About AVGuard

This dialog box displays some information about the AVGuard Service, the device driver and the control program.

Version Information

The first line displays the version and the creation date of the AVGuard/XP control program. The current version of the AntiVir engine is displayed in the second line. The third line contains the version, the creation date and the FUP type of the currently used virus definition file.

License Information

This section contains the user name and the serial number of this license. Additionally, the current contents of your license key file are displayed: From version / Date upto version/date using a specific FUP type. Note that the license is defined as "Whichever is greater". This means e.g. an outdated VDF-file will run properly if the version and FUP type are correct.

Hotline / Product Information

This section contains the information how to contact us if you need technical support or any other information or assistance.

Action Tab

This sheet configures how AVGuard/XP shall react when a virus has been detected.

Action if file not repaired

The following is a little bit tricky :-) When AVGuard/XP discovers a virus, first it depends on the setting "Display Notification Message" that will be done. If activated, AVGuard/XP will display a dialog box to let the user select the action to be taken. If the file could be disinfected and the auto-repair mode is enabled, the user can select to repair the file. If this disinfection fails, the action selected in this group box will be taken. If the user selects another option in the displayed dialog box, the selected action will be taken. If the notification messages are disabled, AVGuard/XP will react automatically on any virus infection. First it will check if the auto-repair mode has been enabled. If it is enabled and the file can be disinfected, AVGuard/XP will try to repair it. If this fails, the marked option in this group box will be executed. If the auto-repair mode is disabled, the previously selected action will be immediately taken.

Delete infected file

The infected file will be deleted but can be restored using appropriate tools.

Wipe infected file

The infected file will be overwritten and deleted and cannot be restored anymore.

Move infected file

The infected file will be moved to the Quarantine directory entered in the appropriate field. Note that only the Administrator should have access rights to this directory!

Rename infected file

The infected file will be renamed to *.001, *.002, ... It can no longer be accessed using the shell.

Do nothing

The infection will oly be reported to the logfile if enabled.

Notifications

Display notification message

Only if this option is enabled, AVGuard/XP will notify the user that an infection has been detected. A dialog window will be displayed where the user is asked to select what to do with the infected file.

Use event log

If enabled, any infection will be reported to the event log. The administrator now can check your workstation if there have been any viruses detected.

Play a sound

If selected, AVGuard/XP will play a short jingle when an infected file has been found. This is the default AntiVir jingle.

Quarantine directory

If a file is to be moved to the Quarantine Directory, AVGuard/XP will move it to the directory specified in this field.

Clear Statistics

This options resets the internal statistics of the AVGuard for Windows Service. All counters will be set to zero, the text fields will be set to a blank line. The button  or the key F6 has the same effect.

Close Control Program

To completely exit and close the Control Program you have to click this item. The program will be completely closed. A restart is only possible using the icon in the AntiVir/XP program folder.

Configuration

This menu displays a property sheet to configure the AVGuard for Windows Service. The button  has the same effect.
The property sheet contains the following tabs:

Scanner	All settings used by the device and the scanner itself.
Action	Actions to take when a virus has been found.
Repair	Disinfection settings.
Heuristic	Settings for the macro virus heuristic and template handling.
Report	Logfile settings
Password	Enables you to enter a password to protect the options dialog.
Network Warnings	Contains the settings for the network warnings.

Help Contents

These help pages are currently available in AVGuard for Windows XP/2000/NT:

Demo Version

Demo-Version

If you don't have a valid license key file, AVGuard/XP will run in the restricted demo mode. This means that it will only scan files on the volume C: of your computer.

To install a full version you just need a valid license key file which has to be copied into the installation directory of AntiVir/XP. After a restart of the AntiVirService, the system will run as a full version.

Device Mode

This displays the current device mode:

Disabled

AVGuard is disabled and deactivated. It will no longer protect your computer from viruses.

Scan on file reads

AVGuard/XP is activated and will scan any file to be read before it can be accessed. (Default)

Scan on file writes

AVGuard/XP is activated and will scan files that are modified or created on the desired volume.

File open and close

AVGuard/XP is activated will scan any file to be read and files that are modified or created. Please note that this could harm the performance of your computer system.

