G DATA

Security Software

Índice

Primeiros passos

Agradecemos que você tenha optado por nosso produto e esperamos que esteja sempre satisfeito com seu novo G DATA Software. Caso algo não funcione imediatamente, nossa documentação da ajuda pode ajudá-lo(a). Para outras perguntas, a nossa equipe de especialistas no **ServiceCenter** está à disposição.

> **Observação**: No software, é possível abrir a qualquer momento a ajuda detalhada do programa e obter todas as informações necessárias. Para isso, clique simplesmente no botão de ajuda mostrado no programa.

Centro de assistência

A instalação e utilização do G DATA Software são intuitivas e descomplicadas. Caso ocorra algum problema, simplesmente entre em contato com os funcionários especializados do nosso Suporte técnico:

G DATA Brasil	www.gdatasoftware.com.br
G DATA Portugal	www.gdata.pt

Instalação

Se o seu computador for novo de fábrica ou se até agora já esteve protegido por um software antivírus, pode efectuar a instalação através dos seguintes passos. No entanto, se tiver uma suspeita justificada de que o seu computador já está infectado por vírus, recomenda-se executar um **BootScan** antes da instalação do G DATA Software.

> **Atenção**: Caso você tenha até agora utilizado software antivírus de outro fabricante, primeiro, ele deve ser desinstalado completamente de seu computador. Como o software antivírus intervém muito profundamente na estrutura de sistema do Windows, é aconselhável não confiar apenas na desinstalação normal do software, mas sim - quando possível - utilizar também as ferramentas de limpeza que este fabricante coloca à disposição em seu centro de suporte online.

Passo 1 - Início da instalação

Inicie a instalação da seguinte forma:

- **Instalação CD/DVD**: Para se iniciar a instalação, insira o CD ou DVD do programa.
- **Descarregar o software**: Para começar com a instalação de uma versão do software baixada da internet, faça simplesmente um clique duplo no arquivo baixado.

Uma janela de instalação é aberta automaticamente.

> **Observação**: Caso a instalação não inicialize: Pode ser que a função de inicialização automática de seu computador não esteja configurada corretamente. Então o software não pode iniciar automaticamente o processo de instalação após inserção do CD do programa e nenhuma janela é aberta pela qual o G DATA Software pode ser instalado.
>
> - Se, em vez disso, se abrir uma janela de selecção para a reprodução automática, clique na opção **Executar AUTOSTRT.EXE**.
> - Se nenhuma janela de opções for aberta, procure, através do Windows Explorer, a mídia de dados com o G DATA Software e inicialize o arquivo **Instalação** ou **Setup.exe**.

Passo 2 - Seleção de idioma

Então, selecione em qual idioma você deseja instalar seu novo G DATA Software.

Passo 3 - Método de instalação

Agora, um assistente o ajudará com a instalação do Software no seu computador. Selecione agora se você quer executar a instalação padrão ou a instalação definida pelo usuário. Recomendamos fazer aqui a instalação padrão.

Iniciativa de informações sobre malware: Os G DATA SecurityLabs pesquisam constantemente processos para proteger os clientes da G DATA contra malware (Vírus, worms e programas maliciosos). Quanto mais informações sobre malware conseguirmos reunir, mais rapidamente conseguiremos desenvolver mecanismos de protecção mais eficientes. No entanto, muitas informações apenas estão disponíveis em sistemas já atacados ou infectados. Para que essas informações possam ser incluídas nas análises, foi criada a Iniciativa de informações sobre malware G DATA. Neste escopo, as informações relacionadas a malware são enviadas para os G DATA SecurityLabs. Com a sua participação, você colabora para que todos os clientes G DATA possam utilizar a Internet de forma mais segura. Durante a

instalação do G DATA Software você pode decidir se deseja disponibilizar informações para o G DATA SecurityLabs ou não.

> **Observação**: Na instalação definida pelo usuário, pode ser feita a escolha de forma individual do local de salvamento dos dados do programa e a marcação ou desmarcação dos módulos do software (por exemplo, proteção contra spam) durante a instalação.

Passo 4 - Acordo de licença

Leia agora o acordo de licença e dê a sua concordância.

Passo 5 - Instalação definida pelo usuário (opcional)

Se a instalação definida pelo usuário foi selecionada, são exibidas duas janelas assistentes nas quais o diretório de instalação para o software e o escopo dos módulos instalados podem ser definidos. Caso tenha sido selecionada a instalação padrão, esse passo pode ser ignorado.

- **Definido pelo usuário**: Aqui você define o escopo de instalação definindo as marcações nos diversos módulos de software (por exemplo, antispam, etc.).
- **Completa**: Todos os módulos de software de sua versão de software são instalados.
- **Mínimo**: Com o módulo AntiVirus, apenas a proteção básica de vírus de seu G DATA Software é instalado.

> **Atualizações**: Pelo setup, a qualquer momento pode ser feita a instalação posterior de módulos do software ou a atualização do seu software. Para isso, inicie novamente o setup e selecione **Adaptar instalação** para ampliar ou reduzir os módulos do software. Se você possuir uma nova versão de programa e quiser atualizar a versão do programa, através da seleção de **Atualização definida pelo usuário** podem ser definidos, quais outros módulos devem ser selecionados ou desmarcados.

Passo 6 - Versão do software

Agora você pode definir se deseja instalar o Software como versão completa ou como versão de teste. Se você comprou o Software e possui um número de registro você deve, naturalmente, selecionar a entrada **Versão completa**. Para conhecer o G DATA Software gratuitamente, você pode utilizar simplesmente o nosso acesso de teste temporário.

Passo 7 - Ativação do produto

Durante a instalação, acontece a ativação do produto. Aqui poderá activar o seu software.

- **Inserir um novo número de registro**: Ao instalar o seu G DATA Software pela primeira vez, selecione esta opção e, em seguida, insira o número de registro que acompanha o produto. Dependendo do tipo do produto, o número pode ser encontrado, por exemplo, no verso do manual de instruções, no e-mail de confirmação do download do software ou na embalagem do produto.

  > **Observação**: Ao inserir o número de registro, o seu produto será ativado e, além disso, você receberá um e-mail com seus dados de acesso para a futura utilização.

- **Introduzir dados de acesso**: Se você já ativou o seu G DATA Software anteriormente, então você recebeu seus dados de acesso (nome de usuário e senha). Para instalar o software novamente ou para registrar mais computadores com uma licença de multiusuários, simplesmente insira os seus dados de acesso aqui.

  > **Observação**: Você recebe os dados de acesso exclusivamente por e-mail. Os dados de acesso não estão acompanhando o produto.
  >
  > Caso tenha perdido ou se tenha esquecido dos seus dados de acesso, na área de ligação clique na entrada **Esqueceu os dados de acesso?** Abre-se uma página Web onde pode introduzir novamente o seu número de registo. Depois de introduzir o número de registo, receberá os dados de acesso no endereço de e-mail facultado durante o registo. Se o seu endereço de e-mail mudou nesse período, entre em contato com a nosso **Suporte técnico**.

- **Activar mais tarde**: Se você quiser simplesmente dar uma olhada no software, pode instalá-lo também sem a informação de dados. No entanto, não será possível efectuar actualizações do programa através da Internet e não será possível fornecer uma protecção verdadeira contra software malicioso. Pode introduzir o seu número de registo ou os seus dados de acesso num período posterior, logo que execute uma actualização.

Passo 8 - Conclusão da instalação

Eventualmente, poderá ter de reiniciar o computador após a instalação. Em seguida, o G DATA Software estará disponível.

Após a instalação

Após a instalação, através do ícone do programa na barra de tarefas pode ser feita a inicialização do seu G DATA Software recém-instalado. Além disso, ainda há outras funções de segurança disponíveis no seu computador:

Ícone Security: Seu G DATA Software protege seu computador permanentemente contra softwares maliciosos e ataques. Um símbolo na barra de tarefas do seu computador alerta você assim que o software determina a necessidade de uma intervenção do usuário. Clicando sobre o símbolo com o botão direito do mouse, você pode abrir a interface do programa G DATA. Para isto, leia também o capítulo **Ícone Security**.

Triturador: Caso você tenha selecionado o triturador na instalação (com G DATA Antivirus, não integrado), ele fica disponível como ícone no Desktop. Dados jogados no triturador são eliminados de forma que não podem mais ser restaurados, mesmo com ferramentas profissionais de recuperação de dados. Os dados são sobrescritos com uma quantidade de etapas definida pelo usuário. Você vai para as configurações ao clicar com o botão direito do mouse no ícone de triturar e acessa as propriedades.

Verificação rápida: Com a verificação rápida, você pode verificar arquivos de forma simples, até mesmo sem precisar iniciar o software. Basta marcar com o mouse os arquivos ou a pasta, por exemplo, no Windows Explorer. Clique então no botão direito do mouse e selecione na janela de diálogo que surge **Verificar a existência de vírus**. Será feita uma verificação de vírus automática dos ficheiros em questão.

Após a instalação do software, seu computador inicia diferentemente do habitual: Isso pode ocorrer quando o CD do programa ainda estiver na unidade. Retire simplesmente o CD e reinicie o seu computador como habitualmente.

SecurityCenter

Você só precisa acessar a Central de segurança, se quiser acessar uma das muitas funções adicionais do Software ativo. A proteção do seu computador contra vírus e outras ameaças ocorre permanentemente em segundo plano. Em casos nos quais o Software necessita de sua intervenção, você é lembrado automaticamente através de informações na barra de tarefas de seu computador.

Estado de segurança

Se tiver uma marca de verificação verde em tudo, o seu sistema está protegido.

Um ponto de exclamação vermelho indica que o seu sistema está sob risco. Neste caso, deve tomar de imediato as medidas necessárias para assegurar a protecção dos seus dados.

Se o símbolo de espaço reservado for exibido, significa que você não ativou a respectiva função de segurança (por exemplo, proteção contra spam).

Um símbolo amarelo indica que é necessária uma intervenção rápida pelo usuário. Por exemplo, este é ocaso quando existe uma atualização do programa do software.

Todas as outras funções e áreas de programa de software (por exemplo, **proteção de vírus** ou **configurações**) podem ser utilizadas quando você desejar se ocupar ativamente da segurança do seu sistema, mas isso não é necessário! Decida você mesmo como deseja se ocupar do assunto da Proteção de vírus e proteção de dados. Uma ajuda detalhada de programa está disponível no software.

Funções gerais

Os seguintes símbolos alertam para o estado de segurança da respectiva área.

Configurações: Através desse botão na parte superior direita, você pode acessar todos os diálogos de configuração das diversas áreas do software. Na área correspondente, você também tem a possibilidade de selecionar diretamente o diálogo de configuração adequado.

Registos: O software lista aqui os registros atuais relativos a todas as ações executadas (verificação de vírus, atualização, detecção de vírus etc.).

No lado superior direito do cabeçalho do software estão ainda as seguintes funções:

Visualizar ajuda: No seu software, poderá aceder a qualquer altura à ajuda detalhada do programa. Para isso, aperte simplesmente o botão de ajuda mostrado no programa.

Actualizar programa: Quando existirem novas versões do programa do software, você poderá atualizá-las, bem como as informações de vírus, de forma confortável através de cliques no mouse. Se obtiver informações de que uma atualização está disponível, basta clicar no registro Atualizar programa. Para informações detalhadas, consulte o capítulo: Actualizações

Info: Aqui você obtém informações sobre a versão do programa. O número da versão pode, por exemplo, ser útil para o contato com o Centro de assistência.

Exibições de status

As seguintes exibições de status informam sobre o estado de segurança do seu sistema. Quando você clicar nestes registros, você pode iniciar ações imediatamente para otimizar o estado de segurança:

Proteção em tempo real

A proteção em tempo real da sentinela de vírus verifica continuamente o seu computador quanto à existência de vírus e controla os processos de escrita e leitura e, assim que um programa desejar executar funções maliciosas ou propagar arquivos danosos, ela o impede. A sentinela de vírus é a sua protecção mais importante! Ela não deve nunca ser desativada!

- **Desativar sentinela de vírus**: Se, ainda assim, você quiser desativar a sentinela de vírus, você pode realizar isto aqui. Se quiser otimizar o desempenho de seu computador pelo desligamento da sentinela, verifique necessariamente se o mesmo resultado não pode ser obtido talvez, com outra configuração da sentinela de vírus. Com esta finalidade, ao desligar a sentinela de vírus existe a opção de acessar as alterações correspondentes das configurações. Para isso, clique em Alterar segurança / desempenho e siga os avisos do capítulo de ajuda com o mesmo nome. De qualquer forma, como alternativa, o desligamento completo da sentinela de

vírus pode ser feito.

- **Desativar monitoramento de comportamento**: O monitoramento de comportamento trata-se de um reconhecimento inteligente de software malicioso desconhecido, que independente das assinaturas de vírus oferece proteção adicional. Geralmente, o monitoramento de comportamento deveria estar ligado.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | Antivírus | Proteção em tempo real**.

Última verificação em modo ocioso

Aqui é apresentada a data da última análise completa do computador quanto à presença de vírus. Quando essa entrada estiver marcada em vermelho, você deverá executar uma verificação de vírus o mais rápido possível.

- **Verificar computador**: Se tiver tempo para isso e o computador não for utilizado para trabalho nas próximas horas, você pode iniciar aqui, diretamente, uma verificação completa do computador. O computador pode continuar sendo usado nesse tempo, mas como a verificação de vírus com esta configuração é feita com o máximo desempenho, pode ocorrer que os outros aplicativos se tornem mais lentos. Mais informações sobre isso podem ser obtidas no capítulo **Verificação de vírus**.

- **Iniciar verificação em modo ocioso agora**: A verificação em modo ocioso começa automaticamente em fases nas quais o seu computador está inativo e, assim, executa automaticamente uma verificação completa do computador em intervalos definidos. Se você desejar iniciar a verificação em modo ocioso antes do próximo momento definido automaticamente, selecione **Iniciar verificação em modo ocioso agora**. Se você não desejar que seu G DATA Software inicie automaticamente a verificação em modo ocioso durante as pausas de trabalho, você também pode desativar (não recomendável) esta função em **Desativar verificação em modo ocioso**.

Firewall

Um firewall protege o seu computador contra a *espionagem*, verificando quais os dados e programas transferidos da Internet ou da rede para o seu computador e quais os dados enviados pelo seu computador. Assim que algo indique que estão a ser transferidos dados para o seu computador, ou descarregados dados a partir do mesmo, sem autorização, o firewall dá o alarme e bloqueia a troca de dados não autorizada. Este módulo de software está disponível nas versões de programa G DATA Internet Security e G DATA Total Security.

- **Desativar firewall**: Se necessário, também pode desligar o firewall. O seu computador estará ainda conectado à Internet e a outras redes, mas não estará protegido (não recomendável) pelo firewall contra ataques ou espionagem.

- **Desativar piloto automático**: Geralmente é razoável utilizar o firewall na função **Piloto automático**. Ele executará praticamente em segundo plano e protegerá você, sem a necessidade de grandes configurações. Utilizando o firewall sem o piloto automático, aparece, em casos de dúvidas, uma janela de diálogo, na qual você pode otimizar as características do sistema passo a passo. Para utilizadores experientes é uma funcionalidade útil. Mas normalmente não é necessário desativar o piloto automático.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | Firewall | Automático**.

Proteção Web

Nesta área pode activar a protecção Web ou desactivá-la. A protecção Web é um módulo que, ao navegar na Internet e durante os downloads, reconhece automaticamente as ameaças e as elimina, se necessário. Serve de suporte útil à sentinela e bloqueia páginas Web e downloads maliciosos, antes de poderem ser executados.

Se uma página da internet for reconhecida pelo G DATA Software como ameaça, você receberá, em vez do website, uma página de informações da G DATA no navegador.

- **Desativar proteção Web**: Desactivar a protecção Web pode oferecer vantagens em termos de tempo, quando efectuar, por exemplo, downloads grandes de uma fonte segura. Em princípio, mesmo sem a protecção Web, o seu computador continua protegido através da sentinela de vírus. No entanto, só deve desistir da protecção Web em casos excepcionais.

- **Definir exceções**: A proteção da web cuida para que você não seja vítima de sites infectados ou fraudulentos. No entanto, em casos raros, pode acontecer que uma página da Internet não seja correctamente visualizada, apesar de ser de uma fonte segura. Neste caso, pode adicionar o endereço de Internet na lista branca, ou seja, poderá defini-lo como excepção e a protecção Web deixará de o bloquear. Leia o capítulo **Definir excepções** para saber como proceder.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | Antivírus | Proteção da Web**.

Verificação de e-mail

Através da verificação de e-mail poderá detectar vírus nos e-mails de entrada e saída, bem como nos respectivos anexos e eliminar possíveis infecções directamente na fonte. Se for detectado um vírus, o software consegue eliminar directamente os anexos de ficheiro ou

reparar ficheiros infectados.

- **Desativar verificação de e-mails**: Se você não desejar que seu G DATA Software verifique e-mails, então desative esta opção. A desactivação constitui, no entanto, um elevado risco de segurança e só deverá ser feito em caso de excepção.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | Antivírus | Verificação de e-mail**.

Microsoft Outlook: A verificação de e-mail é realizada através de um plugin. Esse oferece a mesma proteção que as funções de proteção orientadas a POP3/IMAP dentro das opções do AntiVírus. Após a instalação desse Plug-in, você encontrará no menu Extras do Outlook a função **Verificar a existência de vírus na pasta**, com a qual você poderá verificar a existência de vírus em suas pastas de e-mail individuais.

Proteção contra Spam

Ofertas, anúncios, boletins informativos – a onda de e-mails indesejados aumenta cada vez mais. Tem a sua caixa de correio a transbordar devido a mensagens de correio electrónico não solicitadas? O G DATA Software protege com segurança contra lixos de spam, bloqueia de forma eficiente remetentes de spam e evita reconhecimentos errôneos devido à combinação de critérios modernos de verificação de spam. Este módulo de software está disponível nas versões de programa G DATA Internet Security e G DATA Total Security.

- **Registro: Spam**: Aqui você obtém uma visão geral detalhada sobre todos os e-mails que foram classificados como spam pelo G DATA Software. Através do botão **Actualizar** pode consultar o estado dos dados mais actual do software e, através do botão **Eliminar**, remove todas as entradas marcadas até à data. Naturalmente, os e-mails propriamente ditos não serão eliminados no seu programa de e-mail. Através do botão **Na Whitelist**, você pode colocar diversos e-mails marcados na Whitelist para que os respectivos endereços de e-mail sejam em geral excluídos de outra verificação de spam. Através do botão **Na Blacklist**, você pode colocar um e-mail marcado na Blacklist e, com isso, verificar os respectivos endereços de e-mail especialmente quanto a elementos de spam.

- **Registro: Nenhum Spam**: Aqui você obtém uma visão geral detalhada sobre todos os e-mails que não foram classificados como spam pelo G DATA Software. Através do botão **Actualizar** pode consultar o estado dos dados mais actual do software e, através do botão **Eliminar**, remove todas as entradas marcadas até à data. Naturalmente, os e-mails propriamente ditos não serão eliminados no seu programa de e-mail. Através do botão **Na Whitelist**, você pode colocar diversos e-mails marcados na Whitelist para que os respectivos endereços de e-mail sejam em geral excluídos de outra verificação de spam. Através do botão **Na Blacklist**, você pode colocar um e-mail marcado na Blacklist e, com isso, verificar os respectivos endereços de e-mail especialmente quanto a elementos de spam.

- **Editar Whitelist**: Através da Whitelist você pode excluir determinados endereços de remetentes ou domínios, explicitamente da suspeita de spam. Para isso, clique no botão **Novo** e então insira no campo **Remetente/Domínios de remetente** o endereço de e-mail desejado (por exemplo, newsletter@informationsseite.de) ou o domínio (por exemplo, informationsseite.de) que deseja excluir da suspeita de spam e o G DATA Software não tratará e-mails desse remetente ou domínio remetente como spam. Através do botão Importar, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Whitelist. Os endereços e domínios têm de ser enumerados numa lista deste género em linhas individuais. O formato utilizado é um ficheiro txt simples, que pode ser criado, por exemplo no Windows Notepad. Através do botão **Exportar** você também pode exportar uma Whitelist como arquivo de texto.

- **Editar blacklist**: Através da Blacklist, você pode colocar determinados endereços de remetentes ou domínios explicitamente em suspeita de spam. Para isso, clique no botão **Novo** e então insira no campo **Remetente/Domínios de remetente** o endereço de e-mail desejado (por exemplo, newsletter@megaspam.de.vu) ou o domínio (por exemplo, megaspam.de.vu) que deseja excluir da suspeita de spam e o G DATA Software não tratará e-mails desse remetente ou domínio remetente como uma probabilidade muito alta de spam. Através do botão **Importar** também pode importar endereços de e-mail ou domínios para a lista negra. Os endereços e domínios têm de ser enumerados numa lista deste género em linhas individuais. O formato utilizado é um ficheiro txt simples, que pode ser criado, por exemplo no Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Blacklist como arquivo de texto.

- **Desativar protecção contra spam**: Caso necessário, pode desactivar aqui a protecção anti-spam no seu computador, por ex. se não tiver qualquer programa de e-mail instalado no seu computador.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | AntiSpam | Filtro de spam**.

Última actualização

Aqui é apresentada a data em que o seu computador recebeu pela última vez assinaturas de vírus actuais pela Internet. Se esta entrada estiver marcada a vermelho, deverá efectuar uma actualização de vírus o mais rapidamente possível. Para isso, clique simplesmente na entrada e seleccione a opção **Actualizar assinaturas de vírus**.

- **Atualizar assinaturas de vírus**: Habitualmente, as actualizações das assinaturas de vírus são feitas automaticamente. Se desejar executar uma actualização imediatamente, clique neste botão.

- **Desativar actualizações automáticas**: Caso que você não queira que o G DATA Software cuide automaticamente da atualização das assinaturas de vírus, selecione esta opção. A desactivação constitui, no entanto, um elevado risco de segurança e só deverá ser feito em caso de excepção.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | Antivírus | Atualizações**.

Próxima actualização

Nessa entrada é possível visualizar a próxima atualização prevista. Se você quiser fazer a atualização, clique simplesmente no registro e selecione a opção **Atualizar assinaturas de vírus**.

- **Actualizar assinaturas de vírus**: Habitualmente, as actualizações das assinaturas de vírus são feitas automaticamente. Se desejar executar uma actualização imediatamente, clique neste botão.

- **Desativar actualizações automáticas**: Caso que você não queira que o G DATA Software cuide automaticamente da atualização das assinaturas de vírus, selecione esta opção. A desactivação constitui, no entanto, um elevado risco de segurança e só deverá ser feito em caso de excepção.

- **Outras configurações**: Informações sobre isso estão no capítulo **Configurações | Antivírus | Atualizações**.

BankGuard

Os cavalos de troia bancários são uma ameaça crescente. A cada hora, os criminosos on-line desenvolvem novas variantes de malware (p. ex., ZeuS, SpyEye) para roubar seu dinheiro. Os bancos protegem o tráfego de dados na internet, mas os dados são decodificados no navegador e é lá que os cavalos de troia atacam. A tecnologia inovadora do G DATA BankGuard protege as suas negociações bancárias desde o começo e faz a proteção exatamente onde o ataque está ocorrendo. Através de uma verificação da veracidade das bibliotecas da rede usadas, o G DATA BankGuard garante que o seu navegador de internet não seja manipulado por um cavalo de troia bancário. Recomendamos sempre deixar ativada a proteção do G DATA BankGuard.

Prot. keylogger

A proteção do Keylogger monitora, independentemente das assinaturas de vírus, se as entradas do teclado no seu sistema são espionadas. Com isso, são eliminadas as possibilidades de atacantes registrarem as suas inserções de senhas. Esta função deve sempre permanecer ligada.

Exploit Protection

Um exploit apoveita as fraquezas do software de aplicação comum e, no pior dos casos, pode assumir o controle do seu computador com estas vulnerabilidades. Os exploits podem atacar mesmo quando os aplicativos (por exemplo, visualizador de PDF, navegador, e etc.) são atualizados regularmente. A Exploit Protection protege de tais ataques, também de forma proativa contra os ataques até então desconhecidos.

Licença

Na entrada **Licença**, do lado esquerdo da interface do programa, verá até quando é que a sua licença é válida para as actualizações de vírus. Em nenhum outro tipo de software as actualizações permanentes são tão importantes como no software antivírus. Antes que a sua licença expire, o software lembrá-lo-á automaticamente de renovar a sua licença. De forma confortável e simples através da Internet!

Dados de acceso

Quando você clica no campo **Dados de acceso** na área da licença, aparece uma caixa de diálogo informando o seu nome de usuário. Informações sobre isso estão no capítulo **Configurações | Antivírus | Actualizações**. Se você tiver dúvidas se tem licença, podemos ajudar com **G DATA ServiceCenter** estas informações. Se você esquecer a sua senha, você pode gerar uma nova senha de forma rápida e sem complicações através desta caixa de diálogo.

Módulos de software

Os seguintes módulos de software estão disponíveis, dependendo da versão instalada do software:

SecurityCenter: Se centro de segurança pessoal. Aqui são encontradas informações necessárias para a proteção do computador contra software malicioso e que reagem especificamente contra ameaças.

Proteção antivírus: Nesta área são encontradas informações sobre quando o computador foi verificado a última vez contra vírus e se a sentinela de vírus está fazendo a proteção ativa contra infecções, além disso, pode ser feita a verificação direta contra software malicioso do computador e memória de dados, a edição de arquivos infectados na quarentena e a criação de uma mídia de boot.

Firewall: Um firewall protege o seu computador de ser "espionado", verificando quais os dados e programas transferidos da Internet ou da rede para o seu computador e quais os dados enviados pelo seu computador. Assim que algo indique que estão a ser transferidos dados para o seu computador, ou descarregados dados a partir do mesmo, sem autorização, o firewall dá o alarme e bloqueia a troca de dados não autorizada. Este módulo de software está disponível nas versões de programa G DATA Internet Security e G DATA Total Security.

