

KASPERSKY LAB

Kaspersky Anti-Virus
für Lotus Notes/Domino

BENUTZERHANDBUCH

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

Benutzerhandbuch

© Kaspersky Lab Ltd.
Besuchen Sie unsere WEB-Seite:
<http://www.kaspersky.com/de/>

Redaktionsdatum: Februar 2002

Inhalt

1.	KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO	8
1.1.	Anwendungsbereich und Grundfunktionen	8
1.2.	Lieferumfang	11
1.2.1.	Komponenten des Lieferumfangs	11
1.2.2.	Lizenzvertrag	11
1.2.3.	Registrierungskarte	12
1.3.	Thematischer Umfang des Benutzerhandbuchs	13
1.4.	Textformatierung von besonderer Bedeutung	15
1.5.	Service für registrierte Benutzer	16
2.	INSTALLATION DES PROGRAMMS KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO	18
2.1.	Systemvoraussetzungen	18
2.2.	Installation des Programms auf einem Server	19
3.	FUNKTIONSSCHEMA VON KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO	24
4.	VORBEREITUNGEN FÜR DEN BETRIEB VON KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO	28
4.1.	Reihenfolge der Vorbereitungen für den Betrieb	28
4.2.	Öffnen der Datenbanken	29
4.3.	Autorisation zum Zugriff auf die Datenbanken	33
4.4.	Benutzeroberfläche der Konfigurationsdatenbank	35
4.5.	Hilfesystem	37
4.6.	Terminologie	38

5.	KONFIGURATION DER PARAMETER FÜR DEN ANTIVIRENSCHUTZ	40
5.1.	Prinzipien für die Konfiguration des Programms	40
5.2.	Allgemeine Optionen für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino. Optionen → Allgemein.....	43
5.3.	Parameter für das Scannen von Datenbanken. Optionen → Überprüfung der Datenbanken.....	46
5.3.1.	Allgemeine Informationen zur Überprüfung von Datenbanken.....	46
5.3.2.	Desinfektion von infizierten Objekten der Datenbanken. Registerkarte GLOBAL.....	47
5.3.3.	Planung der Überprüfung von Datenbanken. Registerkarte PLANUNG.....	48
5.3.4.	Zu scannende Datenbank-Objekte. Registerkarte OBJEKTE ZUR ÜBERPRÜFUNG	50
5.3.5.	Parameter für das Scannen von Anlagen. Registerkarte ENDUNGEN	51
5.3.6.	Informationen über das Scannen. Starten der Überprüfung. Registerkarte INFORMATION	53
5.4.	Parameter für das Scannen von Mail-Nachrichten. Optionen → Mail-Überprüfung.....	55
5.4.1.	Allgemeine Informationen zur Überprüfung von Mails.....	55
5.4.2.	Desinfektion von Mail-Nachrichten. Registerkarte GLOBAL.....	56
5.4.3.	Typen der zu scannenden Mail-Objekte. Registerkarte OBJEKTE ZUR ÜBERPRÜFUNG	56
5.4.4.	Parameter für das Scannen von Anlagen. Registerkarte ENDUNGEN	58
5.5.	Bearbeitungsregeln für die zu scannenden Objekte. Optionen → Regeln.....	59
5.5.1.	Was ist ein zu scannendes Objekt?.....	59
5.5.2.	Auswahl der zu scannenden Objekte.....	61

5.5.3.	Parameter für die Bearbeitung von zu scannenden Objekten	61
5.5.4.	Parameter für das Versenden von Benachrichtigungen ..	63
5.5.5.	Parameter für den Überprüfungsvermerk	65
5.5.6.	Parameter für das Aufzeichnen des Ereignisjournals.....	67
5.6.	Bearbeitungsarten für zu scannende Objekte	68
5.6.1.	Konfiguration der Bearbeitungsart	68
5.6.2.	Verschieben in den Quarantäne-Ordner für infizierte Objekte	69
5.6.3.	Desinfektion infizierter Objekte.....	71
5.6.4.	Löschen infizierter Objekte.....	72
5.6.5.	Weiterleitung infizierter Objekte	73
6.	START UND BEENDEN DER ANTIVIREN-ÜBERPRÜFUNG.....	76
7.	ZUSATZFUNKTIONEN FÜR DEN ANTIVIRENSCHUTZ	78
7.1.	Einleitung	78
7.2.	Arbeit mit Objekten in der Analyse-Datenbank. Daten → In der Warteschlange	80
7.3.	Quarantäne-Datenbank	83
7.3.1.	Auswahl eines Abschnitts der Quarantäne-Datenbank....	83
7.3.2.	Arbeit mit Mail-Objekten in der Quarantäne-Datenbank. Daten → Quarantäne (Mail).....	84
7.3.3.	Arbeit mit Datenbank-Dokumenten in der Quarantäne- Datenbank. Daten → Quarantäne (Dokumente)	87
7.4.	Arbeit mit den Aufzeichnungen des Ereignisjournals	89
7.4.1.	Auswahl einer Gruppe von Einträgen.....	89
7.4.2.	Regeln für die Arbeit mit Einträgen des Ereignisjournals .	90

8.	DEINSTALLATION VON KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO	93
8.1.	Deinstallation des Programms mit Hilfe des Deinstallationsprogramms	93
8.2.	Manuelle Deinstallation des Programms	95
9.	KASPERSKY ANTI-VIRUS UPDATER	97
9.1.	Wofür wird das Kaspersky Anti-Virus Updater-Programm verwendet?	97
9.2.	Starten des Kaspersky Anti-Virus Updater	98
9.3.	Benutzeroberfläche des Kaspersky Anti-Virus Updater	99
9.3.1.	Fenster Willkommen	99
9.3.2.	Fenster Verbindung	100
9.3.2.1.	Einstellungen für das Update aus dem Internet ...	101
9.3.2.2.	Aktualisierung von einem lokalen Ordner aus	108
9.3.3.	Auswahl der zu aktualisierenden Objekte	108
9.3.4.	Fenster Optionen	109
9.3.5.	Fenster Aktualisierung läuft	110
9.3.6.	Fenster Aktualisierung abgeschlossen	111
10.	KASPERSKY ANTI-VIRUS CONTROL CENTRE	113
10.1.	Beschreibung von des Kaspersky Anti-Virus Control Centre	113
10.2.	Start des Kaspersky AV Control Centre	114
10.3.	Die Oberfläche des Kaspersky AV Control Centre	117
10.3.1.	Registerkarte Tasks	117
10.3.1.1.	Fenster Eigenschaften	124
10.3.2.	Registerkarte Komponenten	125
10.3.3.	Registerkarte Einstellungen	127
10.3.3.1.	Kategorie Sicherheit	130

**KASPERSKY ANTI-VIRUS FÜR LOTUS
NOTES / DOMINO**

10.3.3.2.	Kategorie Alarme	131
10.3.3.3.	Kategorie Anpassen	137
10.4.	Task-Assistent	140
10.4.1.	Fenster Tasks	141
10.4.2.	Fenster Zeitsteuerung für Kaspersky Anti-Virus Updater	143
10.4.2.1.	Start von Tasks nach Eintreten bestimmter Ereignisse	144
10.4.2.2.	Bedingungsgesteuerter Start von Tasks	146
10.4.2.3.	Task jede Stunde starten	147
10.4.2.4.	Task jeden Tag starten	148
10.4.2.5.	Task jede Woche starten	149
10.4.2.6.	Task jeden Monat starten	150
10.4.3.	Fenster Alarme	151
10.4.4.	Fenster Benutzerkonto	151
10.4.5.	Task-Einstellungen	153
11.	KASPERSKY REPORT VIEWER	154
11.1.	Wofür wird Kaspersky Report Viewer verwendet?	154
11.2.	Aktivierung der Report-Anzeige	154
11.3.	Beschreibung der Benutzeroberfläche von Report Viewer ..	155
12.	TREE-CHART™	159
12.1.	Was ist Tree-Chart?	159
12.2.	Einstellungsbaum	160
12.3.	Bedienelemente	161
12.3.1.	Kontrollkästchen	161
12.3.2.	Options-Schaltfläche	162
12.3.3.	Textfeld	163

- 12.3.4. Eingabefeld: Festlegen eines Pfades für 163
- 12.3.5. Eingabefeld: Festlegen von Zahlenwerten für 164
- 12.3.6. Dropdown-Liste..... 165
- 12.4. Kontrollindikatoren..... 165
- 13. ANHANG A. KLASSIFIKATION DER COMPUTERVIREN 168**
- 14. ANHANG B. KASPERSKY LAB LTD. 172**
 - 14.1. Über die Firma "Kaspersky Lab" 172
 - 14.2. Andere Antiviren-Produkte von "Kaspersky Lab." 173
 - 14.3. Unsere Adresse..... 176
- 15. ANHANG C. INDEX..... 177**

Achtung! Jeden Tag tauchen neue Viren auf. Um die Aktualität des Produkts zu gewährleisten, sollten Sie deshalb Ihre Antiviren-Datenbanken jeden Tag aktualisieren (weitere Informationen finden Sie unten). Vergessen Sie bitte nicht, die Antiviren-Datenbanken sofort nach der Installation des Produkts auf dem Server zu aktualisieren!

Kapitel

1

1. Kaspersky Anti-Virus für Lotus Notes/Domino

1.1. Anwendungsbereich und Grundfunktionen

Beschreibung von Kaspersky Anti-Virus für Lotus Notes/Domino

Kaspersky Anti-Virus™ für Lotus Notes/Domino dient dem Antivirenschutz von Mail-Systemen, die auf der Basis von Lotus Notes/Domino aufgebaut sind. Das Programm wird auf einem Server installiert, der mit dem Betriebssystem Linux oder Windows NT¹ betrieben

¹ Die für Linux-Server bestimmte Version des Programms verwendet den Antiviren-Kern KAVDaemon für Linux. Die Programmversion, die für NT-Server bestimmt ist, verwendet den Antiviren-Kern Kaspersky Anti-Virus für Windows NT Server.

wird, und überprüft den gesamten Mailverkehr, der über den Server ein- und ausgeht, auf das Vorhandensein von Viren.

Kaspersky Anti-Virus für Lotus Notes/Domino erfüllt auf dem Server folgende Funktionen:

- Alle Nachrichten, die über das Mail-System Lotus Domino auf dem betreffenden Server ein- und ausgehen, werden auf das Vorhandensein von Viren überprüft. Die Virussuche wird sowohl im Text der Nachrichten, als auch in den an die Nachricht angehängten Dateien durchgeführt. Außerdem sucht Kaspersky Anti-Virus für Lotus Notes/Domino auch innerhalb von angehängten Archiven und komprimierten .exe-Dateien, sowie innerhalb von angehängten Dateien in Mail-Formaten und Dateien in Mail-Datenbanken nach Viren.
- Wenn das Programm dafür konfiguriert wird, dann werden die durch Viren infizierten Nachrichten desinfiziert, falls die Reparatur möglich ist. Dabei kann Kaspersky Anti-Virus für Lotus Notes/Domino sowohl Textnachrichten, als auch an solche angehängte Dateien reparieren.
- Infizierte, beschädigte und verdächtige Objekte werden in der Quarantäne-Datenbank verwahrt.
- An die Benutzer werden Benachrichtigungen gesendet, die sie über den Versuch informieren, ihnen infizierte Nachrichten zu schicken.
- Eine Benachrichtigung über ein infiziertes Objekt wird an die Adressen einer Verteilerliste gesendet.
- An den Absender eines infizierten Objekts wird eine entsprechende Benachrichtigung gesendet.
- Die Arbeitsergebnisse werden in einem Ereignisjournal aufgezeichnet.



Bitte beachten Sie folgende Beschränkungen für die Funktionen des Programms Kaspersky Anti-Virus für Lotus Notes/Domino:

- Nachrichten, die mit einem Sicherheitskennwort verschlüsselt sind, werden nicht überprüft;

- Die Integrität einer elektronischen Signatur von Nachrichten, die von dem Absender unterzeichnet wurden, kann durch das Einfügen eines Überprüfungsvermerks in den Text der Nachricht und/oder durch das Ersetzen angehängter Dateien durch desinfizierte Dateien verletzt werden;
- Dateien, die in OS/2 oder Macintosh erstellt wurden, werden nicht überprüft;
- Nachrichten werden aus dem MIME-Format in das Rich Text Format konvertiert.

Das Programm kann von jedem Administrator konfiguriert werden, der Zugriff auf die Konfigurationsdatenbank besitzt (s. Pkt. 5.1). Die Konfiguration wird von einer Workstation aus durchgeführt, auf der der Client Lotus Notes installiert ist. Wenn der Server das HTTP-Protokoll unterstützt, kann die Konfigurationsdatenbank auch von jeder anderen Workstation aus mit Hilfe eines Web-Browsers geändert werden.

📁 Bei der Virensuche verwendet Kaspersky Anti-Virus für Lotus Notes/Domino die *Antiviren-Datenbanken*, in denen Informationen gespeichert sind, die das Auffinden und die Desinfektion einer großen Anzahl von Viren erlauben. Kaspersky Lab aktualisiert die Antiviren-Datenbanken wöchentlich durch Informationen über neue Viren.

1.2. Lieferumfang

*Komponenten des Lieferumfangs: Lizenzvertrag
Registrierungskarte*

1.2.1. Komponenten des Lieferumfangs

Der Lieferumfang des Softwareprodukts besteht aus folgenden Komponenten:

- ein versiegelter Umschlag mit der Installations-CD (oder den Disketten), auf der die Dateien des Softwareprodukts gespeichert sind;
- ein Benutzerhandbuch;
- eine Schlüssel-Diskette;
- eine Registrierungskarte (mit Angabe der Seriennummer des Produkts);
- ein Lizenzvertrag.

 Bitte lesen Sie vor dem Öffnen des versiegelten Umschlags mit der Installations-CD (oder den Disketten) sorgfältig den Lizenzvertrag.

1.2.2. Lizenzvertrag

Der Lizenzvertrag ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab Ltd. Dieser Vertrag legt Ihre Lizenzrechte und Lizenzbedingungen fest und bezieht sich auf die Nutzung des von Ihnen erworbenen Softwareprodukts.

 **Bitte lesen Sie den Lizenzvertrag sorgfältig!**

Wenn Sie den im Lizenzvertrag festgelegten Bedingungen nicht zustimmen, dann können Sie die Packung mit Kaspersky Anti-Virus an den Händler zurückgeben, bei dem Sie sie gekauft haben, und der Kaufbetrag des Abonnements wird Ihnen unter der Voraussetzung, dass Sie den Umschlag mit der Installations-CD (oder den Disketten) nicht geöffnet haben, vollständig erstattet.

Durch das Öffnen des versiegelten Umschlags mit der Installations-CD (oder den Disketten) zeigen Sie Ihre volle Zustimmung zu den Bedingungen und Bestimmungen des Lizenzvertrags.

1.2.3. Registrierungskarte

Bitte füllen Sie den abtrennbaren Abschnitt der Registrierungskarte aus. Geben Sie Ihren Vor- und Nachnamen, Telefonnummer und (falls vorhanden) E-Mail-Adresse vollständig an, und senden Sie die Karte an den Händler, bei dem Sie das Softwareprodukt erworben haben.

Sollte sich Ihre Anschrift, E-Mail-Adresse oder Telefonnummer in Zukunft ändern, dann teilen Sie dies bitte der Firma mit, an die Sie den abtrennbaren Abschnitt der Registrationskarte geschickt haben.

Die Registrierungskarte ist ein Dokument, auf dessen Grundlage Ihnen der Status eines registrierten Benutzers unserer Firma verliehen wird. Dieser Status gibt Ihnen das Recht, während der gesamten Laufzeit des Abonnements technische Unterstützung in Anspruch zu nehmen. Außerdem erhalten registrierte Benutzer, die den Newsletter von Kaspersky Lab Ltd. abonniert haben, Informationen über das Erscheinen neuer Softwareprodukte von.

1.3. Thematischer Umfang des Benutzerhandbuchs

Welche Fragen das vorliegende Benutzerhandbuch behandelt und was darüber hinausgeht.

Diese Dokumentation enthält die für Installation, Konfiguration und Betrieb des Softwareprodukts notwendigen Informationen. Außerdem werden die grundlegenden Konzepte des Produkts und deren Anwendung behandelt. Zusätzlich werden Empfehlungen für die Konfiguration gegeben. Die unten folgende Tabelle enthält eine Liste der Kapitel des Handbuchs und eine kurze Beschreibung jedes Kapitels.

Bezeichnung des Kapitels	Kurzbeschreibung
Kaspersky Anti-Virus für Lotus	Einleitende Informationen über das Produkt, Beschreibung des Lieferumfangs und der Struktur des Handbuchs.
Installation des Programms Kaspersky Anti-Virus für Lotus Notes/Domino	Systemvoraussetzungen für den Server, auf dem das Programm installiert wird. Wie das Programm Kaspersky Anti-Virus für Lotus Notes/Domino mit Hilfe des Installationsprogramms auf einem Computer installiert wird.
Funktionsschema von Kaspersky Anti-Virus für Lotus Notes/Domino	Beschreibung des Interaktionsschemas der Module, die zum Bestand von Kaspersky Anti-Virus für Lotus Notes/Domino gehören.