Edit File Extension

You can enter a new file extension in this dialog box. The maximum length of a new extension is 6 characters.

{button OK,}

The current extension will be inserted into the list of file extensions.

{button Cancel,}

The current extension will be thrown away an not inserted into the file extension list.

{button Help,}

Displays this help screen.

File Action

In this field the current action taken when a virus has been found will be displayed. Note that these actions are only taken if the option Display Notification Message has been disabled or if the file cannot be repaired.

Repair file

AVGuard/XP will try to repair the infected file. If a disinfection is not possible, the action set with 'Action if file not repaired' will be taken.

Delete file

The infected file will be deleted. It can be restored using some special tools. The signature of this virus can be found on your volume in the future.

Wipe file

The infected file will be overwritten with a default pattern and deleted afterwards. It can't be restored anymore.

Move file

The infected file will be moved to the quarantine directory set in the filed 'Quarantine Directory'. If a file with the same name already exists, the file to move will be renamed to *.001, *.002, etc. The files in this directory can be disinfected later on or you can send us such files for further investigations if needed.

Rename file

The infected fie will be renamed to *.001, *002, etc. Any direct shell shortcut to the file will be disabled. You can re-rename and disinfect the file later on.

Notify only

AVGuard/XP will only notify you that the file could be repaired. If enabled, only an entry will be written to the logfile.

File Extensions

The file extensions used by AVGuard/XP when 'Program Files Only' is enabled are stored in this list.

You can edit the list as follows:

{button OK,}

This closes and saves the current list

{button Cancel,}

The changes made are cancelled.

{button Insert,JI(`',`HELP_EDIT_EXTENSION')}

Opens a window to edit and insert a new file extension.

{button Delete,}

This deletes the currently marked item in the list.

{button Default,}

This sets the list to the default file extensions as shipped by H+BEDV.

{button Help,}

Displays this help screen

File Menu

This menu contains two sub menus. Both entries are used to exit the Control Program

Minimize Control Program or Alt-F4 or button 

Click this Item if you would like to exit the Control Program but don´t want to close it.

Close Control Program

To completely exit and close the Control Program you have to click this item. Please note that this will **not** stop the AVGuard service so that AVGuard will search for viruses anyway.

Files To Scan

AntiVir Guard can use a filter to select the file types to be scanned:

All Files

All files accessed will be scanned. No filter is enabled.

Use extension list

Only the files with a file extension as defined in the extension list will be scanned. This is the default setting. The default list could change from version to version since new types of viruses are found.

Help Menu

Here you can find some more information to operate you AVGuard.

Help (F1) or button 

This will show you this help system.

Using Context Sensitive Help

This shows you how to use the context sensitive help system

Help Index

This displays links to all available pages in this help file

About AVGuard/XP

Displays some information about AVGuard/XP, the running service and the used engine / virus definition file.

Heuristic Tab

This contains the settings for the heuristic macro virus scanner and how to deal with suspicious macros and Word 6/7 templates.

Suspicious macros

AVGuard includes a heuristic macro virus scanner which is able to detect even unknown macro viruses. This is done by analyzing the macros and investigating them for virus typical actions. Such macros are reported as suspicious. Suspicious macros can be deleted - which is the easiest method to destroy the virus or be reported only. Since a document can include more than one macro, the question is what to do with the other possibly good and useful macros. Note that this only takes effekt, if the auto-repair mode has been enabled and the user selected to repair the file.

Delete suspicious macros only

Only macros reported as suspicious will be deleted. This ensures that no possibly useful macro will be deleted by fault. The disadvantage is, that other macros belonging to the virus could possibly survive.

Delete all if one is suspicious

If selected, all macros in this document will be deleted. The disadvantage is that possible useful good macros will be deleted too.

Report suspicious macros only

Not a very good option. This could cause your application to be infected if the document really contains a macro virus. To make sure that there is no virus, you should send us the document for further investigations. We will send you the result of our investigatons as fast as possible.