Cópia de segurança: Com a digitalização progressiva da vida diária, a utilização de serviços de música on-line, câmeras digitais e correspondências de e-mail, é cada vez mais importante proteger os seus dados pessoais. Quer seja pelo perigo latente de erros de hardware, de um descuido pessoal ou de danos provocados por vírus ou ataques de hackers, deve criar regularmente uma cópia de segurança dos seus documentos privados. O módulo de backup assume essa tarefa para você e protege assim a sua documentação e arquivos importantes, sem que você tenha que pensar constantemente no assunto. Este módulo de software está disponível nas versões de programa G DATA Total Security.

Gerenciador de senhas: Com o gerenciador de senhas você pode gerenciar com comodidade as suas senhas e utilizá-lo como plug-in no seu navegador. Este módulo de software está disponível nas versões de programa G DATA Total Security.

Optimizador: Desde o lembrete automático para Windows Updates, desfragmentação automática periódica, até a remoção regular de registros desnecessários do registro e arquivos temporários, com o otimizador, você tem uma ferramenta nas mãos que torna o seu sistema Windows significativamente mais rápido e claro. Este módulo de software está disponível nas versões de programa G DATA Total Security.

Protecção infantil: Com a proteção infantil é possível controlar o comportamento na navegação e a utilização do computador para suas crianças. Este módulo de software está disponível nas versões de programa G DATA Internet Security e G DATA Total Security.

Criptografia: O módulo de criptografia serve como um cofre de banco para a proteção de dados sensíveis. Um cofre pode ser usado, por exemplo, como uma unidade adicional como uma partição adicional do disco rígido e pode ser operado facilmente. Este módulo de software está disponível nas versões de programa G DATA Total Security.

Gerenciador de inicialização automática: Com o Gerenciador de inicialização automática é possível administrar programas que são inicializados automaticamente ao iniciar o Windows. Normalmente estes programas são carregados diretamente na inicialização do sistema. Quando são administrados pelo Gerenciador de inicialização automática, podem ser iniciados também com atraso de tempo ou de acordo com a capacidade do sistema ou do disco rígido. Isso permite uma inicialização mais rápida do sistema, melhorando assim o desempenho do computador.

Controlo de dispositivos: Com esta função, o usuário pode limitar a utilização de dispositivos como mídia de dados removível, unidade de disquete, de CD e de DVD. Deste modo é possível, por exemplo, prevenir a exportação ou importação indesejada de arquivos ou a instalação indesejada de softwares. Agora também com USB Keyboard Guard. Informações sobre isso estão no capítulo Controle de dispositivo.

Proteção antivírus

Por este módulo pode ser feita a verificação específica sobre infecção ou software malicioso no seu computador ou mídia de dados selecionada. Isso é recomendado quando, por exemplo, você receber CDs gravados ou pen drives de amigos, parentes ou colegas de trabalho. Também ao instalar novos softwares ou fazer downloads da internet, é recomendada uma verificação de vírus.

> **Atenção**: A verificação do computador ou mídia de dados selecionada serve como proteção adicional. Basicamente, você está protegido de forma ideal contra ameaças por software malicioso com a G DATA Verificação em modo ocioso e a sentinela de vírus da G DATA, os quais estão sempre ativos em segundo plano. Uma verificação de vírus também encontraria vírus que tivessem sido copiados para seu computador, antes que o G DATA Software tivesse sido instalado, ou que você tivesse adquirido enquanto a sentinela de vírus não estivesse ligada.

Verificação de vírus

Selecione aqui qual área do computador ou qual memória de dados você deseja verificar especificamente:

Verificar o computador (todos os discos rígidos locais): Quando desejar controlar o seu computador de forma independente da verificação automática através da verificação em modo ocioso (por ex., devido a uma atual suspeita de vírus), basta clicar neste registro. Será então efectuada uma análise do seu computador com vista à detecção de vírus. Leia também o seguinte capítulo: Fazer a verificação de vírus.

Comprobaciones programadas: Com este recurso você pode programar verificações automáticas. Leia também o seguinte capítulo: Verificações automáticas de vírus.

Verificar memória e início automático: Através desta opção, para todos os processos em andamento são verificados os arquivos de programa e as bibliotecas de programas (DLLs). Desta forma, os programas maliciosos poderão ser removidos diretamente da memória e da área de memória e inicialização automática. Portanto, é possível eliminar directamente os vírus activos sem que seja necessário efectuar uma pesquisa no disco rígido inteiro. Essa função não é uma substituição de um controle de vírus constante dos dados armazenados, ela é apenas uma complementação.

Verificar directórios/ficheiros: Através dessa opção, você verifica a existência de vírus em unidades, diretórios ou arquivos. Ao clicar nesta ação, uma opção de diretório e arquivo é aberta. Aqui é possível verificar objetivamente a existência de infecção de vírus em arquivos individuais e também em diretórios completos. Na árvore de diretórios, clicando nos sinais de "mais", é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada directório ou cada ficheiro com marca de verificação colocada será verificado pelo software.

Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Verificar suportes amovíveis: Com esta função, verifique CD-ROMs ou DVD-ROMs, cartões de memória ou pen drives quanto à infecção por vírus. Clique nesta acção para verificar todos os suportes amovíveis ligados ao computador (incluindo CDs ou cartões de memória inseridos, discos rígidos ligados por USB ou pen drives USB). Tenha em atenção que, naturalmente, o software não consegue remover vírus dos suportes que não permitam o acesso para gravação (por exemplo CD-ROMs gravados). Nestes casos, o vírus detectado é registado.

Verificar RootKits: Os Rootkits tentam escapar dos métodos comuns de detecção de vírus. Com esta função pode procurar vírus de Rootkits de forma orientada, sem ter de efectuar uma verificação integral dos discos rígidos ou dos dados guardados.

Ficheiros em quarentena

Durante a verificação de vírus tem a possibilidade de reagir de várias formas aos vírus detectados. Uma das opções é enviar o ficheiro infectado para a quarentena. A quarentena é uma área protegida dentro do software onde os ficheiros infectados são armazenados e codificados, sendo assim impedidos de passar o vírus a outros ficheiros.

Exibir a quarentena: Quando você clicar nesse botão, é aberta a área da quarentena.

Os arquivos em quarentena permanecem então no estado em que foram encontrados pelo G DATA Software e você pode decidir como deseja proceder.

- **Actualizar**: Se tiver a janela de diálogo aberta durante um período de tempo mais longo e entretanto for detectado um vírus, que seja enviado para a quarentena (por ex. automaticamente através da sentinela de vírus), pode actualizar a interface através deste botão.

- **Permitir no futuro**: Se o monitor de comportamento colocou na quarentena um arquivo inofensivo por engano, você pode adicioná-lo à lista branca para evitar que o monitor de comportamento mova o arquivo para a quarentena no futuro.
- **Desinfectar**: Em muitos casos ainda é possível salvar ficheiros infectados. O software elimina os componentes do vírus no ficheiro infectado e, deste modo, reconstrói o ficheiro original não infectado. Se a desinfecção for bem sucedida, o ficheiro é enviado automaticamente para a localização onde estava guardado antes da verificação de vírus e voltará a estar à sua disposição sem quaisquer restrições.
- **Mover para a localização original**: Por vezes, pode ser necessário mover de novo da quarentena para o seu local de armazenamento original um ficheiro infectado, que não possa ser desinfectado. Isto pode ser efectuado, por exemplo, para salvar dados. Esta função só deve ser executada em casos excepcionais e sob medidas de segurança rigorosas (por ex., separar o computador da rede/ Internet, criar previamente uma cópia de segurança de dados não infectados).
- **Eliminar**: Se já não precisar do ficheiro infectado pode eliminá-lo simplesmente da quarentena.

Mídia de boot

A mídia de boot é uma ferramenta útil para livrar de vírus, computadores que já estejam contaminados. Principalmente para computadores que, antes da instalação do G DATA Software, não tinham nenhuma proteção de vírus, recomenda-se a utilização de uma mídia de boot. Como usar uma **mídia de boot** pode ser visto no capítulo **BootScan**.

Para criar uma mídia de boot, clique no botão **Criar mídia de boot** e siga as instruções do assistente de instalação. Aqui você tem a possibilidade de baixar as últimas assinaturas de vírus, para poder criar a mídia de boot já atualizada, além disso, pode ser feita a seleção de gravar a mídia de boot em CD/DVD ou usar um pen drive como mídia de boot.

Se a versão de programa usada for o G DATA Total Security, é possível fazer a restauração de uma unidade de backup com uma mídia de boot também no volume no qual o sistema está atualmente. A restauração de um backup de unidades ou de arquivos para outros destinos também é possível aqui. Para isso, insira a mídia de boot e selecione a função **Iniciar restauração**.

Firewall

Um firewall protege o seu computador contra a *espionagem*, verificando quais os dados e programas transferidos da Internet ou da rede para o seu computador e quais os dados enviados pelo seu computador.

No módulo de firewall estão disponíveis três áreas:

- **Estado**: Na área de status do Firewall, você obtém informações básicas sobre a situação atual do seu sistema e do Firewall.
- **Redes**: Na área de redes, são listadas as redes (por ex. LAN, DFÜ, etc.) com as quais o seu computador está conectado.
- **Conjuntos de regras**: Nesta área podem ser criadas regras especiais para diferentes redes e assim otimizar o comportamento de seu Firewall.

Assim que algo indicar que os dados em seu computador foram reproduzidos ou descarregados indevidamente, o firewall dá um alarme e bloqueia a troca de dados indevida.

 **Configurações:** Através desse botão na parte superior direita, você pode acessar todos os diálogos de configuração do Firewall.

Estado

Na área de estado do firewall acede a informações básicas sobre o actual estado do seu sistema e do firewall. Estas encontram-se à direita da respectiva entrada em forma de indicação textual ou numérica. Além disso, o estado dos componentes também é representado de forma gráfica. Através de um clique duplo no respectivo registro, é possível executar ações diretamente ou alterar para a respectiva área de programa.

Assim que tiver otimizado as configurações de um componente com o ícone de aviso, o ícone na área de status alterna novamente para o símbolo de marcação verde.

- **Segurança**: Enquanto utiliza o computador para o seu trabalho diário, o firewall aprende, gradualmente, quais os programas que utiliza para aceder à Internet, quais os que não utiliza e quais os que representam um risco de segurança. Independentemente do seu grau de conhecimento sobre tecnologia firewall, pode configurar o firewall de modo a que este ofereça uma excelente protecção básica, sem necessitar de muita assistência ou uma protecção profissional, adaptada ao seu tipo de utilização do computador, mas que também exige da sua parte determinados conhecimentos como utilizador. O status de proteção pode configurado aqui: **Configurações | Firewall | Automático**.
- **Modo**: Aqui será informado com que configuração básica se encontra o seu firewall a funcionar de momento. As possibilidades aqui são a criação manual de regras ou o Automático (Piloto automático).

  Piloto automático: Aqui, o firewall funciona de forma totalmente autónoma, afastando automaticamente o perigo do computador doméstico. Essa configuração oferece uma proteção geral prática e é, na maioria dos casos, recomendável. O piloto automático deveria estar ligado por padrão.

  Outras configurações: Se desejar configurar o seu Firewall de forma individual ou não desejar que determinados aplicativos trabalhem junto com o modo piloto automático, você poderá ajustar a sua proteção de Firewall para as suas necessidades pessoais com a criação manual de regras. Outras informações estão no seguinte capítulo: **Configurações | Firewall | Automático**.
- **Redes**: Aqui você pode ser feita a exibição de redes, nas quais se encontra o seu computador. Outras informações estão no seguinte capítulo: **Firewall | Redes**.
- **Ataques Impedidos**: Logo que o firewall registe um ataque no seu computador, este será bloqueado e registado. Ao clicar no item de menu, pode receber informações mais detalhadas.
- **Radar de aplicações**: O campo de diálogo exibe os programas que estão sendo bloqueados pelo Firewall no momento. Se você desejar permitir que um dos aplicativos bloqueados acesse a rede, basta selecioná-los e clicar no botão **Permitir**.

Redes

Na área de redes, são listadas as redes (por ex. LAN, dial-up, etc.) com as quais o seu computador está conectado. Aqui também será exibido de acordo com qual conjunto de regras (consulte o capítulo **Conjuntos de regras**) cada rede é protegida. Se remover a marca de verificação que se encontra antes da respectiva rede, esta será excluída da protecção do firewall. No entanto, a protecção apenas deve ser desactivada em casos singulares justificados. Se assinalar uma rede com o rato e clicar no botão **Editar** poderá visualizar ou alterar ou ver as configurações do firewall para esta rede.

Editar rede

As seguintes informações e possibilidades de configuração para a rede selecionada são mostradas nesta visão geral:

- **Informações sobre a rede**: Aqui você obtém informações sobre a rede - desde que disponível - como informações do endereço IP, máscara da sub-rede, gateway padrão, servidor DNS e WINS.
- **Firewall activo nessa rede**: Aqui poderá desactivar o firewall para a rede, devendo fazê-lo apenas em situações únicas e justificadas.
- **Utilização conjunta da ligação da Internet**: Em conexões diretas com a internet, é possível definir se todos os computadores da rede devem ter ou não acesso à internet através de um computador conectado à internet. Esta autorização de ligação à Internet (ICS) pode ser, por norma, activada para uma rede doméstica.
- **Permitir a configuração automática (DHCP)**: Na conexão do seu computador com a rede, é fornecido um endereço IP dinâmico (através do DHCP = Protocolo dinâmico de configuração de host). Se o utilizador estiver ligado à rede por meio destas configurações padrão deverá deixar o visto a marcar esta opção.
- **Conjunto de regras**: Aqui, poderá muito rapidamente escolher entre conjuntos de regras pré-estruturados e estabelecer se, para efeitos de monitorização do firewall, a rede se trata, por exemplo, de uma rede confiável, não confiável ou de uma rede a ser bloqueada. Com o botão **Editar conjunto de regras** também tem a possibilidade de configurar individualmente os conjuntos de regras. Para mais informações, leia também o capítulo **Criar conjuntos de regras**.

Conjuntos de regras

Nesta área poderá criar regras especiais para as diversas redes. Estas regras são depois combinadas num conjunto de regras. Conjuntos de regras para a conexão direta com a internet, redes não confiáveis, redes confiáveis e redes a serem bloqueadas são predefinidos. Na vista geral, o respectivo conjunto de regras é visualizado com o nome. Com a ajuda do botão **Novo**, **Eliminar** e **Editar** poderá alterar os conjuntos de regras já existentes ou adicionar conjuntos adicionais de regras.

Os conjuntos de regras estabelecidos para a **ligação directa à Internet**, as **redes fiáveis**, as **redes não fiáveis** e as **redes que devem ser bloqueadas** não podem ser eliminados. Os conjuntos de regras adicionais criados pelo próprio utilizador podem certamente ser eliminados a qualquer altura.

Criar conjuntos de regras

Você pode atribuir a cada rede um conjunto de regras próprio (ou seja, uma coleção especial de regras definidas para isso). Desta forma, o firewall consegue proteger de forma diferente as redes com diferentes níveis de perigosidade. Assim, uma rede doméstica privada precisa possivelmente de menos proteção (e também trabalho de gerenciamento) do que uma rede dial-up que está em contato direto com a Internet.

Além disso, com o botão **Novo** poderá criar também conjuntos de regras próprios para redes. Para isso, clique na área de conjunto de regras no botão **Novo**e defina o seguinte na caixa de diálogo que aparece:

- **Nome do conjunto de regras**: Introduza aqui um nome explícito para o conjunto de regras.
- **Criar um conjunto de regras vazio**: Aqui você pode criar um conjunto de regras totalmente vazio e preenchê-lo exclusivamente com regras próprias definidas.
- **Criar um conjunto de regras que contenha algumas regras úteis**: Nessa seleção, você pode decidir se, no novo conjunto de regras, as regras básicas para redes não confiáveis, confiáveis e redes a serem bloqueadas deverão ser predefinidas. Com base nessas pré-definições poderá então executar as alterações individuais.

O firewall contém três conjuntos de regras predefinidos para os seguintes tipos de rede:

- **Conexão direta com a Internet**: Isto inclui regras, que tratam do acesso direto à Internet.
- **Redes não confiáveis**: Aqui estão incluídas em geral as redes abertas, como por exemplo, redes dial-up que têm acesso à internet.

- **Redes confiáveis**: Confiáveis são em geral as redes domésticas e redes empresariais.

- **Redes a serem bloqueadas**: Se o contacto de um computador a uma rede tiver de ser temporária ou permanentemente bloqueado pode usar-se esta opção. Isto faz sentido, por exemplo, durante a ligação a redes estranhas cujo nível de segurança não é suficientemente claro (por exemplos em Partys LAN, redes de outras empresas, locais de trabalho públicos para computadores portáteis, etc.)

O novo conjunto de regras aparecerá agora na área de conjuntos de regras abaixo do respectivo nome do conjunto de regras (p.ex., *Novo conjunto de regras*) na lista. Se clicar em **Editar**, abre-se, dependendo da configuração efectuada em **Configurações | Outros** (ver capítulo com o mesmo nome), o Assistente de regras ou omodo de edição avançado para poder editar cada regra deste conjunto de regras. Se quiser atribuir novas regras ao conjunto de regras leia por favor o capítulo **Utilizar o assistente de regras** ou **Utilizar o modo de edição avançado**.

Além da introdução directa de regras, o utilizador tem também a possibilidade de criar novas regras por meio da caixa de diálogo do alarme do firewall. Este processo de aprendizagem do firewall é descrito no capítulo **Alarme do firewall** seguintes.

Utilizar o assistente de regras

Com o assistente de regras, você pode definir regras adicionais para o respectivo conjunto de regras ou alterar as regras existentes. Principalmente para usuários que não têm bons conhecimentos sobre o assunto tecnologia de firewall, recomendamos utilizar o assistente de regras, e não o modo de edição.

Com o assistente de regras pode alterar uma ou várias regras dentro do conjunto de regras escolhido. Assim, o utilizador está sempre a criar uma regra dentro de um conjunto de regras que já contém diversas outras regras.

Dependendo do conjunto de regras que escolheu para a respectiva rede, uma aplicação pode estar bloqueada dentro de um conjunto de regras (por exemplo para redes não fiáveis), tendo no entanto noutro conjunto de regras (por exemplo para redes fiáveis) o acesso total. Dessa forma será possível, por exemplo, limitar um navegador com regras diferentes, de forma que no entanto este possa aceder a páginas que se encontram disponíveis na sua rede doméstica, mas não tendo qualquer possibilidade de aceder a conteúdos da rede de transmissão de dados.

O assistente de regras disponibiliza-lhe as seguintes regras básicas:

- **Liberar ou bloquear aplicativos**: Aqui poderá escolher directamente uma aplicação (um programa) no seu disco rígido e autorizar ou proibir explicitamente o seu acesso à rede definida por meio do conjunto de regras. Para isso, selecione no assistente o programa desejado (**Caminho do programa**) e informe em **Direção** se o programa deve ser bloqueado para conexões de entrada, conexões de saída ou tanto para conexões de entrada como para conexões de saída. Dessa forma, você pode, p.ex., impedir que o software do seu MP3 repasse dados sobre seus hábitos de áudio (conexões de saída) ou cuidar para que atualizações automáticas do produto sejam executadas (conexões de entrada).

- **Liberar ou bloquear serviços de rede**: Por **porta** são designadas áreas especiais de endereços, por meio dos quais uma rede encaminha automaticamente dados transmitidos a um determinado protocolo e depois a um determinado software. Assim, por exemplo, a transmissão de páginas da Internet regulares ocorre pela Porta 80, o envio de e-mails pela Porta 25, a recolha de e-mails pela Porta 110 e assim por diante. Se não tiver firewall, geralmente todas as portas no seu computador se encontram abertas, apesar de a maioria não ser necessária aos utilizadores normais. Assim, bloqueando uma ou várias portas poderão rapidamente fechar-se algumas brechas que de outra forma poderiam ser aproveitadas pelos hackers para a realização de ataques. No assistente terá então a possibilidade de bloquear totalmente as portas ou bloquear apenas para uma determinada aplicação (por exemplo o seu software de reprodução de MP3).

- **Liberação de arquivos e impressora**: Se o acesso for permitido, existe a possibilidade de usar as pasta e impressora liberadas na rede. Ao mesmo tempo, outros computadores e usuários na rede podem ter acesso às liberações (desde que assim definido).

- **Liberar ou bloquear serviços de domínio**: Um Domínio é um tipo de diretório estrutural para computadores em uma rede e possibilita com isso, um gerenciamento centralizado dos computadores vinculados em uma rede. As permissões para os serviços de domínio em redes não fiáveis deveriam, por norma, ser negadas.

- **Utilização compartilhada da conexão de Internet**: Em conexões diretas com a internet, é possível definir se todos os computadores da rede devem ter ou não acesso à internet através de um computador conectado à internet. Essa liberação da conexão à internet geralmente pode ser ativada para uma rede doméstica.

- **Liberar ou bloquear serviços de VPN**: VPN é a abreviatura para redes virtuais privadas e identifica a possibilidade de vincular exclusivamente computadores e fazer quase uma conexão direta entre estes computadores. Para que serviços de VPN possam funcionar, eles devem ser liberados pelo firewall.

- **Editor de conjunto de regras avançado (Modo expert)**: Aqui pode alternar do assistente de regras para o modo de edição avançado. Poderá aceder a mais informações sobre o modo de edição avançado no capítulo **Utilizar o modo de edição avançado**.

Utilizar o modo de edição avançado

No modo de edição avançado poderá (partindo do pressuposto que tem alguns conhecimentos em segurança de redes) definir regras muito individuais para a respectiva rede. Naturalmente que aí poderão também ser criadas todas as regras que também pode criar por meio do Assistente de regras, mas aqui tem ainda a possibilidade de executar configurações mais extensivas.

Encontram-se à sua disposição as seguintes possibilidades de configuração:

- **Nome**: Aqui poderá modificar, se necessário, o nome para o conjunto de regras actual. É com este nome que o conjunto de regras é então apresentado na lista na área do Conjuntos de regras, podendo ser combinado com as redes aí identificadas pelo firewall.
- **Modo furtivo**: Com o modo furtivo, as consultas ao computador que servem para verificar a acessibilidade da respectiva porta não obterão resposta. Desta forma, dificulta a obtenção de informações sobre o sistema por parte dos hackers.
- **Acção, caso nenhuma regra se aplique**: Aqui é possível definir se o acesso à rede deve ser, em geral, permitido, recusado ou regulado sob solicitação. Se outras regras forem definidas para programas individuais através da função autodidata do firewall, essas serão naturalmente consideradas.
- **Modo adaptativo**: O modo adaptativo auxilia você com os aplicativos que utilizam a chamada tecnologia de canal reverso (por ex., FTP e diversos jogos on-line). Esse tipo de aplicativo conecta-se a um computador remoto e trata com ele um canal reverso, a partir do qual o computador remoto se *reconecta* a seu aplicativo. Se o modo adaptativo estiver activado, o firewall reconhece esse canal de retorno e mantém-no fechado sem o questionar.

Regras

Na lista de regras, você pode encontrar todas as regras definidas para esse conjunto de regras. Aqui o utilizador poderá, por exemplo, conceder a programas seleccionados um acesso abrangente à rede, apesar de essa mesma rede não ter sido definida como uma rede fiável. As regras que entram para este conjunto podem ser geradas de diferentes formas:

- Por meio do **Assistente de regras**.
- Directamente pelo **modo de edição avançado** através do botão **Novo**.
- Na caixa de diálogo da caixa Info, que aparece em um **Alarme do firewall**.

Claro que cada conjunto de regras tem uma lista própria com regras.

Como as regras do firewall são estruturadas parcialmente de forma hierárquica, em alguns casos, é importante observar a classificação das regras. Por isso pode acontecer que uma das autorizações relativas a uma porta possa voltar a ser bloqueada através da proibição de um acesso de protocolo. Poderá alterar a posição de classificação de uma regra, marcando-a com o rato e movimentando-a para cima ou para baixo na lista, com as teclas de seta em **Classificação**.

Se você criar uma nova regra através do modo de edição avançado ou alterar uma regra existente através da caixa de diálogo **Editar**, aparece a caixa de diálogo **Editar regra** com as seguintes possibilidades de configuração:

- **Nome**: Aqui é encontrado, em regras predefinidas e geradas automaticamente, o nome do programa para o qual a respectiva regra se aplica.
- **Regra ativa**: Removendo o visto de marcação de uma regra poderá desactivá-la sem, no entanto, a apagar.
- **Comentário**: Aqui pode ficar a saber de que forma a regra foi criada. Em regas predefinidas para o conjunto de regras é exibido Regra predefinida, em regras, que foram geradas a partir da caixa de diálogo do **Alarme do firewall** é exibida gerada por solicitação e, para as regras geradas por você mesmo através do modo de edição avançada, você pode inserir o seu próprio comentário.
- **Direção da conexão**: Com a direção, é definido se essa é uma regra para regra de conexões de entrada, de saída ou de conexões de entrada e saída.
- **Acesso**: Aqui é definido se o acesso deverá ser permitido ou proibido para o programa correspondente dentro deste conjunto de regras.
- **Registro**: Aqui poderá escolher a que protocolos de ligação pretende conceder uma autorização ou pretende proibir. Aí terá a possibilidade de bloquear ou autorizar registos a nível geral, ou interligar a utilização do registo com o uso de um determinada aplicação ou de várias aplicações (**Atribuir aplicativo**). Do mesmo modo, poderá definir de forma precisa as portas indesejadas ou desejadas, clicando no botão **Atribuir serviço da Internet**.
- **Janela de tempo**: Também poderá configurar o acesso aos recursos da rede tornando-os dependentes a nível temporal fazendo, por

exemplo, com que o acesso apenas seja autorizado durante o período de trabalho e não fora deste período de tempo específico.