**KASPERSKY ANTI-VIRUS FÜR LOTUS
NOTES/DOMINO**

Bezeichnung des Kapitels	Kurzbeschreibung
Vorbereitungen für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino	Beschreibung der aufeinanderfolgenden Schritte zur Organisation der Arbeit mit dem Programm: Öffnen der Datenbanken, Autorisation für den Zugriff auf die Datenbanken, Benutzeroberfläche der Konfigurationsdatenbank.
Konfiguration der Parameter für den Antivirenschutz	Vorgehen zur Konfiguration der Parameter für den Antivirenschutz mit Hilfe der Konfigurationsdatenbank.
Start und Beenden der Antiviren-Überprüfung	Wie die Antiviren-Überprüfung der zu scannenden Objekte gestartet und beendet wird.
Zusatzfunktionen für den Antivirenschutz	Überprüfen der Reporte. Arbeit mit den Objekten der Analyse-Datenbank und Quarantäne-Datenbanken.
Deinstallation von Kaspersky Anti-Virus für Lotus Notes/Domino	Beschreibung des Vorgehens zur Deinstallation des Programms von Ihrem Computer.
Kaspersky Anti-Virus Updater	Beschreibung der Konfiguration und Arbeit mit dem Hilfsprogramm zur Aktualisierung der Antiviren-Datenbanken.
Kaspersky Anti-Virus Control Centre	Ausführliche Beschreibung der Konfiguration und Arbeit mit Kaspersky Anti-Virus Control Centre – der Zentrale zur Steuerung des Antivirenschutzes.
Kaspersky Report Viewer	Anwendungsbereich und Funktionen des Programms Kaspersky Report Viewer.




Bezeichnung des Kapitels	Kurzbeschreibung
Tree-Chart™	Beschreibung der Funktionsprinzipien des speziellen Bedienungselements, das zur Konfiguration von Kaspersky AV Updater verwendet wird.
Anhang A. Klassifikation der Computerviren	Ausführliche Informationen über die zur Zeit existierenden Arten von Computerviren.
Anhang B. Kaspersky Lab Ltd.	Informationen über die Firma. Antiviren-Produkte. Adressen.
Anhang C. Index	Index der Grundbegriffe.

1.4. Textformatierung von besonderer Bedeutung

Bedeutung der Markierung verschiedener Teile des Benutzerhandbuchs

Bestimmte Textteile dieser Dokumentation sind abhängig von ihrer Bedeutung und Definition unterschiedlich formatiert. In der folgenden Tabelle werden die verwendeten Textformatierungen mit besonderer Bedeutung erläutert.

Formatierung	Bedeutung
Fette Schrift	Namen von Menüs, Menüpunkten, Fenstern, Elementen von Dialogfenstern, usw.

Formatierung	Bedeutung
 Hinweis.	Zusätzliche Informationen, Bemerkungen.
 Bitte beachten!	Sehr wichtige Information.
 Um diese Aktion durchzuführen, 1. Schritt 1. 2. ...	Beschreibung einer Reihe von Schritten oder möglichen Aktionen, die der Benutzer durchführt.
Name eines Bedienungselements – Funktion des Bedienungselements.	Beschreibung von Bedienungselementen.

1.5. Service für registrierte Benutzer

Serviceleistungen für registrierte Benutzer:

Kaspersky Lab Ltd. bietet seinen registrierten Kunden ein umfangreiches Servicepaket, das die effektive Nutzung von Kaspersky Anti-Virus ermöglicht.

Wenn Sie ein Abonnement erwerben, dann erhalten Sie den Status eines registrierten Programmbenutzers und können für die Gültigkeitsdauer Ihres Abonnements folgende Serviceleistungen in Anspruch nehmen:

- Möglichkeit täglicher Updates der Antiviren-Datenbanken per E-Mail.

- Nutzung von neuen Versionen des vorliegenden Softwareprodukts.
- Beratung bei Fragen im Zusammenhang mit der Installation und Nutzung des vorliegenden Produkts (per Telefon oder E-Mail).
- Benachrichtigung über das Auftauchen neuer Viren (dieser Service wird für Benutzer angeboten, die den Newsletter von Kaspersky Lab Ltd. abonniert haben).

Es werden keine Informationen über die Funktion und den Gebrauch von Betriebssystemen und anderen Technologien zur Verfügung gestellt.

2. Installation des Programms Kaspersky Anti-Virus für Lotus Notes/Domino

2.1. Systemvoraussetzungen

*Systemvoraussetzungen für die Installation des
Programms auf einem Server:*

Für den Betrieb des Programms Kaspersky Anti-Virus für Lotus Notes/Domino auf einem Server, müssen folgende Softwarevoraussetzungen erfüllt werden:

- Betriebssystem Linux Red Hat 6.0 oder höher, oder Windows NT.
- Lotus Notes/Domino R5.02 (oder höher) für Linux oder für Windows NT.

Der Server muss folgende Voraussetzungen erfüllen:

- Prozessor Pentium 133 oder höher.
- RAM 64 MB (128 MB werden empfohlen).

Der auf der Festplatte benötigte freie Speicherplatz richtet sich nach der durchschnittlichen Größe und Anzahl der E-Mail-Nachrichten.

2.2. Installation des Programms auf einem Server

Vorgehen zur Installation des Programms Kaspersky Anti-Virus für Lotus Notes/Domino auf einem Server:

Vor dem Beginn der Installation von Kaspersky Anti-Virus für Lotus Notes/Domino, muss Notes/Domino R5.02 (oder höher) installiert werden.



Um das Programm Kaspersky Anti-Virus für Lotus Notes/Domino auf dem Server zu installieren:

1. Kopieren Sie die Datei *kav_install.nsf* in den Ordner mit den Daten von Lotus Notes/Domino. Dieser Ordner befindet sich im Root-Verzeichnis von Lotus Notes/Domino: für einen Windows NT Server kann das zum Beispiel der Ordner **Laufwerk:\notes\data** oder **Laufwerk:\lotus\domino\data** sein, für einen Linux-Server – **/opt/lotus/notesdata/**.
2. Erstellen Sie mit Hilfe des Programms Domino Administrator die Gruppe **LocalDomainAdmins**. Diese Gruppe besitzt in der Grundeinstellung Managerrechte für den Zugriff auf alle Datenbanken des Programms Kaspersky Anti-Virus für Lotus Notes/Domino.

3. Autorisieren Sie sich für den Zugriff auf den Server. Klicken Sie dazu auf die Registerkarte **Security** des Server-Dokuments, auf dem Sie das Programm installieren. Geben Sie in der Gruppe **Agent Restrictions** den Benutzernamen, unter dem Sie sich bei dem Programm Domino Administrator anmelden möchten, in die Liste **Unrestricted LotusScript/Java Agents** ein.
4. Nehmen Sie den Benutzernamen, unter dem Sie sich bei dem Programm Domino Administrator anmelden möchten, in die Gruppe **LocalDomainAdmins** auf.
5. Signieren Sie mit Hilfe des Programms Domino Administrator alle Elemente der Datenbank *kav_install.nsf*. Suchen Sie dafür auf der Registerkarte **Files** die Zeile mit *kav_install.nsf*. Klicken Sie mit der rechten Maustaste auf diese Zeile. Wählen Sie in dem erscheinenden Kontextmenü den Punkt **Sign**. Aktivieren Sie in dem erscheinenden Dialogfenster das Kontrollkästchen **All design documents** und klicken Sie auf die Schaltfläche **OK**.
6. Starten Sie auf dem Server den Task "HTTP", falls dieser noch nicht gestartet wurde. Geben Sie dazu von der Konsole des Servers oder von der Konsole eines Remote-Computers aus den Befehl **load http** ein. Den Task "HTTP" können Sie auch mit Hilfe des Programms Domino Administrator starten. Wählen Sie dazu auf der Registerkarte **Server** den Punkt **Task, Start**, und wählen Sie in dem erscheinenden Dialogfenster **Start New Task** den Task "HTTP Web server".
7. Öffnen Sie in einem WEB-Browser die Datenbank *kav_install.nsf* (zum Beispiel: **http://Serveradresse/kav_install.nsf**).
8. Wählen Sie auf der erscheinenden Seite die Sprache (Russisch, Englisch oder Deutsch), in der die Datenbanken dargestellt werden sollen. Dadurch wird die Seite mit der Konfiguration von Kaspersky Anti-Virus für Lotus Notes/Domino (s. Bild 1) geöffnet.

9. Überprüfen Sie auf der erscheinenden Seite **System Info**, ob das Programm die Konfiguration der Ordner richtig identifiziert hat, in die der Lotus Domino Server installiert wurde.

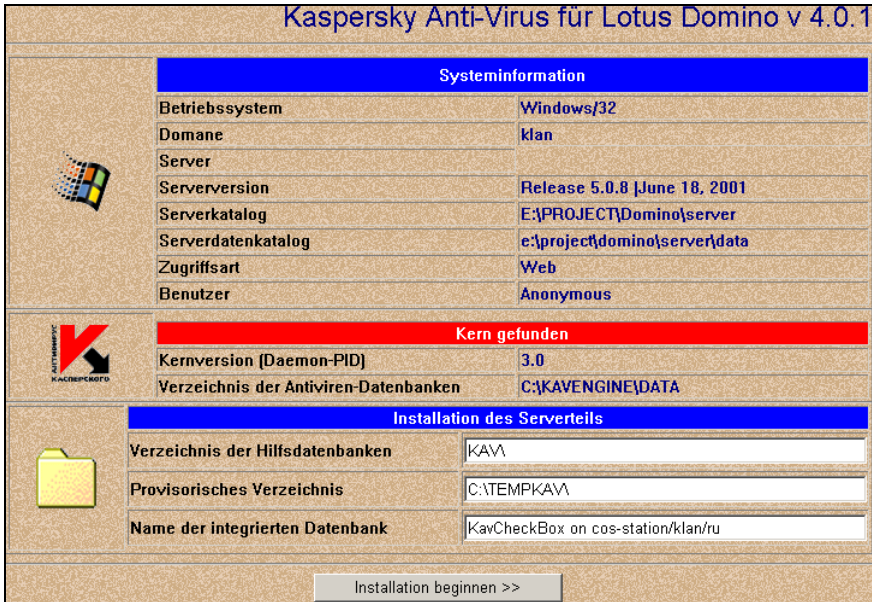



Bild 1. Programminstallation

10. Geben Sie im Abschnitt **Installation des Serverteils** die Werte für folgende Parameter ein:

- **Verzeichnis der Hilfsdatenbanken** – der vollständige Pfad des Ordners, in den das Programm installiert werden soll. Zum Beispiel: **\KAV**.

☞ Damit ist der Pfad gemeint, der mit dem Ordner **D:\Lotus\Domino\Data** beginnt. Unter dem Pfad **\KAV** ist also der Pfad **D:\Lotus\Domino\Data\KAV** zu verstehen.

- **Provisorisches Verzeichnis** – der vollständige Pfad des Ordners für die temporären Dateien. Zum Beispiel: **C:\TEMPKAV**.

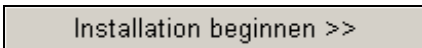
 Hier darf kein allgemein genutzter Ordner verwendet werden (wie z.B. **c:\tmp**), da während der Arbeit des Produkts der Inhalt dieser Ordner regelmäßig gelöscht wird.

- **Name der integrierten Datenbank** – der Name des **Mail-In** Dokuments, das die Beschreibung der Analyse-Datenbank enthält. Zum Beispiel:
KavCheckBox on Server/Development/Local.

11. Geben Sie im Feld **Ordner zur Installation** des Abschnitts **Antiviren-Kern** einen der folgenden Werte an:

- den vollständigen Pfad des Ordners in den der AVP API Antiviren-Kern installiert wird, wenn Sie eine Version des Programms für Windows NT installieren;
- den vollständigen Pfad des Ordners, in dem die Installationsdateien des Programms Daemon for Linux gespeichert werden, wenn sie eine Version des Programms für Linux installieren.

12. Klicken Sie auf die Schaltfläche



Nach einiger Zeit erscheint im unteren Teil der Seite ein Report der Installation (s. Bild 2).

 **Wenn Sie eine Version des Programms für Windows NT installieren,**

dann führen Sie einen Neustart des Servers durch.


```

Create folder : ... OK
Create folder : ... OK
Create INI var : KavOptionsDatabase ... OK
Extract template : kav_domcc.nif ... OK
Create NSF Database : \kav_domcc ... OK
Update config Database [SHARED]: ... OK
Update config Database [SCAN]: ... OK
Update config Database [SCHEDULER]: ... OK
Update config Database [RULES]: ... OK
Extract template : kav_cbox.nif ... OK
Create NSF Database : \kav_cbox ... OK
Extract template : kav_qbox.nif ... OK
Create NSF Database : \kav_qbox ... OK
Update INI var : EXTMGRR_ADDIN ... OK
Extract file : nKavHook.dll ... OK
Update INI var : SERVERTASKS ... OK
Extract file : nKavScan.exe ... OK
Update INI var : SERVERTASKS ... OK
Extract file : nKavScheduler.exe ... OK
Create Mail-In document...Mail-In document created.
KAV FOR LOTUS/NOTES INSTALLATION COMPLETE
Create folder : C:\KAVENGINE\ ... OK
Extract file : C:\KAVENGINE\SETUP\Setup.zip ... OK
Extract file : C:\KAVENGINE\regsvr32.exe ... OK
Extract file : C:\KAVENGINE\Avp_io32.dll ... OK
Extract file : C:\KAVENGINE\Avp_iont.dll ... OK
Extract file : C:\KAVENGINE\avpbase.dll ... OK
Extract file : C:\KAVENGINE\avpssi.dll ... OK
Extract file : C:\KAVENGINE\klav.exe ... OK
Extract file : C:\KAVENGINE\klavgui.dll ... OK
Extract file : C:\KAVENGINE\klavps.dll ... OK
Extract file : C:\KAVENGINE\Avp_io.vxd ... OK
KAV ENGINE INSTALLATION COMPLETE
    
```

Bild 2. Der Report über die Ergebnisse der Installation.

 **Wenn Sie eine Version des Programms für Linux installieren,**

1. Melden Sie sich als Benutzer **root** beim System an und installieren Sie mit Hilfe des Skripts **install** den Antiviren-Kern **KAVDaemon für Linux**, der sich in dem von Ihnen bei der Installation gewählten Ordner befindet (**Ordner zur Installation**).
2. Führen Sie einen Neustart des Servers durch.

 **Der Schlüssel muss manuell in den gleichen Ordner kopiert werden, in den der Kern installiert wurde. Sollte das Programm während des Kopierens des Schlüssels bereits gestartet worden sein, dann muss das Modul **kavscan** entfernt und erneut geladen werden, damit der Kern den Schlüssel findet.**

3. Funktionsschema von Kaspersky Anti-Virus für Lotus Notes/Domino

Funktionsschema des Programms. Beschreibung der einzelnen Module des Programms: Scan, Hook und Scheduler. Interaktion der Module. Datenbanken.

Das Programm Kaspersky Anti-Virus für Lotus Notes/Domino dient dem Schutz von Mail-Nachrichten für Lotus Notes/Domino der Version 5.02 und höher. Nach der Installation auf einem Linux oder Windows NT Server, auf dem das System Lotus Notes/Domino installiert ist, überprüft das Programm alle Mail-Nachrichten für Lotus Notes/Domino auf das Vorhandensein von Viren. Das Programm verwendet bei seinem Betrieb die *Parameter für den Antivirenschutz* (s. Kap. 5), die von einem Administrator, der über das Kennwort für den Zugriff auf die Parameter verfügt, von jedem beliebigen Computer eines lokalen Netzwerks aus geändert werden können.

Das Programm Kaspersky Anti-Virus besteht aus folgenden Modulen:

- **Hook** – Modul zum Abfangen von Mail-Nachrichten;

- **Scan** – Modul zur Überprüfung von Mail-Nachrichten;
- **Scheduler** – Modul zur Überprüfung von Datenbanken des Domino Servers.

Unten werden die Namen der ausführbaren Module von Kaspersky Anti-Virus für Lotus Notes/Domino für die Betriebssysteme Windows NT/2000 und Linux, sowie die in diesem Handbuch für die Module verwendeten Bezeichnungen genannt.

Modul	Name des Moduls für das Betriebssystem Windows NT/2000	Name des Moduls für das Betriebssystem Linux	Bezeichnung des Moduls im vorliegenden Handbuch
Modul zum Abfangen von Mail-Nachrichten	<i>nKavHook.dll</i>	<i>libkavhook.so</i>	Hook
Modul zur Überprüfung von Mail-Nachrichten	<i>nKavScan.exe</i>	<i>kavscan</i>	Scan
Modul zur Überprüfung von Datenbanken	<i>nKavScheduler.exe</i>	<i>kavscheduler</i>	Scheduler

Das Programm benutzt während seines Betriebs außerdem bestimmte Datenbanken, die auf der Festplatte des Servers gespeichert werden:

- die Konfigurationsdatenbank (s. Kapitel 5).
- die Analyse-Datenbank (s. Pkt. 7.2).
- die Quarantäne-Datenbank für Mails und für Dokumente (s. Pkte. 7.3.2, 7.3.3).
- Ereignisjournal (s. Pkt. 7.4).

Das Modul **Hook** und die Analysemodule **Scan** und **Scheduler** werden beim Start des Domino Servers automatisch gestartet (wenn in der Konfigurationsdatei *notes.ini* die entsprechenden Einstellungen vorgenommen wurden²). Diese Vorgänge werden im Ereignisjournal durch betreffende Zeilen vermerkt (zu Einzelheiten s. Pkt. 7.4).

Nach dem Start fängt das Modul **Hook** alle Nachrichten ab, die durch den Domino Server in Mailboxen (Dateien mail*.box) abgelegt werden, und leitet sie an die Analyse-Datenbank weiter (zu Einzelheiten s. Pkt. 7.2).

Das Modul **Scan** überprüft alle Nachrichten aus der Analyse-Datenbank auf das Vorhandensein von Viren und bearbeitet diese Nachrichten entsprechend der in der Konfigurationsdatenbank eingestellten Parameter für den Antivirenschutz (zu Einzelheiten s. Kapitel 5). Das Modul kann beispielsweise alle infizierten Objekte desinfizieren und jene Objekte, deren Reparatur nicht gelungen ist, in die Quarantäne-Datenbank verschieben. Außerdem teilt das Modul **Scan** seine Aktionen an die Konsole des Servers und an das Ereignisjournal mit, wenn in der Konfigurationsdatenbank die entsprechenden Einstellungen vorgenommen wurden.

