About AVGuard/XP

The AntiVir Personal Edition with the resident scanner AVGuard/XP has been developed especially for home users. It is completely free of charge for private use and can be obtained from the following Internet URL. Updates are also available from this address via automatic FTP download: http://www.free-av.com.

AntiVir 6 Professional

If you need support of network drives or if you need any more functionality, we recommend the enhanced version of AntiVir: AntiVir 6 Professional. The professional version is currently available for the following platforms: DOS, Windows 3.1x, Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, OS/2, Linux (i386), FreeBSD (i386), OpenBSD (i386) Novell NetWare, Windows 2000 Server, Exchange Server, Exchange Workstation, Outlook, Eudora Mail Client and MS Mail. More information about these products is available from one of the address below or from the Internet:

H+BEDV Datentechnik GmbH	Internet:	http://www.hbedv.com
Lindauer Strasse 21	Email:	info@hbedv.com
88069 Tettnang	Phone:	+49 (0) 7542-93040
Germany	Fax	+49 (0) 7542-52510

About AVGuard/XP

This dialog box displays some information about the AVGuard/XP 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.

Hotline

Technical support is available via Internet only.

Technical inquiries via Phone/Fax/Letter and e-mail can not be answered!

In order to facilitate your inquiries to the technical support, we have created an Internet Support Forum for you.

You find the AntiVir Support Forum on the internet at: http://www.free-av.de/forum.

You will find the frequently asked questions about AntiVir Personal Edition and you will have the possibility to submit technical questions to all other forum members and our moderators. Additionally, you can discuss with other users of AntiVir and share your own experiences and hints.

Additional Product Information

This section contains the information how to contact us if you need technical support, any other information or assistance concerning our AntiVir Professional products.

AntiVir Professional Edition

Besides the AntiVir Personal Edition, H+BEDV Datentechnik GmbH offers the **AntiVir 6 Professional Edition**. This package provides a very enhanced functionality and a flexible and cheap licensing, especially in multi-user environments.

Additional Features:

▶ Support of network drives.
▶ Support of network messages and warnings.
▶ Support of search profiles.
▶ Scanning of single and multiple directories.
▶ Scanning of user-defines archives.
▶ Explicit scanning of boot records.
▶ Intranet-Update-Wizard. This is a tool to automatically distribute the software and updates in your network.
▶ Start of external programs depending on the search results.
▶ Scheduler.
▶ Password protection for the configuration.
▶ CRC option.
▶ Enhances configuration possibilities for the scan- and repair engine.
▶ The email scanner for MS Mail, Qualcomm Eudora, MS Outlook and MS Exchange Client are included.

The Professional Version is currently available for the following platforms: DOS, Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, OS/2, Linux (i386), FreeBSD, OpenBSD, Novell NetWare, Windows 2000 Server, Exchange Server, Exchange Workstation, Outlook, Eudora Mail Client, MS Mail. A SMTP solution ("AVMailGate") is available for Linux, FreeBSD and OpenBSD.

Information about the AntiVir Professional products is available at:

H+BEDV Datentechnik GmbH	Internet:	http://www.hbedv.com
Lindauer Strasse 21	Email:	info@hbedv.com
88069 Tettnang	Phone:	+49 (0) 7542-93040
Germany	Fax:	+49 (0) 7542-52510

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 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 or unwanted program has been found.
Repair	Disinfection settings.
Heuristic	Settings for the macro virus heuristic and template handling.
Logfile	Logfile settings.
Filters	These options can be used to configure excepted objects for the on-access scan.
Unwanted Programs	AntiVir reports viruses and other malware in any case. In addition AntiVir will report all marked types of unwanted programs.

Contents

These help pages are currently available in AVGuard for Windows XP Personal Edition:

Demo Version

If you don't have a valid license key file, AVGuard/XP Personal Edition 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 Personal Edition. After a restart of the AntiVir service, the system will run as a full version.