Templates

Word 6/7 templates consist of normal text like documents, additionally they may contain data. When Word 6/7 opens such a template, it will look for this data. To infect a document, a virus first has to convert it into the template format. AVGuard/XP is now able to convert such templates back into the document format if no additional data is present. All macros must have been deleted, no menus or shortcuts are allowed.

Never convert templates

Templates will never be converted back into the document format.

Convert .DOC-files only

In most cases, templates have a file extension like *.DOT, *.WIT. Pure documents normally have the extension .DOC. Activate this option if AVGuard/XP shall convert all repaired .DOC files back into the document format.

Convert templates always

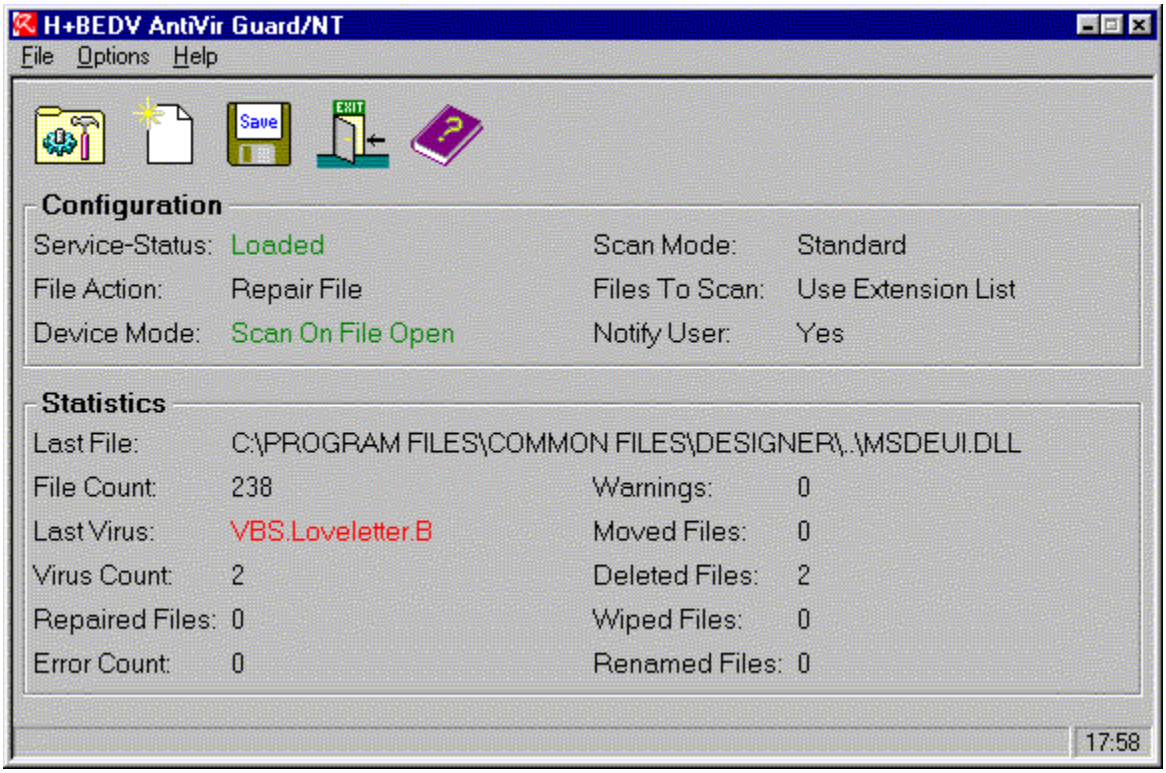
If selected, AVGuard/XP will try to convert all repaired Word 6/7 files back into the document format.

Compress template data table

If selected, AVGuard will delete even references to deleted macros and their names from the template. If a macro has been deleted, it´s name will be still present in the file. The macro itself has been overwritten and marked deleted. Since some antivirus programs only look for those names they could report a virus in a file which is definatly clean.