Das Modul **Scheduler** überprüft alle Datenbanken des Domino Servers und bearbeitet sie entsprechend der eingestellten Parameter für den Antivirenschutz. Alle Funktionen und Aktionen dieses Moduls entsprechen den Funktionen des Moduls **Scan**, mit dem einzigen Unterschied, dass es sich nicht auf die Mail-Nachrichten, sondern auf die Datenbanken des Servers bezieht.

Der Start der Module auf dem Server kann mit Hilfe des Client Lotus Notes oder jedes anderen WEB-Browsers (s. Pkt. 4.1) vom Server oder von einem anderen Computer aus vorgenommen werden, der an ein lokales Netzwerk angeschlossen ist oder über Remote-Zugriff auf den Server mit dem Protokoll TCP/IP verfügt.

² Das Modul **Hook** ist implementiert als Task für Domino/Notes Extension Manager. Bei der Installation von Kaspersky Anti-Virus für Lotus/Notes wird in der Datei *notes.ini* zum Namen dieses Moduls der Parameter `EXTMGR_ADDINS` hinzugefügt. Die Module **Scan** und **Scheduler** sind implementiert als Servertasks für Lotus Domino. Bei der Installation von Kaspersky Anti-Virus für Lotus/Notes wird in der Datei *notes.ini* zu den Namen dieser Module der Parameter `SERVERTASKS` hinzugefügt.

Bei einer Änderung der Einstellungen der Module arbeiten Hook, Scan und Scheduler schon eine Minute nach dem Speichern der Änderung in der Konfigurationsdatenbank mit den neuen Werten für die Parameter.

4. Vorbereitungen für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino

4.1. Reihenfolge der Vorbereitungen für den Betrieb

Beschreibung der für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino notwendigen Vorbereitungen.

Zur Vorbereitung von Kaspersky Anti-Virus für Lotus Notes/Domino auf den Betrieb sind nacheinander folgende Aktionen durchzuführen:

1. Öffnen der Konfigurations-, Analyse- und Quarantäne-Datenbanken des Programms (zu Einzelheiten s. Pkt. 4.2);

2. Autorisation zum Zugriff auf die Konfigurations-, Analyse- und Quarantäne-Datenbanken für die Mitarbeiter, die den Antivirenschutzprozess der Mail für Lotus Domino verwalten werden (zu Einzelheiten s. Pkt. 4.3).

Nach dem Ausführen der oben genannten Aktionen können Sie dazu übergehen, mit Hilfe der Konfigurationsdatenbank die Funktionen von Kaspersky Anti-Virus für Lotus Notes/Domino zu konfigurieren (zu Einzelheiten s. Kapitel 5).

4.2. Öffnen der Datenbanken

Öffnen der Konfigurations-, Analyse- und Quarantäne-Datenbanken mit Hilfe eines Web-Browsers und des Programms Lotus Notes Client.

Die Reihenfolge der Aktionen zum Öffnen der einzelnen Datenbanken sind absolut identisch. Der einzige Unterschied besteht in der Auswahl der jeweiligen Datenbank. Alle drei Datenbanken müssen geöffnet werden.

Das Öffnen der Konfigurations-, Analyse- und Quarantäne-Datenbanken kann auf zwei Arten durchgeführt werden: mit Hilfe eines Web-Browsers oder mit Hilfe des Programms Lotus Notes Client.



Um eine Datenbank mit Hilfe eines Web-Browsers zu öffnen,

1. Starten Sie den Web-Browser.
2. Geben Sie folgende Adresse ein
[http://\[Servername\]/\[Ordner_KAV\]/kav_domcc.nsf](http://[Servername]/[Ordner_KAV]/kav_domcc.nsf), wobei:
 - **Servername** – die Bezeichnung des Servers, auf dem Kaspersky Anti-Virus für Lotus Notes/Domino installiert wurde;

- **Ordner_KAV** – der Ordner, in den er installiert wurde.
3. Geben Sie im Dialogfenster zur Kennwortabfrage den Namen und das Kennwort des Administrators ein, der über Manager-Zugriffsrechte für alle Datenbanken des Programms Kaspersky Anti-Virus für Lotus Notes/Domino verfügt.
 4. Klicken Sie auf die Schaltfläche **OK**.

 **Um eine Datenbank mit Hilfe des Programms Lotus Notes Client zu öffnen,**

1. Starten Sie Lotus Notes Client.
2. Geben Sie in dem erscheinenden Fenster zur Kennwortabfrage Ihre Kennwort für den Zugriff ein und klicken Sie auf die Schaltfläche **OK**.
3. Wählen Sie im Menü **File** den Befehl **Database**, und wählen Sie dann aus erscheinenden Liste den Befehl **Open...** Dadurch wird das Fenster **Open Database** (s. Bild 4) geöffnet.
4. Geben Sie den Namen des Servers, auf dem **Kaspersky Anti-Virus für Lotus Notes/Domino** installiert wurde, im Eingabefeld Server ein oder wählen Sie ihn aus der Dropdown-Liste aus.

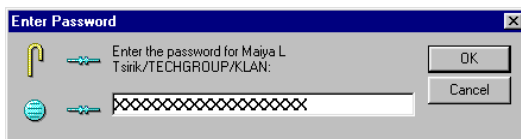


Bild 3. Das Dialogfenster zur Kennwortabfrage

5. Wählen Sie in der Liste **Database** den Ordner des Servers aus, auf den **Kaspersky Anti-Virus für Lotus Notes/Domino** installiert wurde. Wählen Sie aus dem Ordner die Bezeichnung der Datenbank aus, die Sie öffnen

wollen. Die Datenbanken sind unbedingt in folgender Reihenfolge zu öffnen:

- **Kaspersky AntiVirus for Lotus Notes Control Centre** – Konfigurationsdatenbank.
- **Kaspersky AntiVirus for Lotus Notes Capture Database** – Analyse-Datenbank.
- **Kaspersky AntiVirus for Lotus Notes Quarantined Database** – Quarantäne-Datenbank.

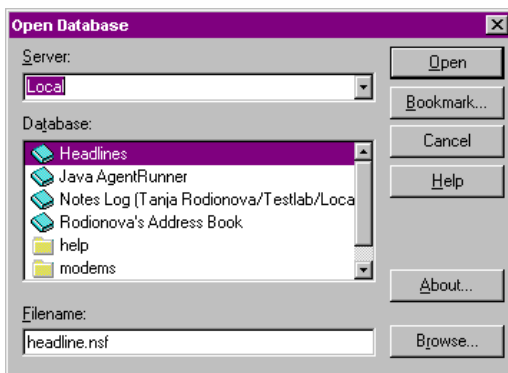


Bild 4. Auswahl einer Datenbank

- ☞ Wenn Sie den Client für Lotus Notes von dem Server aus starten, auf dem Kaspersky Anti-Virus für Lotus Notes/Domino installiert wurde, dann wird beim Versuch, die Konfigurationsdatenbank zu öffnen, das Dialogfenster **Choose Servers to Search** geöffnet. In diesem Fenster wird Ihnen die Auswahl des Servers angeboten, auf dem die Datenbanken gesucht werden sollen. Markieren Sie die Bezeichnung des Servers, auf dem das Programm installiert wurde, und klicken Sie auf die Schaltfläche **OK**.

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

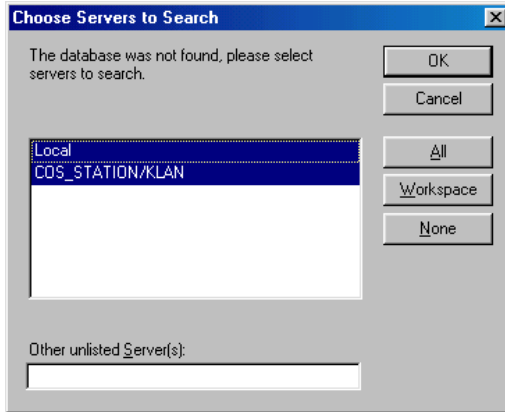


Bild 5. Auswahl des Servers

Als Ergebnis werden auf der Registerkarte **Workspace** Verknüpfungssymbole für die Konfigurations-, Analyse- und Quarantäne-Datenbanken hinzugefügt (s. Bild 6).

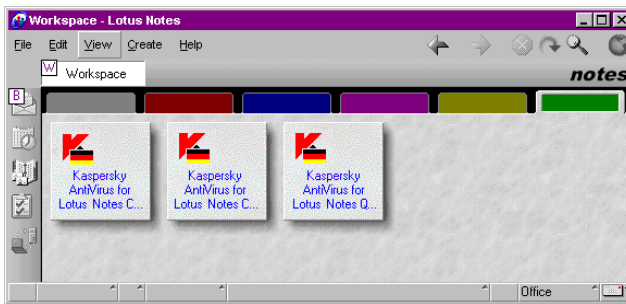


Bild 6. Der Arbeitsplatz
von Kaspersky Anti-Virus für Lotus Notes/Domino

4.3. Autorisation zum Zugriff auf die Datenbanken

Autorisation zum Zugriff für die Arbeit mit den Konfigurations-, Analyse- und Quarantäne-Datenbanken.

Die Vorbereitungen auf den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino schließen das Erteilen des Zugriffs auf das Programm sowie auf die Quarantäne- und Analyse-Datenbank für jene Mitarbeiter ein, die den Prozess zum Antivirenschutz der Mail für Lotus Domino verwalten werden.

Das Hinzufügen eines neuen Administrators und die Definition seiner Rechte werden im Fenster **Access Control List** durchgeführt.



Um in das Fenster Access Control List zu wechseln,

1. Klicken Sie mit der rechten Maustaste auf das Verknüpfungssymbol einer Datenbank.
2. Zeigen Sie in der erscheinenden Liste (s. Bild 7) auf den Punkt **Database**.
3. Wählen Sie im erscheinenden Menü den Punkt **Access Control...**

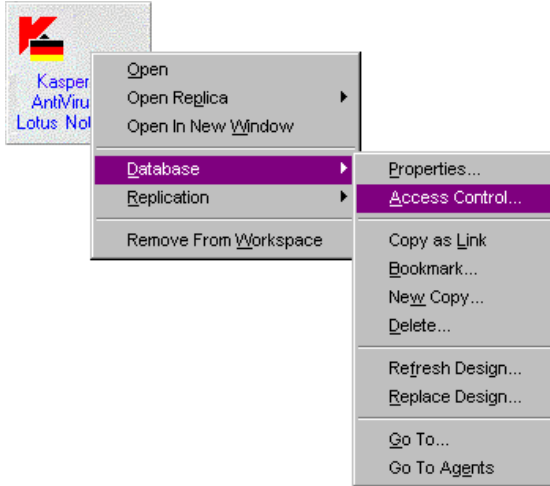


Bild 7. Der Weg zum Fenster **Access Control List**

Als Ergebnis wird das Fenster **Access Control List** (s. Bild 8) geöffnet, in dem die Konfiguration der Administratorenliste und ihrer Rechte vorgenommen wird.

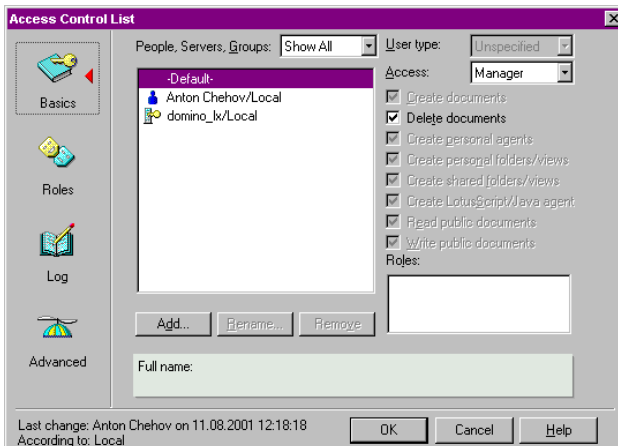



Bild 8. Das Fenster **Access Control List**

Nachdem die Zugriffsrechte für die Arbeit mit den Datenbanken von Kaspersky Anti-Virus für Lotus Notes/Domino erteilt wurden, kann eine beliebige Datenbank geöffnet werden, indem zweimal mit der linken Maustaste auf ihr Verknüpfungssymbol geklickt wird. Die Datenbank steht dann für die Arbeit zur Verfügung.

Die Analyse- und die Quarantäne-Datenbank können sowohl aus dem Arbeitsplatz (**Workspace**) von **Kaspersky Anti-Virus für Lotus Notes/Domino**, als auch aus der Konfigurationsdatenbank geöffnet werden (s. Pkte. 7.2-7.3).

 Die Reihenfolge der Arbeitsschritte für die Analyse- und die Quarantäne-Datenbank ist einheitlich, mit Ausnahme der Art wie sie geöffnet werden. In diesem Handbuch wird das Vorgehen zur Arbeit mit den Datenbanken von der Konfigurationsdatenbank aus beschrieben.

4.4. Benutzeroberfläche der Konfigurationsdatenbank

Beschreibung der Benutzeroberfläche der Konfigurationsdatenbank.

 **Um die Konfigurationsdatenbank zu öffnen,**

klicken Sie mit der linken Maustaste zweimal auf das Verknüpfungssystembol der Konfigurationsdatenbank.

Dadurch wird das Fenster der Konfigurationsdatenbank geöffnet, das in zwei Rahmen unterteilt ist (s. Bild 9).

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

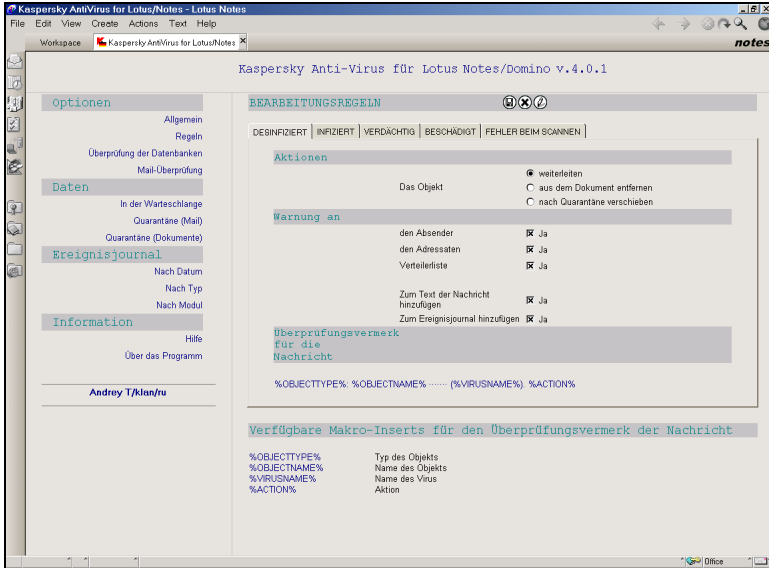


Bild 9. Gesamtansicht des Fensters der Konfigurationsdatenbank

Im linken Rahmen befinden sich folgende Abschnitte:

- **Optionen** – die Parameter für die Funktionen des Programms.
- **Daten** – eine Liste der Dokumente, die sich in der Warteschlange für die Überprüfung (Analyse-Datenbank) befinden, sowie die Quarantäne-Datenbanken für Nachrichten und Dokumente.
- **Ereignisjournal** – alle Aufzeichnungen, die über die Ergebnisse der Programmaktionen gemacht werden, geordnet nach Erstellungsdatum, Informationstyp und Modul.
- **Information** – allgemeine Informationen über das Programm und Hilfesystem.

Der rechte Rahmen wird entsprechend der Auswahl von Parametern im linken Rahmen aktualisiert.

4.5. Hilfesystem

Hilfesystem und Methoden zur Navigation im Hilfesystem.

Bei der Arbeit mit dem Programm Kaspersky Anti-Virus für Lotus Notes/Domino steht Ihnen dessen *Hilfesystem* zur Verfügung.

☞ **Um das Hilfesystem der Konfigurationsdatenbank aufzurufen,**

verwenden Sie den Hyperlink **Hilfe**, der sich im Abschnitt **Information** im linken Rahmen des Fensters der Konfigurationsdatenbank befindet. Dadurch wird das Fenster des Hilfesystems geöffnet (s. Bild 10).

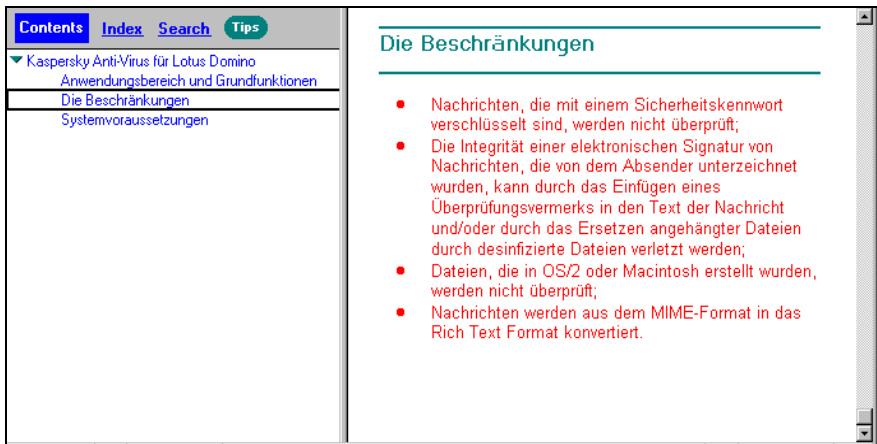


Bild 10. Das Hilfesystem

Das Fenster des Hilfesystems ist in zwei Rahmen unterteilt. Im oberen Teil des linken Rahmens befinden sich die Schaltflächen, mit deren Hilfe Sie im rechten Rahmen die Informationen des Hilfesystems durchsuchen können:

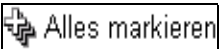

- **Contents** – Anzeige des Inhaltsverzeichnisses für das Hilfesystem;
- **Index** – Suche von Informationen mit dem Index;
- **Search** – Suche von Informationen nach Schlüsselbegriffen;
- **Tips** – Anzeige von Tipps zur Verwendung des Programms.