- **Espaço de end. IP**: Justamente para as redes com IPs fixos atribuídos faz sentido organizar a sua utilização através de uma limitação do espaço de endereço IP. Um espaço de endereço IP claramente definido diminui significativamente o perigo de ataques por parte de hackers.

Cópia de segurança

Com o avanço da digitalização do quotidiano, com a utilização dos serviços de música online, das câmaras digitais e da correspondência electrónica, a protecção dos seus dados pessoais ganha cada vez mais importância. Quer seja pelo perigo latente de erros de hardware, de um descuido pessoal ou de danos provocados por vírus ou ataques de hackers, deve criar regularmente uma cópia de segurança dos seus documentos privados. O G DATA Software assume essa tarefa para você, protegendo, assim, seus documentos e arquivos importantes, sem que você tenha que pensar constantemente no assunto.

Salvar e restaurar

Assim que uma tarefa de backup é criada pela função **Nova tarefa**, você pode editá-lo e controlá-lo diretamente pelos seguintes ícones:

Restauração: Assim, os dados arquivados no backup são restaurados para o sistema. O processo da restauração é explicado no capítulo **Restaurar backup** seguintes.

Backup: Assim, o procedimento de backup é iniciado imediatamente para a tarefa de backup definida e fora de sequência, independente de uma programação pré-definida para este backup.

Configurações: Aqui podem ser feitas as alterações para a tarefa de backup correspondente, que foram definidas na primeira criação desta tarefa de backup em **Nova tarefa de backup**.

Registros: Aqui você tem uma visão geral de todos os processos que são feitos por esta tarefa de backup. Aqui estão registros sobre processos de backup feitos manualmente ou programados, informações sobre eventuais restaurações e também mensagens de erro, por exemplo se o diretório de destino não tinha mais espaço suficiente para o salvamento do backup a ser feito.

Nova tarefa de backup

Para atribuir uma nova tarefa de backup, clique no botão **Nova tarefa**.

Seleção de arquivos / Discos rígidos / Partições

Agora o assistente de backup pergunta, que tipo de backup você deseja executar.

Backup de ficheiro: Aqui trata-se de um backup de determinados arquivos e pastas de um arquivo compactado selecionados por você.

Na visualização de diretório selecione quais arquivos e pastas deseja salvar. Em geral, recomenda-se salvar arquivos pessoais durante um backup e não fazer o backup de arquivos de programa instalados. Na árvore de diretórios, clicando nos sinais de mais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada diretório ou arquivo com uma marcação será usado pelo software para o backup. Se nem todos os arquivos e pastas forem usados em um diretório para o backup, haverá uma marcação em cinza nesse diretório.

Backup de unidade: Trata-se aqui de um backup completo de discos rígidos ou partições em um arquivo compactado.

Selecção do destino

Aqui é possível definir o destino, ou seja, o local onde o G DATA Software deverá criar a cópia de segurança dos arquivos e das pastas ou discos rígidos e partições. Pode tratar-se de uma unidade de CD ou DVD-ROM, um outro disco rígido, uma pen drive USB, outros suportes amovíveis ou um directório na rede.

Nome do arquivo: Aqui pode ser definido um nome significativo para o arquivo compactado que será criado, por ex., *Arquivos próprios do backup semanal*, *Backup de MP3* ou semelhantes.

Nova pasta: Se você quiser criar uma nova pasta para o backup, selecione na visualização do diretório o local desejado para salvamento e clique no botão **Nova pasta**.

> **Observação**: Preste atenção para que o backup não seja feito no mesmo disco rígido onde se encontram os dados originais. Se este disco tiver um defeito, perdem-se os dados originais e os dados de cópia de segurança. Conserve uma cópia de segurança num local, que esteja separado dos ficheiros originais em termos de espaço, ou seja, por ex. noutra divisão, num disco rígido USB ou gravada num CD/DVD-ROM.

Criar arquivo na nuvem: Utilize um serviço de nuvem simples como, por exemplo, Dropbox, Microsoft OneDrive*, TeamDrive** ou GoogleDrive, para fazer uma cópia de segurança do seu backup. Basta se registrar com os dados de acesso do seu serviço de nuvem e o arquivo de backup será vinculado automaticamente ao seu serviço de nuvem.

> **Observação**: Você deve observar ao fazer o backup na nuvem que os seus dados de backup estão criptografados. Na área **Opções** em **Nova tarefa de backup** você pode ativar ou desativar a encriptação dos seus dados.
>
> **(*) Observação sobre o OneDrive**: Você pode utilizar o OneDrive se você integrou este serviço como drive virtual no Windows Explorer. O arquivo é criado normalmente através do diretório de arquivos e não através da função **Criar arquivo na nuvem**.
>
> **(**) Nota sobre o TeamDrive**: Você pode selecionar TeamDrive depois de usar o software TeamDrive no seu PC para configurar e selecionar um espaço TeamDrive.

Agendamento

Aqui pode ser definido em qual ritmo os seus arquivos selecionados devem ser protegidos por um backup, por outro lado, pode ser feita a definição de qual tipo de backup deve ser executado. Há o backup básico, no qual todos os dados selecionados são completamente protegidos, por opção, também a possibilidades de salvar por backups parciais apenas alterações feitas desde o último backup.

Se você selecionar **Manual** o backup não será executado automaticamente, mas deve ser iniciado pessoalmente, especificamente pela interface do programa. Em **Diariamente**, é possível definir com a ajuda das indicações em dias da semana que, p.ex., o seu computador só executará a otimização em dias úteis ou até mesmo a cada dois dias ou, nos fins de semana onde ele não é utilizado para trabalhar. Além disso, pode ser feita a definição para backups semanais e mensais.

Não executar no modo de bateria: Para que um procedimento de backup em um notebook não seja interrompido de repetente por que a bateria do notebook está vazia, pode ser feita a definição, para que backups sejam feitos apenas quando o notebook estiver conectado na energia elétrica.

Executar cópia de segurança completa

Em **Executar o backup completo**, informe a frequência, os dias e o horário em que o backup correspondente deverá ocorrer. Assim, no turno escolhido, será automaticamente criado um backup de todos os dados em **Seleção de arquivos / Discos rígidos / Partições** selecionados para tal.

> **Atenção**: O Backup de programação controlada não funciona com CD-ROM ou DVD-ROM, porque aqui, será necessário a intervenção do usuário na troca da mídia.

Na seção **Excluir pastas antigas**, é possível definir como o G DATA Software deverá proceder com backups já existentes. O G DATA Software arquiva os seus dados respectivamente em um único arquivo com a extensão ARC. As cópias de segurança que não são substituídas aumentam adicionalmente a segurança dos seus dados, porque mesmo em caso de dano do arquivo actual, estará disponível um arquivo mais antigo, ou seja, nem todos os ficheiros estarão perdidos. Em geral, os arquivos precisam de muito espaço nos suportes de dados e, por isso, é necessário evitar que se acumulem demasiados ficheiros de arquivo. Em **Conservar cópia de segurança completa** é conveniente indicar um número máximo de cópias de segurança a serem guardadas no seu suporte de cópia de segurança. A pasta mais antiga será então substituída pela pasta actual.

Fazendo a marcação em **Criar backup(s) parcial(is)**, o software executará após o primeiro backup completo apenas backups parciais, que são muito mais rápidos no procedimento de backup, ou tem maior duração, quando deles precisa ser feita uma restauração de backup completo. A desvantagem do Backup parcial é um comparável aumento da necessidade de espaço de armazenamento, porque os dados que não mais necessários no Backup completo não são excluídos diretamente. Contudo, depois da próxima cópia de segurança completa, os dados das cópias de segurança completa e parcial são novamente reunidos e a quantidade de dados volta a ser igual à quantidade de dados numa cópia de segurança completa.

Executar backups parciais

As cópias de segurança parciais servem para acelerar uma cópia de segurança de dados. Ao invés de utilizar todos os dados para um backup, o backup parcial estrutura-se em um backup completo existente e salva apenas os dados que tiverem sido alterados desde o último backup completo ou que foram recentemente criados. Dessa forma, um backup completo do seus dados está á disposição onde o procedimento de backup é executado muito mais rapidamente.

Diferencial / Incremental: Na cópia de segurança diferencial, são armazenados todos os dados alterados ou criados desde da última cópia de segurança completa. As cópias de segurança baseiam-se sempre na última cópia de segurança completa criada. Em comparação com uma nova cópia de segurança completa, poupa-se tempo e espaço de armazenamento. A cópia de segurança incremental ainda sobe um nível e cria uma cópia de segurança entre duas cópias de segurança parciais, que tenham sido alteradas de cópia de segurança parcial em cópia de segurança parcial. A desvantagem nisto é que para o restauro dos dados são necessários vários arquivos.

Opções

Na área opções você pode alterar as opções gerais do backup. Em geral, não é necessário efetuar aqui nenhuma alteração porque as opções padrão G DATA abrangem a maioria das aplicações.

Opções gerais de arquivos

Nas Opções gerais de arquivos dispõe das seguintes possibilidades de configuração:

- **Limitar tamanho do arquivo**: Se você gravar arquivos em CD/DVD-ROM ou outras mídias graváveis, é importante que o G DATA Software limite o tamanho desses arquivos compactados. Aqui pode seleccionar entre vários tamanhos padrão, que lhe permitem guardar posteriormente os dados de arquivo em CD, DVD ou discos Blu-ray. O arquivo será dividido ao atingir o tamanho máximo informado e as informações de backup serão distribuídas em um ou mais arquivos compactados.

- **Criar CD/DVD de sessão múltipla**: Selecionando estas opções, são criados CDs ou DVDs de backup, que são regraváveis. Sendo que, no entanto, o conteúdo gravado anteriormente não é excluído, mas apenas complementado com o novo conteúdo.

- **Apagar arquivos temporários**: Esta opção deve permanecer normalmente activada. Após um determinado número de processos de backup, os arquivos temporários ocupam muito espaço no seu disco rígido e geralmente não são necessários após a sua utilização temporária.

- **Copiar ficheiros do programa de restauro**: Ativando esta função, além dos dados de backup arquivados no local de salvamento do seu backup de dados, será reproduzido um programa, com o qual será possível restaurar os seus dados mesmo sem o G DATA Software instalado. Inicie o programa *AVKBackup* ou *AVKBackup.exe* a partir do CD/DVD-ROM.

  O programa de restauração será agora copiado também para o CD/DVD-ROM. No caso de cópias de segurança em mídias removíveis (pen-drives e discos rígidos externos), isso não será feito.

  Se você tiver instalado o G DATA Software no computador,no qual a restauração deverá ser feita, não execute a restauração com o programa de restauração do CD/DVD-ROM, mas através da função **Importar arquivos**.

- **Antes de arquivar, verificar se os ficheiros têm vírus**: Se estiver instalado o módulo AntiVirus, pode verificar se os seus dados contêm vírus antes de os gravar num arquivo de cópia de segurança.

- **Verificar arquivo ao criar**: Esta função serve para verificar, após a criação do arquivo, se este está completo e não contém erros.

- **Encriptar arquivo**: Se desejar proteger seus arquivos em pasta contra o acesso de estranhos, poderá atribuir a eles uma senha. Neste caso, o restauro dos dados só pode ser efectuado com essa palavra-passe. Memorize bem a palavra-passe ou anote-a num local seguro. Sem a palavra-passe não poderá recuperar os seus dados de arquivo.

- **Teste de integridade ao criar cópia de segurança diferencial**: Essa função serve para verificar um backup parcial após sua criação, mais uma vez quanto à integralidade e perfeição.

- **Teste de integridade ao restaurar a partir do disco rígido**: Esta função serve para verificar a reversão correcta dos dados após o restauro. No **Diretório para arquivos temporários** trata-se de um local de salvamento para dados, os quais o G DATA Software registra temporariamente no disco rígido. Caso não haja espaço suficiente na sua partição predefinida, pode alterar aqui a partição e a localização temporária destes ficheiros.

- **Utilizar Windows Shadow Copy**: Se esta opção for desativada, não se pode criar uma imagem da partição do sistema durante a operação em andamento.

Indicações de utilizadores

Para poder executar backups programados, é necessário colocar uma marcação na área **Executar tarefa como** e lá, informar os dados de acesso para a sua conta do usuário do Windows. Estes dados são necessários para que a cópia de segurança possa ser executada com horário fixado mesmo que não esteja inscrito como utilizador.

Compressão

Na área compressão é possível definir o nível de compactação, entre fraco e forte, de seus arquivos ou pastas.

- **Boa compressão**: Para a cópia de segurança, os ficheiros são muito comprimidos. Desta forma irá poupar espaço durante a cópia de segurança, mas a cópia de segurança em si demora mais tempo.

- **Compressão equilibrada**: A cópia de segurança não é comprimida de forma tão forte, sendo portanto executada com um pouco mais de rapidez.

- **Execução rápida**: Não é feita qualquer compressão dos ficheiros, de forma que por isso a cópia de segurança é feita com mais rapidez.

Excluir ficheiros

Em geral, o G DATA Software salva arquivos com base no seu formato de arquivo. No seu sistema de computador, esses formatos de ficheiro também se encontram em áreas que são geridas automaticamente e que não são relevantes para uma cópia de segurança, dado que os respectivos ficheiros só foram guardados temporariamente (por exemplo, para acelerar a apresentação de páginas na Internet). Para que o G DATA Software não armazene esses arquivos desnecessariamente, é possível ignorá-los colocando a respectiva marcação.

- **Directório temporário com ficheiros**: Quando essa opção tiver sido selecionada, as pastas temporárias, assim como as subpastas e os arquivos lá existentes, não são incluídos no backup de dados.
- **Directórios de Internet temporários com ficheiros**: Quando esta opção é seleccionada, as pastas para armazenamento de páginas de Internet, assim como as subpastas e ficheiros nelas contidas não são incluídos na cópia de segurança.
- **Thumbs.db**: Quando essa opção tiver sido selecionada, os arquivos thumbs.db criados automaticamente pelo Windows Explorer, não são incluídos no backup. Estes ficheiros servem, por exemplo, para gerir as miniaturas para apresentações de diapositivos e são criadas automaticamente a partir das imagens originais.
- **Ficheiros temporários (atributo de ficheiro)**: Quando essa opção tiver sido selecionada, os arquivos com o atributo de arquivo temporário atribuído pelo sistema, não são incluídos no backup.
- **Ficheiros de sistema (atributo de ficheiro)**: Quando essa opção tiver sido selecionada, os arquivos com o atributo de arquivo como arquivo do sistema atribuído pelo sistema, não são incluídos no backup.
- **Ignorar tipos de arquivos**: Com esta função é possível definir as extensões de arquivo que não devem ser consideradas no seu backup. Proceda da seguinte forma: Em **Tipo de arquivo** (por ex., *.txt), informe a extensão ou o nome do arquivo que deseja ignorar. A seguir, clique em **OK**. Repita o procedimento para todos os outros tipos e nomes de arquivos que deseja ignorar, por ex., picasa.ini, *.ini, *bak, etc. O símbolo do asterisco e o ponto de interrogação podem ser utilizados aqui como espaço reservado. A forma de funcionamento de espaços reservados é a seguinte:

  O ponto de interrogação (?) é substituto para caracteres individuais.

  O asterisco (*) é substituto para sequências de caracteres inteiras.

  Para verificar todos os arquivos com a extensão de arquivo e, digite *.exe. Para verificar formatos de planilhas (*.xlr, *.xls) digite simplesmente *.xl?. Para verificar tipos diferentes de arquivos com um nome de arquivo de início igual, digite, por exemplo, texto*.*.

Repor opções padrão actuais

Clicando neste botão, você aceita as opções para o G DATA Software que foram definidas como opções padrão. Portanto, se tiver definido inadvertidamente as opções falsas na criação do backup e não souber como repará-las, clique no botão **Aplicar opções padrão atuais**.

Restaurar backup

Aqui é possível restaurar os seus arquivos originais após uma perda de dados, com base nos seus dados de backup armazenados. Clique no botão **Restaurar**.

Uma janela de diálogo é aberta, na qual estão listados todos os processos de backup armazenados para cada tarefa de backup.

Selecione aqui o backup desejado (por ex., último backup executado, caso queira fazer a restauração de documentos excluídos sem querer) e toque no botão **Restaurar**.

Agora você tem a possibilidade de definir, qual forma de restauração é desejada:

- **Restaurar completamente os discos rígidos e as partições**: Todos os arquivos e pastas que foram salvos neste backup são restaurados.
- **Restaurar somente as(os) partições/arquivos selecionados**: Aqui é exibida a visualização do backup onde pode ser feita a seleção específica de quais arquivos, pastas ou partições você deseja ou não restaurar. Na árvore de diretórios, clicando nos sinais de mais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada diretório ou arquivo com uma marcação será restaurado do backup. Se nem todos os arquivos tiverem que ser verificados em um diretório, haverá uma marcação em cinza nesse diretório.

Em seguida, pode ser feita a definição se os arquivos devem ou não ser restaurados para os seus diretórios originais. Se os arquivos devem ser salvos em outro local, pode ser feita a seleção de uma pasta em **Nova pasta**, na qual os arquivos devem ser arquivados. Em **Senha**, digite a senha de acesso, caso você tenha compactado o seu backup protegido por senha.

Quando a restauração é feita nos diretórios originais, há as seguintes opções para fazer regravação específica de arquivos alterados:

- **Substituir sempre**: Com esta configuração, os ficheiros da cópia de segurança de dados são considerados sempre mais importantes do que os dados que se encontram no directório de origem. Se colocar um visto aqui, os dados que ainda possam existir são substituídos integralmente pelos dados que se encontram no arquivo.

- **Quando houve uma alteração do tamanho**: Com esta configuração, os dados existentes no directório de origem só serão substituídos, se o ficheiro de origem foi alterado. Os ficheiros com o mesmo tamanho são ignorados. Dessa forma, a restauração de dados poderá possivelmente ser mais rápida.

- **Quando o período "Modificado em" na pasta for mais recente**: Neste caso, os ficheiros no directório de origem são substituídos pelas cópias do arquivo sempre que forem mais recentes do que os dados do arquivo. Aqui, uma restauração dos dados também poderá ser mais rápida porque, possivelmente, nem todos os arquivos terão de ser restaurados, mas apenas os dados alterados.

- **Quando o período "Modificado em" tiver sido alterado**: Neste caso, os dados no directório de origem são substituídos sempre que a data de alteração se tenha alterado face aos ficheiros arquivados.

Para encerrar, clique no botão **Concluir**, para que a restauração seja feita de acordo com as especificações.

Acções

Nesta área pode, entre outras, realizar acções de actualização e manutenção das suas cópias de segurança de dados.

Os seguintes programas de serviço estão disponíveis para isso:

Gravar pasta posteriormente em CD/DVD

Também pode gravar os ficheiros de cópia de segurança posteriormente num CD ou DVD. Para tal, seleccione na janela de diálogo apresentada um projecto que deseje gravar e a seguir clique no botão **Continuar**.

Selecione agora a unidade na qual deseja gravar o backup dos dados.

As seguintes opções estão disponíveis aqui:

- **Depois de gravar, verificar os dados**: Se colocar um visto, os dados gravados serão verificados mais uma vez após a gravação. Isto requer mais tempo do que uma gravação sem verificação, mas geralmente é recomendável.

- **Copiar ficheiros do programa de restauro**: Ativando esta função, além dos dados de backup arquivados no local de salvamento do seu backup de dados, será reproduzido um programa, com o qual será possível restaurar os seus dados mesmo sem o G DATA Software instalado. Inicie o programa *AVKBackup* ou *AVKBackup.exe* a partir do CD/DVD-ROM.

Clique no botão **Gravar** para iniciar o processo de gravação. Após o processo de gravação, o CD/DVD de cópia de segurança é ejectado automaticamente.

> **Observação**: Naturalmente, os dados de backup não serão excluídos da mídia de dados original após o processo de gravação. A gravação posterior em CD/DVD é uma segurança adicional.

Importar pastas

Para restaurar arquivos e backups de dados que não estejam em uma unidade administrada pelo G DATA Software, utilize a função **Importar arquivos**. Abre-se uma janela de diálogo onde pode procurar os ficheiros de arquivo desejados com a extensão *ARC*, por exemplo, num CD, DVD ou na rede. Se encontrou o arquivo desejado, marque-o com um visto e clique no botão **OK**. Uma janela de informações avisa-o que o arquivo foi importado com sucesso. Se desejar utilizar agora este arquivo para restaurar os dados, basta aceder à área **Restaurar** o G DATA Software, selecionar o backup desejado e iniciar a restauração.

> Nota: Os arquivos compactados criados pelo G DATA Software tem a extensão de arquivo ARC.

Criar mídia de boot

Para poder restaurar backups também sem o G DATA Software instalado, pode ser criado um CD/DVD ou um pendrive USB, que tem um software especial com o qual a restauração de dados pode ser feita. Para restaurar backups desta forma, iniciar a mídia de boot e lá selecionar o programa *AVKBackup* ou *AVKBackup.exe*. Agora você pode selecionar o backup desejado e iniciar a restauração.

> **Observação**: Como você pode criar uma mídia de boot, é explicado no capítulo **Mídia de boot**. A mídia de boot realiza uma tarefa dupla no G DATA Software. Com ela você pode fazer a restauração de backup e fazer a verificação do seu computador com o Bootscan antes de iniciar o Windows.

Gerenciador de senhas

Com o gerenciador de senhas você pode gerenciar com comodidade as suas senhas e utilizá-lo como plug-in no seu navegador.

O gerenciador de senhas suporta os seguintes navegadores nas suas respectivas últimas gerações:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

Nota: Observe que, dependendo das configurações do seu navegador (por exemplo, configurações de proteção de dados), a funcionalidade do gerenciador de senhas pode ser restringida.

Crie primeiro um cofre de senhas e instale o plug-in no navegador de sua escolha. Você também pode instalar o cofre de senhas em todos os navegadores compatíveis.

Criar novo cofre e instalar o plug-in

Clique na entrada **Cofre de senhas**. Agora é aberto um diálogo, através do qual você pode criar um novo cofre ao selecionar **Criar novo cofre**.

Defina uma senha, confirme e clique em **Criar cofre** e o cofre será criado. A frase de recordação pode ajudar, caso você precise se lembrar de uma senha que esqueceu.

Agora o cofre foi criado e você pode selecionar no lado direito da janela do programa em qual navegador você deseja instalar o plug-in do gerenciador de senhas. Para isso, basta clicar no nome do navegador e o plug-in será instalado.

Quando você abrir o navegador novamente, você pode ser consultado se deseja utilizar o novo plug-in. Confirme isso para o gerenciador de senhas G DATA.

Agora será exibido o seguinte símbolo na barra de tarefas do navegador. Basta clicar no símbolo para poder utilizar o gerenciador de senhas.

Insira a sua senha no diálogo que apareceu e clique em **Destravar**. A utilização do plug-in do navegador está explicada nos capítulos seguintes.

Utilização do plug-in do navegador

Ao clicar no seguinte símbolo na barra de tarefas do navegador, você pode utilizar o gerenciador de senhas.

Nota: Observe que a utilização do plug-in não é possível dependendo das configurações da esfera privada (por exemplo, salvar o decurso). Por isso, em caso de problemas com o plug-in, verifique primeiro as configurações do seu navegador.

Insira a sua senha no diálogo que apareceu e clique em **Destravar**. Agora estão disponíveis as seguintes áreas:

Favoritos: Com esta função você também poderá acessar rapidamente páginas de internet protegidas por senha utilizadas regularmente.

Logins: Aqui você gerencia os logins de páginas de internet protegidas por senha.

Contatos: Com ajuda dos dados de contato inseridos aqui, os formulários, por exemplo, dos endereços de entrega, são preenchidos automaticamente.

Notas: Aqui você pode salvar notas adicionais protegidas por senha.

Configurações: Para fechar novamente o gerenciador de senhas, clique em **Travar**. Se você clicar em Configurações, você pode gerenciar favoritos, logins, contatos e notas de forma confortável no campo de diálogo. Através do gerador de senhas, você pode criar uma senha segura automaticamente e reutilizá-la diretamente através da área de transferência.

Na área de gerenciamento do gerenciador de senhas, você pode adicionar, editar e excluir novas entradas da seguinte maneira.

Nova entrada: Ao clicar neste botão, você pode elaborar uma nova entrada e inserir todos os dados necessários no campo de diálogo respectivo para logins, contatos ou notas.

Salvar entrada: Ao clicar neste botão, a entrada é salva e depois aparece na seleção rápida do plug-in do navegador.

Excluir entrada: Aqui você pode excluir as entradas de que não precisa mais.

Optimizador

Desde o lembrete automático para recordar actualizações do Windows, passando por uma desfragmentação regular com horário fixado, até à eliminação regular de entradas de registo supérfluas e ficheiros temporários, o Optimizador é uma ferramenta que torna o sistema Windows visivelmente mais rápido e simples.

Você pode fazer a otimização do seu computador manualmente ao pressionar um botão ou através da programação para executar trabalhos de otimização regulares.

Última otimização: Aqui é exibido quando foi a última vez em que a otimização do seu computador foi feita. Para iniciar uma nova otimização, selecione aqui, clicando no registro **Executar agora a otimização**. Assim que a otimização é iniciada, uma barra de progresso exibe o status atual da otimização.

Otimização automática: Se quiser automatizar a otimização do seu computador, clicando aqui no registro **Ativar otimização automática**, você pode criar a tarefa programada correspondente. Para configurar a otimização automática, selecione a opção **Outras configurações**.