Main Screen

This is the Main Screen of AntiVir Guard for Windows XP (2000 + NT):



Menu Options

File
Options
Help

Configuration

Service-Status:	This displays the current status of the AVGuard service. (Loaded or not loaded)
File Action:	This field displays the action taken if an infected file has been found and the user notification has been disabled.
Device Mode:	Displays when files are to be scanned.
Scan Mode:	The current scanner mode.
Files To Scan:	All files or only files with a specific file extension.
Notify User:	Notify the user when an infection occurs or take the action automatically.

Statistics

In these fields that current statistics of the Guard will be displayed. Note that - from performance reasons - these fields will be updated only twice a second. These statistics can be reset using the option 'Clear statistics data'.

Last File: This field displays the last file scanned by the guard.
File Count: The number of files scanned.
Last Virus: The name of the last virus found.
Virus Count: The number of viruses found.
Repaired Files: The number of successfully disinfected files.
Error Count The number of errors occurred.
Warnings The number of warnings occurred.
Moved Files: The number of files successfully moved to the quarantine directory.
Deleted Files: The number of successfully deleted files.
Wiped Files: The number of successfully wiped files.
Renamed Files: The number of files that have been successfully renamed.

Minimise Control Program

or use the button 

Click this item if you would like to exit the Control Program but don´t want to close it. It will be minimized and you can see it´s icon placed in the system tray. A double click on the small icon in the system tray will enlarge it for further use. When minimized, the AVGuard Control Program does not connsume any CPU cycles.

News

New Features And News About AVGuard/XP

Password protection for configuration

AVGuard now provides a password protection for the options dialog. This enables the administrator to protect the options dialog against illegal modification.

Did You Know ...

... that AntiVir MailGate is now available for Linux, FreeBSD and OpenBSD? It provides powerful virus scanning and content filtering features combined with maximum performance.
... that servers running Lotus Domino can be protected using AntiVir SAVAPI combined with Group GT WatchDog?
... the new AntiVir search engine can detect nearly 60.000 viruses and virus strains?
... AntiVir is also available for Windows NT/2000 servers?
... that computers using AntiVir have been protected against VBS.LoveLetter (ILOVEYOU) already 2 hours after detection?
... AntiVir is now available for Linux, FreeBSD and OpenBSD and it is free for private, non-commercial use? All you need to do is to register. More information can be found in the Internet at www.hbedv.com.
... that the AntiVir Personal Edition for Windows 9x/Me and NT/2000/XP is free of charge for private, non-commercial use? The Personal Edition may be downloaded from http://www.free-av.com.
... that a graphical user interface (GUI) called TkAntiVir now is available for AntiVir for Linux? The product is subject to the GNU General Public Licence (GPL) and can be downloaded free of charge from the author's homepage at http://www.geiges.de/tkantivir/index_en.htm.
... that the Secure AntiVirus Application Programming Interface (SAVAPI) from H+BEDV provides an antivirus function library to build your own antivirus software. Common host applications are email gateway, firewalls and some client-server applications.
... that H+BEDV has developed the first resident antivirus guard for linux in the world.

You'll find the latest AntiVir news at http://www.hbedv.com or in german language at http://www.antivir.de

Notify User

The AVGuard/XP can be configured to react automatically when an infection occurrs or to ask the user for the action to be taken.

If the user has to be notified, a dialog box will be displayed when an infected file is detected. The user is asked to select whether to repair the file (if possible) or delete, move or rename the infected file. If this option is disabled, the action taken is the one selected in the field 'File Action'.

Options Menu

This menu contains three entries:

Configuration or button 

Select this to configure the AVGuard for Windows

Clear Statistics or button 

To Clear the statistics screen you have to select this item.

Save Configuration or button 

The AVGuard for Windows Service will save it´s configuration when selected.

Clear Access Cache

AVGuard has a feature to increase system performance that avoids scanning the same files every time they are accessed again. This feature is called "access cache" or filename cache. If you select this option, this access cache will be cleared so that all files are marked to be scanned again.

Password Tab

This sheet includes the passwodt protection option for the configuration property sheet.

Password

Please enter password

Please enter the password to be used if the configuration dialog is to be displayed. The password will not be visible in clear text, only asterisks will be displayed. A maximum of 39 characters is allowed. If the password has been entered once, the Guard/XP will ask every time for the password when the options dialog is to be displayed. A blank line means no 'password'.