Die Navigation wird im Hilfesystem auf die für Hypertext-Dokumente übliche Art vorgenommen.

4.6. Terminologie



Grundlegende Begriffe, die in diesem Handbuch verwendet werden.

Zur Bezeichnung von Elementen der Benutzeroberfläche wird in diesem Handbuch die in der folgenden Tabelle aufgeführte Terminologie verwendet. Das sich die Benutzeroberfläche der Konfigurationsdatenbank je nachdem unterscheidet, ob sie mit Hilfe des Programms Lotus Notes Client oder mit Hilfe eines Web-Browsers geöffnet wird, sind in der Tabelle die wichtigsten Unterschiede der Elemente der Benutzeroberfläche angegeben³.

Element der Benutzeroberfläche	Bezeichnung
	Schaltfläche.
	Eingabefeld in Lotus Notes Client und im Web-Browser.

³ Im Folgenden werden in diesem Handbuch die Bilder der Benutzeroberfläche für die Konfigurationsdatenbank gezeigt, die mit Hilfe von Lotus Notes Client geöffnet wurde.

VORBEREITUNGEN FÜR DEN PROGRAMMBETRIEB

Element der Benutzeroberfläche	Bezeichnung						
	Auswahlknopf.						
	Kontrollkästchen.						
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Absender</th> <th style="text-align: left;">Adressaten</th> <th style="text-align: left;">Betreff</th> </tr> </thead> <tbody> <tr> <td>Server Administrator/klan/ru</td> <td>Tatyana Rodionova/tech/klan/ru@klan</td> <td>EICAR-TEST-FILE</td> </tr> </tbody> </table>	Absender	Adressaten	Betreff	Server Administrator/klan/ru	Tatyana Rodionova/tech/klan/ru@klan	EICAR-TEST-FILE	Tabelle mit Dropdown-Liste.
Absender	Adressaten	Betreff					
Server Administrator/klan/ru	Tatyana Rodionova/tech/klan/ru@klan	EICAR-TEST-FILE					

5. Konfiguration der Parameter für den Antivirenschutz

5.1. Prinzipien für die Konfiguration des Programms

Beschreibung der Prinzipien für die Konfiguration des Programms.

Alle ein- und ausgehenden Mail-Nachrichten des Domino Servers werden von dem Modul Scan, und die Dateien der Server-Datenbanken von dem Modul Scheduler gescannt und bearbeitet. Dabei verwenden beide Programme die Parameter für den Antivirenschutz. Diese Parameter befinden sich im Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) und sind in folgende Gruppen unterteilt:

- **Allgemein** – eine Reihe allgemeiner Einstellungen, durch die der Ort des Ordners für die temporären Dateien, die Adressenliste zur Verteilung von Benachrichtigungen, sowie die internen Datenbanken des Servers festgelegt werden.

- **Regeln** – eine Auswahl von Parametern, die für die Module Scan und Scheduler die Bearbeitungsregeln für infizierte, verdächtige, beschädigte und desinfizierte Objekte, sowie für Objekte, bei deren Scannen ein Fehler verursacht wird, festlegen.
- **Überprüfung der Datenbanken** – eine Reihe von Parametern, durch die die Häufigkeit der Untersuchung von Server-Datenbanken durch das Modul Scheduler, sowie der Typ der zu scannenden Objekte und andere Parameter festgelegt werden.
- **Mail-Überprüfung** – eine Auswahl von Parametern, die die zu scannenden Objekte und andere von dem Modul Scan verwendete Parameter für die Virussuche in Mail-Nachrichten festlegen.

Die Bezeichnung jeder Parameter-Gruppe besitzt die Form eines Hyperlinks, durch dessen Anklicken Sie im rechten Rahmen das Fenster mit einer entsprechenden Auswahl von Parametern öffnen können.


Zur Vereinfachung wird in diesem Handbuch in der Bezeichnung jedes Abschnitts, der ein bestimmtes Fenster beschreibt, die Angabe des Wegs zu diesem Fenster genannt. Der Abschnitt, der die Beschreibung der allgemeinen Optionen für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino enthält, hat zum Beispiel folgendes Aussehen:





Allgemeine Optionen für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino. Optionen → Allgemein,

wobei: **Optionen → Allgemein** – der Weg zum Fenster, in dem sich die entsprechenden Parameter befinden (**Optionen** – der Abschnitt im linken Rahmen des Fensters der Konfigurationsdatenbank, **Allgemein** – der Hyperlink des Abschnitts, mit dessen Hilfe das Fenster im rechten Rahmen geöffnet werden kann).

In jedem Fenster kann die Konfiguration der Parameter auf eine der folgenden Arten vorgenommen werden:

- Wenn zur Konfiguration eines Parameters die Eingabe eines Werts notwendig ist, dann wird der betreffende Wert in einem

Eingabefeld angegeben (im Redaktionsmodus besitzt das Feld folgendes Aussehen: )

- Wenn die Konfiguration eines Parameters die Auswahl bestimmter Varianten zulässt, dann wird diese Auswahl mit Hilfe des Auswahlknopfs , oder mit Hilfe eines Hyperlinks, der rechts vom Auswahlknopf angebracht ist, durchgeführt. Zum Beispiel:  **weiterleiten**.
- Wenn ein Parameter das Aktivieren eines bestimmten Modus festlegt, dann kann dieser aktiviert werden, indem mit Hilfe der linken Maustaste das Kontrollkästchen  aktiviert wird oder der Hyperlink, der rechts von dem Kontrollkästchen angebracht ist, verwendet wird. Zum Beispiel:  **Ja**. Das Deaktivieren eines Modus wird analog zum Aktivieren durchgeführt.

Außer den Parametern befinden sich folgende Schaltflächen in den Fenstern:



– Speichern der vorgenommenen Einstellungen.



– Zurückgehen in das vorhergehende Fenster der Konfigurationsdatenbank.



Wenn Sie zur Arbeit mit der Konfigurationsdatenbank den Client für Lotus Notes verwenden, dann wird nach dem Klicken auf diese Schaltfläche ein Dialogfenster geöffnet, das Ihnen die Wahl zwischen dem Abbrechen ohne Speichern der vorgenommenen Änderungen und dem Speichern der vorgenommenen Einstellungen stellt.



– Öffnen des aktuellen Fensters im Redaktionsmodus zum Ändern von Parametern.



In der Grundeinstellung werden alle Fenster des Abschnitts **Optionen** der Konfigurationsdatenbank im Ansichtsmodus geöffnet. Deshalb ist zum Ändern von Parametern dieser Fenster das Aktivieren des Redaktionsmodus durch Klicken dieser Schaltfläche notwendig.

5.2. Allgemeine Optionen für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino. Optionen → Allgemein

Beschreibung der allgemeinen Optionen von Kaspersky Anti-Virus für Lotus Notes/Domino

Das Fenster **ALLGEMEINE OPTIONEN** (s. Bild 11) umfasst generelle Parameter für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino, die sich auf folgenden Registerkarten befinden:

- **ORDNER** – der vollständige Pfad des Ordners für die temporären Dateien, der von Kaspersky Anti-Virus für Lotus Notes/Domino beim Scannen verwendet wird;
- **LISTEN** – eine Liste der Benutzeradressen für das Versenden von Benachrichtigungen;
- **DATENBANKEN** – die Bezeichnung der internen (Analyse-) Datenbank des Servers.

In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit dem Hyperlink **Allgemein** wechseln.




Für den Betrieb von Kaspersky Anti-Virus für Lotus Notes/Domino sind folgende Einstellungen für die allgemeinen Parameter vorzunehmen:

1. Geben Sie auf der Registerkarte **ORDNER** im Eingabefeld für den Parameter **Temporärer** den vollständigen Pfad des Ordners für die temporären Dateien an.

- Bitte beachten Sie, dass nach dem Namen des temporären Ordners das Zeichen "\" zu setzen ist.



Bild 11. Die Registerkarte **ORDNER** des Fensters **ALLGEMEINE OPTIONEN**.

- Geben Sie auf der Registerkarte **LISTEN** (s. Bild 12) im Eingabefeld des Parameters **Benachrichtigung** die Namensliste der Benutzer an, an die Mitteilungen über den Fund infizierter, verdächtiger, beschädigter und desinfizierter Objekte, sowie solcher Objekte, bei deren Scannen ein Fehler verursacht wurde, gesendet werden sollen, wenn die entsprechenden Einstellungen vorgenommen wurden. Diese Liste wird im Fenster **Names** erstellt, das mit der Schaltfläche  geöffnet wird, die rechts vom Eingabefeld für diesen Parameter angebracht ist.

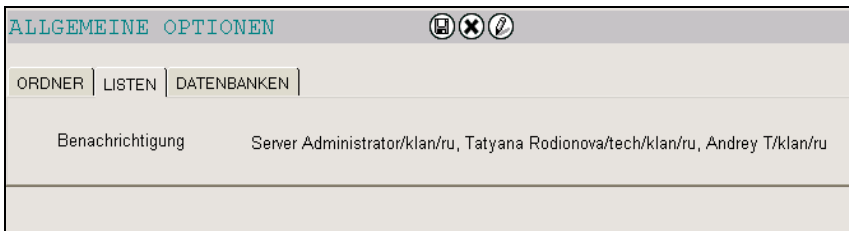


Bild 12. Die Registerkarte **LISTEN** des Fensters **ALLGEMEINE OPTIONEN**

3. Geben Sie auf der Registerkarte **DATENBANKEN** (s. Bild 13) im Eingabefeld für den Parameter **Interne** den vollständigen Namen der Analyse-Datenbank ein.

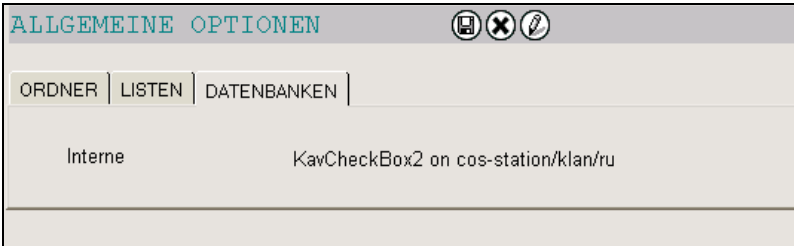


Bild 13. Die Registerkarte **DATENBANKEN** des Fensters **ALLGEMEINE OPTIONEN**

5.3. Parameter für das Scannen von Datenbanken.

Optionen → Überprüfung der Datenbanken

*Beschreibung der Konfiguration der Parameter für das
Scannen von Datenbanken des Domino Servers.*

5.3.1. Allgemeine Informationen zur Überprüfung von Datenbanken

Für das Scannen von Dateien der Datenbanken des Domino Servers verwendet das Modul Scheduler die Parameter, die vom Benutzer im Fenster **ÜBERPRÜFUNG DER DATENBANKEN** (s. Bild 14) festgelegt werden. In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks Überprüfung der Datenbanken wechseln.

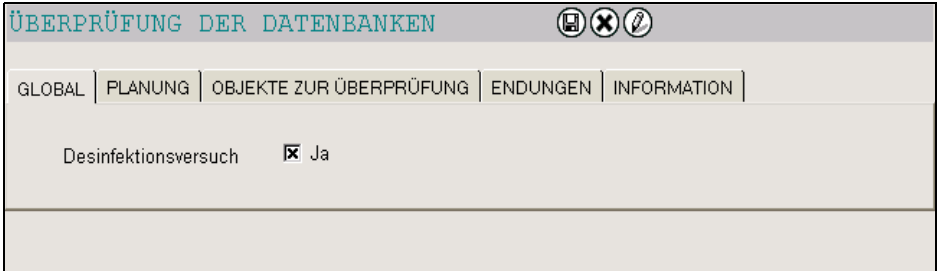


Bild 14. Die Registerkarte **GLOBAL** des Fensters **ÜBERPRÜFUNG DER DATENBANKEN**

Bei der Konfiguration der Parameter für das Scannen von Datenbanken stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Aktivieren des Modus zur Desinfektion infizierter Objekte der Datenbanken (s. Pkt. 5.3.2).
- Planung der Häufigkeit des Scannens und Liste einer Maske für die Datenbanken (s. Pkt. 5.3.3).
- Festlegen der Typen der zu scannenden Objekte (s. Pkt. 5.3.4).
- Konfiguration zusätzlicher Parameter für das Scannen von Anlagen der Datenbanken (s. Pkt. 5.3.5).
- Anzeige der Daten über die letzte und nächste Überprüfung, und Auftrag zur Überprüfung von Datenbanken innerhalb von einer Minute (s. Pkt. 5.3.6).

5.3.2. Desinfektion von infizierten Objekten der Datenbanken. Registerkarte GLOBAL

Auf der Registerkarte **GLOBAL** (s. Bild 14) können Sie den Modus zur Desinfektion infizierter Objekte, die beim Scannen der Datenbanken des Domino Servers gefunden werden, aktivieren (deaktivieren).

☞ Um den Modus zur Desinfektion infizierter Objekte, die beim Scannen der Datenbanken gefunden werden, zu aktivieren,

aktivieren Sie das Kontrollkästchen Ja für den Parameter **Desinfektionsversuch**.

Der Modus zur Desinfektion wird deaktiviert, indem das Kontrollkästchen Ja deaktiviert wird.

5.3.3. Planung der Überprüfung von Datenbanken. Registerkarte **PLANUNG**

Auf der Registerkarte **PLANUNG** (s. Bild 15) können Sie den Ablauf des Scannens von Datenbanken des Domino Servers, sowie eine Liste von Datenbanken, die gescannt werden oder unbedingt vom Scannen ausgeschlossen werden sollen, festlegen.

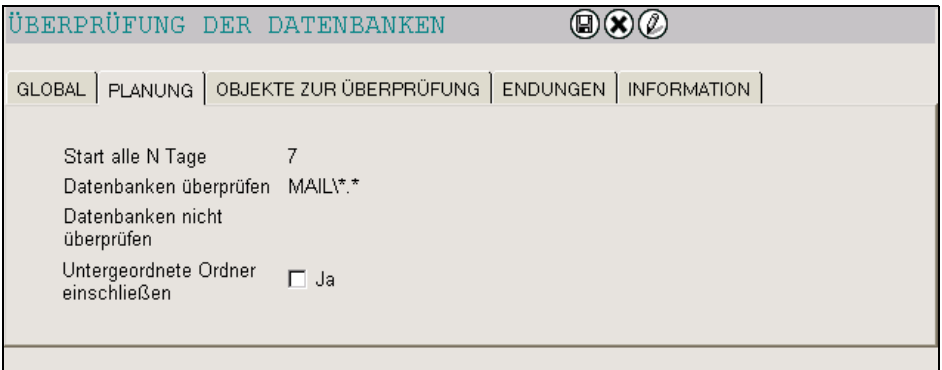




Bild 15. Die Registerkarte **PLANUNG** des Fensters **ÜBERPRÜFUNG DER DATENBANKEN**

 **Planen Sie den Ablauf des Scannens der Datenbanken, indem Sie die Werte für folgende Parameter festlegen:**

1. **Start alle N Tage** – der Zeitraum (Anzahl in Tagen, von 1 bis 365) zwischen dem Durchführen des Scannens von Datenbanken des Servers. Das Datum des nächsten Scannens, das auf der Registerkarte **INFORMATION** angezeigt wird, wird nach dem Festlegen dieses Parameters automatisch korrigiert.
2. **Datenbanken überprüfen** – die Liste der Masken für die Datenbanken, die zum Scannen vorgesehen sind. Die Elemente der Liste werden durch das Zeichen ";" getrennt.

 Hierbei geht es um die Datenbanken, die sich im Ordner **D:\Lotus\Domino\Data** befinden. Wird also die Maske ***.*** angegeben, dann werden dadurch alle Verzeichnisse bezeichnet, die sich im Ordner **D:\Lotus\Domino\Data** befinden.

3. **Datenbanken nicht überprüfen** – die Liste der Masken für die Datenbanken, die vom Scannen auszuschließen sind. Die Elemente der Liste werden durch das Zeichen ";" getrennt.
4. **Untergeordnete Ordner einschließen** – Modus zur Überprüfung von untergeordneten Ordnern der Datenbanken. Sie können diesen Modus aktivieren, indem Sie das Kontrollkästchen **Ja** gegenüber dem entsprechenden Parameter aktivieren.

5.3.4. Zu scannende Datenbank- Objekte. Registerkarte **OBJEKTE** ZUR ÜBERPRÜFUNG

Auf der Registerkarte **OBJEKTE ZUR ÜBERPRÜFUNG** (s. Bild 16) können Sie die Typen der Datenbank-Objekte angeben, die auf das Vorhandensein von Viren überprüft werden sollen.



Geben Sie die Typen der Datenbank-Objekte an, die auf das Vorhandensein von Viren überprüft werden sollen,

indem Sie das Kontrollkästchen **Ja** gegenüber der folgenden Parameter aktivieren:

- **Anlagen** – Scannen von angehängten Dateien der Datenbanken. In der Grundeinstellung werden alle angehängten Dateien auf das Vorhandensein von Viren überprüft.



Auf der Registerkarte **ENDUNGEN** können Sie mit Hilfe des Parameters **Maske** die Typen der zu scannenden Anlagen angeben, oder bestimmte Typen angehängter Dateien vom Scannen ausschließen, die mit Hilfe des Parameters **Ausschlussmaske** festgelegt werden (zu Einzelheiten über diese Parameter s. Pkt. 5.3.5).

- **OLE-Objekte** – Überprüfen von angehängten OLE-Objekten in den Datenbanken auf das Vorhandensein von Viren.
- **Rich Text Feld** – Scannen von Feldern im Format Rich Text.
- **Skripts** – Überprüfen von Server-Datenbanken der Typen LotusScript und JavaScript auf das Vorhandensein von Viren.
- **Bibliotheken** – Überprüfen von Bibliotheken der Datenbanken auf das Vorhandensein von Viren.