Configuração: Nesta rea você pode selecionar todos os módulos que o otimizador deverá utilizar para um procedimento de otimização. Os módulos seleccionados são então iniciados ou por meio de uma acção automática controlada temporalmente (ver capítulo Agendamento) ou manualmente. Para activar um módulo faça simplesmente duplo clique com o rato sobre o mesmo. Pode optimizar, aqui, individualmente as principais áreas de optimização que se seguem:

- *Segurança*: Diversas funções que transferem automaticamente dados da Internet só têm aspectos que se justificam para o fornecedor e não para si. Muitas vezes, essas funções abrem a porta a software malicioso. Estes módulos permitem-lhe proteger o sistema e mantê-lo actualizado.
- *Desempenho*: Os ficheiros temporários, por exemplo, cópias de segurança que já não são necessárias, ficheiros de registo ou de instalação, que após a instalação apenas ocupam espaço no disco, tornam o seu disco rígido mais lento e apenas ocupam espaço valioso no disco. Além disso, os processos que já não são necessários e os atalhos para os ficheiros afectam bastante a velocidade do seu sistema. Com os módulos aqui apresentados poderá libertar o seu computador dessa carga desnecessária e acelerá-lo.
- *Protecção de dados*: A seguir são apresentados os módulos relacionados com a protecção dos seus dados. Aqui são eliminados os rastos deixados involuntariamente ao navegar na Internet e que ao utilizar o computador revelam muito sobre os seus hábitos de utilização ou até mesmo dados e palavras-passe importantes.

Restauração: Em cada alteração executada, o software define um ponto de restauração. Caso algumas das tarefas de optimização tenha resultados não desejados, esta poderá ser anulada restaurando o estado do sistema antes de ter sido efectuada a alteração correspondente. Leia também o capítulo Restauro.

Browser Cleaner: O G DATA Browser Cleaner bloqueia ou remove os componentes indesejados do programa e os programas adicionais. Estes programas são muitas vezes instalados com o software gratuito e modificam as configurações do navegador ou até mesmo espionam os dados. Leia também o capítulo Browser Cleaner.

Restauro

Para cada alteração executada o software estabelece um ponto de restauro. Caso algumas das tarefas de optimização tenha resultados não desejados, esta poderá ser anulada restaurando o estado do sistema antes de ter sido efectuada a alteração correspondente.

Selecionar todos: Se quiser descartar todas as alterações feitas pela otimização, selecione aqui todos os pontos de restauração e depois clique no botão **Restaurar**.

Restaurar: Se quiser descartar só determinadas alterações feitas pela otimização, selecione aqui o ponto de restauração desejado e depois clique no botão **Restaurar**.

Excluir selecionados: Pontos de restauração que não são mais necessários, podem ser excluídos com esse botão.

Browser Cleaner

O G DATA Browser Cleaner bloqueia ou remove os componentes indesejados do programa e os programas adicionais. Estes programas são muitas vezes instalados com o software gratuito e modificam as configurações do navegador ou até mesmo espionam os dados. Com o Browser Cleaner, você também pode decidir se estes programas indesejados ("PUP" = Potentially Unwanted Programs) exibidos nos navegadores Internet Explorer, Firefox e Google Chrome somente devem ser desativados ou completamente removidos. A desativação das ampliações pode ser desfeita a qualquer momento.

> **Nota:** O G DATA Browser Cleaner trabalha junto com o Microsoft Internet Explorer, Mozilla Firefox e Google Chrome e permite o fácil gerenciamento de todas as extensões instaladas do navegador. Com o clique do mouse, é possível desativar ou remover todos os Plug-ins da lista para liberar o navegador de todas as extensões indesejadas. Opcionalmente, a ferramenta mostra todos os Plug-ins classificados por ordem de segurança, para você poder conseguir diferenciar facilmente todas as extensões não seguras ou indesejadas. O G DATA Browser Cleaner está contido na ampla solução de segurança abrangente G DATA Total Security e sempre está disponível para os usuários.

Protecção infantil

Com a proteção infantil é possível controlar o comportamento na navegação e a utilização do computador para suas crianças.

Selecione em **Usuário** um usuário registrado no seu computador e configure as respectivas limitações para este usuário. Através do botão **Adicionar novo usuário** é possível criar uma nova conta no seu computador (por exemplo, para seus filhos).

- **Proteção infantil para esse usuário**: Aqui pode ser ligada ou desligada a proteção infantil para o usuário selecionado acima.
- **Conteúdo proibido**: Nessa área é aberta uma janela de diálogo na qual você pode bloquear conteúdos especiais na Internet para o usuário exibido no momento. Clique em **Editar**, para definir os conteúdos proibidos para cada usuário.
- **Conteúdo permitido**: Através dessa área é aberta uma janela de diálogo na qual você pode permitir conteúdos especiais na Internet para o usuário exibido no momento. Clique em **Editar**, para definir os conteúdos permitidos para cada usuário.
- **Monitorar tempo de utilização da Internet**: Aqui você pode determinar por quanto tempo e quando o usuário selecionado terá acesso à internet. Clique em **Editar**, para definir os tempos de utilização para cada usuário.
- **Monitorar tempo de utilização do computador**: Aqui, é possível definir por quanto tempo e em quais horários o usuário selecionado pode utilizar o computador. Clique em **Editar**, para definir os tempos de utilização para cada usuário.

Configurações: Aqui você pode alterar as configurações básicas para o funcionamento da proteção infantil e adaptá-las às necessidades individuais.

Adicionar novo usuário

Clique no botão **Adicionar novo usuário**. Irá abrir-se uma caixa de diálogo onde poderá introduzir o nome de utilizador e a palavra-passe para esse utilizador.

> **Observação**: Do aspecto da segurança, uma senha deverá ter pelo menos oito caracteres, conter letras maiúsculas e minúsculas, assim como números.

Em seguida, em **Usuário**, aparecerá o novo nome de usuário criado e, ao mesmo tempo, será criada uma conta do usuário do Windows para esse usuário. Isso significa que a protecção infantil fica automaticamente activa, com as respectivas configurações, para a pessoa que iniciou a sessão no Windows com o seu nome de utilizador. Faça agora duplo clique com o rato sobre a área das configurações que deverão ser definidas para esse utilizador, por exemplo, o impedimento de acesso a **Conteúdos proibidos** ou a autorização exclusiva de **Conteúdos permitidos**, ou então estabeleça se, para esse utilizador, se deverá monitorizar o **Tempo de utilização da Internet** ou **Período de utilização do computador**.

Conteúdo proibido

Nesta área abre-se uma caixa de diálogo, em que determinados conteúdos na Internet podem ser bloqueados para o utilizador actualmente exibido. Seleccione as categorias que deseja bloquear, colocando uma marca de verificação. Clique agora em **OK** e as páginas da Internet que correspondem aos critérios de bloqueios serão bloqueadas.

Se clicar no botão **Novo**, será aberta uma janela de diálogo onde é possível definir seus próprios critérios de bloqueio (também chamadas de Blacklists). Para isso, defina primeiro o nome e, se necessário, um texto de informações para o filtro criado individualmente.

Se agora clicar em **OK**, abre-se outra janela onde pode resumir conteúdos que deseja impedir através desse filtro.

Digite em **Filtro**, um termo que deva ser bloqueado e, em **Local para a pesquisa**, a área de um site onde deva ocorrer a pesquisa.

Aqui pode seleccionar o seguinte:

- **URL**: se colocar a marca de verificação aqui, o texto a bloquear será procurado no endereço Web. Se desejar interditar páginas como por exemplo, *www.chatcity.no*; *www.crazychat.co.uk* ou semelhante, basta colocar como **Filtro** *chat*, colocar a marcação em **URL** e clicar no botão **Adicionar**. Serão bloqueadas todas as páginas que utilizarem de alguma forma no nome do domínio, ou seja, o endereço da Internet que use a sequência de letras *chat*.
- **Título**: Se colocar a marca de verificação aqui, o texto a bloquear será procurado no título da página Web. Essa é a área que você vê, quando por exemplo, deseja inserir uma página na sua lista de favoritos como um marcador. Se desejar interditar páginas como, por exemplo, *Chat City Detroit*; *Teenage Chat 2005* ou semelhante, basta colocar como **Filtro** *chat*, a marcação em **Título** e clicar no botão **Adicionar**. Agora serão bloqueadas todas as páginas que, no título, usem de alguma forma a sequência de letras *chat*.
- **Meta**: As chamadas metatags são registros de texto ocultos em sites, que servem para listá-las em mecanismos de busca de forma

mais útil ou apenas com mais frequência. Aqui utilizam-se conceitos de pesquisa como *sexo* ou *chat* para aumentar o números de acessos a páginas. Se desejar interditar páginas que tenham *chat* em algum lugar da metatag, basta colocar **chat** como *filtro*, a marcação em **Meta** e clicar no botão **Adicionar**. Agora serão bloqueadas todas as páginas que, nos meta tags, usem de alguma forma a sequência de letras *chat*.

- **No texto inteiro**: Se desejar verificar conteúdos legíveis de uma página diretamente em relação ao conteúdo a ser bloqueado, coloque o termo a ser bloqueado - p.ex., *chat* - coloque a marcação em **No texto inteiro** e, clique em seguida no botão **Adicionar**. Agora serão bloqueadas todas as páginas que, no texto da página exibida, usem de alguma forma a sequência de letras *chat*.

Páginas que caiam na classificação do filtro por engano, podem ser novamente liberadas explicitamente, através da função exceção. Para isso, clique no botão **Exceção** e insira o site correspondente.

> **Observação**: Filtros criados por você podem ser editados ou, se necessário, excluídos como desejados, na área do **próprio filtro**. Para mais informações, leia o capítulo **Filtros próprios**.

Conteúdo permitido

Através desta área é aberta uma caixa de diálogo, onde poderá autorizar conteúdos especiais na Internet para o utilizador indicado. Para tal, seleccione as categorias desejadas que pretende autorizar colocando um visto. A seguir, clique em **OK** para autorizar as páginas de Internet que correspondem aos critérios desejados.

Se clicar no botão **Novo**, é aberta uma janela de diálogo onde é possível definir o conteúdo próprio a ser permitido (também chamadas de Whitelists). Para isso, defina primeiro o nome e, se necessário, um texto de informações para o filtro criado individualmente.

A seguir, clique em **OK**. Abre-se uma caixa de diálogo onde poderá preencher a lista branca com sítios Web, por exemplo, próprios para crianças.

Para tal, introduza em **Filtro** os componentes do nome do domínio que deseja autorizar. Se desejar liberar, por exemplo, a página com conteúdos infantis próprios, poderá inserir aqui, por exemplo, *www.fragfinn.de* e permitindo assim o acesso a esse site. Insira agora em **Descrição**, o que pode ser encontrado nesse site, por exemplo, *fragFINN - a rede para as crianças* e, em **Link para o serviço**, insira o endereço exato do site. A descrição e o link para a oferta são importantes quando o seu filho, por exemplo, realmente tentar abrir uma página que não foi permitida. Em vez de uma mensagem de erro, surge uma página HTML no browser com todas as páginas Web que constam da lista branca, incluindo as descrições. Deste modo, o seu filho pode voltar a aceder directamente às páginas que lhe são permitidas. Depois de ter introduzido todos os dados, clique em **Adicionar** e os dados são adicionados à lista branca.

> **Observação**: O filtro procura segmentos no nome dos domínios. Dependendo dos dados inseridos no filtro, poderá distinguir os resultados. Certas restrições adicionais ou mais rigorosas podem ser úteis em função do sítio Web.

Gerir o tempo de utilização da Internet

Aqui pode definir a duração e as horas em que o utilizador seleccionado tem acesso à Internet. Para tal, coloque o visto em **Gerir o tempo de utilização da Internet**. Poderá agora determinar durante quanto tempo por mês o utilizador pode aceder à Internet, quanto tempo por semana e quantas horas em determinados dias da semana. Deste modo, pode gerir, por exemplo, os fins-de-semana para crianças em idade escolar de forma diferente dos dias da semana. Poderá simplesmente introduzir os períodos correspondentes em **Dias/hh:mm**, sendo que a introdução *04/20:05* significa um tempo de utilização da Internet de 4 dias, 20 horas e 5 minutos.

> **Observação**: Em relação aos dados para a utilização da Internet, contam sempre respectivamente, os valores menores. Assim, se pretender estabelecer, para o mês, uma limitação temporal de quatro dias e pretender permitir durante a semana, por exemplo cinco dias, o software limita a utilização da Internet para esse utilizador automaticamente para quatro dias.

Quando o respectivo usuário tentar acessar a Internet acima do contingente de tempo, aparece um aviso, que informa que seu contingente foi ultrapassado.

Bloquear períodos

Através do botão **Bloquear períodos** pode chamar um campo de diálogo, permitindo-lhe bloquear - para além da restrição quantitativa da utilização do computador - por categorias os períodos especiais na semana. Os períodos bloqueados estão representados a vermelho, os períodos desbloqueados a verde. Para desbloquear ou bloquear um período, seleccione-o com o rato. Ao lado do cursor do rato aparece um menu de contexto onde poderá: **Desbloquear período** e **Bloquear período**. Se o respectivo utilizador tentar aceder à Internet durante os períodos bloqueados, surge no browser um ecrã informativo que o informará que naquele momento não tem qualquer acesso à Internet.

Gerir tempo de utilização do computador

Aqui, é possível definir por quanto tempo e em quais momentos o usuário selecionado pode utilizar o computador. Coloque o visto em **Gerir tempo de utilização do computador**. Agora pode definir quanto tempo o utilizador pode utilizar o computador por mês, quantas horas por semana e quantas horas em determinados dias da semana. Deste modo, pode gerir, por exemplo, os fins-de-semana para crianças em idade escolar de forma diferente dos dias da semana. Poderá simplesmente introduzir os períodos correspondentes em **Dias/ hh:mm**, sendo que a introdução *04/20:05* significa então um tempo de utilização da computador de 4 dias, 20 horas e 5 minutos. Através do botão **Exibir aviso antes da expiração do tempo**, pode informar um utilizador pouco antes de o computador ser desligado automaticamente, para que tenha tempo de guardar os seus dados. Se o computador for desligado sem aviso, pode levar à perda de dados.

> **Observação**: Em relação aos dados para a utilização do computador, contam sempre respectivamente, os valores menores. Se definir um limite de tempo de quatro dias para o mês, mas permitir, por exemplo, cinco dias na semana, o software limita automaticamente a utilização do computador pelo utilizador para quatro dias.

Bloquear períodos

Através do botão **Bloquear períodos** pode chamar um campo de diálogo, permitindo-lhe bloquear - para além da restrição quantitativa da utilização do computador - por categorias os períodos especiais na semana. Os períodos bloqueados estão representados a vermelho, os períodos desbloqueados a verde. Para desbloquear ou bloquear um período, seleccione-o com o rato. Ao lado do cursor do rato aparece um menu de contexto onde poderá: **Desbloquear período** e **Bloquear período**.

Filtros próprios

Nesta área, você pode modificar as suas Whitelists (conteúdos permitidos) e Blacklists (conteúdos proibidos) propriamente criadas e criar manualmente listas completamente novas.

Os seguintes tipos de lista distinguem-se essencialmente no seguinte:

- **Conteúdo permitido**: Se escolher uma lista branca para um dos utilizadores acima seleccionados, este só poderá ver páginas da Web que se encontrem nesta lista branca. Como administrador, você pode estruturar essa Whitelist como desejar ou selecionar uma lista adequada para um usuário nas Whitelists predefinidas. Uma lista branca é particularmente útil para permitir um acesso muito limitado à Internet a crianças mais pequenas, oferecendo-lhes, portanto, a possibilidade de tirar partido apenas de páginas da Web com conteúdos recomendáveis a nível pedagógico.

- **Conteúdo proibido**: Com uma lista negra, é possível bloquear páginas da Web seleccionadas para um utilizador. Para além destas, o utilizador tem acesso livre à Internet. Tenha em atenção que através desta função pode bloquear determinadas páginas, mas que também podem estar disponíveis conteúdos do mesmo tipo noutras páginas da Web. Neste sentido, uma lista negra de endereços da Internet nunca constitui uma protecção perfeita de conteúdos indesejados.

Os seguintes botões possibilitam-lhe a edição das listas de exclusão:

- **Eliminar**: Através da função **Eliminar** é possível eliminar, com o rato e de forma simples, listas seleccionadas.

- **Novo**: Esta opção permite-lhe criar uma lista negra ou uma lista branca completamente nova. Neste caso, o procedimento é igual ao descrito no capítulo **Conteúdo proibido** e a **Conteúdos permitidos**.

- **Editar**: Esta opção permite-lhe alterar o conteúdo de uma lista existente.

Configurações: Registo

Nesta área, você pode modificar configurações essenciais para as informações na área de registro. Poderá determinar se as infracções contra conteúdos permitidos e/ou proibidos deverão ou não ser registadas. Caso os conteúdos devam ser registados, poderá consultar os registos dos diferentes utilizadores na área de registos.

Como os arquivos de registro podem ficar muito grandes com a utilização constante, você pode, a partir da Proteção infantil em **Exibir mensagem quando o arquivo atingir ____KB**, solicitar o lembrete informando que o arquivo de registro ultrapassou um determinado tamanho e, excluí-lo manualmente na área de **Registo** em **Excluir registros**.

Criptografia

O módulo de criptografia serve como um cofre de banco para a proteção de dados sensíveis. Um cofre pode ser utilizado, por exemplo, como uma partição adicional do disco rígido e é muito fácil de utilizar.

Para criar e administrar cofres existem as seguintes possibilidades de seleção:

- **Actualizar**: Se cofres foram abertos ou fechados nesse meio tempo, fora do módulo de criptografia, recomenda-se clicar em **atualizar**, para atualizar a visualização de status dos cofres administrados pelo cofre de dados.
- **Abrir/Fechar**: Aqui você pode abrir ou fechar os cofres que se encontram no seu computador e nas mídias de armazenamento vinculadas. Observe que, para abrir o cofre é necessária a senha que foi atribuída ao cofre durante a sua criação. Aqui os cofres podem ser fechados sem senha.
- **Criar nova criptografia**: Por meio desta função você pode criar um novo cofre. Para isso, um assistente é aberto que o ajudará na criação do cofre. Para mais informações, leia o capítulo **Criar novo cofre**.
- **Criar cofre móvel**: Assim que um cofre tenha sido criado também pode ser feito um cofre portátil, ou seja, ele pode ser configurado para que possa ser usado em um pen drive ou mesmo possa ser enviado por e-mail. Para mais informações, leia o capítulo **Criar cofre móvel**.
- **Excluir**: No gerenciamento de cofres, você tem uma visão geral de todos os cofres que se encontram no seu computador e nas mídias de armazenamento vinculadas. Aqui você também pode excluir cofres que não são mais necessários. Observe que, aqui você também pode excluir cofres sem conhecer suas senhas. Por isso você deve assegurar que o conteúdo do cofre a ser excluído realmente não seja mais necessário.

Criar novo cofre

Se você quiser criar um novo cofre, terá o suporte de uma caixa de diálogo interativa. Clique em **Continuar** para prosseguir.

Localização e tamanho do cofre

Indique agora onde deseja guardar o cofre e o tamanho que o cofre deve ter.

> **Observação**: O cofre é, na realidade, um arquivo protegido que age como uma partição do disco rígido quando está aberto. Ou seja, pelo local de salvamento você cria uma arquivo-cofre em um local desejado no seu disco rígido. Aqui os seus dados são salvos de forma criptografada. Quando você tiver aberto o cofre e estiver trabalhando com ele, é possível editar, excluir, copiar e mover arquivos e diretórios nele como em um disco rígido normal ou partição de disco rígido.

Local de salvamento

Aqui, você seleciona em que mídia (por ex. Mídia de dados local (C:)) deve ser criado o cofre.

> **Observação**: Cofres criados em um diretório protegido podem ser visualizados no seu computador apenas se o G DATA Software estiver instalado no seu computador. Se desejar desinstalar o software, os cofres de dados criados já não são visualizados.

Tamanho do dispositivo de armazenamento

Em seguida, selecione um tamanho do cofre através do posicionamento adequado do botão deslizante. Tem tanto espaço disponível como o espaço disponível no local de armazenamento seleccionado. Mas, geralmente você deverá permanecer pelo menos 2 GB para que o seu sistema de computador não seja comprometido por razões de falta de memória.

> **Observação**: O botão à esquerda do botão deslizante oferece uma possibilidade para uma seleção rápida do tamanho do cofre. Assim pode, por exemplo, definir o tamanho do seu cofre de forma precisa ou definir o mesmo tamanho, de forma a que possa ser gravado para um CD, DVD ou Blu-ray.

A seguir, clique no botão **Continuar**.

Parâmetros do cofre

Nesta janela de diálogo pode executar as seguintes indicações e configurações para o cofre:

- **Designação do cofre**: O nome com qual o cofre será gerenciado pelo G DATA Software.
- **Descrição**: Uma breve descrição que contém, por exemplo, informações sobre o conteúdo do cofre.
- **Sistema de ficheiros**: Aqui pode definir se a unidade virtual, que o cofre gera, utiliza o sistema de ficheiro FAT ou NTFS. Geralmente o registro **Seleção Automática** deve permanecer aqui.
- **Seleccionar automaticamente a unidade do cofre**: O cofre aparece no seu computador como uma unidade de disco rígido. Aqui pode ou atribuir uma letra de unidade fixa para o cofre ou deixar o sistema escolher automaticamente por si. Em regra, recomendamos a selecção automática.
- **Atribuir unidade**: Esta escolha apenas está disponível se não deixar o software seleccionar automaticamente a unidade do cofre.

A seguir, clique no botão **Continuar**.

Acesso ao cofre

Aqui poderá atribuir uma palavra-passe para um cofre. Em seguida, clique no botão **Adicionar**.

Agora, no campo de diálogo que aparece, informe a senha desejada em **Senha** e em **Repetir senha**. A palavra-passe apenas é aceite se ambas as introduções de palavras-passe forem idênticas. Isto destina-se a impedir, por exemplo, que seja atribuída acidentalmente uma palavra-passe ao introduzir um erro de dactilografia, que já não poderá recuperar.

Clique em **Adicionar**, para activar a palavra-passe e de seguida em **Continuar**, para concluir a configuração do cofre.

> **Observação**: Na criação de um cofre, você pode atribuir várias diferentes senhas e, assim, definir diferentes permissões. Assim, você pode criar um cofre para você mesmo, no qual você pode ler e modificar arquivos, e, com uma outra senha, permitir o acesso de outras pessoas para que estas possam ler o conteúdo deste cofre, mas não modificá-lo.

Se depois da criação do cofre, este for seleccionado e clicar no botão **Autorização**, terá as seguintes possibilidades de configuração:

- **Processar início automático**: Em cada cofre encontra-se um diretório com o nome Inicialização automática. Quando esta opção estiver definida para Sim, os arquivos executáveis existentes serão iniciados automaticamente com a abertura do cofre.
- **Abrir no modo "Somente leitura"**: Um utilizador que inicia sessão com o método de acesso apenas de leitura não pode guardar nem alterar os ficheiros existentes no cofre. Pode apenas lê-los.
- **Abrir como suporte amovível**: O G DATA Software abre os cofres de dados no Explorer como discos rígidos locais. Quando desejar que o cofre seja visível no sistema como Mídia de dados removível marque esta opção.
- **Utilização partilhada**: A selecção desta opção permite a utilização partilhada do directório do cofre para outros computadores na rede. Advertência: Nesta configuração, é possível o acesso ao cofre sem a necessidade de introduzir uma palavra-passe. Recomenda-se uma selecção cautelosa e consciente da utilização partilhada do cofre. A utilização partilhada do cofre para todos os membros da rede não faz aqui sentido, uma vez que os dados estão acessíveis a todos os utilizadores.
- **Fechar o cofre após o fim da sessão do utilizador**: Por norma, esta opção deve estar activada, pois se o cofre ainda permanecer aberto após o fim da sessão do utilizador, os outros utilizadores podem visualizar o seu conteúdo.
- **Cofre automático**: Todos os cofres com esta propriedade podem ser abertos com um único comando.

Configuração do cofre

O assistente de criação de cofre informa-o sobre os parâmetros de configuração, no último passo. Se desejar alterar essas configurações, clique no botão **Voltar**. Se estiver satisfeito com as configurações, clique em **Criar**.

O cofre de dados virtual e codificado será criado no disco rígido do seu computador. Com um último clique no botão **Concluir** o cofre é criado e aberto se assim o desejar.

Criar cofre móvel

Assim que um cofre tenha sido criado também pode ser feito um cofre portátil, ou seja, ele pode ser configurado para que possa ser usado em um pen drive ou mesmo possa ser enviado por e-mail.

Selecione um cofre na visualização do cofre de dados e então clique no botão **Criar cofre móvel**. Então é aberto uma caixa de diálogo que o ajudará a criar um cofre portátil. Clique em **Continuar**, para fazer sua inicialização.

Parâmetros do cofre

Assim como na atribuição dos parâmetros do cofre para cofres padrão, aqui também existe a possibilidade de alterar o parâmetro. Assim, no entanto, as possibilidades de configuração para cofres portáteis são limitadas:

- **Seleccionar automaticamente a unidade do cofre**: Enquanto está aberto, o cofre aparece como uma unidade de disco rígido. Aqui pode ou atribuir uma letra de unidade fixa para o cofre ou deixar o sistema escolher automaticamente por si. Em regra, recomendamos a selecção automática.

- **Associar o cofre ao suporte de dados**: Aqui você pode definir que o cofre portátil será usado exclusivamente com o pen drive ou com unidade de disco rígido, no qual foi criado. Quando a vinculação do cofre não é feita com uma memória de dados, o arquivo do cofre (reconhecido pela extensão de arquivo **tsnxg**) também pode, por ex., ser enviada como anexo de e-mail ou movido/copiado para outras memórias de dados.

Suporte

Defina aqui em qual mídia você quer salvar o cofre portátil. Aqui pode tratar-se, por ex., de um pen drive, um disco rígido externo ou também de um CD/DVD.