Device Mode

This displays the current device mode:

AVGuard disabled

AVGuard/XP is disabled and deactivated. It will no longer protect your computer from viruses and unwanted programs.

Scan on file read

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

Scan on file write

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

Scan on file read and write

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 and not inserted into the file extension list.

{button Help,}

Displays this help screen.

File Action

In this box, you will see the currently selected action to be performed by AVGuard/9x in case of an infection.

Repair File

AVGuard/XP attempts to repair an infected file. If the repair attempt fails, the action selected under Action if File not Repaired is performed.

Please note that the following actions will only be performed if the virus or unwanted program is unable to be repaired.

Delete File

The infected file will be deleted. It can be restored using some special tools. The signature of this virus or unwanted program 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 cannot 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 Fle

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

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

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 Datentechnik GmbH.

{button Help,}

    Displays this help screen.

File Menu

Activate AVGuard

This menu option activates AVGuard/XP. On initial installation, AVGuard should always be ready activated. In order to use this menu option, you must first select the menu option "Deactivate AVGuard". This function is only selectable provided AVGuard is deactivated.

Deactivate AVGuard

This menu option deactivates AVGuard/XP. You may use this option in order to deactivate the resident virus monitoring temporarily. Please note that you may need a password if a password is set in the options. This function is only selectable provided AVGuard is activated.

Start AntiVir Main Program

This will start the AntiVir Main Program directly from the AVGuard Control Program. This is for example to scan complete drive c: immediately for viruses and unwanted programs.

Start Internet Update

The internet updater can now also be started via this menu option. This improves user-friendliness, as you no longer have to load the main program whenever you want to start the updater. This menu option is only selectable provided the internet updater is already installed and activated.

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/XP Service so that AVGuard/XP will search for viruses and unwanted programs 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 file 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 and unwanted programs are found.

The Help Menu

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

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.

Main Window

The main window of AntiVir Guard for Windows (Personal Edition) consists of 3 main areas: the menu bar, the tool bar and the display area for statistical data. More detailed statistical data and additional configuration options are available with our professional version, <u>AntiVir 6 Professional</u>.

Menu Options

<u>File</u>
<u>Options</u>
<u>Help</u>

Configuration

<u>Service-Status</u>:   This displays the current status of the AVGuard/XP Service.
<u>File Action</u>:   This field displays the action taken if an infected file has been found and the user notification has been disabled.
<u>Device Mode</u>:   Displays when files are to be scanned.
<u>File To Scan</u>:   All files or only files with a specific file extension.

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 Detection: The name of the last virus or unwanted program found.
Detections: The number of viruses and unwanted programs found.
Warnings: The number of warnings occurred.
Error Count: The number of errors occurred.

Minimize 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 its 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/XP Control Program does not consume any CPU cycles.

The Options Menu

This menu contains the following entries:

<u>Configuration</u> or button

      Select this to configure the AVGuard/XP.

<u>Show Logfile</u>

      Shows the logfile of the AVGuard/XP.

Property Tab Action

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

Action If File Not Repaired

When AVGuard/XP discovers a virus or unwanted program it 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.

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.

Deny access to file

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

Notifications

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 and unwanted programs 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.

Property Tab Filters

These options can be used to configure excepted objects for the on-access scan. The objects concerned will then be disregarded by the on-access scanner. Using the list of processes to be omitted, AntiVir can ignore their file accesses during the on-access scan. This is useful in the case of databases or backup solutions, for example.

Processes to exclude form realtime scanning

All file accesses by processes in this list are ignored. To add a new process to this list, enter the name of the process in the box on the left and click on {button Add >>,}. The easiest way to find the name of the relevant process is via the task manager. You will find the names of all currently active processes on the "Processes" page. Look for "your" process and enter its name (to find under "Image Name"). You can delete the currently highlighted entry from the list with {button <<   Delete,}.