Please re-enter password

Please re-enter the password for confirmation. This ensures that you do not lockout yourself by a spelling mistake. The password will not be visible in clear text, only asterisks will be displayed. A maximum of 39 characters is allowed.

Extra password protection for

Start of AntiVir main application

If you enable this option, AVGuard asks for the password each time the user would like to start the AntiVir main application from the AVGuard Control Program. Without this password, the user will not be able to start the program.

Maximize of AVGuard Control Program

If you enable this option, you'll be asked for a password if you would like to maximize the AVGuard Control Program by Double-Clicking the small red icon in the system tray. Without this password, you'll will not be able to maximize the application.

Repair Tab

This sheet includes the repair properties.

Infected Files

Repair automatically

If selected, AVGuard/XP will try to repair infected files automatically. This option is required to be able to repair files. NOTE: This option has to be activated too, if you would like to have the repair option enabled that is shown in the virus found dialog box displayed when an infected file has been detected.

Backup

Create backup

If this is enabled, AVGuard/XP will copy the infected file (create a backup) to the directory specified in the field below. This can be useful for documentation reasons and - if the heuristic macro virus scanner has detected and removed a suspicious macro inside a document - to save the infected original to be able to send it to us. We will then include a scan string for this virus into the product to be able to remove the virus after the next software update.

Backup directory

This is the directory where to create the backups.

Logfile Tab

AVGuard/XP has a very powerful log function included. It is able to give the administrator a complete report of what´s going on with your machine. You can choose what AVGuard/XP shall include into the logfile.

Name of logfile

This is the name and the path of the logfile to write. Each entry will be added to this file.

Logging level

This goup defines what to include into to logfile.

Disable reporting

Reporting will be disabled completely. This option is only useful for tests with lots of viruses when a maximum performance is required.

Standard information

All important information like infections, warnings, errors etc. will be included in the logfile. Minor important things will be ignored to give you a fast and easy overview onto the current status.

Extended information

Even minor important things like additional infos will be included in the logfile.

Complete information

File size, types and dates as well as the rest of all possible information will be included.

Limit logfile to

Limit size to n kilobytes

AVGuard/XP can limit the size of the logfile for the on-demand scan automatically. A margin of approx. 50 kilobytes is allowed in order to minimize the CPU utilization. If the logfile exceeds the specified size by 50 kilobytes, old entries are automatically deleted until the specified size minus 50 kilobytes is reached.

Save Configuration

or button 

This will immediately send a command to the AVGuard Service in order to save the current configuration. However, this will be done automatcally when the service stops or the system shuts down.

Scan Mode

The AntiVir Engine can be configured to scan in two different modes:

Standard

In this mode, the AntiVir Engine will only scan the significant parts of a file for viruses. Any found virus signature will be validated. False positives are reported very rarely. This mode could cause some virus signatures not to be reported since they are not runnable (invalid). This is the default mode.

Advanced

The Engine will scan the whole file (!) for viruses. Note that signatures found will not be validated so that false positives could occur. This mode is much slower than the standard mode.

Scanner Tab

These settings are used to configure the scanner of AVGuard for Windows.

Device Mode

This group specifies the time when to scan an accessed file. This can be configured to optimize AVGuard for you specific needs.

AVGuard disabled

If selected, AVGuard has been completely disabled and will no longer protect your computer against viruses. However, all modules stay loaded in system memory. Please use this feature with care and only for a short period of time.

Scan on file read

If selected, all files will be scanned before they have been read or executed by the application or the operating system. This means that AVGuard will scan a file for viruses before you can execute or open it. This is a good choice since AVGuard/XP includes a filename cache which will cause a file only be scanned once and though increases system throughput.

Scan on file write

If this option is selected, all files will be scanned after they have been written to the volume. This means that a file file be scanned immediately for viruses if you save it to a volume.

Scan on file read and write

AVGuard will scan files before they are opened/executed and after thay have been written or created. Please note that this feature could decrease your system performance.