> **Observação**: Quando for feito o salvamento de um cofre em um CD ou DVD, naturalmente a leitura deste só pode ser feita quando aberto. Uma alteração em arquivos e diretórios no cofre não é possível neste tipo de memória de dados.

Tamanho do dispositivo de armazenamento

Aqui podem ser obtidas informações sobre quanto espaço de salvamento o cofre necessita na memória de dados de destino. Se o espaço de salvamento for grande demais, aqui pode ser feito o cancelamento da criação do cofre portátil.

> **Observação**: Além disso, para o tamanho real do cofre são adicionados ainda 6 MB de dados de drivers para que o cofre também possa ser aberto em um sistema Windows, no qual o G DATA Software não está instalado.

Concluir

Conclua agora a criação do cofre portátil clicando no botão **Concluir**. Se você desejar, o arquivo é exibido no navegador de arquivos, no qual o cofre portátil se encontra na mídia de armazenamento desejada.

Abrir cofre portátil

Se quiser abrir o cofre portátil em um computador com Windows, que não tenha o módulo de segurança do arquivo G DATA, o acesso aos dados pode ser feito selecionando no pendrive, no disco rígido móvel ou no CD/DVD o arquivo de programa **start.exe** ou **iniciar** na pasta **TSNxG_4**. Clicando nesta pasta, é exibida uma caixa de diálogo, pela qual o cofre pode ser aberto ou (se já estiver aberto) fechado.

> **Atenção**: Quando a segurança do arquivo G DATA for utilizada pela primeira vez em um computador, os respectivos dados do driver e elementos do programa serão carregados. De seguida, será necessário reiniciar o computador. Após a reinicialização do computador, selecione novamente o registro **Iniciar** ou **Start.exe**.

Introduza agora a sua palavra-passe ou use outro dos métodos de acesso ao cofre.

O cofre é agora aberto, podendo ser utilizado o seu conteúdo.

Depois de um início de sessão bem-sucedido no cofre irá aparecer no explorador do Windows, ao lado das unidades locais, o ícone do cofre como unidade adicional, com a respectiva letra da unidade. Qualquer utilizador do cofre móvel poderá executar informações do cofre no computador. Aquando da utilização de um cofre móvel num suporte de dados USB ou num suporte de dados de memória flash, o respectivo utilizador autorizado pode copiar os dados do cofre do computador para o cofre.

O fechamento do cofre móvel é feito analogamente à sua abertura. Dê um clique duplo nas letras da unidade do cofre ou selecione o respectivo comando com o botão direito do mouse no menu contextual.

Atenção: Recomenda-se, após ter executado todas as tarefas, que feche o cofre ainda antes de retirar o suporte de dados móvel. Para isso, vá para a mídia removível, abra o diretório da G DATA e clique em Start.exe. É exibida uma janela de diálogo na qual é possível fazer o fechamento do cofre.

Gerenciador de inicialização automática

Com o Gerenciador de inicialização automática é possível administrar programas que são inicializados automaticamente ao iniciar o Windows. Normalmente estes programas são carregados diretamente na inicialização do sistema. Quando são administrados pelo Gerenciador de inicialização automática, podem ser iniciados também com atraso de tempo ou de acordo com a capacidade do sistema ou do disco rígido. Isso permite uma inicialização mais rápida do sistema, melhorando assim o desempenho do computador.

Quando o Gerenciador de inicialização automática é aberto, no lado esquerdo é exibida uma listagem de todos os programas com inicialização automática que estão instalados no computador. Estes inicializam normalmente sem atraso, ou seja, diretamente com a inicialização do Windows e pode ocorrer que a inicialização do computador fique lenta.

Selecione facilmente com o ícone de seta os programas de inicialização automática que você deseja inicializar com atraso, equalizando assim o processo de inicialização do Windows. O sistema operacional Windows é carregado e fica pronto para operar mais rapidamente.

Quando quiser fazer novamente a inicialização de um programa de inicialização automática sem atraso, movimente-o de volta da pasta **Inicialização automática com atraso** para a pasta **Inicialização automática sem atraso**.

Configurar atraso

Quando um programa está na pasta inicialização automática com atraso, pode ser feita a definição de quantos minutos deve ser o atraso na inicialização deste software. Para isso, clique no programa, e na coluna Atraso selecione o período de tempo desejado.

Os seguintes registros estão disponíveis aqui:

- **Não inicializar**: O aplicativo é gerenciado pelo Gerenciador de inicialização automática, mas não será inicializado conjuntamente na próxima reinicialização do sistema. Ele fica inativo.
- **1 - 10 minutos**: O aplicativo é inicializado com atraso de acordo com o número de minutos determinado.
- **Inicialização automática**: O aplicativo é inicializado automaticamente dependendo da capacidade do disco rígido e do CPU. Isto significa, que outros aplicativos de inicialização automática serão inicializados, apenas quando a carga do sistema for reduzida novamente pela inicialização de outros aplicativos de inicialização automática ou outros processos.

Propriedades

Quando um clique duplo é feito na entrada de um programa, nas listas do administrador de inicialização automática, são obtidas informações abrangentes sobre o software administrado.

Controlo de dispositivos

Através do controle de dispositivo pode ser feita a definição para o seu computador de quais mídias de armazenamento são permitidos para leitura e/ou escrita de dados. Assim você pode, por ex., impedir que dados pessoais sejam movidos para um pen drive ou gravados em um CD. Além disso, pode ser feita a definição com qual mídia de dados removível os dados podem ser baixados em mídias de dados removíveis como pen drives ou discos rígidos USB externos. Assim você pode usar, por ex., o seu próprio disco rígido USB para o backup de dados, mas outros discos rígidos não têm acesso.

Nesta visão geral, você vê quais efeitos as configurações do seu controle de dispositivo possui para o atual usuário. Através do botão "Editar regras" você pode adaptar as configurações para o dispositivo e do usuário conforme desejado.

> **USB Keyboard Guard:** O nosso software te protege até das mais novas ameaças: Pendrives USB infectados, que se registram como teclado no seu sistema operacional e, assim, permitem a infiltração e softwares maliciosos. O software te informa se o seu sistema detecta um novo teclado ao conectar um aparelho USB e, através da inserção de um PIN, você pode confirmar se é um novo teclado ou não. O software memoriza todos os teclados já aprovados e não pede a confirmação novamente.

Configurações

Na área **Configurações** pode configurar os respectivos módulos do programa da forma que desejar. Em geral, não é necessário executar alterações aqui, pois o G DATA Software já foi configurado na instalação de maneira ideal para o seu sistema. As seguintes funções gerais estão disponíveis para as configurações:

Salvar configurações: As configurações feitas podem ser salvas em um arquivo GData de configurações. Se o G DATA Software for usado em vários computadores, as configurações podem ser feitas desta forma em um computador, salvas, e o arquivo de configurações pode ser carregado em outro computador.

Carregar configurações: Assim, pode ser carregado um arquivo com as configurações GData criado neste ou em qualquer outro computador.

Redefinir configurações: Caso tenha ocorrido um erro na configuração do seu G DATA Software, por este botão pode ser feita a redefinição de todas as configurações do programa nas condições de fábrica. Você também pode definir, se quer fazer a redefinição de todas ou apenas determinadas áreas da configuração. Para isso, selecione com marcação as áreas que deseja redefinir.

Geral

Segurança / Desempenho

Se você quiser usar a sua proteção de vírus em um computador lento, existe a possibilidade de melhorar o nível de segurança em favor do desempenho, ou seja, melhorar a velocidade de trabalho do computador. Na representação gráfica é possível ver os efeitos de uma otimização obtidos com a configuração.

- **Computador padrão (recomendado)**: Aqui você tem disponível a proteção ideal do G DATA Software. Os dois mecanismos de antivírus do programa trabalham lado a lado. Além disso, os acessos para leitura e escrita ao seu computador são verificados quanto a códigos maliciosos.

  Motor: O seu G DATA Software trabalha com dois mecanismos de antivírus. De forma geral, a utilização de ambos os motores garante os melhores resultados na prevenção de vírus.

- **Computador lento**: Para não limitar a velocidade de trabalho em computadores lentos, o seu G DATA Software também pode trabalhar com apenas um mecanismo. Esta proteção está disponível exclusivamente em muitos programas antivírus no mercado, que desde o início trabalham apenas com um mecanismo. A proteção dessa maneira ainda é boa. Além disso, você pode definir que um modo de sentinela seja verificado apenas quando processos de escrita são feitos. Dessa maneira são verificados apenas dados novo salvos, o que melhora ainda mais o desempenho.

- **Definido pelo usuário**: Aqui pode ser feita a seleção individual, se você quiser usar os dois ou somente um mecanismo e definir para a sentinela, se esta deve ficar ativa ao escrever e ler, somente ao escrever (executar) ou inativo de modo nenhum (não recomendável).

Palavra-passe

Através de atribuição de uma senha você pode proteger as configurações do seu G DATA Software. Desta forma um outro usuário de seu computador não pode desligar a sentinela de vírus ou a verificação em modo ocioso.

Para fazer a atribuição de uma senha, dê entrada em "Senha" e em seguida em "Repetir senha", para evitar erros de ortografia. Além disso, em "Dica de senha" pode ser dada uma dica sobre a senha.

Observação: A dica sobre a senha é exibida quando é dada a entrada de uma senha incorreta. Por isso, a dica sobre a senha deveria permitir conclusão somente para você.

Observação: Essa proteção de senha representa uma proteção ampliada do software. Segurança máxima é alcançada através do trabalho com várias contas de usuário. Você como administrador deveria fazer a gestão, em sua conta do usuário, por exemplo, da proteção de vírus e, outros usuários (por ex., filhos, amigos e parentes) não podem fazer mudanças aqui através de suas contas do usuário com direitos restritos.

Observação: Se você, por exemplo, não necessitar mais de senha para o seu G DATA Software após aplicar várias contas de usuário, você pode cancelar a obrigação de digitar senha através do botão "Remover senha".

AntiVirus

Proteção em tempo real

A proteção em tempo real da sentinela de vírus verifica continuamente o seu computador quanto à existência de vírus e controla os processos de escrita e leitura e, assim que um programa desejar executar funções maliciosas ou propagar arquivos danosos, ela o impede. A sentinela de vírus é a sua protecção mais importante! Ela não deve nunca ser desativada!

As seguintes opções estão disponíveis aqui:

- **Estado da sentinela**: Defina aqui se a sentinela deve estar activa ou inactiva.
- **Utilizar motores**: O software trabalha com dois mecanismos (engine = máquina/motor em inglês), ou seja, dois programas de verificação de vírus independentes entre si. Cada um destes motores oferece, por si só, um elevado grau de protecção contra vírus, mas é precisamente a combinação dos dois motores que oferece os melhores resultados. Nos computadores mais antigos ou mais lentos é possível acelerar a verificação de vírus, utilizando apenas um dos motores. No entanto, deverá, geralmente, manter a configuração **Ambos os motores**.
- **Ficheiros infectados**: Quando é detectado um vírus, é-lhe perguntado, na configuração padrão, como quer proceder com o vírus e o ficheiro infectado. Se desejar realizar sempre a mesma acção, poderá defini-la aqui. A máxima segurança para os seus dados oferece a configuração **Desinfectar (se não for possível: em quarentena)**.
- **Arquivos infectados**: Defina aqui se os arquivos compactados (ou seja, arquivos com a extensão RAR, ZIP ou também PST) deverão ser tratados de forma diferente dos arquivos normais. No entanto, observe que, mover um arquivo para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta da **quarentena**.
- **Monitoramento de comportamento**: Quando a vigilância de comportamento está activada, cada actividade no seu sistema é monitorizada independentemente da sentinela de vírus. Assim, também são reconhecidos vírus para os quais ainda não existe assinatura.
- **Anti-Ransomware**: Proteção contra Trojans de criptografia.
- **Exploit Protection**: Um exploit apoveita as fraquezas do software de aplicação comum e, no pior dos casos, pode assumir o controle do seu computador com estas vulnerabilidades. Os exploits podem atacar mesmo quando os aplicativos (por exemplo, visualizador de PDF, navegador, e etc.) são atualizados regularmente. A Exploit Protection protege de tais ataques, também de forma proativa contra os ataques até então desconhecidos.

Excepções

Clicando no botão Exceções, você pode excluir determinadas unidades, diretórios e arquivos da verificação e, dessa forma, acelerar significativamente a detecção de vírus.

Então proceda da seguinte forma:

1. Clique no botão **Exceções**.
2. Na janela **Excepções da sentinela**, clique em **Novo**.
3. Defina agora se deseja excluir uma unidade, um directório ou um ficheiro ou um tipo de ficheiro.
4. Então, selecione o diretório ou a unidade que deseja proteger. Para proteger arquivos, digite o nome completo do arquivo no campo de entrada na máscara de arquivos. Também poderá trabalhar com marcadores de posição.

   Observação: A forma de funcionamento de espaços reservados é a seguinte:

   - O ponto de interrogação (?) é substituto para caracteres individuais.
   - O asterisco (*) é substituto para sequências de caracteres inteiras.

   Para, por exemplo, proteger todos os arquivos com a extensão de arquivo ".sav", digite *.sav. Para proteger uma seleção especial com nomes de arquivo sequenciais, (p.ex., text1.doc, text2,doc, text3.doc), digite, por exemplo, text?.doc.

Pode repetir esta operação as vezes necessárias e voltar a eliminar ou modificar as excepções existentes.

Avançadas

Além disso, se clicar no botão **Avançadas**, pode definir quais as verificações adicionais que a sentinela de vírus deve realizar.

Por norma, não precisa de efectuar aqui mais configurações.

- **Modo**: Aqui pode definir se ao executar os ficheiros estes devem ser verificados aquando da leitura ou da escrita e leitura. Se a verificação ocorrer durante a escrita de um ficheiro, é verificado, aquando da criação de um ficheiro novo ou versão de ficheiro, se um processo desconhecido infectou eventualmente esse ficheiro. Caso contrário, os ficheiros são apenas verificados quando é feita a leitura com programas.

- **Monitorar principalmente as pastas críticas**: Com esta função, é possível pode verificar principalmente as pastas críticas, por exemplo, pastas liberadas para uso na rede, dados pessoais ou serviços de nuvem (como, por exemplo, Microsoft Dropbox, OneDrive, GoogleDrive e etc). Depois de selecionar esta caixa de diálogo, estas pastas serão, independentemente das configurações utilizadas para as outras pastas, arquivos ou diretórios, sempre monitoradas no modo **Verificar ao ler e escrever**. Se você selecionou o modo **Verificar ao ler e escrever** para todos os arquivos, está excluída a possiblidade de configuração para as pastas críticas.

- **Verificar acessos à rede**: Se o seu computador estiver ligado a uma rede com computadores desprotegidos (por exemplo, computadores portáteis desconhecidos), é aconselhável verificar também os acessos à rede quanto à transferência de programas maliciosos. Se utilizar o seu computador como posto de trabalho individual sem ligação em rede, não é necessário activar esta opção. Se todos os computadores ligados em rede estiverem protegidos contra vírus, é também aconselhável desactivar esta opção para evitar uma dupla verificação de determinados ficheiros e consequentemente um impacto negativo na velocidade do sistema.

- **Heurística**: Na análise heurística, os vírus não são detectados apenas com a ajuda das actualizações de vírus, que lhe disponibilizamos regularmente online, mas também com base em determinadas características específicas dos vírus. Este método constitui uma vantagem de segurança adicional, mas por vezes também pode dar origem a um falso alarme.

- **Verificar arquivos**: A verificação de arquivos compactados (reconhecidos através das extensões de arquivo ZIP, RAR ou também PST), demanda muito tempo e pode ser ignorada por via de regra, quando a sentinela de vírus estiver ativada no sistema em geral. Para aumentar a velocidade da verificação de vírus, você pode limitar o tamanho das pastas que serão verificados, para um determinado valor em kilobytes.

- **Verificar arquivos de e-mail**: Como o software já verifica a infecção de vírus na entrada e na saída de e-mails, na maioria dos casos é recomendável não fazer a verificação regular dos arquivos de e-mail, porque esse procedimento, dependendo do tamanho do arquivo de e-mail, poderá demorar alguns minutos.

- **Verificar áreas do sistema ao iniciar o sistema**: Normalmente, as áreas do sistema (por exemplo, sectores de arranque) do seu computador não devem ser excluídas da detecção de vírus. Poderá definir aqui se pretende que a verificação seja efectuada ao iniciar o sistema ou na troca de média (por exemplo, ao introduzir um CD-ROM novo). Normalmente, deverá ter pelo menos uma destas funções activadas.

- **Verificar áreas de sistema na troca de suporte**: Normalmente, as áreas do sistema (por exemplo, sectores de arranque) do seu computador não devem ser excluídas da detecção de vírus. Poderá definir aqui se pretende que a verificação seja efectuada ao iniciar o sistema ou na troca do suporte (ao introduzir um CD-ROM novo, por exemplo). Normalmente, deverá ter pelo menos uma destas funções activadas.

- **Verificar Dialer/Spyware/Adware/Riskware**: Com o software é possível verificar a existência de discadores e outros programas maliciosos no seu sistema. Aqui, trata-se de programas que estabelecem conexões caras e indesejadas à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.

- **Verificar apenas ficheiros novos ou modificados**: Se você ativar esta função, os arquivos que não são verificados há muito tempo e que antes tinham sido reconhecidos como inofensivos serão ignorados. Isso leva a um ganho de desempenho no trabalho diário – sem risco de segurança.

Verificação manual de vírus

Poderá efectuar configurações básicas de programa para a Verificação de vírus.

No entanto, no modo normal, tal não será necessário.

- **Utilizar motores**: O software trabalha com dois mecanismos (engine = máquina/motor em inglês), ou seja, dois programas de verificação de vírus coordenados entre si. Nos computadores mais antigos ou mais lentos é possível acelerar a verificação de vírus, utilizando apenas um dos motores. No entanto, deverá, geralmente, manter a configuração **Ambos os motores**.
- **Ficheiros infectados**: O seu software detectou um vírus? Na configuração padrão, o software pergunta o que pretende fazer com o vírus e com o ficheiro infectado. Se desejar realizar sempre a mesma acção, poderá defini-la aqui. A máxima segurança para os seus dados oferece a configuração **Desinfectar (se não for possível: em quarentena)**.
- **Arquivos infectados**: Defina aqui se os arquivos compactados (ou seja, arquivos com a extensão RAR, ZIP ou também PST) deverão ser tratados de forma diferente dos arquivos normais. No entanto, observe que, mover um arquivo para a quarentena pode danificá-lo, de forma que ele também não poderá mais ser usado após movê-lo de volta da **quarentena**.
- **Interromper a verificação de vírus no caso de sobrecarga do sistema**: Normalmente a verificação de vírus deve decorrer quando não estiver a utilizar o computador. Se voltar a utilizar o computador, a verificação de vírus é interrompida, para que seja disponibilizada a velocidade habitual do sistema. A verificação de vírus é efectuada, portanto, durante os intervalos de trabalho.

Excepções

Clicando no botão Exceções, você pode excluir determinadas unidades, diretórios e arquivos da verificação e, dessa forma, acelerar significativamente a detecção de vírus.

Então proceda da seguinte forma:

1. Clique no botão **Exceções**.
2. Na janela **Excepções para a verificação manual do computador** clique em **Novo**.
3. Defina agora se deseja excluir uma unidade, um directório ou um ficheiro ou um tipo de ficheiro.
4. Então, selecione o diretório ou a unidade que deseja proteger. Para proteger arquivos, digite o nome completo do arquivo no campo de entrada na máscara de arquivos. Também poderá trabalhar com marcadores de posição.

   Observação: A forma de funcionamento de espaços reservados é a seguinte:

   - O ponto de interrogação (?) é substituto para caracteres individuais.
   - O asterisco (*) é substituto para sequências de caracteres inteiras.

   Para, por exemplo, proteger todos os arquivos com a extensão de arquivo ".sav", digite *.sav. Para proteger uma seleção especial com nomes de arquivo sequenciais, (p.ex., text1.doc, text2,doc, text3.doc), digite, por exemplo, text?.doc.

Pode repetir esta operação as vezes necessárias e voltar a eliminar ou modificar as excepções existentes.

Aplicar excepções também à verificação em inactividade: Enquanto na verificação manual de vírus o computador é objetivamente verificado quanto a vírus e não deveria ser utilizado para outras tarefas, a verificação em modo ocioso é uma verificação inteligente de vírus, em que todos os arquivos do seu computador são sempre verificados se já não estão infectados com um vírus. A verificação em inactividade funciona como uma protecção de ecrã. Quando não utiliza o seu computador durante um determinado tempo, a verificação inicia-se e logo que continue a trabalhar, pára para lhe oferecer o máximo de desempenho. Aqui pode determinar, se devem ser definidas excepções para ficheiros ou directórios para a verificação em inactividade.

Avançadas

Clicando sobre o botão "Avançado", você pode efetuar configurações avançadas para a verificação de vírus.

Na maioria dos casos, basta utilizar as configurações padrão predefinidas.

- **Tipos de ficheiro**: Aqui pode definir que tipos de ficheiros devem ser analisados pelo software quanto à existência de vírus. A seleção da opção Somente arquivos de programa e documentos aumenta a velocidade.
- **Heurística**: Durante a análise heurística, os vírus são detectados não apenas com a ajuda das bases de dados de vírus, obtidas em cada actualização do software de antivírus, mas também com base em determinadas características dos vírus. Este método constitui uma vantagem de segurança adicional, mas por vezes também pode dar origem a um falso alarme.
- **Verificar arquivos**: A verificação de arquivos compactados (reconhecidos através das extensões de arquivo ZIP, RAR ou também PST), demanda muito tempo e pode ser ignorada por via de regra, quando a sentinela de vírus estiver ativada no sistema em geral. Para aumentar a velocidade da verificação de vírus, você pode limitar o tamanho das pastas que serão verificados, para um determinado valor em kilobytes.
- **Verificar arquivos de e-mail**: Aqui pode determinar, se os seus arquivos de e-mail devem ser verificados em relação a infecções.
- **Verificar áreas do sistema**: Normalmente, as áreas do sistema (por exemplo, sectores de arranque) do seu computador não devem ser excluídas da detecção de vírus.
- **Verificar Dialer/Spyware/Adware/Riskware**: Com essa função é possível verificar a existência de discadores e outros softwares maliciosos no seu sistema. Aqui, trata-se de programas que estabelecem conexões caras e indesejadas à Internet e não ficam nada atrás dos vírus em relação ao seu potencial de dano comercial, que p.ex., armazenam secretamente o seu comportamento na navegação ou até mesmo todos os dados digitados (e com isso também suas senhas) e, na próxima oportunidade, encaminham através da Internet a terceiros.
- **Verificar RootKits**: Os Rootkits tentam escapar dos métodos comuns de detecção de vírus. Contudo, é sempre aconselhável realizar uma análise adicional para malware.
- **Verificar apenas ficheiros novos ou modificados**: Se você ativar esta função, os arquivos que não são verificados há muito tempo e que antes tinham sido reconhecidos como inofensivos serão ignorados. Isso leva a um ganho de desempenho no trabalho diário – sem risco de segurança.
- **Criar relatório**: Com esta marcação, é possível definir se o software deve criar um registro sobre o processo de verificação de vírus. Este pode se consultado em Registos.
- **Oferecer verificação de vírus para Mídia de dados removível**: Quando você fizer essa marcação, ao conectar uma mídia de dados removíveis (como pen drives, discos rígidos externos, etc.) com o computador é perguntado se este dispositivo também deve ser verificado.

Actualizações

Se não conseguir actualizar o software ou as assinaturas de vírus pela Internet, poderá introduzir nesta área todos os dados necessários para possibilitar uma actualização automática. Insira nas opções, os seus dados de acesso (nome de usuário e senha) que você recebeu por e-mail no registro on-line do seu software. Com a ajuda desses dados você será reconhecido pelo servidor de atualização G DATA e as atualizações poderão ocorrer automaticamente.

Se você adquiriu uma licença nova e quer ativá-la, selecione **Ativar licença**, A função **Configurações da Internet** exibe opções especiais que são necessárias apenas em alguns casos excepcionais (servidor proxy, outra região). Deve desactivar temporariamente a verificação da versão, se tiver dificuldades na actualização das assinaturas de vírus.

Gerenciar acessos: Com esta opção, você tem a possibilidade de terminar através de quais conexões de internet podem ser feitas atualizações do programa. Isso é muito útil se você estiver conectado temporariamente com uma rede onde a transferência de dados é paga, ou seja, por exemplo, por terminadas tarifas de rede móvel sem taxa fixa de dados.

Importar/exportar a assinatura do antivírus: Nos computadores que raramente são conectados à internet ou que possuem restrições sobre o volume de dados para download, você pode atualizar a assinatura do antivírus com um suporte de dados (por exemplo, pendrive USB), ou seja, realizar uma **Atualização Offline**. Para isso, é preciso exportar para o suporte de dados as assinaturas do antivírus em um computador conectado à internet e que tenha o direito necessário, e depois, importar para o computador sem conexão com a internet com a função "Importar de". Então, o sistema neste computador ficará protegido com a mais nova assinatura do antivírus. Em contraste com as atualizações periódicas da assinatura do antivírus pela internet, aqui, o usuário é obrigado a garantir ele mesmo a realização de atualizações da assinatura do antivírus o mais frequente possível.

Actualizar automaticamente as assinaturas de vírus

Caso você não queira que o G DATA Software cuide da atualização das assinaturas de vírus automaticamente, você pode desmarcar a caixa aqui. A desactivação representa no entanto um elevado risco de segurança e só deverá ser feito em caso de excepção. Se o intervalo entre as actualizações for demasiado pequeno, poderá ajustá-lo individualmente e determinar, por exemplo, que sejam efectuadas quando estabelece uma ligação à Internet. Esta selecção é útil, por exemplo, nos computadores que não estão permanentemente ligados à Internet.