WARNING:

Please note that all file accesses by processes included in the list are excluded from the scan for viruses and unwanted programs!

Property Tab Heuristic

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/XP 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 effect, 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 investigations 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/XP will delete even references to deleted macros and their names from the template. If a macro has been deleted, its 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 definitely clean.

Property Tab Logfile

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 group 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 and unwanted programs 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 information 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 of logfile 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.

Property Tab Repair

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 dialog box displayed when an infected file has been detected.

Backup

Create backup before repair

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 detection into the product to be able to remove it after the next software update.

Backup directory

This is the directory where to create the backups.

Property Tab Scanner

These settings are used to configure the scanner of AVGuard/XP.

Device Mode

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

AVGuard disabled

AVGuard/XP is disabled and will not protect your system against viruses and unwanted programs.

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 a file will be scanned for viruses and unwanted programs before you'll get access to it. This is a good choice since AVGuard/XP includes a filename cache which will cause a file only be scanned once.

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 just saved to a volume will be scanned for viruses and unwanted programs before anyone will get access to it. This is a good option for Internet downloads.

Scan On file read and write

Files will be scanned for viruses and unwanted programs before they have been open or executed and after they have been written to a volume (see above). Please note that this option may decrease system performance because files may be scanned more than once.

Drives To Monitor

AVGuard/XP can be configured to monitor only a specific set of drives on your computer. In the Home edition, these are only the local drives. Support of network drives is included in the professional version: AntiVir 6 Professional.

Local drives

Only files located on local drives (e.g. Floppy Disks, Hard disks, CD-ROMs, ZIP-Drives, MO-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 or unwanted program cannot be enclosed in such a compressed file.

Files to Scan

AVGuard/XP can be configured to use a filter to exclude some files that are normally not hosts for viruses and/or unwanted programs. This can improve the system performance depending on you environment.

All files

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

<u>Use file extension list</u>

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

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

Property Tab Unwanted Programs

AntiVir protects you against computer viruses.

In addition, it will also scan selectively for <u>dialers</u>, <u>Backdoor Clients (BDC)</u>, <u>games</u>, <u>jokes</u> and <u>Possible Malicious Software (PMS)</u>.

- ▶ Possible Malicious Software (PMS)
- ▶ Jokes
- ▶ Games
- ▶ Dialers
- ▶ Backdoor Client (BDC)

The selection is activated by clicking on the relevant box.

To activate all types, click on <u>Select all</u>.

If a type is deactivated, files which are identified as being of that program type will no longer be reported entered in the report file.

Service-Status

This field displays the current status of the AVGuard/XP Service.

Loaded

This means that the service is loaded and active. Communication between the monitoring program and service is now possible. The service operates according to the chosen settings.

Note: Even when AVGuard/XP is activated, this doesn't necessarily mean that AntiVir will scan for viruses or unwanted programs, as the device driver, drives to be monitored or other equipment may be deactivated.

Not loaded

The monitoring program of AVGuard/XP was unable to find an active AVGuard/XP service on the computer, or communication is not possible. This means that all files can pass through the system unchecked, i.e. you are unprotected against viruses and unwanted programs.

This message can also point to a problem, however, e.g. the service may not be loaded or it may have been terminated manually. Alternatively, the monitoring program and service may be incompatible (different versions) or there may be a communication problem. In this case, check the event log on the target computer.

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 umbrella in the system tray must not be opened. Please activate the service if necessary: at the right bottom: Select the "Start" button, and then "Settings / Control Panel" and activate the applet "Services" with a double-click. Now look for the entry "AntiVir Service". The startup type must be automatic", status must be "Started". Additionally, you should check in the group "Log on as" that "System Account" and "Allow service to interact with desktop" are enabled. If needed, please start the service 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 the option "AVGuard disabled" must not be checked.
▶   The option "Local Drives" in the group Drives to monitor must be checked.
▶   Check the settings of the group Files to scan. If "Use file extension list" 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 logfile property tab, accessing the file and checking the logfile afterwards.
▶   If your logfile contains lot of entries like "access denied", you should check the following: The AVGuard/XP Service "AntiVirService" needs desktop access rights to be able to display its 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/XP Service "AntiVirService" must not be installed to other accounts!