Drives to monitor

AVGuard/XP can be configured to monitor only a specific set of drives on your computer. Select the option depending on your network environment. E.g. if you are connected to a server with AntiVir for NT/2000 server loaded, monitoring files on network drives located on this server would be not useful since the server has already done this job.

Local drives

Only files located on local drives (e.g. Floppy Disks, Harddisks, CD-ROMs, ZIP-Drives, MO-Drives, etc.) will be scanned.

Network drives

Files on remote drives (e.g. Server volumes, Peer-Drives) will be scanned.

Archives

AVGuard/XP is able to decompress archives and to scan the included files afterwards. Note that this can cause an impressive loose of performance.

PKLite/LZExe

If selected, PKLite/LZExe runtime-compressed files will be decompressed and scanned afterwards. This will ensure that a virus cannot be enclosed in such a compressed file.

Scan Mode

Every antivirus product in the AntiVir-family is able to use two different modes when scanning for viruses.

Standard

This mode is the default for all AntiVir products. Using this mode, only the significant parts of a file will be scanned. Any virus signature found will be verified if it is at the right offset so that false positives are avoided. This mode is very fast.

Advanced

Using advanced mode, the whole file will be scanned. Any found virus signature is not verified, false positives can occur. Scanning speed will be reduced.

Files to Scan

AVGuard can be configured to use a filter to exclude some files that are normally not hosts for viruses. This can improve the system performance depending on your environment. File extensions are used by the Windows operating system and by its applications to determine the type of a file. E.g. an executable in general has the file extension ".EXE".

All files

If selected, all files accessed in the specified device mode will be scanned automatically.

Use file extension list

Only files with a file extension that matches an extension in the file extension list will be scanned.

{button File extensions,JI(`',`HELP_FILE_EXTENSIONS')} Opens a window with a list of file extensions used by the scanner

Service-Status

This field displays the current status of the AVGuard for Windows Service.

Loaded

means that the device driver and the service are up and running. Communication between the AVGuard control porgram and the service is working properly and AVGuard is ready to scan files for viruses. Please note that AVGuard will only scan for viruses if the device mode is set to "Scan on File Open" or above.

Not loaded

indicates that the AVGuard control program could not establish a communication channel to the service. This means that the service is not loaded or that there's a communication problem. Please refer to the event log to get more information.

Trouble Shooting

If AVGuard/XP does not work properly or if you have any problems with AVGuard/XP or if you have an infection which you are not able to manage yourself, please check the following:

- Please check if the service is active. The small red umbrella in the system tray must be opened. Please activate the service if necessary: at the right bottom: Select the 'Start' button, and then 'Settings / Control Panel' and activate the applat 'Services' with a double-click. Now look for the entry 'AntiVir Service'. The startup typew must be automatic', status must be 'Started'. If needed, please start the servce manually by selecting the appropriate line and clicking the 'Start' button. If an error occurs, please check the event log. If you are not successful you probably should remove your AntiVir/XP package completely by using 'Start / Setting / Control Panel / Software'. Please restart your workstation afterwards and re-install the software from your CD-Rom.
- If the service is already active, please check the following: Control Program / Configuration: In the group 'Device Mode' at lease one of the two options must be checked.
- At lease one of the two options in the group 'Drives To Scan' must be checked. Normally, this is the option 'Local Drives'.
- Check the settings of the group 'Files To Scan'. If 'Program Files Only' is selected, you should have a look into the file extension list. Please set it to default values if needed.
- To be able to disinfect a file, it is important that the option 'Repair automatically' is enabled.
- Check if AVGuard/XP has scanned the file. This can be done by enabling the enhanced logging mode in the report property sheet, accessing the ile and checking the logfil afterwards.
- If your logfile contains lot of entries like "access denied", you should check the following: The AVGuard service "AntiVirService" needs desktop access rights to be able to display it's warning dialog boxes. This means that it must log on as Local System Account ("SYSTEM"). Additionally, it needs the option "Allow service to interact with desktop" enabled in the Services applet of the Control Panel. Please note that the SYSTEM account needs unlimited access to all local drives. The AVGuard service "AntiVirService" must not be installed to other accounts!