Criar relatório: Quando você fizer a marcação aqui, cada atualização das assinaturas de vírus será integrada no registro que pode ser verificado nas funções adicionais do G DATA Software (em **SecurityCenter** em **Registos**). Além desses registros, você encontra em Registro, por exemplo, informações sobre descobertas de vírus e outras ações que foram efetuadas pelo programa.

Ativar licença

Se você ainda não tiver registrado o seu G DATA Software, poderá fazê-lo agora e inserir seu número de registro e os dados do cliente. Você encontra o número de registro, dependendo do tipo do produto, por ex., na contracapa do manual de utilização, no e-mail de confirmação no download do software ou na capa do CD. Através da inserção do número de registro, o produto é ativado.

Clique agora no botão **Registrar** e os seus dados de acesso serão gerados no servidor de atualização. Se o registro tiver sido realizado com sucesso, aparecerá uma tela de informações com a observação **O registro foi concluído com sucesso**, a qual pode ser fechada com o botão fechar.

> **Atenção**: Para a sua documentação e novas reinstalações do software, seus dados de acesso também serão enviados por e-mail. Por isso, certifique-se de que o endereço de e-mail introduzido durante o registo online está correcto. Caso contrário, não receberá os dados de acesso.

Em seguida, os dados de acesso são assumidos automaticamente pela máscara de introdução original e a partir daí poderá actualizar as assinaturas de vírus através da Internet.

> **Você não consegue ativar sua licença?** Se não conseguir estabelecer ligação ao servidor isto poderá ser devido a um servidor proxy. Clique no botão **Configurações da Internet** aqui poderá efectuar configurações para a sua ligação à Internet. Normalmente, em caso de problemas com a atualização das assinaturas de vírus, você deve primeiro verificar se consegue acessar a Internet com um navegador (por exemplo, com o Internet Explorer). Se não conseguir estabelecer qualquer ligação à Internet, o problema estará relacionado com a ligação à Internet e não com os dados do servidor Proxy.

Configurações da Internet

Se um servidor proxy é usado, coloque a marcação em **Utilizar servidor proxy**. Apenas deverá alterar estas configurações no caso de a actualização das assinaturas de vírus não funcionar. Caso necessário, contacte o seu administrador do sistema ou fornecedor de acesso à Internet por causa do endereço proxy. Se necessário, poderá inserir aqui os dados de acesso para o servidor proxy.

> **Servidor proxy**: Um servidor proxy compila os pedidos a redes e distribui-os pelos seus computadores ligados. Se quiser, por exemplo, utilizar o computador numa rede empresarial, é possível que esteja a fazê-lo através de um servidor proxy. Em geral, quando surgem problemas com a sua actualização das assinaturas de vírus deve verificar se consegue aceder à Internet em geral através de um browser da Internet. Se não conseguir estabelecer qualquer ligação à Internet, o problema estará relacionado com a ligação à Internet e não com os dados do servidor Proxy.

Protecção Web

Quando a proteção da web está ativada, os conteúdos da internet já são verificados quando a eventuais softwares maliciosos já na navegação. Aqui podem ser feitas as seguintes configurações.

- **Verificar conteúdo da Internet (HTTP)**: Nas opções de Proteção da web, você pode definir que a existência de vírus em todo o conteúdo da Web por HHTP seja verificada já na navegação. Os conteúdos Web infectados não são sequer executados, sendo que as respectivas páginas não são apresentadas. Para isso, coloque a marcação em **Verificar conteúdo da Internet (HTTP)**.

  Se você não desejar permitir a verificação dos conteúdos da Internet, a sentinela de vírus entra naturalmente em ação quando arquivos infectados forem executados. Assim, o seu sistema continuará protegido mesmo sem a verificação dos conteúdos da Internet enquanto a sentinela de vírus estiver activa.

  Também pode definir determinadas páginas Web como excepções, se estas forem consideradas inofensivas. Para mais informações, leia o capítulo **Definir excepções**. Através do botão **Avançadas** podem ser feitas outras configurações para lidar com conteúdos da internet.

- **Proteção contra phishing**: Com o chamado Phishing, os trapaceiros da Internet tentam direcionar os clientes de um determinado

banco ou loja, para um site falsificado e lá, roubar seus dados. Recomenda-se vivamente que active a protecção de phishing.

- **Enviar endereços de páginas da Internet infectadas**: Através desta função, você pode - naturalmente de forma anônima - informar automaticamente as páginas da Internet que foram consideradas como perigosas pelo software. Deste modo, optimiza a segurança para todos os utilizadores.

- **Proteção do navegador BankGuard**: Os cavalos de troia bancários são uma ameaça crescente. A cada hora, os criminosos on-line desenvolvem novas variantes de malware (p. ex., ZeuS, SpyEye) para roubar seu dinheiro. Os bancos protegem o tráfego de dados na internet, mas os dados são decodificados no navegador e é lá que os cavalos de troia atacam. A tecnologia inovadora do G DATA BankGuard protege as suas negociações bancárias desde o começo e faz a proteção exatamente onde o ataque está ocorrendo. Através de uma verificação da veracidade das bibliotecas da rede usadas, o G DATA BankGuard garante que o seu navegador de internet não seja manipulado por um cavalo de troia bancário. Recomendamos sempre deixar ativada a proteção do G DATA BankGuard.

  Informações: Além do método Man-in-the-Middle, em que o atacante influencia a comunicação entre o usuário e o computador de destino, também existe o método de ataque Man-in-the-Browser (MITB). Neste método, o atacante se infiltra no próprio navegador e coleta os dados antes que eles sejam codificados. O módulo BankGuard também te protege deste tipo de ataque, a impressão digital de um arquivo ou de parte de uma página da internet é comparada com um banco de dados na internet. Deste modo, uma fraude é descoberta imediatamente e o G DATA Software troca imediatamente a conexão de dados fraudulenta pela original.

- **Proteção do Keylogger**: A proteção do Keylogger monitora, independentemente das assinaturas de vírus, se as entradas do teclado no seu sistema são espionadas. Com isso, são eliminadas as possibilidades de atacantes registrarem as suas inserções de senhas. Esta função deve sempre permanecer ligada.

Definir excepções

Para adicionar uma página da Internet como excepção à lista branca, proceda da seguinte forma:

1. Clique no botão **Definir excepções**. Agora a janela Whitelist será exibida. Aqui são apresentadas as páginas Web que considerou seguras e adicionou à lista.

2. Para adicionar outras páginas da Internet, clique em **Novo**. Abre-se uma máscara de introdução. Em **URL** introduza o endereço da página Web, como por exemplo (www.paginainsuspeita.pt) e em **Comentário** eventualmente uma nota por que adicionou esta página Web. Confirme a inserção com um clique em **OK**.

3. Confirme então clicando em **OK** todas as alterações feitas na Whitelist.

Para eliminar uma página Web novamente da lista branca, marque-a com o rato na lista e depois clique simplesmente no **botão** Eliminar.

Avançadas

Aqui é possível definir quais números de porta de servidor devem ser monitorados pela proteção da Web. Em regra, basta o número de porta 80 para uma monitorização de navegação normal.

- **Evitar ultrapassar o limite de tempo no navegador**: Uma vez que o software processa o conteúdo da Internet antes de sua exibição no navegador da Internet e necessita de um certo tempo dependendo dos resultados dos dados, pode aparecer uma mensagem de erro no navegador da Internet, porque este não consegue fornecer os dados imediatamente, pois estes estão sendo verificados pelo software antivírus quanto a rotinas maliciosas. Com a colocação da marcação no campo **Evitar ultrapassar limite de tempo no navegador**, evita-se uma mensagem de erro e, assim que a existência de vírus for verificada em todos os dados do navegador, esses serão transmitidos normalmente para o navegador da Internet.

- **Notificações ativadas na verificação de downloads**: Ative este recurso para receber notificações quando um download está sendo verificado.

- **Limite de tamanho para downloads**: Aqui pode suprimir a verificação HTTP para conteúdos da Web demasiado grandes. Os conteúdos então são verificados pela sentinela de vírus assim que sejam activadas possíveis rotinas maliciosas. A vantagem desta limitação do tamanho é a de não existirem demoras por parte do controlo de vírus, enquanto o utilizador navega na Web.

Verificação de e-mail

Através da verificação de e-mail poderá detectar vírus nos e-mails de entrada e saída, bem como nos respectivos anexos e eliminar possíveis infecções directamente na fonte. Se for detectado um vírus, o software consegue eliminar directamente os anexos de ficheiro ou reparar ficheiros infectados.

> **Atenção**: No Microsoft Outlook a verificação de e-mail é realizada através de um plugin. Isso oferece a mesma proteção que as funções de proteção orientadas a POP3/IMAP dentro as opções do Antivírus. Após a instalação desse Plug-in, você encontrará no menu **Extras** do Outlook a função **Verificar a existência de vírus na pasta**, com a qual você poderá verificar a existência de vírus em suas pastas de e-mail individuais.

E-mails a receber

As seguintes opções estão disponíveis para proteção de vírus para e-mails de entrada:

- **No caso de uma infecção**: Aqui poderá determinar o que deve acontecer caso se descubra um mail infectado. De acordo com a utilização que tiver o seu computador aconselha-se a utilização de diversas configurações. Por norma, aconselha-se a configuração **Desinfectar (se não for possível: Eliminar anexo/texto)**.
- **Verificar e-mails recebidos**: Com a ativação dessa opção, a existência de vírus é verificada em todos os e-mails que chegam até você durante o seu trabalho no computador.
- **Anexar relatório aos e-mails recebidos e infectados**: Se tiver activado a opção de relatório, no caso de detecção de um vírus surge na linha de assunto do e-mail infectado o aviso **VIRUS** e no início da mensagem a advertência **Atenção! Este e-mail contém o seguinte vírus** seguido do nome do vírus e da informação se o vírus foi eliminado ou se foi possível reparar o ficheiro infectado.

E-mails a enviar

Para que você não encaminhe vírus inadvertidamente, o software oferece também a possibilidade de verificar a existência de vírus em seus e-mails antes do envio. Caso o utilizador esteja preste a enviar um vírus (não intencionalmente), irá aparecer a mensagem **O mail [linha de assunto] contém o vírus seguinte: [Nome do vírus]**. O mail não pode ser enviado, sendo que a mensagem electrónica correspondente não é enviada. Para que os e-mails de saída sejam verificados, faça a marcação em **Verificar e-mails antes do envio**.

Opções de verificação

Aqui podem ser ligadas ou desligadas opções básicas da verificação de vírus:

- **Utilizar motores**: O software trabalha com dois mecanismos de antivírus, duas unidades de análise coordenadas entre si. De forma geral, a utilização de ambos os motores garante os melhores resultados na prevenção de vírus.
- **OutbreakShield**: Aqui pode activar o OutbreakShield. O software cria, com a OutbreakShield ativada, somas de teste de e-mails, compara-as com as blacklists AntiSpam constantemente atualizadas na Internet e, com isso, é capaz de reagir a um envio de e-mails em massa antes que existam as respectivas assinaturas de vírus. A OutbreakShield consulta na Internet sobre acumulações especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente. O OutbreakShield encontra-se integrado no bloqueio de vírus do e-mail.

Conexões criptografadas (SSL)

Diversos servidores de e-mail (por exemplo, GMX, WEB.DE, T-Online e Freenet) mudaram para a criptografia SSL neste meio tempo. Deste modo, os e-mails e as contas de e-mail se tornaram muito mais seguros. No entanto, ainda é preciso proteger os seus e-mails com um programa de anti-vírus. Para isso, a G DATA oferece o modo de **conexão criptografada (SSL)**. Você também tem a possibilidade de verificar os e-mails criptografados SSL quanto à vírus e malwares.

Para fazer a verificação de e-mails criptografados SSL pelo G DATA Software, é preciso importar um certificado do G DATA Software para o programa do e-mail. Deste modo, pode ser garantido que o G DATA Software possa verificar os e-mails que chegarem.

São suportados todos os programas de e-mail que podem importar certificados ou acessar janelas de certificado no Windows, por exemplo:

- Outlook 2003 ou mais recente
- Thunderbird
- The Bat

- Pegasusmail

Por favor, proceda do seguinte modo se o certificado da G DATA não foi instalado automaticamente:

1. Ao instalar o certificado, os seus programas de e-mail não podem estar ativos. Feche uma vez todos os programas de e-mail antes de criar e instalar o certificado.

2. Marque as verificações conexões SSL do G DATA Software.

3. Clique no botão para exportar o certificado. O G DATA Software irá criar um certificado. Este arquivo se chama GDataRootCertificate.crt.

4. Abra o arquivo GDataRootCertificate.crt. Aparece uma janela de diálogo onde você pode instalar o certificado no seu computador.

5. Clique no botão **Instalar certificado** na janela de diálogo e siga as instruções do assistente de instalação.

Pronto. Agora o Outlook e todos outros programas de e-mail que tem acesso à janela de certificado do Windows possuem o certificado necessário para poder verificar os e-mails criptografados com SSL recebidos quanto à vírus e outros malwares.

Observação: Se você utilizar o **Thunderbird (portable)** e o certificado não for automaticamente importado, você precisa importá-lo depois e gerenciar as configurações de confiança do certificado G DATA criado. Para isso, selecione em Thunderbird (portable) **Configurações > Ampliada > Certificados** o botão **Certificados**. Uma aba diferente aparece quando você clica aqui. Selecione a aba **Locais de certificação** e depois o botão **Importar**. Agora você pode selecionar o certificado **G DATA Mail Scanner Root**.

Se você marcar os seguintes campos de opção e clicar em OK, o seu Thunderbird portable será protegido pela G DATA:

- **Confiar neste CA, para identificar sites.**
- **Confiar neste CA, para identificar usuários de e-mail.**
- **Confiar neste CA, para identificar criadores de software** .

Nos outros programas de e-mail, existem funções similares para importar os certificados. Em caso de dúvidas, leia no ajuda correspondente como funciona no seu programa de e-mail.

Avançadas

Se na utilização do seu programa de e-mail você não usar as portas padrão, você poderá informar em **Número da porta do servidor** também a porta que utiliza para e-mails de entrada ou saída. Clicando no botão **Padrão**, são repostos automaticamente os números de porta padrão. Poderá também especificar várias portas. No entanto, separe-as por uma vírgula.

Atenção: O Microsoft Outlook é protegido por um Plugin especial, através do qual é possível verificar pastas e e-mails diretamente do Outlook. Para fazer a verificação de vírus de um e-mail ou uma pasta do Outlook, clique no ícone da G DATA e, a pasta de e-mail selecionada atualmente é verificação quanto a vírus.

Como o software processa os e-mails de entrada antes do próprio programa de e-mail poderá aparecer, em grandes quantidades de e-mail ou conexões lentas, uma mensagem de erro do programa de e-mail, porque esse não recebe imediatamente os dados dos e-mails, pois estes estão sendo verificados pelo software quanto a vírus. Ao ativar a marcação em **Evitar ultrapassar limite de tempo no servidor de e-mail**, evita-se uma mensagem de erro do programa de e-mail e, assim que a existência de vírus for verificada em todos os dados de e-mails, esses serão encaminhados normalmente pelo software para o programa de e-mail.

Verificações automáticas de vírus

Aqui é possível ativar ou desativar a verificação em modo ocioso. Para além disso, pode em vez disso ou até adicionalmente verificar o seu computador ou áreas do seu computador quanto a infecções. Pode, por exemplo, efectuar essas verificações em períodos nos quais não utiliza o seu computador.

Verificações de vírus programadas: Em muitos casos, é suficiente que o computador seja verificado em modo ocioso. No entanto, através do botão **Novo** também pode criar diversas verificações automáticas de vírus individuais. Por exemplo, imagina-se que você faça a verificação diária da pasta downloads, enquanto a sua coleção de MP3 é verificada apenas uma vez por mês.

Nos próximos capítulos será esclarecido como criar verificações individuais de vírus.

Geral

Determine aqui que nome deverá ter a nova verificação de vírus automática criada. Para se distinguirem melhor, aconselham-se nomes expressivos como, por exemplo, *Discos rígidos locais (verificação semanal)* ou *Arquivos (verificação mensal)*.

Se colocar um visto em **Depois de terminada a tarefa, desligar o computador**, o computador é automaticamente desligado depois de ter sido executada a detecção automática de vírus. Isto é conveniente se desejar efectuar a verificação de vírus, por exemplo, depois do trabalho no escritório.

> **Tarefa**: Cada uma das ordens automáticas definidas para a verificação do computador ou de determinadas áreas é denominada tarefa.

Âmbito da análise

Defina aqui se a verificação de vírus deverá ser feita nos discos rígidos locais, se a área da memória e da inicialização automática deve ser testada ou, se deseja verificar apenas determinados diretórios e arquivos. Se for o caso, introduza os directórios desejados através do botão **Selecção**.

Verificar directórios/ficheiros: Na árvore de diretórios, clicando nos sinais de mais (+), é possível abrir e selecionar os diretórios cujo conteúdo será então exibido na visualização de arquivo. Cada directório ou cada ficheiro com marca de verificação colocada será verificado pelo software. Se num determinado directório não forem verificados todos os ficheiros, então nesse directório encontra-se um símbolo de marcação cinzento.

Agendamento

Através desta ficha pode determinar quando e a que ritmo deve ser efectuado o trabalho em questão. Em **Executar**, indique uma definição que especificará depois com as entradas em **Período**. Se você selecionar **Na inicialização do sistema**, não há necessidade de limitar o tempo, e o software executará a verificação sempre que o seu computador for reinicializado.

- **Iniciar tarefa no próximo arranque, se o computador estiver desligado à hora de início da tarefa**: Activando esta opção, as verificações automáticas de vírus não executadas serão automaticamente efectuadas mais tarde, logo que o computador seja ligado.
- **Não executar no modo de bateria**: Para não reduzir a duração da bateria desnecessariamente, você pode, por ex., definir para notebooks que as verificações automáticas de vírus ocorram somente quando o computador portátil estiver conectado à rede elétrica.

Configurações de verificação

Nesta área pode definir quais as configurações que o programa deve utilizar para fazer a verificação automática de vírus.

- **Utilizar motores**: O software trabalha com dois mecanismos, ou seja, dois programas de verificação de vírus otimizados, independentes entre si. Nos computadores mais antigos ou mais lentos é possível acelerar a verificação de vírus, utilizando apenas um dos motores. No entanto, deverá, geralmente, manter a configuração **Ambos os motores**.
- **Ficheiros infectados**: O seu software detectou um vírus? Na configuração padrão, o software pergunta o que pretende fazer com o vírus e com o ficheiro infectado. Se desejar realizar sempre a mesma acção, poderá defini-la aqui. A máxima segurança para os seus dados oferece a configuração **Desinfectar (se não for possível: em quarentena)**.
- **Arquivos infectados**: Defina aqui se os arquivos compactados (ou seja, arquivos com a extensão RAR, ZIP ou também PST) deverão ser tratados de forma diferente dos arquivos normais. No entanto, tenha em conta que ao deslocar um arquivo para a quarentena este pode ficar danificado de modo que, mesmo depois de restaurado no seu local de origem, deixa de poder ser utilizado.

Se clicar no botão **Avançadas**, pode definir quais as verificações adicionais que devem ser realizadas ou excluídas.

Na maioria dos casos, basta utilizar as configurações padrão predefinidas.

- **Tipos de ficheiro**: Aqui pode definir que tipos de ficheiros devem ser analisados pelo software quanto à existência de vírus.
- **Heurística**: Na análise heurística, os vírus não são reconhecidos somente por meio dos bancos de dados de vírus que você obtém a cada atualização do software antivírus, mas também através de determinadas características típicas de vírus. Este método constitui uma vantagem de segurança adicional, mas por vezes também pode dar origem a um falso alarme.
- **Verificar arquivos**: A verificação de arquivos compactados (reconhecidos através das extensões de arquivo ZIP, RAR ou também PST) demanda muito tempo e pode ser ignorada por via de regra, quando a sentinela de vírus estiver, em geral, ativada no sistema. Ao

extrair o arquivo, a sentinela de vírus detecta vírus ocultos e previne automaticamente que se propaguem.

- **Verificar arquivos de e-mail**: Aqui pode determinar, se os seus arquivos de e-mail devem ser verificados em relação a infecções.
- **Verificar áreas do sistema**: Normalmente, as áreas do sistema (por exemplo, sectores de arranque) do seu computador não devem ser excluídas da detecção de vírus.
- **Verificar Dialer/Spyware/Adware/Riskware**: Com esta função, o seu sistema pode ser verificado também quanto a discadores e outros softwares maliciosos (Spyware, Adware e Riskware). Estes são, por exemplo, programas que estabelecem indesejadamente ligações dispendiosas à Internet e cujo potencial malicioso, do ponto de vista económico, não fica atrás dos vírus que, por exemplo, guardam secretamente os seus hábitos de navegação na Internet ou todas as sequências de teclas carregadas no teclado (e consequentemente as suas palavras-passe) e, assim que possível, os transmitem, através da Internet, a pessoas desconhecidas.
- **Verificar RootKits**: Os Rootkits tentam escapar dos métodos comuns de detecção de vírus. Contudo, é sempre aconselhável realizar uma análise adicional para malware.
- **Criar relatório**: Através desta caixa de opção pode definir se o software cria um relatório acerca do processo de verificação de vírus. Este pode se consultado em **Registos**.

Conta do utilizador

Aqui pode introduzir a conta de utilizador no computador em que deve ser efectuada a verificação de vírus. Esta conta é necessária para aceder às unidades de rede.

AntiSpam

Filtro de spam

Através do filtro de spam, tem um vasto leque de opções de configuração para bloquear, de forma eficaz, e-mails com conteúdos indesejados ou de remetentes indesejados (por exemplo, remetentes de e-mails em massa). O programa verifica muitas características dos e-mails típicas para spam. Com base nas características em questão, é calculado um valor que reflecte a probabilidade de spams. Aqui, através do botão **Utilizar filtro de spam**, você ativa ou desativa o filtro de spam.

Para ativar ou desativar os diferentes tipos de filtragem do filtro de spam, coloque ou remova a marcação do respectivo registro. Para fazer alterações em vários filtros, clique no respectivo registro e uma janela de diálogo será aberta para fazer a alteração dos parâmetros. Estão disponíveis as seguintes opções de configuração:

- **Spam-OutbreakShield**: Com o OutbreakShield é possível detectar e combater vírus em e-mails em massa ainda antes de as assinaturas de vírus actualizadas se encontrarem disponíveis para esse efeito. Através da Internet, o OutbreakShield averigua se existem acumulações especiais de e-mails suspeitos e, nesse âmbito elimina, praticamente em tempo real, a falha existente entre o início de um envio de e-mails em massa e o seu combate através de assinaturas de vírus especificamente personalizadas. Se você utiliza um computador atrás de um servidor proxy, para ajustar clique no botão **Configurações da Internet** e faça as respectivas alterações. Esta configuração só deve ser alterada se o OutbreakShield não funcionar.
- **Utilizar Whitelist**: Através da Whitelist você pode excluir determinados endereços de remetentes ou domínios, explicitamente da suspeita de spam. Para isso, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (por exemplo, *newsletter@informationsseite.de*) ou o domínio (por exemplo, *informationsseite.de*) que você deseja excluir da suspeita de spam, e o G DATA Software não tratará e-mails desse remetente ou do domínio do remetente como spam.

  Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Whitelist. Os endereços e domínios têm de ser enumerados numa lista deste género em linhas individuais. O formato utilizado é um ficheiro txt simples, que pode ser criado, por exemplo no Windows Notepad. Através do botão **Exportar** você também pode exportar uma Whitelist como arquivo de texto.
- **Utilizar Blacklist**: Através da Blacklist, você pode colocar determinados endereços de remetentes ou domínios explicitamente em suspeita de spam. Para isso, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (por exemplo, *newsletter@megaspam.de.vu*) ou o domínio (por exemplo, *megaspam.de.vu*) que deseja colocar em suspeita de spam, e o G DATA Software tratará e-mails esse remetente ou domínio do remetente em geral como e-mails com altíssima probabilidade de spam. Através do botão **Importar** também pode importar endereços de e-mail ou domínios para a lista negra. Os endereços e domínios têm de ser enumerados numa lista deste género em linhas individuais. O formato utilizado é um ficheiro txt simples, que pode ser criado, por exemplo no Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Blacklist como arquivo de texto.
- **Utilizar Blacklists em tempo real (configuração padrão)**: Na Internet, existem listas negras que contém endereços IP de servidores, através dos quais spams são enviados. O G DATA Software apura, através de Consultas nas Blacklists em tempo real, se o servidor

que envia está listado. Caso esteja, aumenta então a probabilidade de existência de spam. Em geral, deve-se utilizar aqui a configuração padrão, no entanto, é possível inserir também na Blacklist 1, 2 e 3 endereços próprios para blacklists da Internet.

- **Utilizar palavras-chave (texto do e-mail)**: Através da lista de palavras-chave, você pode, com a ajuda das palavras utilizadas no texto do e-mail, colocar e-mails em suspeita de spam. Se pelo menos um dos termos aparecer no texto do e-mail, aumenta a probabilidade de spam. Pode alterar esta lista através dos botões **Adicionar**, **Alterar** e **Eliminar**. O botão **Importar** também permite inserir listas predefinidas de palavras-chave na sua lista. As entradas devem estar incluídas numa lista, em linhas diferentes, umas a seguir às outras. O formato utilizado é um ficheiro txt simples, que pode ser criado, por exemplo no Windows Notepad. Através do botão **Exportar**, você também pode exportar uma lista de palavras-chave como arquivo de texto. Através da marcação **Pesquisar somente palavras completas** é possível definir que o G DATA Software só pesquise por palavras inteiras na linha de assunto de um e-mail.

- **Utilizar palavras-chave (assunto)**: Com a lista de palavras-chave, você pode, mediante ajuda das palavras utilizadas na linha de assunto, colocar e-mails em suspeita de spam. Se, pelo menos, um dos termos aparecer na linha de assunto, aumenta a probabilidade de spam.