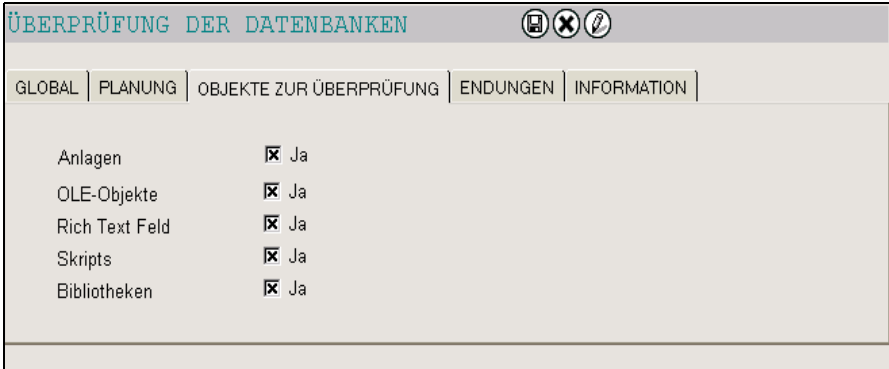


Bild 16. Die Registerkarte **OBJEKTE ZUR ÜBERPRÜFUNG** des Fensters **ÜBERPRÜFUNG DER DATENBANKEN**

5.3.5. Parameter für das Scannen von Anlagen. Registerkarte **ENDUNGEN**

Auf der Registerkarte **ENDUNGEN** (s. Bild 17) können Sie die Typen der Anlagen von Datenbanken festlegen, die auf das Vorhandensein von Viren überprüft werden oder vom Scannen ausgeschlossen werden sollen.



Nehmen Sie folgende Einstellungen für das Scannen von Anlagen der Datenbanken des Servers vor:

- **Überprüfung der Anlagen** – Überprüfung von angehängten Dateien der Datenbanken auf eine der folgenden Arten (dieser Parameter ist nur dann aktuell, wenn der Modus zur Überprüfung der Anlagen aktiviert wurde):
 - **Alle** – Überprüfen aller angehängten Dateien der Datenbanken. Bei Auswahl dieses Werts können Sie eine Reihe von Masken für angehängte Dateien festlegen, die vom

Scannen ausgeschlossen werden sollen. Die Masken werden im Eingabefeld des Parameters **Ausschlussmaske** festgelegt.

● **Nach Maske** – Überprüfen der angehängten Dateien, deren Masken den im Eingabefeld des Parameters **Maske** aufgezählten entsprechen.

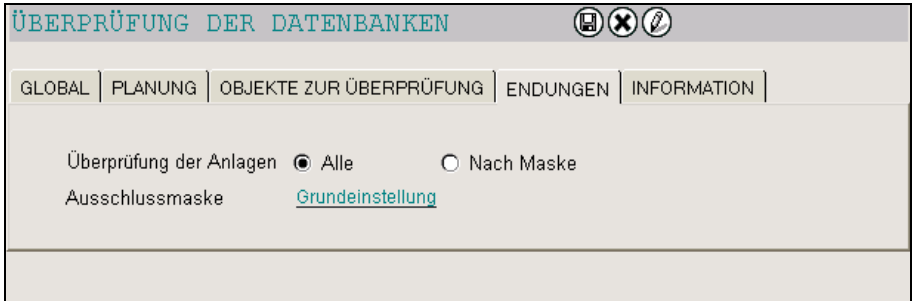


Bild 17. Die Registerkarte **ENDUNGEN** des Fensters **ÜBERPRÜFUNG DER DATENBANKEN**

- **Ausschlussmaske/Maske** – die Liste der Masken für angehängte Dateien, die vom Scannen ausgeschlossen werden sollen. In der Grundeinstellung sind im Eingabefeld dieses Parameters die Masken *.TXT und *.DBF / *.COM; *.EXE; *.DLL; *.DOC und *.XLS angegeben. Falls Sie diese Liste geändert haben und die Grundeinstellung wiederherstellen möchten, dann verwenden Sie den Hyperlink **Grundeinstellung**, der rechts vom Eingabefeld angebracht ist. Die Masken werden durch das Zeichen ";" getrennt eingegeben.

5.3.6. Informationen über das Scannen. Starten der Überprüfung. Registerkarte INFORMATION

Auf der Registerkarte **INFORMATION** (s. Bild 18) können Sie die Informationen über das Datum der letzten und nächsten Überprüfung von Datenbanken des Domino Servers einsehen, und das Scannen starten.



Bild 18. Die Registerkarte **INFORMATION** des Fensters **ÜBERPRÜFUNG DER DATENBANKEN**

Das Datum der nächsten Überprüfung wird nach einer Änderung des Parameters **Start alle N Tage** auf der Registerkarte **PLANUNG** (s. Pkt. 5.3.3) automatisch korrigiert.



Um das Scannen der Datenbanken mit den gewählten Parametern zu starten,

klicken Sie auf die Schaltfläche

Überprüfung durchführen

Innerhalb von einer Minute wird mit der Überprüfung begonnen. Solange die Überprüfung noch nicht begonnen hat, wird im unteren Teil des Fensters der Hinweis **Anfrage wurde gesendet** angezeigt und die

Schaltfläche **Überprüfung durchführen** wird durch die Schaltfläche **Anfrage verwerfen** (s. Bild 19) ersetzt. Durch das Klicken auf diese Schaltfläche können Sie die Anfrage auf Überprüfung der Datenbanken des Servers verwerfen.

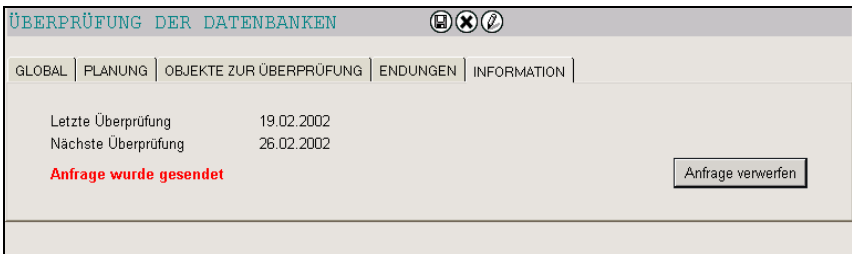


Bild 19. Starten der Überprüfung der Datenbanken

Wird mit der Überprüfung begonnen, dann werden ein Hinweis darüber und über die Ergebnisse der Überprüfung in das Ereignisjournal eingetragen.

5.4. Parameter für das Scannen von Mail-Nachrichten.

Optionen → Mail-Überprüfung

Beschreibung der Parameter für das Scannen von Mail-Nachrichten.

5.4.1. Allgemeine Informationen zur Überprüfung von Mails

Für das Scannen von Mail-Nachrichten des Domino Servers verwendet das Modul Scan die Parameter, die im Fenster **MAIL-ÜBERPRÜFUNG** (s. Bild 20) festgelegt werden. In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks **Mail-Überprüfung** wechseln.

Bei der Konfiguration der Parameter für das Scannen von Mail-Nachrichten stehen Ihnen folgende Möglichkeiten zur Verfügung:

- Aktivieren des Modus zur Desinfektion infizierter Mail-Objekte (s. Pkt. 5.4.2).
- Festlegen der Typen der zu scannenden Objekte (s. Pkt. 5.4.3).
- Konfiguration zusätzlicher Parameter für das Scannen der Anlagen von Mail-Nachrichten (s. Pkt. 5.4.4).

Die Konfiguration der Parameter für das Scannen von Mail-Nachrichten kann in zwei Etappen unterteilt werden: Zuerst sind die Typen der zu scannenden Objekte festzulegen, danach die Parameter für das Scannen auszuwählen.



Bild 20. Die Parameter für Scannen von Mail-Nachrichten

5.4.2. Desinfektion von Mail-Nachrichten. Registerkarte GLOBAL

Auf der Registerkarte **GLOBAL** können Sie einen Modus zur Desinfektion infizierter Objekte, die beim Scannen von Mail-Nachrichten gefunden werden, aktivieren (deaktivieren). Die Regeln für das Aktivieren (Deaktivieren) dieses Modus entsprechen der Beschreibung in Pkt. 5.3.2.


5.4.3. Typen der zu scannenden Mail-Objekte. Registerkarte OBJEKTE ZUR ÜBERPRÜFUNG

Auf der Registerkarte **OBJEKTE ZUR ÜBERPRÜFUNG** (s. Bild 21) können Sie die Typen der Mail-Nachrichten angeben, die auf das Vorhandensein von Viren überprüft werden sollen.

 **Geben Sie die Typen der Mail-Objekte an, die auf das Vorhandensein von Viren überprüft werden sollen,**

indem Sie das Kontrollkästchen **Ja** gegenüber von folgenden Parametern aktivieren:

- **Anlagen** – Scannen von an Mail-Nachrichten angehängten Dateien. In der Grundeinstellung werden alle angehängten Dateien auf das Vorhandensein von Viren überprüft.

 Auf der Registerkarte **ENDUNGEN** können Sie mit Hilfe des Parameters **Maske** die Typen der zu scannenden Anlagen angeben, oder bestimmte Typen angehängter Dateien vom Scannen ausschließen, die mit Hilfe des Parameters **Ausschlussmaske** festgelegt werden (zu Einzelheiten über diese Parameters. Pkt. 5.4.4).

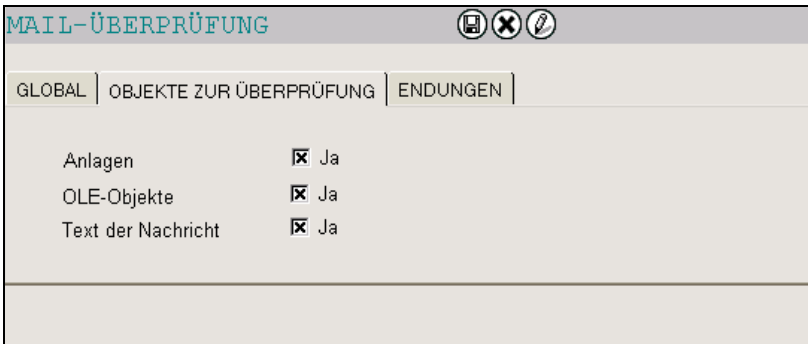



Bild 21. Die Registerkarte **OBJEKTE ZUR ÜBERPRÜFUNG** des Fensters **MAIL-ÜBERPRÜFUNG**

- **OLE-Objekte** – Überprüfen aller an Mail-Nachrichten angehängten OLE-Objekte auf das Vorhandensein von Viren.

 Wird Kaspersky Anti-Virus für Lotus Notes/Domino mit dem Betriebssystem Linux betrieben, dann werden OLE-Objekte nicht gescannt.

- **Text der Nachricht** – Scannen des Texts einer Mail-Nachricht.

5.4.4. Parameter für das Scannen von Anlagen. Registerkarte ENDUNGEN

Auf der Registerkarte **ENDUNGEN** können Sie die Typen der Anlagen von Mail-Nachrichten festlegen, die auf das Vorhandensein von Viren überprüft werden oder vom Scannen ausgeschlossen werden sollen. Die Liste der Anlage-Typen und die Konfiguration für deren Überprüfung entspricht der Beschreibung in Pkt. 5.3.5.

5.5. Bearbeitungsregeln für die zu scannenden Objekte.

Optionen → Regeln

*Beschreibung der Bearbeitung von zu scannenden Objekten (Mail-Nachrichten und Datenbanken).
Parameter für das Versenden von Benachrichtigungen,
für den Überprüfungsvermerk und für das
Ereignisjournal.*

5.5.1. Was ist ein zu scannendes Objekt?

Da Kaspersky Anti-Virus für Lotus Notes/Domino nicht nur das Scannen von Mail-Nachrichten, sondern auch die Untersuchung von Datenbanken des Domino Servers erlaubt, sind unter dem Begriff 'zu scannende Objekte' hier sowohl Objekte in Form von Mail-Nachrichten zu verstehen, die vom Modul Scan überprüft werden, als auch Dateien in Datenbanken, die vom Modul Scheduler gescannt werden.

Ein infiziertes Objekt kann sowohl eine an eine Mail-Nachricht angehängte Datei sein, als auch eine Datei in Form eines OLE-Objekts in einer Datenbank. Trotzdem werden auf diese Objekte die gleichen Einstellungen angewendet, die in der Konfigurationsdatenbank für infizierte Objekte festgelegt werden.

Die Bearbeitungsregeln für Objekte befinden sich im Fenster **BEARBEITUNGSREGELN** (s. Bild 22). In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks **Regeln** wechseln.

BEARBEITUNGSREGELN ⓘ ✕ 🗑

DESINFIZIERT | INFIZIERT | VERDÄCHTIG | BESCHÄDIGT | FEHLER BEIM SCANNEN

Aktionen

	<input checked="" type="radio"/> weiterleiten <input type="radio"/> aus dem Dokument entfernen <input type="radio"/> nach Quarantäne verschieben
Das Objekt	

Warnung an

den Absender	☑ Ja
den Adressaten	☑ Ja
Verteilerliste	☑ Ja
Zum Text der Nachricht hinzufügen	☑ Ja
Zum Ereignisjournal hinzufügen	☑ Ja

Überprüfungsvermerk für die Nachricht

%OBJECTTYPE%: %OBJECTNAME% (%VIRUSNAME%) %ACTION%

Verfügbare Makro-Inserts für den Überprüfungsvermerk der Nachricht

%OBJECTTYPE%	Typ des Objekts
%OBJECTNAME%	Name des Objekts
%VIRUSNAME%	Name des Virus
%ACTION%	Aktion

Bild 22. Die Parameter für die Bearbeitung von zu scannenden Objekten

Vor dem Festlegen von Parametern für die Bearbeitung eines zu scannenden Objekts müssen Sie den Typ des Objekts auswählen, für den die Einstellungen vorgenommen werden sollen (zu Einzelheiten s. Pkt. 5.5.2).

Für jeden gewählten Typ eines zu scannenden Objekts können Sie folgende Einstellungen vornehmen:

- Parameter für die Bearbeitung von zu scannenden Objekten (s. Pkt. 5.5.3).
- Parameter für das Versenden von Benachrichtigungen (s. Pkt. 5.5.4).
- Parameter für den Überprüfungsvermerk (s. Pkt. 5.5.5).

- Parameter für das Aufzeichnen des Ereignisjournals (s. Pkt. 5.5.6).

5.5.2. Auswahl der zu scannenden Objekte

Die Liste mit den Typen der zu scannenden Objekte und die Parameter für deren Bearbeitung befinden sich im Fenster **BEARBEITUNGSREGELN** (s. Bild 22). In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbanken (s. Bild 9) mit Hilfe des Hyperlinks **Regeln** wechseln.

Die Konfiguration von Parametern für das Scannen ist für folgende Objekt-Typen möglich:

- Desinfizierte Objekte (Registerkarte **DESINFIZIERT**).
- Infizierte Objekte (Registerkarte **INFIZIERT**).
- Verdächtige Objekte (Registerkarte **VERDÄCHTIG**).
- Beschädigte Objekte (Registerkarte **BESCHÄDIGT**).
- Objekte, bei deren Scannen ein Fehler verursacht wurde (Registerkarte **FEHLER BEIM SCANNEN**).

Alle Parameter für die Bearbeitung bestimmter Objekte, die zum Scannen vorgesehen sind, befinden sich auf den entsprechenden Registerkarten des Fensters **BEARBEITUNGSREGELN** (s. Bild 22). Die Parameter sind für alle Arten der Objekte einheitlich.

5.5.3. Parameter für die Bearbeitung von zu scannenden Objekten

Jeder Typ der zum Scannen vorgesehenen Objekte kann auf verschiedene Arten bearbeitet werden. Die Parameter für die Bearbeitung befinden sich

im Fenster **BEARBEITUNGSREGELN** (s. Bild 22). In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks **Regeln** wechseln.

Für jeden Typ der zu scannenden Objekte können Sie eine der folgenden Bearbeitungsarten wählen:

- **weiterleiten** – Weiterleiten der Objekte. Dieses Vorgehen wird für desinfizierte Objekte empfohlen. Es können aber Situationen eintreten, in denen dieses Vorgehen auch auf infizierte Objekte anwendbar ist (zu Einzelheiten s. Pkt. 5.6.5).
- **aus dem Dokument entfernen** – Löschen der Objekte. Diese Art der Bearbeitung von Objekten sollte nur dann gewählt werden, wenn Sie absolut sicher sind, dass das Löschen dieser Objekte nötig ist (s. Pkt. 5.6.4).
- **nach Quarantäne verschieben** – Verschieben der Objekte in die Quarantäne-Datenbank zur weiteren Bearbeitung. Diese Behandlungsart wird empfohlen für infizierte, verdächtige und beschädigte Objekte, und für Objekte, bei deren Scannen ein Fehler verursacht wird (s. Pkt. 5.6.2).

🔴 Das Verschieben eines Objekts in die Quarantäne-Datenbank bedeutet, dass das Objekt aus der Mail-Nachricht oder aus der Datenbank gelöscht und in eine Quarantäne-Datenbank verschoben wird.

Im Bezug auf Mail-Nachrichten gilt folgendes Vorgehen: Wird eine infizierte Mail-Nachricht gefunden, dann wird der infizierte Teil aus ihr gelöscht und in eine Quarantäne-Datenbank verschoben. Die Mail-Nachricht wird an den Adressaten weitergeleitet, wobei ihr vorher eine Charakteristik der Nachricht und ein Überprüfungsvermerk für jedes infizierte Objekt hinzugefügt werden. Der Vermerk enthält Informationen über den gefundenen Virus und über die ausgeführten Aktionen (s. Bild 23).

