file infetti potrebbe provocare un malfunzionamento di Windows e rendere necessaria una nuova installazione.

  Quarantena e caselle di posta elettronica: esistono dei file che non è consigliabile spostare in quarantena, ad es. i file di archivio per caselle di posta elettronica. Se una casella di posta elettronica viene spostata in quarantena, il programma di posta elettronica non vi potrà più accedere e probabilmente non funzionerà più. Particolare attenzione deve dunque essere data ai ***file con estensione PST*** poiché questi solitamente comprendono i dati della propria casella di posta elettronica di Outlook.

Allarme del firewall

Generalmente, nella modalità Creazione manuale delle regole, il firewall chiede se deve autorizzare o rifiutare la connessione in presenza di programmi e processi sconosciuti. Si apre una finestra informativa che mostra i dettagli della relativa applicazione. In questa finestra è possibile autorizzare o rifiutare per una sola volta o in modo permanente l'accesso alla rete da parte dell'applicazione. Quando si autorizza o si rifiuta l'accesso a un programma, questa azione viene inclusa come regola nella serie di regole della rispettiva rete e non verrà mai più richiesto cosa si intende fare.

Sono disponibili i seguenti pulsanti:

- **Consenti sempre**: questo pulsante permette di creare una regola per l'applicazione visualizzata sopra (ad esempio Opera.exe, Explorer.exe o iTunes.exe) che consente all'applicazione di accedere sempre alla suddetta rete o a Internet. Questa regola verrà inclusa anche come Regola creata su richiesta nell'area Serie di regole.

- **Consenti temporaneamente**: questo pulsante permette all'applicazione di accedere alla rete una sola volta. Al successivo tentativo di accedere alla rete da parte di questo programma, il firewall rinnoverà la richiesta.

- **Nega sempre**: questo pulsante permette di creare una regola per l'applicazione visualizzata sopra (ad esempio dialer.exe, spam.exe o trojan.exe) che vieta sempre all'applicazione l'accesso alla suddetta rete o a Internet. Questa regola verrà inclusa anche come Regola creata su richiesta nell'area Serie di regole.

- **Nega temporaneamente**: questo pulsante permette di rifiutare all'applicazione l'accesso alla rete una sola volta. Al successivo tentativo di accedere alla rete da parte di questo programma, il firewall rinnoverà la richiesta.

Vengono inoltre fornite informazioni su protocollo, porta e indirizzo IP con i quali l'applicazione cerca di interagire.

Segnalazione Not-a-virus

I file identificati come "not-a-virus" sono applicazioni potenzialmente pericolose. Questi programmi non sono portatori diretti di funzioni dannose ma potrebbero, in alcuni casi, essere utilizzati contro l'utente. Appartengono a questa categoria, ad esempio, alcuni programmi di utilità per la gestione remota, i programmi per la commutazione automatica della tastiera, i client IRC, i server FTP o altri programmi di utilità utilizzati per creare o nascondere determinati processi.

Disinstallazione

Per disinstallare in qualsiasi momento il software G DATA dal proprio computer, eseguire la disinstallazione tramite il Pannello di controllo del sistema operativo. La disinstallazione viene eseguita in modo automatico.

Se durante la disinstallazione fossero ancora presenti file nell'area della Quarantena, il software G DATA richiederà se tali file debbano essere eliminati o meno. Se questi file non vengono eliminati, vengono conservati nel sistema in una speciale cartella di G DATA, crittografata in modo da non arrecare danno. Questi file saranno di nuovo disponibili solo dopo aver reinstallato il software G DATA.

Durante la disinstallazione verrà chiesto se si desidera eliminare le impostazioni e i log. Se non si eliminano questi file, i registri e le impostazioni saranno nuovamente disponibili dopo aver installato nuovamente il software.

Terminare la disinstallazione facendo clic sul pulsante **Fine**. Il software risulta ora completamente disinstallato dal sistema.

FAQ: Domande sulle licenze

Licenze multiple

Con una multilicenza è possibile utilizzare il software G DATA sul numero di computer consentito dalla licenza. Dopo l'installazione sul primo computer e l'aggiornamento Internet, vengono comunicati online i dati di accesso. Quando si installa il software sul computer successivo, basta inserire il nome utente e la password ricevuti dopo la registrazione sul server di aggiornamento G DATA. Ripetere la procedura per ogni ulteriore computer.

Per l'aggiornamento Internet, utilizzare su tutti i PC i propri dati di accesso (nome utente e password) ricevuti dopo la prima registrazione. A questo scopo, procedere nel seguente modo:

1. Avviare il software G DATA.
2. In **SecurityCenter** fare clic su **Aggiorna database antivirus**.
3. Nella finestra che viene aperta, inserire i dati di accesso ricevuti in precedenza via e-mail. Facendo ora clic su **OK** al computer verrà assegnata la licenza.

Prolungamento della licenza

Un paio di giorni prima che scada la licenza, sulla barra delle applicazioni viene visualizzata una finestra informativa. Facendo clic su di essa, si apre una finestra di dialogo nella quale, senza difficoltà ed in pochi passaggi, è possibile estendere la licenza. Fare semplicemente clic sul tasto **Acquista ora**, completare con i propri dati e la protezione antivirus verrà nuovamente garantita. Nei giorni successivi si riceverà la fattura comodamente per email in formato PDF.

> **Nota**: Questa finestra di dialogo compare soltanto allo scadere del primo anno. In seguito la licenza per G DATA viene prolungata automaticamente ogni anno. È possibile disdire questo servizio di prolungamento in qualsiasi momento senza spiegazioni.

Cambio di computer

È possibile utilizzare il software G DATA su un nuovo o su altri computer usando i dati di accesso ricevuti. Installare semplicemente il software e inserire i propri dati di accesso. Il server di aggiornamento effettuerà la connessione al nuovo computer. Se sul vecchio computer è ancora presente il software G DATA, la licenza deve essere trasferita dal vecchio al nuovo computer.

> **Nota**: Il numero di trasferimenti della licenza è limitato: una volta raggiunto il valore limite, la licenza verrà bloccata e non sarà più possibile effettuare alcun aggiornamento.

Copyright