- **Utilizar filtro de conteúdos**: O Filtro de conteúdo é um filtro autodidata que calcula, de acordo com as palavras utilizadas no texto do e-mail, uma probabilidade de spam. Este filtro não trabalha somente com base em listas de palavras pré-determinadas, mas continua a aprender mais palavras por cada e-mail que é recebido. Com o botão **Consultar conteúdos de tabelas** poderá solicitar a apresentação das listas de palavras utilizadas pelo filtro de conteúdos para a classificação de um e-mail como spam. Com o botão **Repor tabelas** poderá apagar todos os conteúdos da tabela gravados, sendo que o filtro de conteúdos autodidacta volta a iniciar o processo de aprendizagem desde o início.

Reacção

Aqui pode definir de que modo o filtro de spam deve processar os e-mails que possam conter spam. Nesse processo, é possível definir três níveis que podem ser influenciados, que nível de probabilidade o G DATA Software utiliza para isso, já que se trata de spam no e-mail afetado.

- **Suspeita de spam**: Aqui é regulado o manuseio de e-mails nos quais o G DATA Software encontra elementos de spam individuais. Aqui geralmente pode não se tratar de spam, mas, em alguns casos raros possivelmente de e-mails com boletins informativos ou e-mails coletivos totalmente desejados pelo destinatário. Neste caso, recomenda-se que o destinatário seja alertado da suspeita de spam.

- **Alta probabilidade de spam**: Aqui são reunidos os e-mails que contém as diversas características de spam e somente em raríssimos casos são realmente desejados pelo destinatário.

- **Altíssima probabilidade de spam**: Aqui encontram-se os e-mails que atendem a todos os critérios de um e-mail de spam. Estes e-mails são quase sempre indesejados e, na maioria dos casos, a rejeição deste tipo de e-mails é recomendável.

Cada um destes três níveis de reacções pode ser ajustado individualmente. Para isso, basta clicar no botão **Alterar** e definir a reação que o G DATA Software deve ter. Através de **Rejeitar e-mail** pode evitar que o e-mail chegue sequer à sua caixa de correio. Em **Inserir aviso de spam no assunto e texto do e-mail**, você pode marcar e-mails identificados como Spam de forma chamativa, para poder organizá-los melhor, por exemplo. Se utilizar **Microsoft Outlook** (atenção: Não confundir com o Outlook Express ou o Windows Mail), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do G DATA Software, definindo a respectiva pasta em **Nome da pasta**.

> **Observação**: Mesmo se não utilizar o Outlook, você poderá mover os e-mails reconhecidos como spam para uma pasta. Para isso, insira uma advertência na linha de assunto (por ex., "*[Spam]*") e crie em seu programa de e-mail uma regra que mova os e-mails com o texto na linha de assunto para uma outra pasta.

Configurações avançadas

Nesta área é possível alterar de forma bastante detalhada o reconhecimento de spam do G DATA Software, e adaptar às condições de seu tráfego de e-mail. A nível geral, no entanto, recomenda-se aqui a utilização das configurações padrão. Apenas deverá proceder a alterações nas configurações avançadas caso esteja familiarizado com o assunto e se souber muito bem o que está a fazer.

Outros filtros

Os seguintes filtros estão configurados por predefinição, mas podem, em caso de necessidade, ser desactivados eliminando o visto.

- **Desativar scripts HTML**
- **Filtrar anexos perigosos**

Além disso, através do botão **Novo**, você pode criar novas regras de filtro ou, através do botão **Editar**, editar os filtros existentes. Os filtros criados são apresentados na lista e podem ser desactivados ou activados quando quiser, no campo de selecção à esquerda da entrada correspondente. O filtro correspondente é activado se colocar um visto no campo da marcação. O filtro correspondente é desactivado se retirar o visto no campo da marcação. Para excluir um filtro permanentemente, selecione-o com um clique do mouse e utilize em seguida o botão **Excluir**.

Nas opções de filtro disponíveis aqui, tratam-se de filtros adicionais que suportam o Filtro de spam do G DATA Software e simplificam as configurações individuais. Através do filtro real de spam, você tem amplas possibilidades de configuração para bloquear de forma eficaz os e-mails com conteúdo ou remetentes indesejados (por ex., remetentes de e-mail em massa). O programa verifica muitas características dos e-mails típicas para spam. Com base nas características em questão, é calculado um valor que reflecte a probabilidade de spams. Para esse efeito, tem à disposição várias fichas que lhe disponibilizam todas as opções de configuração relevantes numa estrutura temática.

Quando um novo filtro é criado, uma janela de opções é aberta, na qual é possível definir o tipo de filtro básico. Todas as indicações adicionais relativas ao filtro a criar poderão então ser introduzidas numa janela de assistente adaptada ao tipo de filtro. Desta forma poderá criar, de forma muito confortável, filtros contra todas as ameaças que se possa imaginar.

- **Desactivar scripts HTML**: Esse filtro desativa scripts na parte HTML de um e-mail. Os scripts, que numa página da Internet até fazem sentido, quando estão anexados a um e-mail HTML tornam-se bastante incómodos. Em alguns casos, os scripts HTML são utilizados ativamente para infectar computadores, onde os scripts têm a possibilidade de não se propagar apenas com a abertura de um anexo infectado, mas, por si só, podem ter efeito já na pré-visualização de um e-mail.

- **Filtrar anexos perigosos**: Ao filtrar anexos, você tem muitas possibilidades para filtrar anexos de e-mail (= Attachments) e outros. A maioria dos vírus de e-mail propagam-se através desses Anexos, que na maioria dos casos contêm ficheiros executáveis bem ou mal dissimulados. Pode tratar-se de um ficheiro exe clássico, que contém um programa malicioso, mas também de scripts VB, que em determinadas condições até podem estar dissimulados em ficheiros de gráficos, de vídeo ou de música aparentemente seguros. Em geral, todos os usuários devem ser extremamente cuidadosos na execução de anexos de e-mail e, em caso de dúvidas, é melhor consultar novamente o remetente do e-mail antes de executar um arquivo que não foi explicitamente solicitado.

  Em **Extensões de arquivos**, é possível listar as extensões de arquivos para as quais os respectivos filtros devem ser aplicados. Assim, é possível por exemplo, reunir todos os arquivos executáveis (como arquivos EXE e COM) em um filtro, mas também filtrar outros formatos (como MPEG, AVI, MP3, JPEG, JPG, GIF etc,), quando esses representarem uma sobrecarga para o servidor de e-mails devido ao seu tamanho. É claro, que é possível também filtrar arquivos compactados (como ZIP, RAR ou CAB). Separe todas as extensões de ficheiro pertencentes a um grupo de filtragem com ponto e vírgula.

  Através da função **Filtrar também os anexos em e-mails incorporados**, você faz com que a filtragem dos tipos de anexos selecionados em **Extensões de arquivo** seja feita também em e-mails que representem, por si só, um anexo de um e-mail. Esta opção deve permanecer normalmente activada.

  A opção **Mudar só o nome de anexos**, muda apenas o nome dos anexos a filtrar, em vez de os apagar automaticamente. Isso é bastante útil, por exemplo, em arquivos executáveis (como EXE e COM), mas também em arquivos do Microsoft Office que possivelmente possam conter scripts executáveis e macros. Ao renomear um anexo, ele não pode ser aberto inadvertidamente com um clique do mouse, mas tem que ser salvo e se necessário renomeado antes que possa ser utilizado. Se não tiver uma marca de verificação em **Mudar só o nome de anexos**, os anexos em causa serão eliminados directamente.

  Em **Sufixo**, você informa a sequência de caracteres desejada com a qual você deseja que a extensão do arquivo seja ampliada, evitando, assim, que um arquivo seja executável através de um simples clique (por ex., exe_danger). Em **Inserir aviso no texto do e-mail** pode informar o destinatário do e-mail filtrado que um anexo foi eliminado ou que o nome do mesmo foi alterado, devido a uma regra de filtro.

- **Filtro de conteúdos**: Por meio do filtro de conteúdos poderá bloquear de uma forma cómoda os e-mails que contenham determinados temas ou textos.

  Para isso, simplesmente insira em **Critério de pesquisa** as palavras-chave e as expressões às quais o G DATA Software deverá reagir. Nesse processo, é possível vincular o texto da forma desejada com operadores lógicos E e OU.

  Agora, digite em **Área de pesquisa** em que áreas de um e-mail os termos devem ser procurados. Como **Cabeçalho** é denominada a área de um e-mail que, entre outras coisas, contém o endereço de e-mail do remetente e do destinatário, a linha de assunto e as informações sobre os programas utilizados, protocolos e dados do remetente. Diferenciando, no **Assunto** apenas é verificado o

conteúdo da linha de assunto, sem informações de texto adicionais do cabeçalho. Em **Texto do e-mail** há, além disso, a opção se a área de pesquisa deve limitar-se apenas a simples e-mails com texto ou abranger também o texto em e-mails em HTML (Texto HTML).

Em **E-mails incorporados**, você pode definir se a procura do filtro de conteúdo deverá englobar também os que estejam presentes como anexo no e-mail recebido.
Em **Reação** é possível definir como deve ser o procedimento com e-mails reconhecidos pelo G DATA Software como Spam. Através de **Rejeitar e-mail** o e-mail correspondente nem é recebido pelo seu programa de e-mail.

Colocando a marcação em **Inserir aviso no assunto e texto do e-mail**, pode ser feita a inserção de uma advertência do texto real da linha de assunto (Prefixo na linha de assunto) por ex., *Spam* ou *Atenção*. Opcionalmente, também é possível inserir um texto que precederá o texto do próprio e-mail (Aviso no texto).

Se utilizar *Microsoft Outlook* (**atenção**: Não confundir com o Outlook Express ou o Outlook Mail), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do G DATA Software, definindo a respectiva pasta em **Nome da pasta**.

- **Filtro de remetente**: O filtro de remetente permite bloquear de forma cómoda os e-mails de determinados remetentes. Para isso, basta inserir em **Remetente/Domínios** os endereços de e-mail ou os nomes dos domínios aos quais o G DATA Software deverá reagir. Diversos registros podem ser separados através de ponto e vírgula.

  Em **Reação** é possível definir como deve ser o procedimento com e-mails reconhecidos pelo G DATA Software como Spam.

  Através de **Rejeitar e-mail** o e-mail correspondente nem é recebido pelo seu programa de e-mail.

  Colocando a marcação em **Inserir aviso no assunto e texto do e-mail**, pode ser feita a inserção de uma advertência do texto real da linha de assunto (Prefixo na linha de assunto) por ex., *Spam* ou *Atenção*. Opcionalmente, também é possível inserir um texto que precederá o texto do próprio e-mail (Aviso no texto).

  Se utilizar *Microsoft Outlook* (**atenção**: Não confundir com o Outlook Express ou o Windows Mail), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do G DATA Software, definindo a respectiva pasta em **Nome da pasta**.

- **Filtro de idioma**: Com o filtro de idioma pode definir e-mails de determinados idiomas automaticamente como spam. Se, por via de regra, você por exemplo, não tiver nenhum contato por e-mail com uma pessoa do idioma inglês, pode filtrar muitos spams através da definição do inglês como idioma de spam. Selecione o idioma do qual você supõe normalmente não receber nenhum e-mail e, assim, o G DATA Software aumenta significativamente a avaliação de spam para esses e-mails.

  Em **Reação** é possível definir como deve ser o procedimento com e-mails reconhecidos pelo G DATA Software como Spam.

  Através de **Rejeitar e-mail** o e-mail correspondente nem é recebido pelo seu programa de e-mail.

  Colocando a marcação em **Inserir aviso no assunto e texto do e-mail**, pode ser feita a inserção de uma advertência do texto real da linha de assunto (Prefixo na linha de assunto) por ex., *Spam* ou *Atenção*. Opcionalmente, também é possível inserir um texto que precederá o texto do próprio e-mail (Aviso no texto).

  Se utilizar *Microsoft Outlook* (**atenção**: Não confundir com o Outlook Express ou o Windows Mail), existe também a possibilidade de mover os e-mails com suspeita de spam para uma pasta livremente definível em sua caixa postal (**Mover e-mail para a pasta**). Essa pasta pode ser criada diretamente através do G DATA Software, definindo a respectiva pasta em **Nome da pasta**.

Outros

Nesta área terá a possibilidade de executar configurações adicionais.

- **Verificar e-mails não lidos na caixa a receber ao iniciar o programa**: *Só para Microsoft Outlook*: Esta opção serve para controlar os e-mails quanto a suspeita de spam. Assim que você abrir o Outlook, todos os e-mails não lidos na pasta da caixa de entrada e das subpastas integradas são verificados pelo G DATA Software.

- **Outros programas de e-mail (utilização de POP3)**: E-mails recebidos por POP3 não podem ser excluídos diretamente por razões técnicas. Se um filtro tiver de rejeitar e-mails, esse e-mail receberá um texto de substituição padrão. O texto de substituição no caso dos e-mails rejeitados é o seguinte: **A mensagem foi rejeitada**. No entanto, pode personalizar o texto destas funções de notificação. No texto livremente definível para o **Assunto** e **Texto do e-mail** estão disponíveis os seguintes espaços reservados (definidos por um sinal de percentual seguido por uma letra minúscula):

  %s Remetente

%u Assunto

Pode definir uma regra no seu programa de e-mail, que elimina automaticamente todos os e-mails com o texto de substituição aqui definido.

Firewall

Automático

Se você não tiver interesse em saber mais sobre o assunto Firewall, deveria deixar a configuração em automático. Além do modo piloto automático, que é para muitos usuários provavelmente a melhor escolha, você ainda tem muitas opções para configurar o Firewall G DATA de forma ideal conforme as suas necessidades e exigências.

Nas configurações de firewall existem duas grandes áreas que podem ser configuradas individualmente:

Piloto automático

Aqui você pode definir se o firewall age de forma independente e com autoaprendizagem e não faz perguntas ao usuário na decisão de bloqueio ou liberação de pedidos da internet, ou se o usuário será consultado em caso de dúvida.

- **Modo de piloto automático**: Aqui, o firewall funciona de forma totalmente autónoma, afastando automaticamente o perigo do computador doméstico. Essa configuração oferece uma proteção geral prática e é, na maioria dos casos, recomendável.
- **Criação manual de regras**: Se desejar configurar seu firewall individualmente, através da criação manual de regras você poderá ajustar a proteção de firewall totalmente às suas necessidades pessoais.
- **Oferecer modo de piloto automático quando é iniciado um aplicativo em ecrã inteiro**: Principalmente em jogos de computadores (e outros aplicativos de tela cheia), pode ser perturbador quando o firewall interrompe o fluxo do jogo com muitas consultas ou simplesmente perturba a exibição com janelas de consultas. Para garantir o prazer de jogar sem comprometer a segurança, o piloto automático é uma configuração útil, dado que suprime as caixas de perguntas do firewall. Se o piloto automático não for utilizado como configuração padrão, esta função pode cuidar para que ele seja sempre oferecido quando você usa um programa que é executado no modo de tela cheia.

Configurações de segurança definidas pelo usuário

Enquanto utiliza o computador para o seu trabalho diário, o firewall aprende, gradualmente, quais os programas que utiliza para aceder à Internet, quais os que não utiliza e quais os que representam um risco de segurança. A vantagem da utilização de níveis de segurança predefinidos é que, mesmo sem esforços administrativos e conhecimentos técnicos na área de segurança de rede, o firewall pode ser adaptado às necessidades individuais. Com o controlo de deslize, ajuste o nível de segurança que precisa. Estão disponíveis os seguintes níveis de segurança:

- **Segurança máxima**: As regras do firewall são criadas com directrizes muito rígidas. Para tal, deve estar familiarizado com a terminologia específica no domínio das redes (TCP, UDP, portas, etc.). O firewall detecta as mais pequenas inconsistências e irá colocar frequentemente perguntas durante a fase de aprendizagem.
- **Segurança alta**: As regras do firewall são criadas com directrizes muito rígidas. Para tal, deve estar familiarizado com a terminologia específica no domínio das redes (TCP, UDP, portas, etc.). É provável, que o firewall faça frequentemente perguntas durante a fase de aprendizagem.
- **Segurança normal**: As regras do firewall são criadas apenas ao nível da aplicação. O assistente não irá incomodá-lo com detalhes específicos da rede. Durante a fase de aprendizagem, receberá o menor número possível de perguntas.
- **Segurança baixa**: As regras do firewall são criadas apenas ao nível da aplicação. O assistente não irá incomodá-lo com detalhes específicos da rede e, durante a fase de aprendizagem, raramente receberá perguntas. A protecção máxima contra pedidos de ligação também está garantida neste nível de segurança.
- **Firewall desactivado**: Se necessário, também pode desligar o firewall. O seu computador continuará ligado à Internet e a outras redes, mas sem estar protegido de ataques ou ameaças de espionagem pelo firewall.

Se desejar configurar o Firewall de forma mais específica, coloque a marcação em **Configurações definidas pelo usuário**. Tenha em consideração que deve possuir algumas noções básicas de segurança de redes para efectuar estas configurações.

Perguntar

Aqui poderá estabelecer quando, como e se o firewall deverá consultar o utilizador quando os programas precisarem de estabelecer uma ligação à Internet ou à rede.

Criar regra

Quando o firewall detecta a aceitação de uma conexão com a rede, aparece uma caixa de informações onde você define como deve ser procedido com o respectivo aplicativo. Aqui poderá determinar o que é que o utilizador pretende em concreto, com a permissão ou proibição de um acesso à rede:

- **Por aplicativo**: Aqui, o acesso à rede para o aplicativo exibido no momento é permitido ou recusado em geral para todas as portas, e com todos os protocolos de transmissão (TCP ou UDP).
- **Por Protocolo/Porta/Aplicativo**: A aplicação que solicita o acesso à rede obtém a permissão para aceder à Internet apenas com o protocolo de transferência solicitado e exclusivamente com a porta solicitada. Caso o mesmo aplicativo solicite um acesso de rede a outra porta ou com outro protocolo, surge novamente a caixa de consulta, podendo ser criada outra regra para esta situação.
- **Por aplicativo, se no mín. x consultas estiverem na fila**: Existem aplicativos (como o Microsoft Outlook) que em uma solicitação de rede, consultam ao mesmo tempo diversas portas ou utilizam ao mesmo tempo diferentes registros. Como isso significaria, p.ex., diversas consultas na configuração por registro/porta/aplicativo, é possível definir aqui, que os aplicativos recebam uma liberação ou recusa generalizada para utilização da rede, assim que a conexão for permitida ou recusada pelo usuário.

Aplicativos de servidor desconhecidos

Aplicativos que ainda não são gerenciados através de uma regra no firewall, podem ser tratados de diferentes formas. A hora da consulta representa um factor decisivo neste caso. Quando o servidor de aplicativo entra Em recepção, isso significa que ele espera quase em standby uma solicitação de conexão. De outra forma a consulta é efectuada quando é feita a solicitação de ligação propriamente dita.

Verificação de redes desprotegidas

Naturalmente, um firewall só pode funcionar sem problemas quando todas as redes que o computador a ser protegido acessa, também possam ser reconhecidas e monitoradas. Por isso deve manter activa a verificação de redes desprotegidas.

Perguntas de aplicativo repetidas

Você pode vincular solicitações de conexão repetidas a um aplicativo. Deste modo, evita que seja constantemente apresentada uma caixa de consulta quando há tentativas de ligação que ainda não foram especificadas através de uma regra, mas antes, por exemplo, em intervalos de 20 segundos ou noutro período definido por si.

Verificação de referência

Na verificação de referência é apurada, para aplicativos aos quais o firewall já permitiu o acesso à rede, uma soma de testes com base no tamanho do arquivo e outros critérios. Se essa soma de verificação do programa divergir subitamente, pode acontecer que o programa tenha sido alterado por um programa malicioso. Neste caso, o firewall activa um alarme.

Verificação de referência para módulos carregados: Aqui são monitorados não apenas os aplicativos, mas também os módulos que são usados pelos aplicativos (por exemplo, DLLs). Como esses se modificam frequentemente ou novos módulos são carregados posteriormente, uma verificação consequente de referências modificadas e desconhecidas em módulos, pode levar a um esforço considerável de administração. Cada módulo alterado iria causar uma consulta de segurança por parte do firewall. Por isso, a verificação do módulo apenas deverá ser utilizada desta forma no caso da existência de grandes exigências no que respeita à segurança.

Outros

Aqui, estão disponíveis outras opções de configuração.

Pré-definição para o assistente de regras

Aqui poderá determinar se, a nível geral, pretende criar novas regras por meio do Assistente de regras ou no modo de edição avançado. Para os usuários que não têm conhecimento sobre o assunto segurança de rede, recomendamos o assistente de regras.

Verificações na inicialização do programa

Aqui você pode definir se o firewall deve procurar por aplicativos desconhecidos do servidor a cada inicialização do programa. Esta função

de procura deveria estar sempre ligada, a menos que esteja a trabalhar numa rede fechada.

Guardar registo de ligação

Aqui você pode definir quanto tempo o firewall deve manter os dados da conexão. Os dados podem ser mantidos de 1 a 60 horas e visualizados na área de registros.

Optimizador

Geral

Aqui poderá efectuar as seguintes configurações:

- **Eliminar dados de restauro**: Aqui você pode definir quando os dados de restauração (que o G DATA Software cria nas alterações) deverão ser excluídos.
- **Eliminar dados antigos**: Aqui você pode definir quando dados antigos (por ex., pastas temporárias antigas) deverão ser excluídos.
- **Eliminar atalhos do ambiente de trabalho**: Aqui você pode definir quando vinculações desnecessárias da área de trabalho (quando não tiverem sido utilizadas por um determinado número de dias) deverão ser excluídas.
- **Na actualização da Microsoft, procurar também por actualizações do Office**: Além disso, é possível definir se o otimizador deve procurar automaticamente na Internet atualizações do Office além das atuais Atualizações do Windows. Uma atualização de ambos os elementos economiza tempo e mantém você no estado mais atual do ponto de vista técnico de segurança. Naturalmente, a procura por atualizações do Office funciona apenas quando o Microsoft Office estiver instalado no respectivo computador.
- **Não criar arquivos de registro com informações detalhadas sobre os elementos excluídos**: O otimizador é estruturado de forma a registrar informações completas sobre as alterações executadas. Se você considerar um risco de segurança um arquivo de registro com as respectivas informações sobre o que o otimizador excluiu, é possível impedir a criação desse tipo de registro de exclusão.
- **Excluir permanentemente os arquivos temporários**: Com essa função, você fecha os arquivos da Web (por ex., cookies, arquivos temporários da Internet) da opção de restauração do otimizador, ou seja, você não poderá mais restaurar esses arquivos. Ao ativar essa função, você reduz substancialmente a quantidade de arquivos que o otimizador tem que administrar na área de restauração. Tudo isto se traduz num melhor desempenho.
- **Não permitir a reinicialização automática do computador através do serviço**: Com essa opção, você impede uma possível reinicialização do computador eventualmente executada pelo otimizador em um procedimento de otimização controlada por tempo. Uma vez que o Optimizador só iria reiniciar o computador sem pedir autorização se não houvesse nenhum utilizador registado, na maioria dos casos não é aconselhável activar esta opção.
- **Permitir restauração de pontos de restauração individuais**: Sem esta função, o G DATA Software não pode mais executar nenhuma restauração.
- **Na desfragmentação, não considerar o tipo de unidade**: Como a maioria dos fabricantes desaconselha a desfragmentação de seus SSD, a desfragmentação para este tipo de unidade no G DATA Otimizador é exceção por padrão. Contanto que as unidades do G DATA Software não possam ser digitadas automaticamente, mas você esteja certo de que nenhuma unidade SSD se encontre em seu computador, você pode deixar a marcação aqui. O otimizador inicia então, em cada execução, a desfragmentação de todos os discos rígidos que se encontram no sistema.

Configuração

Nesta área você pode selecionar todos os módulos que o otimizador deverá utilizar para um procedimento de otimização. Os módulos seleccionados são então iniciados ou por meio de uma acção automática controlada temporalmente (ver capítulo **Agendamento**) ou manualmente. Para activar um módulo faça simplesmente duplo clique com o rato sobre o mesmo. Pode optimizar, aqui, individualmente as principais áreas de optimização que se seguem:

- *Segurança*: Diversas funções que transferem automaticamente dados da Internet só têm aspectos que se justificam para o fornecedor e não para si. Muitas vezes, essas funções abrem a porta a software malicioso. Estes módulos permitem-lhe proteger o sistema e mantê-lo actualizado.
- *Desempenho*: Os ficheiros temporários, por exemplo, cópias de segurança que já não são necessárias, ficheiros de registo ou de instalação, que após a instalação apenas ocupam espaço no disco, tornam o seu disco rígido mais lento e apenas ocupam espaço valioso no disco. Além disso, os processos que já não são necessários e os atalhos para os ficheiros afectam bastante a velocidade do seu sistema. Com os módulos aqui apresentados poderá libertar o seu computador dessa carga desnecessária e acelerá-lo.

- *Protecção de dados*: A seguir são apresentados os módulos relacionados com a protecção dos seus dados. Aqui são eliminados os rastos deixados involuntariamente ao navegar na Internet e que ao utilizar o computador revelam muito sobre os seus hábitos de utilização ou até mesmo dados e palavras-passe importantes.

Protecção de pastas

Por meio dessa guia você pode retirar determinadas pastas (p.ex., também a sua partição do Windows) da exclusão automática de arquivos antigos.

Para tal clique simplesmente no ícone **Adicionar** e escolha então a pasta correspondente ou a unidade desejada.

Para liberar novamente um diretório de exceções, selecione-o na lista visualizada e, em seguida, clique no botão **Excluir**.

Protecção de ficheiros

Com a proteção de arquivos, é possível proteger determinados arquivos da exclusão pelo otimizador, p.ex., status de jogos para computador ou arquivos semelhantes com extensões de arquivo incomuns, que podem ser interpretados como arquivos de backup ou temporários.