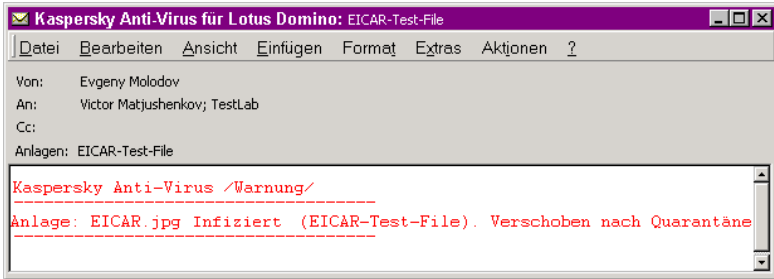



Bild 23. Mail-Nachricht mit einem gelöschten infizierten Objekt, die an den Adressaten zugestellt wird

-  Wenn Sie den Desinfektionsmodus für infizierte Objekte (zu Einzelheiten s. Pkte. 5.3.2, 5.4.2) aktiviert haben und der Desinfektionsversuch wurde erfolgreich abgeschlossen, dann ist zu beachten, dass auf die Daten des Objekts die Bearbeitungsregeln angewendet werden, die Sie für desinfizierte Objekte festgelegt haben. Falls der Desinfektionsversuch erfolglos sein sollte, dann gelten für solche Objekte weiterhin die Regeln, die für infizierte Objekte festgelegt wurden. Geben Sie deshalb vor der Auswahl der Bearbeitungsregel für infizierte Objekte unbedingt an, ob deren Desinfektion versucht werden soll.

5.5.4. Parameter für das Versenden von Benachrichtigungen

Kaspersky Anti-Virus für Lotus Notes/Domino kann so eingestellt werden, dass das Programm Benachrichtigungen über das gescannte Objekt an Adressat, Absender und andere Benutzer sendet. Dieser Modus kann für jede Art der zu scannenden Objekte (infizierte, beschädigte, verdächtige usw.) gewählt werden.

Die Konfiguration der Parameter für das Versenden von Benachrichtigungen werden im Fenster **BEARBEITUNGSREGELN** (s. Bild 22) vorgenommen. In dieses Fenster können Sie aus dem

Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks **Regeln** wechseln.

Bevor die Adressaten der Benachrichtigungen angegeben werden, ist unbedingt die zu scannende Objektart auszuwählen, auf die diese Einstellungen angewendet werden sollen. Es wird empfohlen, diese Einstellungen für alle genannten Arten der zum Scannen vorgesehenen Objekte vorzunehmen.

 **Um den Modus zum Versenden von Benachrichtigungen zu aktivieren,**

geben Sie die Adressaten der Benachrichtigungen an, indem Sie das Kontrollkästchen **Ja** für folgende Parameter markieren:

- **Verteilerliste** – Senden einer Benachrichtigung über das Objekt an die Adressen einer vorher angelegten Verteilerliste (s. Pkt. 5.2). In die Verteilerliste können sowohl Adressen von Administratoren als auch Adressen anderer Benutzer, darunter auch externer Benutzer, aufgenommen werden.

 **Die folgenden Parameter können nur für Mail-Nachrichten eingestellt werden!**

- **den Absender** – Senden einer Benachrichtigung an den Absender der Nachricht.
- **den Adressaten** – Senden einer Benachrichtigung an den Adressaten (die Adressaten) der Nachricht.

Beim Fund eines Virus oder bei Verdacht auf einen Virus wird das Programm eine Benachrichtigung über die infizierte Nachricht senden (s. Bild 24).

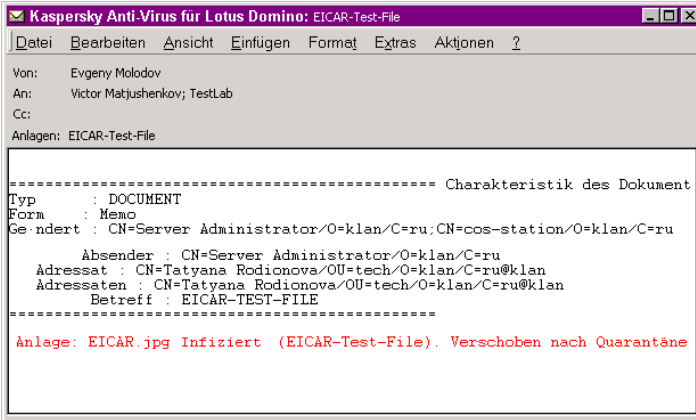


Bild 24. Benachrichtigung über eine infizierte Nachricht an den Adressaten

5.5.5. Parameter für den Überprüfungsvermerk

Das Programm verfügt über einen Modus zum Einfügen eines Überprüfungsvermerks. Dabei wird dem Text der Nachricht in Abhängigkeit der gewählten Bearbeitungsart ein Überprüfungsvermerk hinzugefügt. Für jedes überprüfte Objekt wird ein Vermerk angebracht. Waren in einer Mail-Nachricht zum Beispiel zwei infizierte und ein verdächtiges Objekt vorhanden, dann werden drei Vermerke (ein Vermerk für jedes Objekt) in die Benachrichtigung aufgenommen.

 Die Konfiguration der Parameter für den Überprüfungsvermerk gilt nur für Mail-Nachrichten.

Die Parameter für den Überprüfungsvermerk werden im Fenster **BEARBEITUNGSREGELN** (s. Bild 22) festgelegt. In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des


Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks **Regeln** wechseln.

 Es wird empfohlen, die Konfiguration der Parameter für den Überprüfungsvermerk für alle Objekttypen vorzunehmen.

 **Damit dem Text der Nachricht ein Überprüfungsvermerk hinzugefügt wird, nehmen Sie folgende Einstellungen vor:**

1. Entscheiden Sie, beim Fund welcher Objekttypen das Programm die Benutzer benachrichtigen soll (zum Beispiel bei infizierten Objekten). Öffnen Sie die entsprechende Registerkarte des Fensters **BEARBEITUNGSREGELN**.
2. Aktivieren Sie das Kontrollkästchen **Ja** für den Parameter **Zum Text der Nachricht hinzufügen**, damit ein Vermerk zum Text einer ausgehenden Nachricht hinzugefügt wird.
3. Geben Sie im Abschnitt **Überprüfungsvermerk für die Nachricht** dieser Registerkarte im Eingabefeld für den Vermerk die notwendigen Makro-Inserts an. Sie können folgende Makro-Inserts verwenden:
 - **%OBJECTTYPE%** – der Typ des gescannten Objekts (angehängte Datei, OLE-Objekt usw.).
 - **%OBJECTNAME%** – der Name der gescannten Datei.
 - **%VIRUSNAME%** – der Name des Virus.
 - **%ACTION%** – die Bearbeitungsart für das Objekt.

Zum Beispiel ist es ausreichend, im Eingabefeld für den Überprüfungsvermerk das Makro-Insert **%VIRUSNAME%** anzugeben, damit in den Text einer infizierten Nachricht ein Vermerk mit dem Namen des Virus eingefügt wird.

 Die oben genannten Makro-Inserts werden auch beim Versenden von Benachrichtigungen über Objekte an die Verteilerliste verwendet (s. Pkt. 5.5.4).

5.5.6. Parameter für das Aufzeichnen des Ereignisjournals

Um die Arbeit der Module Scan und Scheduler zu verfolgen, können Sie den Modus zum Aufzeichnen eines Ereignisjournals für jeden zu scannenden Objekttyp wählen.

Der Modus zum Aufzeichnen des Ereignisjournals wird im Fenster **BEARBEITUNGSREGELN** (s. Bild 22) eingestellt. In dieses Fenster können Sie aus dem Abschnitt **Optionen** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) mit Hilfe des Hyperlinks **Regeln** wechseln.



Um den Modus zum Aufzeichnen des Ereignisjournals für einen konkreten Objekttyp, der zum Scannen vorgesehen ist, einzustellen,

1. Entscheiden Sie, beim Fund welcher Objekttypen das Programm einen Eintrag zum Journal hinzufügen soll. Öffnen Sie die Registerkarte des Fensters **BEARBEITUNGSREGELN**, die dem gewählten Objekttyp entspricht (zum Beispiel die Registerkarte **INFIZIERT** für infizierte Objekte).
2. Aktivieren Sie das Kontrollkästchen **Ja** für den Parameter **Zum Ereignisjournal hinzufügen**.


Nachdem diese Einstellungen vorgenommen wurden, werden alle Informationen über ein Objekt des gewählten Typs in dem Ereignisjournal aufgezeichnet, in dem die Informationen dann bearbeitet werden können (zu Einzelheiten s. Pkt. 7.4).

5.6. Bearbeitungsarten für zu scannende Objekte

*Beispiele für die Konfiguration des Scannens und der
Bearbeitungsart für infizierte Objekte*

5.6.1. Konfiguration der Bearbeitungsart

Durch die Konfiguration einer bestimmten Bearbeitungsart werden die Aktionen festgelegt, die von den Modulen Scan und Scheduler beim Fund eines konkreten gescannten Objekttyps durchgeführt werden.


 Im Folgenden werden die möglichen Bearbeitungsarten für infizierte Objekte beschrieben. Diese Parameter entsprechen denen für die anderen Objekttypen (verdächtige, beschädigte usw.).

Sie können eine der folgenden Bearbeitungsarten für infizierte Objekte in Mail-Nachrichten einstellen:

- Verschieben in den Quarantäne-Ordner für infizierte Mail-Objekte (s. Pkt. 5.6.2).
- Desinfektion infizierter Mail-Objekte (s. Pkt. 5.6.3).
- Löschen infizierter Objekte aus Mail-Nachrichten (s. Pkt. 5.6.4).
- Weiterleiten von infizierten Objekten in Mail-Nachrichten (s. Pkt. 5.6.5).


Für infizierte Objekte in Datenbanken kann eine der folgenden Bearbeitungsarten gewählt werden:

- Verschieben in den Quarantäne-Ordner für infizierte Datenbank-Objekte (entsprechend dem in Pkt. 5.6.2 beschriebenen Vorgehen).
- Desinfektion infizierter Objekte in Datenbanken (entsprechend dem in Pkt. 5.6.3 beschriebenen Vorgehen).
- Löschen infizierter Objekte aus Datenbanken (entsprechend dem in Pkt. 5.6.4 beschriebenen Vorgehen).
- Zugriff auf infizierte Objekte in Datenbanken (entsprechend dem in Pkt. 5.6.5 beschriebenen Vorgehen).

 Beachten Sie beim Ändern der Parameter für die Bearbeitung von zu scannenden Objekten, dass diese für Mail-Objekte und für Datenbank-Objekte im Fenster **BEARBEITUNGSREGELN** (s. Bild 22) gleichzeitig eingestellt werden! Zum Beispiel ist es nicht möglich, für infizierte Mail-Objekte das Löschen und gleichzeitig für infizierte Datenbank-Objekte die Desinfektion zu wählen.

5.6.2. Verschieben in den Quarantäne-Ordner für infizierte Objekte

In bestimmten Fällen muss der Zugriff und das Versenden infizierter Mail-Objekte gesperrt oder der Zugriff auf infizierte Objekte von Datenbanken verboten werden. Ist dieser Modus aktiviert, dann werden alle Objekte, die einen Virus enthalten, in die Quarantäne-Datenbank umgeleitet (s. Pkte. 7.3.2-7.3.3), wo sie dann bearbeitet werden können:.

 Unter dem Verschieben von infizierten Mail-Objekten in die Quarantäne-Datenbank ist hier nur das Verschieben des infizierten Teils einer Nachricht (zum Beispiel einer Anlage oder des Nachrichtentexts) in die Quarantäne-Datenbank zu verstehen. Die eigentliche Nachricht wird zusammen mit einem

Überprüfungsvermerk und der Charakteristik der Nachricht an den Adressaten gesendet.

☞ **Um den Modus zum Verschieben aller infizierten Objekte in die Quarantäne-Datenbank zu aktivieren, nehmen Sie folgende Einstellungen vor:**

1. Deaktivieren Sie im Fenster **MAIL-ÜBERPRÜFUNG** auf der Registerkarte **GLOBAL** das Kontrollkästchen **Ja** für den Parameter **Desinfektionsversuch**, falls es aktiviert ist. Machen Sie das gleiche im Fenster **ÜBERPRÜFUNG DER DATENBANKEN**.
2. Öffnen Sie im Fenster **BEARBEITUNGSREGELN** die Registerkarte **INFIZIERT**.
3. Wählen Sie als Bearbeitungsart für infizierte Objekte **nach Quarantäne verschieben**.

Dadurch werden alle infizierten Objekte zur weiteren Bearbeitung in die Quarantäne-Datenbank verschoben. Die Objekte werden dabei in der Quarantäne-Datenbank nach dem Typ der Dokumente gruppiert, in denen sie gefunden wurden: Es gibt also einen Quarantäne-Ordner für Datenbank-Objekte und einen für Objekte aus Mail-Nachrichten.

Außerdem können Sie folgende Modi aktivieren:

- Benachrichtigung von Absender, Adressaten und anderen Benutzern über die Sperrung von infizierten Objekten (zu Einzelheiten s. Pkt. 5.5.4);
- Einfügen eines Überprüfungsvermerks in den Text der Nachricht (zu Einzelheiten s. Pkt. 5.5.5);
- Aufzeichnung aller durchgeführten Aktionen in einem Ereignisjournal (zu Einzelheiten s. Pkt. 5.5.6).

5.6.3. Desinfektion infizierter Objekte

Sie können einen Modus wählen, in dem das Programm versucht, infizierte Objekte zu desinfizieren und die desinfizierten Objekte bei erfolgreicher Reparatur weiterleitet, bei erfolglosem Reparaturversuch aber in der Quarantäne-Datenbank speichert.

 **Um den Modus zur Desinfektion infizierter Objekte festzulegen, nehmen Sie folgende Einstellungen vor:**

1. Aktivieren Sie im Fenster **MAIL-ÜBERPRÜFUNG** auf der Registerkarte **GLOBAL** das Kontrollkästchen **Ja** für den Parameter **Desinfektionsversuch**. Machen Sie das gleiche im Fenster **ÜBERPRÜFUNG DER DATENBANKEN**.
2. Öffnen Sie im Fenster **BEARBEITUNGSREGELN** die Registerkarte **DESINFIZIERT**.
3. Wählen Sie als Bearbeitungsart für desinfizierte Objekte **weiterleiten**.
4. Öffnen Sie im Fenster **BEARBEITUNGSREGELN** die Registerkarte **INFIZIERT**.
5. Wählen Sie als Bearbeitungsart für infizierte Objekte **nach Quarantäne verschieben**.

Dadurch sind für die Benutzer nur jene Mail- und Datenbank-Objekte zugänglich, die nicht infiziert waren oder deren Reparatur erfolgreich war (s. Bild 25). Infizierte Objekte, deren Reparatur nicht gelungen ist, befinden sich in den Quarantäne-Datenbanken.

Außerdem können Sie folgende Modi aktivieren:

- Benachrichtigung von Absender, Adressaten und anderen Benutzern über infizierte Objekte (zu Einzelheiten s. Pkt. 5.5.4);

- Einfügen eines Überprüfungsvermerks in den Text der Nachricht (zu Einzelheiten s. Pkt. 5.5.5);
- Aufzeichnung aller durchgeführten Aktionen in einem Ereignisjournal (zu Einzelheiten s. Pkt. 5.5.6).

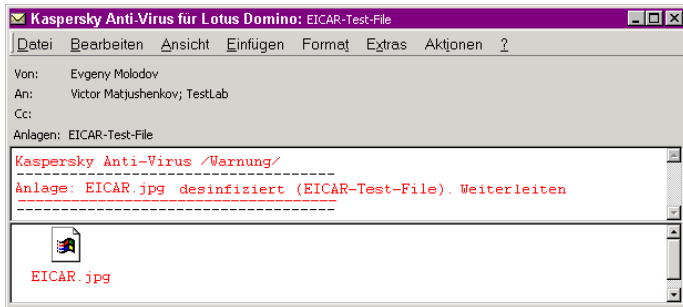


Bild 25. Desinfizierte Nachricht mit Überprüfungsvermerk

5.6.4. Löschen infizierter Objekte

Für den Betrieb des Programms können Sie einen Modus wählen, bei dem im Fall eines erfolglosen Reparaturversuchs von infizierten Objekten oder bei Auftreten eines Fehlers beim Scannen das Programm diese Objekte löscht, und im Fall der erfolgreichen Reparatur die desinfizierten Objekte weiterleitet.



Um den Modus zum Löschen infizierter Objekte, deren Reparaturversuch erfolglos war, festzulegen, nehmen Sie folgende Einstellungen vor:

1. Aktivieren Sie im Fenster **MAIL-ÜBERPRÜFUNG** auf der Registerkarte **GLOBAL** das Kontrollkästchen **Ja** für den Parameter **Desinfektionsversuch**, falls es nicht aktiviert ist. Machen Sie das gleiche im Fenster **ÜBERPRÜFUNG DER DATENBANKEN**.

2. Öffnen Sie im Fenster **BEARBEITUNGSREGELN** die Registerkarte **DESINFIZIERT**.
3. Wählen Sie als Bearbeitungsart für desinfizierte Objekte **weiterleiten**.
4. Öffnen Sie die Registerkarte **INFIZIERT**.
5. Wählen Sie als Bearbeitungsart für infizierte Objekte **aus dem Dokument entfernen**.
6. Öffnen Sie die Registerkarte **FEHLER BEIM SCANNEN**.
7. Wählen Sie als Bearbeitungsart für infizierte Objekte **aus dem Dokument entfernen**.

Außerdem können Sie folgende Modi aktivieren:

- Benachrichtigung von Absender, Adressaten und anderen Benutzern über infizierte Objekte (zu Einzelheiten s. Pkt. 5.5.4);
- Einfügen eines Überprüfungsvermerks in den Text der Nachricht (zu Einzelheiten s. Pkt. 5.5.5);
- Aufzeichnung aller durchgeführten Aktionen in einem Ereignisjournal (zu Einzelheiten s. Pkt. 5.5.6).

5.6.5. Weiterleitung infizierter Objekte

Sie können einen Modus wählen, in dem das Programm infizierte Mail-Objekte an die Benutzer weiterleitet und die Arbeit mit infizierten Datenbank-Objekten zulässt. Dieser Modus kann verwendet werden, wenn Sie sicher sind, dass die betreffenden Benutzer selbst ein Antiviren-Programm zur Desinfektion der infizierten Objekte starten werden.