More information can be found in the file README.WRI in the root directory of your CD-ROM, in the file READ.ME in the program directory of AVGuard/XP or in the internet at http://www.free-av.com or in the Frequently Asked Questions (FAQ) shipped with your AntiVir Personal Edition.

AntiVir Support Forum

In order to facilitate your inquiries to the technical support, we have created the AntiVir Support Forum for you.

You find the AntiVir Support Forum on the internet at: http://www.free-av.de/forum.

You will find the frequently asked questions about AntiVir Personal Edition and you will have the possibility to submit technical questions to all other forum members and our moderators. Additionally, you can discuss with other users of AntiVir and share your own experiences and hints.

To enable us to help you efficiently, please add the following information to your request:

  - 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.

Technical inquiries via Phone/Fax/Letter and e-mail can not be answered!

Unwanted Programs

Dialers

Certain services available in the internet have to be paid for. They are invoiced in Germany via dialers with 0190 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. They replace the internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

To protect yourself generally from unwanted 0190 dialers, we recommend that you ask your telephone provider directly to deny access to these numbers.

If you have activated the option "Dialers" under Unwanted programs in the configuration menu of AntiVir, you will receive a warning whenever AntiVir finds something. You now have the option of simply deleting the unwanted 0190 dialers.

Games

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. Email games are also becoming increasingly widespread, with numerous variants in circulation from simple chess games to "Fleet Maneuvers" (including torpedo battles). The relevant moves are sent via mail programs to partners who then answer them in turn.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Through its extended scanning and identification routines, AntiVir is capable of detecting games and eliminating them as unwanted programs. If you have activated the option "Games" under Unwanted programs in the configuration menu, you will receive an appropriate warning whenever AntiVir reports a find. All you have to do now is press delete - and the game is up in the truest sense of the word!

Jokes

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).
But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least the user, will get quite a shock or be thrown into such a panic he may do real damage.

Through its extended scanning and identification routines, AntiVir is capable of detecting jokes and eliminating them as unwanted programs. If you activate the option "Jokes" with a tick under Unwanted programs in the configuration menu, you will be notified accordingly of any findings.

Possible Malicious Software (PMS)

PMS (possible malicious software) will not normally do any damage to your computer. It is programmed to cause damage to other users. Example: Mail bombers - with this type of program the victim may be attacked with thousands of emails.

AntiVir is able to detect "possible malicious software". If you have activated the option "Possible malicious software (PMS)" under Unwanted programs in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

Backdoor Clients (BDC)

In order to steal data or manipulate computers, a backdoor server program is smuggled in unbeknown to the user. This program can be controlled by a third party using backdoor control software (client) via the internet or a network.

AntiVir is able to detect "Backdoor control programs". If you have activated the option "Backdoor Client (BDC)" under Unwanted programs, in the configuration menu, you will receive a corresponding warning whenever AntiVir reports a find.

Virus Infection

This provides a brief introduction to the steps to take if AVGuard/XP finds a virus, for example. Please note that there are some limits to the functionality of the AntiVir Personal Edition. Should you require antivirus software for other platforms or an extended range of functions, we would recommend the version AntiVir 6 Professional.

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 successful disinfection, you can work with that file as usual. If a disinfection is not possible, 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 the H+BEDV Datentechnik GmbH 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 AVGuard/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 strategy if needed to beware of further infections.

3. Inform your colleagues, 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 colleagues, your boss or your security manager about the infection!

4. New, unknown viruses and suspicious files

Please send new viruses and suspicious files as an encrypted archive file attached to an email to virus@free-av.com. Please don't for get to mention the password and a few comments about the attached file in your mail.