Para proteger determinados ficheiros, clique no botão **Adicionar** e introduza o respectivo nome de ficheiro. Também poderá trabalhar com marcadores de posição.

A forma de funcionamento de espaços reservados é a seguinte:

- O ponto de interrogação (?) é substituto para caracteres individuais.
- O asterisco (*) é substituto para sequências de caracteres inteiras.

Para, por exemplo, proteger todos os arquivos com a extensão de arquivo ".sav", digite *.sav. Para proteger tipos diferentes de arquivos com um nome de arquivo de início igual, digite, por exemplo, texto*.*.

Selecione agora a pasta onde os arquivos deverão ser protegidos, clicando no botão Avançado. A seguir, seleccione o localização onde se encontram os ficheiros a proteger. O Optimizador protege agora os ficheiros definidos, apenas nesta pasta (por exemplo, pontuações de jogos apenas na respectiva pasta de jogos).

Para liberar novamente uma proteção de arquivos, selecione-o na lista visualizada e, em seguida, clique no botão **Excluir**.

Agendamento

Através do separador **Agendamento** pode determinar quando e a que ritmo deve ser efectuado o trabalho de optimização automático.

Em **Diariamente**, é possível definir com a ajuda das indicações em dias da semana que, p.ex., o seu computador só executará a otimização em dias úteis ou até mesmo a cada dois dias ou, nos fins de semana onde ele não é utilizado para trabalhar. Para alterar as entradas de dados e de tempo em **Período**, marque o elemento que pretende alterar (por exemplo, dia, hora, mês, ano) com o rato e utilize depois as teclas de seta ou os pequenos símbolos de seta à direita do campo de entrada, para se movimentar cronologicamente no respectivo elemento.

Quando não desejar que nenhuma otimização seja realizada, remova simplesmente a marcação da entrada **ligado** para o processo automático de otimização.

Controlo de dispositivos

Através do controle de dispositivo pode ser feita a definição para o seu computador de quais mídias de armazenamento são permitidos para leitura e/ou escrita de dados. Assim você pode, por ex., impedir que dados pessoais sejam movidos para um pen drive ou gravados em um CD. Além disso, pode ser feita a definição com qual mídia de dados removível os dados podem ser baixados em mídias de dados removíveis como pen drives ou discos rígidos USB externos. Assim você pode usar, por ex., o seu próprio disco rígido USB para o backup de dados, mas outros discos rígidos não têm acesso.

Para usar o controle de dispositivo, faça a marcação em **Ativar controle de dispositivo** e então selecione, para quais dispositivos deseja definir limitações:

- **Mídia de dados removível (por exemplo pen-drives)**

- **Unidades de CD/DVD**
- **Unidade de disquete**

Agora você tem a possibilidade de definir regras para mídias de armazenamento individuais.

Regras gerais

Aqui você pode definir se o respectivo dispositivo não pode ser utilizado (**Bloquear acesso**), se podem ser baixados apenas dados dele, sem que nele possam ser salvos dados (**Acesso de leitura**) ou se não há limitações para este dispositivo (**Acesso total**). Essa regra é válida para todos os usuários do seu computador.

Regra específica do usuário

Se você desejar que apenas determinados usuários tenham direitos restritos para as mídias de armazenamento, primeiramente selecione nesta área o nome de usuário do usuário em conjunto do seu computador e então faça a limitação de acesso para cada mídia de armazenamento, como descrito em **Regras gerais**. Desta forma, você como administrador e proprietário do computador pode permitir-se acesso total e aos outros usuários apenas direitos restritos.

Selecionar aqui o usuário. Se você clicar agora em OK é aberta outra caixa de diálogo na qual você pode definir, de que tipo de acesso é desejado para este usuário e se a permissão para este usuário está limitada a um tempo determinado (por ex., duas semanas) (**Validade**).

> **Observação**: A regra específica para o usuário substitui as regras gerais, ou seja, se for feita a determinação geral de que o acesso por pen drive não é permitido, mesmo assim, pode ser permitido a um determinado usuário o uso, através da regra específica de usuário. Se um usuário recebeu certas limitações de acesso ao controle de dispositivo, que são limitadas temporariamente, então, decorrido este tempo de limitação, tornam-se novamente válidas as regras gerais para este usuário.

Regra específica para dispositivos

Na utilização de Mídia de dados removível, como, por ex., pen drives ou discos rígidos externos, pode ser feita a definição de que apenas determinadas mídias de dados removíveis devem ter acesso ao seu computador. Para isso, faça a conexão da mídia de dados removível com o seu computador e clique no botão **Adicionar**. Na caixa de diálogo que é exibido, é possível fazer a seleção da mídia de dados removível desejada. Se agora você clicar em OK é aberto outra caixa de diálogo no qual você pode definir, de que tipo de acesso é desejado para este usuário e se a utilização da mídia de dados removível está limitada a um tempo determinado (por ex., duas semanas) (**Validade**) e se todos os usuários podem usar ou não essa mídia de dados removível em seu acesso de usuário.

Cópia de segurança

Nesta área podem ser feitas as configurações gerais para a funcionalidade do módulo de backup.

- **Directório para ficheiros temporários**: Aqui é feita a definição de onde os dados salvos temporariamente devem ser salvos pelo módulo de backup. Estes arquivos são gerados na criação e também na restauração de um backup, mas são excluídos automaticamente após cada procedimento. Mesmo assim, deveria ter espaço suficiente no disco rígido, caso contrário, a velocidade do backup e da restauração fica limitada. Esta configuração deveria ser alterada apenas quando o diretório selecionado para arquivos temporários não tem disponível espaço de salvamento suficiente.
- **Verificação unidade de origem/de destino no mesmo disco rígido**: Normalmente, o módulo de backup faz um alerta sempre que o usuário deseja fazer um backup na mesma mídia de dados, na qual os arquivos originais se encontram. Isso é feito em razão de que, em uma falha/perda da memória de dados, o backup automaticamente também não estaria mais disponível. Se por algum motivo, desejar fazer backups regularmente na memória de dados original, esse aviso de alerta pode ser desligado.

Registos

Para os módulos individuais estão disponíveis funções de registro, com a ajuda das quais é possível ter uma visualização de quais ações o G DATA Software está executando para sua proteção.

Registros de proteção de vírus

Na área de registos são apresentados os registos criados pelo software. Se clicar nos títulos das colunas **Hora de início**, **Tipo**, **Título** ou **Estado**, pode ordenar os registos existentes pela coluna seleccionada. Com os botões **Salvar como** e **Imprimir**, dados de registro podem ser salvos como arquivos de texto ou impressos diretamente. Para excluir um registro, selecione o registro na tabela com o mouse e clique na tecla Del ou pressione o botão **Excluir**.

Registros do Firewall

A área de registro cria um arquivo de registro abrangente para cada ação do firewall. Aqui poderá abrir acções singulares com um duplo clique, podendo se necessário imprimi-las ou guardá-las como ficheiro de texto. Leia também o capítulo **Configurações: Outros**.

Registros de backup

A área registro cria um arquivo abrangente de registro para cada ação e para cada tarefa de backup. Aqui poderá abrir acções singulares com um duplo clique, podendo se necessário imprimi-las ou guardá-las como ficheiro de texto. Leia também o capítulo **Salvar e restaurar**.

Registros de proteção de spam

A área de registro cria um arquivo de registro abrangente para cada ação. Aqui poderá abrir acções singulares com um duplo clique, podendo se necessário imprimi-las ou guardá-las como ficheiro de texto.

Registros de proteção infantil

Na área de registos tem acesso, como administrador, a uma vista geral de todas as tentativas de acesso a conteúdos bloqueados por parte dos outros utilizadores. Em cima ainda poderá escolher da lista o utilizador cujo relatório pretende que lhe seja apresentado. Para mais informações, leia também o capítulo **Configurações: Registo**.

> **Observação**: Naturalmente, estes registros também podem ser excluídos através do botão **Excluir registros**.

Registros de controle do dispositivo

A área de registro cria um arquivo de registro abrangente para cada ação do gerenciador do dispositivo. Leia também o seguinte capítulo: **Configurações: Controlo de dispositivos**.

FAQ: BootScan

Se o seu computador for novo de fábrica ou tiver sido protegido até agora por um software antivírus, será possível executar a instalação com as etapas a seguir.

No entanto, se tiver uma suspeita justificada de que o seu computador já está infectado por vírus, recomenda-se executar um BootScan antes da instalação do G DATA Software.

> **BootScan**: Quando você liga o seu computador, normalmente, o sistema operacional Windows é iniciado automaticamente. Este procedimento é chamado de boot. Há também a possibilidade de iniciar automaticamente outros sistemas operacionais e programas.
>
> Para verificar a existência de vírus no seu computador antes da inicialização do Windows, a G DATA disponibiliza adicionalmente à versão do Windows, uma versão especial com capacidade de boot.

Pré-requisitos

O BootScan o ajuda a combater vírus que se instalaram no seu computador antes da instalação do software de antivírus.

Para isso, existe uma versão especial do programa do Software que pode ser executada já antes da inicialização do Windows.

Inicialização por CD/DVD ROM: Caso o computador não faça a inicialização por CD/DVD ROM, execute primeiramente os seguintes passos:

1. Desligue o seu computador.

2. Reinicie o seu computador. Normalmente, você consegue acesso à configuração da BIOS do computador durante a inicialização (=boot), pressionando a tecla DEL (dependendo do sistema também F2 ou F10).

3. As formas de alterar as configurações no Setup do BIOS divergem de computador para computador.

   Para isso, consulte a documentação do seu computador.

   Em resumo, a sequência do boot deve ser **CD/DVD-ROM:, C,** ou seja, a unidade de CD/DVD-ROM será o **1st Boot Device** e a partição do disco rígido, com o seu sistema operacional Windows, será o **2nd Boot Device**.

4. Guarde as alterações e reinicie o seu computador. O seu computador estará agora pronto para um BootScan.

   Como interromper um BootScan? Se, após uma reinicialização, o seu computador não mostrar o habitual ambiente do Windows, mas uma interface especial do software G DATA BootScan, isso não deverá ser motivo para preocupações.

   Se não tiver planejado nenhum BootScan, basta selecionar com as teclas de seta o registro **Microsoft Windows** e clicar em **Voltar**. Agora o seu Windows iniciará normalmente sem efectuar primeiro um BootScan.

   Inicialização por pen drive: Se a mídia de boot usada for um pen drive, esta também pode ser selecionada como 1st Boot Device.

FAQ: Funções do programa

Ícone Security

O seu G DATA Software protege o seu computador permanentemente contra vírus e softwares maliciosos. Para poder ver que a protecção está activa, é apresentado um ícone na barra de tarefas, no canto inferior direito, ao lado do relógio.

 Este ícone G DATA indica que está tudo em ordem e que a proteção do seu computador está ativa.

 Caso a sentinela tenha sido desativada ou outros problemas existam, o ícone G DATA exibirá um alerta. Neste caso, você deverá iniciar o G DATA Software o mais rápido possível e verificar as configurações.

Se clicar no símbolo com o botão direito do rato, surge um menu de contexto onde poderá controlar aspectos de segurança básicos do software.

Estão disponíveis as seguintes funções:

- **Iniciar o software G DATA**: Com essa opção, ativa-se a SecurityCenter e, com ela, é possível efetuar as configurações para a sentinela de vírus. Para saber o que poderá fazer no SecurityCenter, leia o capítulo: **SecurityCenter**.
- **Desactivar sentinela**: Esta função permite desactivar e activar novamente a sentinela de vírus, sempre que for necessário. Isto pode ser útil se copiar, por exemplo, no seu disco rígido grandes volumes de dados de uma localização para outra ou executar processos que calcula que ocupem um grande espaço de memória (por exemplo, copiar DVDs). Desligue a sentinela de vírus apenas o tempo que for necessário e certifique-se de que o sistema não se liga à Internet ou acede a dados novos não verificados (por exemplo, através de CDs, DVDs, cartões de memória ou pens USB) durante esse período.
- **Desactivar firewall**: Se você usar uma versão do G DATA Software com firewall integrado, também é possível desativar o firewall através do menu de contexto, caso necessário. O seu computador continuará ligado à Internet e a outras redes, mas sem estar protegido de ataques ou ameaças de espionagem pelo firewall.
- **Desactivar piloto automático**: O piloto automático é uma parte do Firewall e decide de forma independente que solicitações e contatos o seu computador deve aceitar ou não através da rede ou da Internet. O piloto automático é ideal para uma utilização normal e deve deixá-lo sempre activado. Como o firewall, o piloto automático está disponível nas versões selecionadas do G DATA Software.
- **Actualizar assinaturas de vírus**: Um software antivírus deve estar sempre actualizado. A actualização dos dados pode ser feita naturalmente de forma automática pelo software. No entanto, se você precisar urgentemente de uma atualização, poderá iniciá-la através do botão **Atualizar assinaturas de vírus**. Para saber a utilidade de uma atualização de vírus, leia o capítulo: **Verificação de vírus**.
- **Estatística**: Aqui, é possível solicitar a exibição de uma estatística sobre os processos de verificação da sentinela de vírus, mas também obter informações sobre verificações em modo ocioso, mensagens do filtro da web e outros parâmetros.

Fazer a verificação de vírus

Através da verificação de vírus pode analisar o seu computador quanto à presença de software malicioso. Quando iniciar a verificação de vírus, esta analisa todos os ficheiros existentes no seu computador, verificando se podem infectar outros ficheiros ou se eles próprios já estão infectados.

Se vírus ou outros softwares maliciosos forem encontrados em uma verificação de vírus, existem diversas possibilidades de como o vírus pode ser removido ou tornado inofensivo.

1 Inicie a verificação de vírus. Para saber como, leia o capítulo: **Proteção antivírus**.

2 O seu computador será então sujeito a uma verificação de vírus. Para tal, abra-se uma janela com informações sobre o estado da verificação.

Uma barra de progresso na parte superior da janela, indica o progresso da verificação no seu sistema. Já durante a verificação antivírus pode optar por várias possibilidades para influenciar o processo da verificação de vírus:

- **Interromper a verificação de vírus no caso de sobrecarga do sistema**: Através deste campo de selecção pode configurar o software para aguardar com a verificação de vírus até o utilizador ter concluído outras actividades no computador.

- **Desligar computador após a verificação de vírus**: Se quiser deixar decorrer a verificação de vírus durante a noite ou depois do trabalho, esta função torna-se muito prática. Assim que a verificação de vírus do G DATA Software for finalizada, o seu computador será desligado.

- **Arquivos protegidos por palavra-passe**: Enquanto uma pasta compactada for protegida por senha, o G DATA Software não pode verificar os arquivos dentro dessa pasta. Se colocar aqui o visto, o software antivírus informa quais os arquivos protegidos por palavra-passe que não pôde verificar. Enquanto estes arquivos não forem descompactados, os vírus que possam conter não representam qualquer risco de segurança para o seu sistema.

- **Acesso negado**: Em geral, no Windows existem ficheiros que são utilizados exclusivamente por aplicativos e que, por isso, não podem ser verificados enquanto estes aplicativos estão a ser executados. Por isso, o melhor será não executar nenhum outro programa no sistema durante uma verificação de vírus. Se colocar aqui um marca de verificação, serão apresentados os dados não verificados.

3a Se o seu sistema estiver livre de vírus, após a verificação pode fechar a janela do assistente através do botão **Fechar**. O seu sistema foi verificado e está livre de vírus.

3b Caso tenham sido encontrados vírus e outros programas maliciosos, tem a possibilidade de decidir como proceder com a detecção de vírus. Por norma, só precisa de clicar no botão **Executar acções**.

O G DATA Software agora usa as configurações padrão (desde que as configurações em **Configurações: Verificação manual de vírus** para arquivos infectados e arquivos com não tenham sido configuradas de forma diferente) e desinfeta arquivos infectados, ou seja, faz a reparação, para que estes possam ser usados novamente sem limitações e não sejam mais perigosos para o seu computador.

Se uma desinfecção não for possível, o arquivo será colocado em quarentena, ou seja, ele será codificado e movido para uma pasta extremamente segura, onde não poderá mais causar danos.

Se necessitar do ficheiro infectado, pode, em casos excepcionais, retirar o ficheiro da quarentena e utilizá-lo.

O seu sistema foi verificado quanto à presença de vírus e está livre de vírus.

3c Se reconhecer os ficheiros/objectos infectados e souber distinguir quais deles já não são necessários, terá a possibilidade de reagir de forma individual a cada um dos vírus detectados.

Na listagem das detecções de vírus, na coluna Ação é possível definir, para cada arquivo infectado, o que deverá ocorrer com o mesmo.

- **Só registar**: Na vista **Registos** a infecção é listada. No entanto, não é feita a reparação ou exclusão do arquivo afetado. **Atenção**: Quando apenas é registado, o vírus continua activo e constitui uma ameaça.

- **Desinfectar (se não for possível: só registar)**: Neste caso, o software tenta remover o vírus de um ficheiro infectado, mas caso tal não seja possível sem danificar o ficheiro, o ficheiro é registado e poderá solucionar o problema mais tarde, através da entrada de registo. Atenção: Quando apenas é registado, o vírus continua activo e constitui uma ameaça.

- **Desinfectar (se não for possível: em quarentena)**: Esta é a configuração padrão. Neste caso, o software tenta remover o vírus de um ficheiro infectado, mas caso não seja possível sem danificar o ficheiro, o ficheiro é enviado para a **quarentena**. Para mais informações leia também o capítulo: **Ficheiros em quarentena**.

- **Desinfectar (se não for possível: eliminar ficheiro)**: Aqui tenta-se remover o vírus; caso tal não seja possível, o ficheiro é então eliminado. Só deve utilizar esta função, se não houver dados importantes no seu computador. No pior dos casos, a eliminação consequente de ficheiros infectados pode levar a que o Windows deixe de funcionar e seja necessária uma reinstalação.

- **Enviar ficheiro para a quarentena**: Os ficheiros infectados são enviados directamente para a quarentena. Na quarantena os ficheiros são guardados de forma qualificada. Por isso, o vírus não pode causar danos e o ficheiro infectado continua disponível para eventuais tentativas de reparação. Para mais informações leia também o capítulo: **Ficheiros em quarentena**.

- **Eliminar ficheiro**: Só deve utilizar esta função, se não houver dados importantes no seu computador. No pior dos casos, a eliminação consequente de ficheiros infectados pode levar a que o Windows deixe de funcionar e seja necessária uma reinstalação.

Se clicar agora no botão **Executar ações** o G DATA Software procederá com cada detecção de vírus da forma como foi definido.

O seu sistema foi verificado quanto à presença de vírus. No entanto, se tiver usado uma configuração com a opção **Registrar**, pode ser que o seu computador não esteja livre de vírus.

Alarme de vírus

Quando o G DATA Software encontra um vírus ou outro programa malicioso em seu computador, é exibida uma janela de aviso na margem da tela.

Agora você tem as seguintes possibilidades para lidar com o arquivo infectado.

- **Só registar**: Na vista Registos é apresentada a infecção, sem que os ficheiros afectados sejam reparados ou eliminados. No entanto, através do registo pode verificar individualmente os vírus detectados e eliminá-los de forma orientada. Atenção: Quando apenas é registado, o vírus continua activo e constitui uma ameaça.
- **Desinfectar (se não for possível: enviar para a quarentena)**: Neste caso, o software tenta remover o vírus de um ficheiro infectado, mas caso não seja possível sem danificar o ficheiro, o ficheiro é enviado para aquarentena. Para mais informações leia também o capítulo: Como funciona a quarentena?
- **Enviar ficheiro para a quarentena**: Os ficheiros infectados são enviados directamente para a quarentena. Na quarantena os ficheiros são guardados de forma qualificada. Por isso, o vírus não pode causar danos e o ficheiro infectado continua disponível para eventuais tentativas de reparação. Para mais informações leia também o capítulo: **Ficheiros em quarentena**.
- **Eliminar ficheiro infectado**: Só deve utilizar esta função, se não houver dados importantes no seu computador. No pior dos casos, a eliminação consequente de ficheiros infectados pode levar a que o Windows deixe de funcionar e seja necessária uma reinstalação.

> **Quarentena e caixas de correio electrónico**: Existem ficheiros que não devem ser enviados para a quarentena, por exemplo, ficheiros de arquivo de caixas de correio electrónico. Se uma caixa de correio electrónica for enviada para a quarentena, o programa de e-mail deixará de lhe poder aceder e possivelmente deixará de funcionar. Você deve ter cuidado especialmente com os ***arquivos com a extensão PST***, pois estes, em geral, contém os dados de sua caixa postal de e-mail do Outlook.

Alarme do firewall

Em geral, o Firewall no modo de criação manual de regras pergunta se o acesso de programas e processos desconhecidos que querem se conectar à rede deve ser permitido ou recusado. Para o efeito, abre-se uma caixa de informações que lhe fornece detalhes sobre a aplicação em questão. Tem ainda a possibilidade de permitir ou recusar o acesso à rede da aplicação, apenas desta vez ou de forma permanente. Assim que autorizar ou negar o acesso a um programa de forma permanente, esta regra passa a incluir o conjunto de regras definidas para a rede em questão e deixa de ser questionado, se deseja autorizar ou não.

Estão disponíveis os seguintes botões:

- **Permitir sempre**: Com este botão, você cria uma regra para o aplicativo mencionado acima (por ex. Opera.exe ou Explorer.exe ou iTunes.exe) que permite um acesso permanente à rede ou à internet na rede do referido aplicativo. Esta regra pode depois ser consultada como regra criada sob consulta na área Conjuntos de regras.
- **Permitir temporariamente**: Através deste botão permite que a aplicação em questão aceda uma única vez à rede. Da próxima vez que este programa tentar aceder à rede, o firewall volta a perguntar se permite ou não.
- **Recusar sempre**: Com este botão, você cria uma regra para o aplicativo mencionado acima (por ex. dialer.exe ou spam.exe ou trojan.exe) que nega um acesso permanente à rede ou à internet na rede do referido aplicativo. Esta regra pode depois ser consultada como regra criada sob consulta na área Conjuntos de regras.
- **Proibir temporariamente**: Através deste botão proíbe que a aplicação em questão aceda uma única vez à rede. Da próxima vez que este programa tentar aceder à rede, o firewall volta a perguntar se permite ou não.

Outras informações sobre registro, porta e endereço IP podem ser obtidas no próprio aplicativo com o qual você deseja interagir.

Mensagem "not-a-virus"

Arquivos informados como "not-a-virus", são aplicativos potencialmente perigosos. Estes programas não dispõem directamente de funções maliciosas, mas em determinadas circunstâncias podem ser utilizados contra si por hackers. Desta categoria fazem parte, por exemplo, utilitários para a administração remota, programas para alternar automaticamente o esquema do teclado, clientes IRC, servidores de FTP ou vários utilitários para criar ou ocultar processos.

Desinstalação

Quando desejar remover em algum momento o G DATA Software do seu computador, realizar a desinstalação pelo painel de controle do seu sistema operacional. A desinstalação decorre então de forma totalmente automática.

Se durante a desinstalação ainda existirem arquivos na área de quarentena do G DATA Software, é feita uma consulta para saber se os arquivos devem ser excluídos ou não. Se não excluir os arquivos, eles permanecerão em uma pasta especial da G DATA codificada no seu computador e, dessa forma, não poderão causar danos. Esses arquivos estarão novamente disponíveis quando o G DATA Software for reinstalado no seu computador.

Durante a desinstalação será perguntado se você deseja excluir as configurações e registros. Se não eliminar esses ficheiros, os registos e as configurações voltarão a estar disponíveis ao reinstalar o software.

Conclua a desinstalação clicando no botão **Concluir**. O software está agora, completamente, desinstalado do sistema.

FAQ: Questões sobre licenciamento

Licenças multiusuários

Com uma licença multiusuário, o G DATA Software pode ser utilizado na quantidade de computadores licenciados. Após a instalação no primeiro computador e a actualização da Internet, receberá os dados de acesso online. Quando o software for instalado no próximo computador, insira o nome de usuário e a senha, obtidos no registro no servidor de atualizações G DATA. Repita esse processo em todos os computadores.

Utilize em todos os PCs os seus dados de acesso (nome de usuário e senha) para a atualização na Internet, os quais foram fornecidos após o seu primeiro registro. Para tal deverá proceder desta forma:

1. Inicie o G DATA Software.
2. No **SecurityCenter** clique em **Atualizar assinaturas de vírus**.
3. Na janela que se abre, insira os dados de acesso que recebeu previamente por e-mail. Se clicar em **OK** será validada a licença para o seu computador.

Extensão da licença

Uns dias antes de a sua licença expirar, é apresentada uma janela de informação na barra de tarefas. Se clicar na janela, abre-se uma caixa de diálogo onde poderá prolongar directamente a sua licença em poucos passos e de forma simples. Clique simplesmente no botão **Comprar agora**, insira os seus dados e a sua protecção antivírus volta de imediato a estar garantida. Você receberá a fatura confortavelmente nos próximos dias via e-mail no formato PDF.

> **Observação**: Esta caixa de diálogo aparece apenas ao término do primeiro ano. Depois disso, sua licença G DATA se renova automaticamente a cada ano. Mas você pode cancelar este serviço de renovação a qualquer hora e sem mencionar as razões.

Mudança de computador

Você pode utilizar o seu produto da G DATA em um novo ou em outro computador com os seus dados de acesso existentes. Simplesmente instale o software e introduza os seus dados de acesso. Nesse caso, o servidor de actualizações estabelece uma ligação como o novo computador. Caso o G DATA Software ainda se encontre no antigo computador, é preciso transferir a licença deste para o novo computador.

> **Observação**: A quantidade de transferências de licença é limitada - ao atingir o valor limite, a licença será totalmente bloqueada, de modo a que já não seja mais possível descarregar actualizações.

Copyright