Das Programm kann infizierte Objekte entweder ohne einen Desinfektionsversuch oder nach erfolglosem Desinfektionsversuch weiterleiten.



Damit das Programm infizierte Objekte ohne einen Desinfektionsversuch weiterleitet,

1. Deaktivieren Sie im Fenster **MAIL-ÜBERPRÜFUNG** auf der Registerkarte **GLOBAL** das Kontrollkästchen **Ja** für den Parameter **Desinfektionsversuch**, falls es aktiviert ist. Das Programm wird dann mit infizierten Nachrichten keinen Desinfektionsversuch durchführen. Machen Sie das gleiche im Fenster **ÜBERPRÜFUNG DER DATENBANKEN**.
2. Öffnen Sie im Fenster **BEARBEITUNGSREGELN** die Registerkarte **INFIZIERT**.
3. Wählen Sie als Bearbeitungsart für desinfizierte Objekte **weiterleiten**.



Damit das Programm infizierte Objekte, deren Reparaturversuch erfolglos war, weiterleitet,

1. Aktivieren Sie im Fenster **MAIL-ÜBERPRÜFUNG** auf der Registerkarte **GLOBAL** das Kontrollkästchen **Ja** für den Parameter **Desinfektionsversuch**, falls es nicht aktiviert ist. Das Programm wird dann versuchen, infizierte Nachrichten zu desinfizieren. Machen Sie das gleiche im Fenster **ÜBERPRÜFUNG DER DATENBANKEN**.
2. Öffnen Sie im Fenster **BEARBEITUNGSREGELN** die Registerkarte **INFIZIERT**.
3. Wählen Sie als Bearbeitungsart für desinfizierte Objekte **weiterleiten**.

Bei diesen Einstellungen besteht die Möglichkeit, dass die Benutzer infizierte Nachrichten erhalten (s. Bild 26).

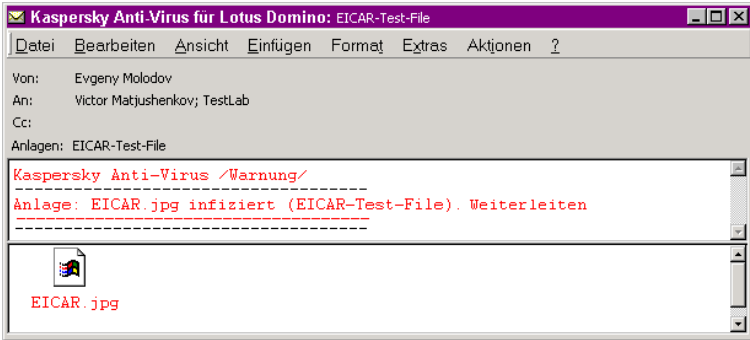


Bild 26. Infizierte Nachricht mit Überprüfungsvermerk

Außerdem können Sie folgende Modi aktivieren:

- Benachrichtigung von Absender, Adressaten und anderen Benutzern über infizierte Objekte (zu Einzelheiten s. Pkt. 5.5.4);
- Einfügen eines Überprüfungsvermerks in den Text der Nachricht (zu Einzelheiten s. Pkt. 5.5.5);
- Aufzeichnung aller durchgeführten Aktionen in einem Ereignisjournal (zu Einzelheiten s. Pkt. 5.5.6).

6. Start und Beenden der Antiviren-Überprüfung

Start, Beenden und Neustart des Moduls Scan zur Überprüfung von Mail-Nachrichten und des Moduls Scheduler zur Überprüfung von Datenbankdateien.

Die Überprüfung von Nachrichten und Datenbankdateien auf das Vorhandensein von Viren wird beim Auftreten kritischer Ereignisse beendet. Um die Überprüfung wiederaufzunehmen, muss das Überprüfungsmodul neu gestartet werden. Geben Sie dazu in der Befehlszeile ein:

```
load kavscan
```

oder

```
load kavscheduler
```

In bestimmten Fällen kann es notwendig sein, die Überprüfung zu unterbrechen. Geben Sie dazu in der Befehlszeile ein:

```
tell kavscan exit
```

oder

START UND BEENDEN DER ÜBERPRÜFUNG

```
tell kavscheduler exit
```

Um das hohe Sicherheitsniveau des Antivirenschutzes aufrechtzuerhalten, sollten die Antiviren-Datenbanken jede Woche mit Hilfe des Programms Kaspersky Anti-Virus Updater aktualisiert werden (s. Kap. 9).

Damit die Module bei der Arbeit die neuen Antiviren-Datenbanken verwenden, müssen sie neu gestartet werden. Geben Sie dazu in der Befehlszeile ein:

```
tell kavscan exit  
load kavscan
```

oder

```
tell kavscheduler exit  
load kavscheduler
```

7. Zusatzfunktionen für den Antivirenschutz

Beschreibung der Arbeit mit der Analyse-Datenbank und den Quarantäne-Datenbanken. Arbeit mit dem Ereignisjournal.

7.1. Einleitung

Während seiner Arbeit verwendet Kaspersky Anti-Virus für Lotus Notes/Domino folgende Datenbanken:

- **Analyse-Datenbank** – die Datenbank, in der die Objekte enthalten sind, die sich im Moment in der Warteschlange für die Bearbeitung durch das Modul Scan befinden. Sie können mit den Objekten dieser Datenbank arbeiten (zu Einzelheiten s. Pkt. 7.2).

- **Quarantäne-Datenbank für:**
 - **Mail-Nachrichten** – die Datenbank für Mail-Nachrichten, die auf Grund einer Überprüfung zur weiteren Bearbeitung in den Quarantäne-Ordner verschoben wurden (zu Einzelheiten s. Pkt. 7.3.2).
 - **Dokumente** – die Datenbank für Dokumente, die auf Grund einer Überprüfung durch das Modul Scheduler in den Quarantäne-Ordner verschoben wurden, wo sie ebenfalls bearbeitet werden können (zu Einzelheiten s. Pkt. 7.3.3).

Zur Vereinfachung wird in diesem Handbuch in der Bezeichnung jedes Abschnitts, der eine bestimmte Datenbank beschreibt, die Angabe des Wegs zu dieser Datenbank genannt. Der Abschnitt, der die Beschreibung der Analyse-Datenbank enthält, hat zum Beispiel folgendes Aussehen:

Arbeit mit Objekten in der Analyse-Datenbank.

Daten → In der Warteschlange,

wobei: **Daten → In der Warteschlange** – der Weg zum Fenster, das die Analyse-Datenbank enthält, ist (**Daten** – der Abschnitt im linken Rahmen des Fensters der Konfigurationsdatenbank, **In der Warteschlange** – der Hyperlink des Abschnitts, mit dessen Hilfe man in das Fenster wechseln kann).

Alle Arbeitsergebnisse der Module Scan und Scheduler werden in einem *Ereignisjournal* aufgezeichnet. Die Einträge des Journals können bearbeitet werden (zu Einzelheiten s. Pkt. 7.4).

7.2. Arbeit mit Objekten in der Analyse-Datenbank. Daten → In der Warteschlange

Für die Zeit der Überprüfung von Mail-Nachrichten verschiebt das Modul Scan alle Objekte in die Analyse-Datenbank. Nach dem Beenden der Überprüfung werden die Objekte in Abhängigkeit der vorgenommenen Einstellungen (s. Kapitel 5) an den Adressaten weitergeleitet, in der Quarantäne-Datenbank gespeichert, oder gelöscht. Da die Analyse-Datenbank während der Arbeit des Moduls Scan als dessen Warteschlange dient, wird dem Administrator empfohlen, nicht mit der Analyse-Datenbank zu arbeiten. Es kann allerdings zu Situationen kommen, in denen der Administrator gezwungen ist, den Inhalt der Analyse-Datenbanken zu kontrollieren und ein infiziertes Objekt aus ihr zu entfernen.

Zur Ansicht der Analyse-Datenbank wird der Hyperlink **In der Warteschlange** verwendet, der im Abschnitt **Daten** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) angebracht ist.

Dadurch wird der rechte Rahmen des Fensters aktualisiert, in dem dann eine Liste der Nachrichten angezeigt wird, die sich im Moment in der Analyse-Datenbank befinden (s. Bild 27).

Der rechte Rahmen besteht aus zwei Teilen:

- Der obere Teil besitzt die Form einer Tabelle mit folgenden Spalten:
 - **Auswahlspalte** – in dieser Spalte kann gegenüber der Zeile mit dem Objekt das Zeichen ✓ gesetzt werden, um das Objekt weiter zu bearbeiten. Sie können das Häkchen setzen/entfernen, indem Sie in dieser Spalte gegenüber der gewünschten Zeile mit der linken Maustaste klicken.

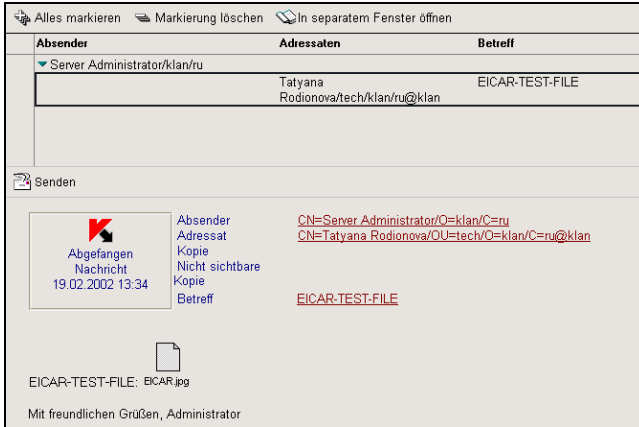
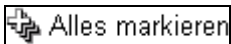


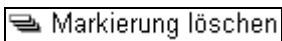
Bild 27. Die Analyse-Datenbank für Mail-Nachrichten

- **Absender** – die Adresse des Absenders des bearbeiteten Objekts.
- **Adressaten** – die Adresse des Adressaten der Mail-Nachricht.
- **Betreff** – Betreff der Nachricht.
- Der untere Teil stellt das Übersichtsfenster für das im oberen Teil ausgewählte Objekt dar.


Zur Arbeit mit der Liste der Mail-Nachrichten in der Analyse-Datenbank dienen folgende Schaltflächen:




Alles markieren – Alle Objekte der Analyse-Datenbank für das anschließende Löschen markieren. Dadurch wird jedes Element der Liste in der Auswahlspalte mit dem Zeichen ✓ versehen. Wenn Sie ein einzelnes Element der Liste markieren möchten, klicken Sie mit der linken Maustaste in der Auswahlspalte gegenüber dem gewünschten Element.



Markierung löschen – Markierung aller Objekte in der Analyse-Datenbank entfernen.

 **In separatem Fenster öffnen** – Öffnen des Objekts zur Ansicht in einem separaten Fenster (s. Bild 28). Dadurch wird im rechten Rahmen ein Fenster geöffnet, das eine vollständige Beschreibung der Nachricht enthält, einschließlich deren Charakteristik und Überprüfungsvermerk.

 **Senden** – Senden der Nachricht an den Adressaten unabhängig von den Überprüfungsresultaten.

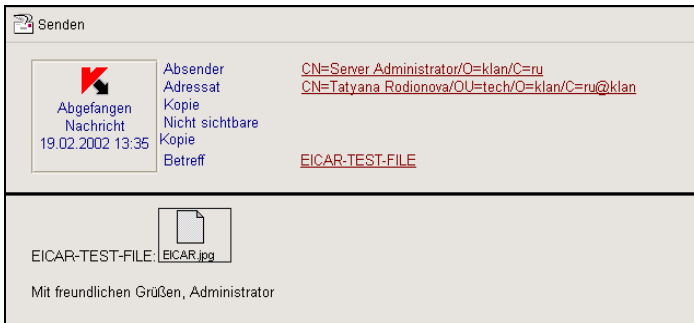


Bild 28. Eine Nachricht, die sich in der Analyse-Datenbank befindet

7.3. Quarantäne-Datenbank

Beschreibung der Auswahl von Daten und der Arbeit mit der Quarantäne-Datenbank.

7.3.1. Auswahl eines Abschnitts der Quarantäne-Datenbank

Wenn Sie bei der Konfiguration des Programms als Bearbeitungsart für die zu scannenden Objekte deren Verschieben in den Quarantäne-Ordner angegeben haben (s. Pkt. 5.4), dann verschiebt das Programm diese in eine spezielle Datenbank.

☞ Kaspersky Anti-Virus für Lotus Notes/Domino erlaubt das Erkennen von Viren in infizierten Nachrichten. Zum Löschen von Viren wird dem Administrator aber die Verwendung anderer Produkte, zum Beispiel des Scanner-Programms empfohlen. Sind infizierte und archivierte Dateien an eine Nachricht angehängt und Kaspersky Anti-Virus für Lotus Notes/Domino findet darin Viren, dann kann er die Viren nicht unmittelbar aus dem Archiv löschen. Zur Reparatur der infizierten Dateien muss der Administrator diese zuerst aus dem Archiv extrahieren und danach ein Antiviren-Programm starten.

Die Daten in der Quarantäne-Datenbank sind in Mail-Objekte und in Datenbank-Dateien des Domino Servers unterteilt:

- **Quarantäne (Mail)** – der Abschnitt der Quarantäne-Datenbank für Mail-Objekte.
- **Quarantäne (Dokumente)** – der Abschnitt der Quarantäne-Datenbank für Objekte der gescannten Daten des Domino Servers.


Die Bezeichnungen der Abschnitte der Quarantäne-Datenbank sind im Abschnitt **Daten** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) angebracht. Der Name jedes Abschnitts stellt einen Hyperlink dar, mit dessen Hilfe der rechte Rahmen des Fensters aktualisiert werden kann.

7.3.2. Arbeit mit Mail-Objekten in der Quarantäne-Datenbank.

Daten → Quarantäne (Mail)

Für die Arbeit mit der Quarantäne-Datenbank für Mail-Nachrichten wird der Hyperlink **Quarantäne (Mail)** verwendet, der im Abschnitt **Daten** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) angebracht ist. Dadurch wird der rechte Rahmen des Fensters aktualisiert, in dem eine Liste der Mail-Objekte angezeigt wird, die sich auf Grund einer Überprüfung in der Quarantäne-Datenbank befinden (s. Bild 29) .

Absender	Adressaten	Betreff
Server Administrator/klan/ru	Tatyana Rodionova/tech/klan/ru@klan	EICAR-TEST-FILE

 Quarantäne (Mail-Nachricht) 19.02.2002 11:48	Absender	CN=Server Administrator/C=klan/C=ru
	Adressaten	CN=Tatyana Rodionova/OU=tech/O=klan/C=ru@klan
	Nicht sichtbare Kopie	
	Betreff	EICAR-TEST-FILE


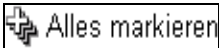
TYPE	NAME	KATEGORIE	VIRUS	OBJEKT
Anlage	EICAR.jpg	Infiziert	EICAR-Test-File	 -EICAR.jpg

Bild 29. Die Quarantäne-Datenbank für Mail-Nachrichten

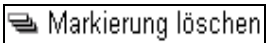
Der rechte Rahmen besteht aus zwei Teilen:

- Der obere Teil besitzt die Form einer Tabelle mit folgenden Spalten:
 - **Auswahlspalte** – in dieser Spalte kann gegenüber der Zeile mit dem Mail-Objekt das Zeichen ✓ gesetzt werden, um das Objekt weiter zu bearbeiten. Sie können das Häkchen setzen/entfernen, indem Sie in dieser Spalte gegenüber der gewünschten Zeile mit der linken Maustaste klicken.
 - **Absender** – die Adresse des Absenders des zurückgehaltenen Mail-Objekts.
 - **Adressat** – die Adresse des Adressaten der Mail-Nachricht.
 - **Betreff** – Betreff der Nachricht.
- Der untere Teil stellt das Übersichtsfenster für die im oberen Teil ausgewählte Nachricht dar.

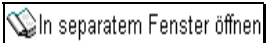
Zur Arbeit mit der Liste der Mail-Nachrichten in der Analyse-Datenbank dienen folgende Schaltflächen:



– Alle Mail-Objekte der Quarantäne-Datenbank für das anschließende Löschen markieren. Dadurch wird jedes Element der Liste in der Auswahlspalte mit dem Zeichen ✓ versehen. Wenn Sie ein einzelnes Element der Liste markieren möchten, klicken Sie mit der linken Maustaste in der Auswahlspalte gegenüber dem gewünschten Element.



– Markierung aller Mail-Objekte entfernen.



– Öffnen des Mail-Objekts zur Ansicht in einem separaten Fenster (s. Bild 30).

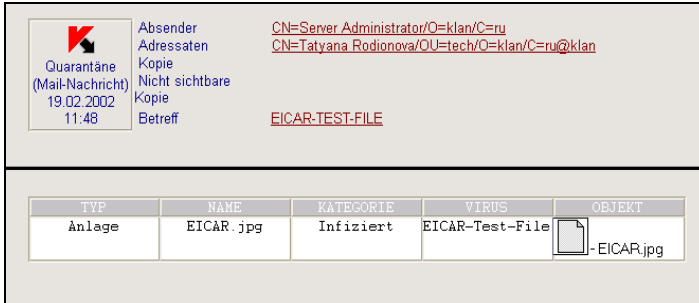



Bild 30. Eine Nachricht, die in der Quarantäne-Datenbank zurückgehalten wird

Jedes Mail-Objekt in der Quarantäne-Datenbank stellt ein Dokument dar, das ein infiziertes Objekt und die folgenden Ergebnisse der Überprüfung enthält:

- **TYP** – der Typ des gescannten Objekts (angehängte Datei, OLE-Objekt usw.).
- **NAME** – der Name des gescannten Objekts.
- **KATEGORIE** – der Typ des gescannten Objekts (infiziert, verdächtig usw.).
- **VIRUS** – der Name des Virus, mit dem das Objekt infiziert ist.
- **OBJEKT** – das infizierte Objekt selbst.