More information can be found in the file README.WRI in te root directory of your CD-ROM, in the file READ.ME in the program directory of AVGuard/XP or in the internet at www.hbedv.com.

If you cannot solve your problems yourself, it would be a pleasure for our hotline to assist you. To enable us helping you efficiently, we keep the following information ready:

- Your serial number (From the 'About' window of the Control program).
- Version information of VDF-file, engine and program.
- The version information of your operating system and the possibly installed service packs.
- Installed software packages, e.g. antivirus applications from other vendors.
- The exact (!) messages displayed by the application or shown in the logfile.

Our addresses:

H+BEDV Datentechnik GmbH	Internet:	www.hbedv.com
Techn. Support	eMail:	support@hbedv.com
Lindauer Strasse 21	Tel:	(+49) 0 7542-93040
88069 Tettnang	Fax:	(+49) 0 7542-52510
Germany		

Virus Infection

This sheet contains a short introduction to virus removal and infection handling, especially if AVGuard/XP detected a virus:

If AVGuard/XP detected a virus ...

1. Don't panic and beware calm!

AVGuard/XP has done all the important jobs automatically if it is configured correctly. If you tried to access or to start an infected file, it will be disinfected or moved or the access to this file will be denied. After a successfull disinfection, you can work with that file as usual. If a disinfection is not possile, the file will be normally moved to the quarantine directory and you'll get a warning.

2. Follow the antivirus instructions step by step, don't rush the things!

Now, it is important to check your complete workstation and all possibly infected floppy disks for viruses. It would be a good choice to let AntiVir/XP do this job since it has already been installed on your system. Please try to disinfect all infected files and boot records on your hard disk and all floppy disks. Ask your dealer or call H+BEDV if you need any assistance. Possibly it would be a good idea to activate the automatic repair option inside AVGuard/XP. If AntiVir/XP or AVGuad/XP is not able to disinfect the file, please send us a copy for further analysis. We will provide you with a solution as fast as possible. At least, try to investigate where the virus did come from. Check your anti-virus strategie if needed to beware of further infections.

3. Inform your colleques, your boss and your business partners!

It is not a very pleasant job, however information is very important in such cases. Especially, if the virus has been imported from outside your site. Please inform your colleques, your boss or your security manager about the infection!

Register Card Network Warnings

This tab contains all options to send warning messages via LAN to other computers running Windows XP/NT/2000 in case of a virus found. This means that AVGuard will send a configurable warning message to all computers in the list if an infected file has been found. Please note that the warnings will be send to the specified computers and not to specified users.

Activate network warnings

Use this switch to enables network warnings in case of a virus found. Please note that there must be at least one computer in the receiver list.

Send message to

This list contains names of computers to send warning messages to if a virus has been found in a file during real-time scan.

Using the button {button Insert,} you can add another computer to the list. This will open a new window where you can enter the name of the computer to whom to send the warning messages. The maximum length for a computer name is 15 characters. Alternatively, you can select the computer directly from your network neighborhood using the button  Please note that the message will only be sent to computers running Windows XP/2000/NT. Computers running Windows 95/98/Me are not supported. You can add a computer only once to this list.

Using the button {button Delete,} you can delete the selected item from the list.

Message to send

The message in this field will be sent to the appropriate computers. There's a maximum of 500 characters allowed. Please note that you can format the message inside the edit box as desired. The formatted message will be displayed on the destination computer in the same way.

You can use the following key sequences to format your message:

{button Ctrl ,} {button TAB,} inserts a tabulator. The current line will be indented for a few characters to the right.
{button Ctrl ,} {button ENTER,} insers a new line.

The message also may contain variables for that are replaced by the appropriate text when sending the message:

%FILE%	this variable will be replaced by the full qualified path and filename of the infected file.
%VIRUS%	this variable will be replaced by the name of the virus found in the file.
%COMPUTER%	this variable will be replaced by the name of the local computer.

An example:

```
********************** W A R N I N G ***********************
AVGuard detected the virus %VIRUS on the computer %COMPUTER%
in the local file

   %FILE%!

Please contact your administrator via phone at 4573.
```

If you press the button {button Default,}, the default message will be inserted to the field.