 **Gehen Sie vorsichtig mit infizierten Objekten um. Ein infiziertes Objekt darf nicht gestartet oder geöffnet werden, da dies ernste Folgen nach sich ziehen kann!**

7.3.3. Arbeit mit Datenbank- Dokumenten in der Quarantäne- Datenbank. Daten → Quarantäne (Dokumente)

Verwenden Sie zur Arbeit mit der Quarantäne-Datenbank für Datenbank-Objekte des Domino Servers den Hyperlink **Quarantäne (Dokumente)**, der im Abschnitt **Daten** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9) angebracht ist. Dadurch wird der rechte Rahmen des Fenster aktualisiert, in dem eine Liste der Dokumente angezeigt wird, die auf Grund der Überprüfungsergebnisse zurückgehalten werden (s. Bild 31).

Der rechte Rahmen besteht aus zwei Teilen:

- Der obere Teil besitzt die Form einer Tabelle mit folgenden Spalten:
 - **Auswahlspalte** – in dieser Spalte kann gegenüber der Zeile mit dem Objekt das Zeichen ✓ gesetzt werden, um das Objekt weiter zu bearbeiten. Sie können das Häkchen setzen/entfernen, indem Sie in dieser Spalte gegenüber der gewünschten Zeile mit der linken Maustaste klicken.
 - **Datenbank** – der vollständige Pfad der Datenbank, in der das infizierte Objekt gefunden wurde.
 - **Typ** – der Typ des infizierten Objekts (Seite, Form, Dokument).
 - **Geändert** – der Name des Benutzers, der das Objekt zuletzt geändert hat.

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

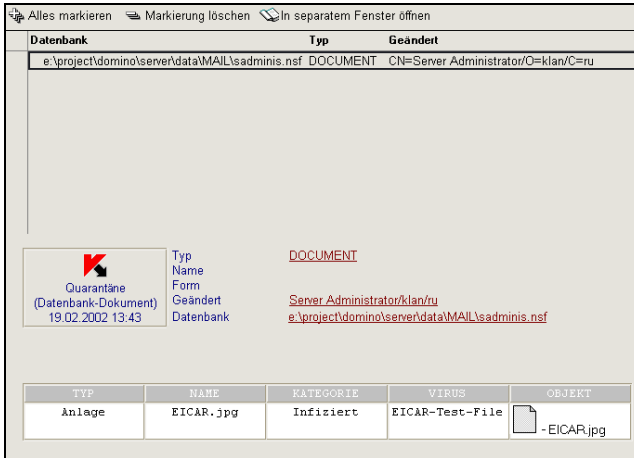


Bild 31. Die Quarantäne-Datenbank für Datenbank-Dokumente

- Der untere Teil stellt das Übersichtsfenster für das im oberen Teil ausgewählte Objekt dar.

Zur Arbeit mit der Liste der in der Quarantäne-Datenbank enthaltenen Objekte können Sie die Schaltflächen verwenden, die der Beschreibung in Pkt. 7.3.2 entsprechen.

Jedes Dokument der Quarantäne-Datenbank besitzt folgende Informationen:

- **TYP** – der Typ des gescannten Objekts (angehängte Datei, OLE-Objekt usw.).
- **NAME** – der Name des gescannten Objekts.
- **KATEGORIE** – der Typ des gescannten Objekts (infiziert, verdächtig usw.).
- **VIRUS** – der Name des Virus, mit dem das Objekt infiziert ist.
- **OBJEKT** – das infizierte Objekt selbst.

7.4. Arbeit mit den Aufzeichnungen des Ereignisjournals

*Beschreibung der Arbeit mit den Aufzeichnungen des
Ereignisjournals.*

7.4.1. Auswahl einer Gruppe von Einträgen

Die Arbeitsergebnisse der Module Scan und Scheduler werden im Ereignisjournal aufgezeichnet, falls die entsprechenden Einstellungen vorgenommen wurden (s. Pkt. 5.5.6). Dabei sind alle Einträge über die Ergebnisse der Arbeit in folgenden Gruppen angeordnet:

- **Nach Datum** – eine Liste der Einträge, die nach dem Erstellungsdatum geordnet sind.
- **Nach Typ** – eine Liste der Einträge, die nach dem Typ der in ihnen enthaltenen Informationen geordnet sind. Folgende Arten von Informationen können im Journal vorkommen:
 - INFORMATION – Informativer Hinweis;
 - WARNING – Hinweis auf ein Ereignis.
- **Nach Modul** – eine Liste der Einträge, die nach den Modulen geordnet sind, deren Arbeitsergebnisse sie enthalten (Scan oder Scheduler).

Die Gruppenliste der Einträge befindet sich im Abschnitt **Ereignisjournal** im linken Rahmen des Fensters der Konfigurationsdatenbank (s. Bild 9). Die Bezeichnung jeder Gruppe

stellt einen Hyperlink dar, mit dessen Hilfe der rechte Rahmen aktualisiert werden kann.

7.4.2. Regeln für die Arbeit mit Einträgen des Ereignisjournals

Die Struktur des rechten Rahmens besteht für alle Typen von Gruppen der Journaleinträge aus zwei Teilen:

- Der obere Teil besitzt die Form einer Tabelle mit folgenden Spalten:
 - **Auswahlspalte** – in dieser Spalte kann gegenüber der Zeile mit dem Journaleintrag das Zeichen ✓ gesetzt werden, um den Eintrag weiter zu bearbeiten. Sie können das Häkchen setzen/entfernen, indem Sie in dieser Spalte gegenüber der gewünschten Zeile mit der linken Maustaste klicken.
 - **Datum** – das Erstellungsdatum des Eintrags im Journal.
 - **Zeit** – die Erstellungszeit des Eintrags im Ereignisjournal.
 - **Modul** – die Bezeichnung des Moduls (Scan oder Scheduler), dessen Arbeitsergebnisse in dem Eintrag enthalten sind.
 - **Typ** – der Typ der Information, die in dem Eintrag enthalten ist.
- Der untere Teil stellt das Übersichtsfenster für die im oberen Teil ausgewählte Operation dar, die von dem Modul durchgeführt wurde

Zur Arbeit mit den Einträgen einer beliebigen Gruppe dienen die folgenden Schaltflächen:



Alles markieren – Alle Einträge der Gruppe für das anschließende Löschen markieren. Dadurch wird jedes Element der Liste in der Auswahlspalte mit dem Zeichen ✓ versehen. Wenn Sie ein einzelnes Element der Liste markieren möchten, klicken Sie mit der linken Maustaste in der Auswahlspalte gegenüber dem gewünschten Element.



Markierung löschen – Markierung aller Einträge der Gruppe entfernen.



In separatem Fenster öffnen – Öffnen des Journaleintrags zur Ansicht in einem separaten Fenster (s. Bild 33).



Um zum Beispiel den Journaleintrag für einen bestimmten Tag anzusehen,

1. Verwenden Sie den Hyperlink **Nach Datum** und im rechten Rahmen des Fensters der Konfigurationsdatenbank werden die Journaleinträge gruppiert nach Datum angezeigt (s. Bild 32).
2. Klicken Sie auf das Dreieck ▶, das neben dem gewünschten Datum zu sehen ist. Danach wird die Liste mit den Einträgen geöffnet, die an diesem Tag im Ereignisjournal aufgezeichnet wurden.
3. Zur Ansicht eines bestimmten Journaleintrags in einem separaten Fenster wählen Sie diesen Eintrag in der Liste aus und klicken auf die Schaltfläche

Dadurch wird im rechten Rahmen ein Fenster geöffnet, das die vollständige Beschreibung der Arbeitsergebnisse des Moduls enthält (s. Bild 33). Dazu gehören die Bezeichnung des Moduls, dessen Arbeitsergebnisse im Journal aufgezeichnet wurden, Datum und Zeit der Erstellung der Aufzeichnung, Informationstyp, sowie eine ausführliche Charakteristik des Dokuments.

**KASPERSKY ANTI-VIRUS FÜR LOTUS
NOTES/DOMINO**

Alles markieren
 Markierung entfernen
 In separatem Fenster öffnen

Datum	Zeit	Modul	Typ
▼ 19.02.2002			
	11:48:19	KavScan	WARNING

Modul KavScan
 Datum 19.02.2002
 Zeit 11:48:19
 Typ

```

===== Charakteristik des Dokuments
Typ      : DOCUMENT
Form     : Memo
Ge-ndert : CN=Server Administrator/O=klan/C=ru;CN=cos-station/O=klan/C=ru
Absender : CN=Server Administrator/O=klan/C=ru
Adressat : CN=Tatyana Rodionova/OU=tech/O=klan/C=ru@klan
Adressaten : CN=Tatyana Rodionova/OU=tech/O=klan/C=ru@klan
Betreff  : EICAR-TEST-FILE
=====
Anlage: EICAR.jpg Infiziert (EICAR-Test-File). Verschoben nach Quarantäne
  
```

Bild 32. Eine Gruppe von Antworten, nach Datum geordnet

```

Modul            KavScan
Datum            19.02.2002
Zeit              11:48:19
Typ
=====
===== Charakteristik des Dokuments
Typ      : DOCUMENT
Form     : Memo
Ge-ndert : CN=Server Administrator/O=klan/C=ru;CN=cos-station/O=klan/C=ru
Absender : CN=Server Administrator/O=klan/C=ru
Adressat : CN=Tatyana Rodionova/OU=tech/O=klan/C=ru@klan
Adressaten : CN=Tatyana Rodionova/OU=tech/O=klan/C=ru@klan
Betreff  : EICAR-TEST-FILE
=====
Anlage: EICAR.jpg Infiziert (EICAR-Test-File). Verschoben nach Quarantäne
  
```

Bild 33. Der Journaleintrag eines Ereignisses

8. Deinstallation von Kaspersky Anti-Virus für Lotus Notes/Domino

*Beschreibung der Deinstallation des Programms mit
Hilfe des Deinstallationsprogramms und manuell.*

8.1. Deinstallation des Programms mit Hilfe des Deinstallationsprogramms



Um Kaspersky Anti-Virus für Lotus Notes/Domino mit Hilfe des Deinstallationsprogramms zu entfernen,

1. Entfernen Sie die Module **kavscan** und **kavscheduler** durch die Eingabe folgender Befehle in der Befehlszeile:
tell kavscan quit und **tell kavscheduler quit**.

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

2. Starten Sie auf dem Server den Task **HTTP**, falls dieser noch nicht gestartet wurde.
3. Öffnen Sie mit einem WEB-Browser die Datenbank *kav_install.nsf* (zum Beispiel:
http://Serveradresse/kav_install.nsf).
4. Überprüfen Sie auf der erscheinenden Seite (s. Bild 34), ob das Programm die Konfiguration der Ordner richtig identifiziert hat, in die Lotus Domino Server und Kaspersky Anti-Virus für Lotus Notes/Domino installiert wurden.

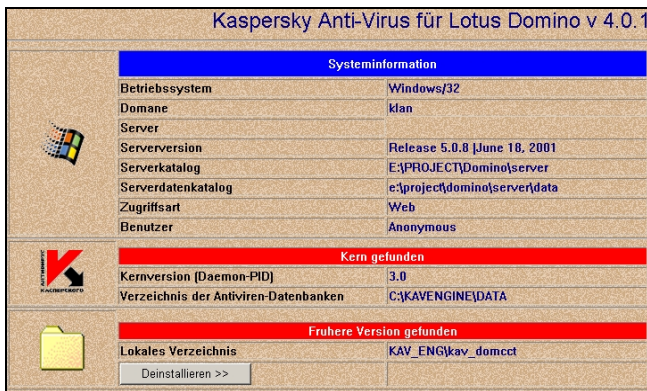



Bild 34. Das Fenster zur Deinstallation des Programms.

5. Klicken Sie auf die Schaltfläche . Nach einiger Zeit erscheint auf der Seite das Protokoll über die Deinstallation (s. Bild 35).

```

Delete INI var : KavOptionsDatabase ... OK
Delete template : kav_domcc.ntf ... OK
Delete NSF Database : D:\Lotus\Domino\Data\KAV\kav_domcc...
Delete template : kav_cbox.ntf ... OK
Delete NSF Database : D:\Lotus\Domino\Data\KAV\kav_cbox...
Delete template : kav_qbox.ntf ... OK
Delete NSF Database : D:\Lotus\Domino\Data\KAV\kav_qbox...
Update INI var : EXTMGR_ADDIN ... OK
Delete file : nKavHook.dll ... OK
Update INI var : SERVERTASKS ... OK
Delete file : nKavScan.exe ... 75: Path/file access error
OK
Update INI var : SERVERTASKS ... OK
Delete file : nKavSheduler.exe ... 75: Path/file access error
OK
Delete directory: D:\Lotus\Domino\Data\KAV\... OK
Found 2 mail-in documents
Delete it.
    
```

Bild 35. Das Protokoll über die Deinstallation.

6. Starten Sie den Server neu.

8.2. Manuelle Deinstallation des Programms

 Um das Programm Kaspersky Anti-Virus für Lotus Notes/Domino manuell zu deinstallieren,

1. Beenden Sie die Arbeit des Servers.
2. Entfernen Sie in der Datei *notes.ini* den Wert **kavhook** aus der Variablen **EXTMGR_ADDINS** und entfernen Sie aus der Variablen **ServerTasks** die Programme **kavscan** und **kavscheduler**.
3. Entfernen Sie aus dem Ordner der Daten von Lotus Domino Server die Dateien *kav_domcc.ntf*, *kav_qbox.ntf* und *kav_cbox.ntf*.

4. Entfernen Sie den Ordner, in dem die Installation durchgeführt wurde, mit seinem gesamten Inhalt.
5. Entfernen Sie den Ordner mit den temporären Dateien.
6. Entfernen Sie aus dem Adressbuch das Dokument **Mail-In database**, das auf die Datenbank *kav_cbox.nsf* verweist.
7. Starten Sie den Server.

 **Um den Antiviren-Kern AVP API manuell zu deinstallieren,**

1. Starten Sie im Ordner des Antiviren-Kerns die Datei *unreg.bat*.
2. Entfernen Sie den Ordner zusammen mit seinem Inhalt.

 **Um das Programm KAVDaemon für Linux manuell zu deinstallieren,**

1. Geben Sie von der Konsole des Servers oder von einem Remote-Computer des Administrators aus den Befehl **KavDaemon - ka** ein.
2. Entfernen Sie den Ordner des Programms KAVDaemon für Linux zusammen mit seinem Inhalt.

9. Kaspersky Anti-Virus Updater

Wofür wird das Update-Programm verwendet? Starten des Update-Programms für die Antiviren-Datenbanken und die ausführbaren Module. Beschreibung der Oberfläche

9.1. Wofür wird das Kaspersky Anti-Virus Updater-Programm verwendet?

Das Kaspersky Anti-Virus Updater-Programm ist ein Teil von **Kaspersky Anti-Virus**, der zur automatischen Aktualisierung der Antiviren-Datenbanken, der Viren-Definitionen, der Reparaturmethoden für infizierte Dateien und der Paketkomponenten dient.

Das Update-Programm kann Antiviren-Datenbanken und ausführbare Module aus dem **Internet** (unter Verwendung einer Netzwerk- oder Remote-Verbindung) oder aus einem lokalen Ordner kopieren.

9.2. Starten des Kaspersky Anti-Virus Updater

Es gibt mehrere Möglichkeiten zum Starten des Kaspersky Anti-Virus Updaters:

- aus dem **Windows-Hauptmenü**;
- aus Control Centre (automatisch);
- über eine Befehlszeile;
- aus anderen Anwendungen des **Kaspersky Anti-Virus** Pakets.

Um das Kaspersky Anti-Virus Updater vom **Windows**-Hauptmenü aus zu starten, klicken Sie auf das Menü **Start**, zeigen Sie auf das Submenü **Programme**, und klicken Sie dann in der Programmgruppe **Kaspersky Anti-Virus** auf die Option **Kaspersky Anti-Virus Updater**.

Wenn Sie Kaspersky AV Control Centre installiert haben, können Sie einen Task für den automatischen Start des Kaspersky Anti-Virus Updater erstellen (Näheres über Kaspersky AV Control Centre siehe Kapitel 6).

Alternativ können Sie Kaspersky Anti-Virus Updater aus einer Befehlszeile starten. Wechseln dazu Sie in den den gemeinsam genutzten Ordner des **Kaspersky Anti-Virus (KAV Shared Files)** und klicken Sie auf die Datei *avpupd.exe*. Der Pfad zum gemeinsam genutzten Ordner kann beispielsweise so aussehen: **C:\Programme\Gemeinsame Dateien\KAV Shared Files**.

9.3. Benutzeroberfläche des Kaspersky Anti-Virus Updater

Die Benutzeroberfläche des Updaters ist ähnlich wie ein **Windows Wizard** gestaltet und besteht aus einer Abfolge von Fenstern (Schritten), zwischen denen mithilfe von Schaltflächen **Zurück** und **Weiter** gewechselt werden kann. Um Aktualisierung zu beenden, klicken Sie auf **Fertigstellen**. Um das Programm auf einer beliebigen Stufe abzubrechen, klicken Sie auf **Abbrechen**.

In der Mitte jedes Fensters ist ein **Einstellungsbaum** platziert (zu seiner Funktion siehe Kapitel 12). Dieses Element enthält Optionen, die als hierarchischer Baum angeordnet sind.

9.3.1. Fenster Willkommen

Nach dem Start des Update-Programms öffnet der Wizard das erste Fenster: **Willkommen** (Bild 1). Wenn Sie das Kontrollkästchen **Einstellungen ändern** aktivieren, können Sie den Update-Modus, die zu aktualisierenden Objekte und die Report-Optionen auswählen.



Bild 1. Fenster **Willkommen**.

9.3.2. Fenster **Verbindung**

Möchten Sie die als Vorgabe gespeicherten Einstellungen ändern, können Sie dies im Fenster **Verbindung** tun (Bild 2).

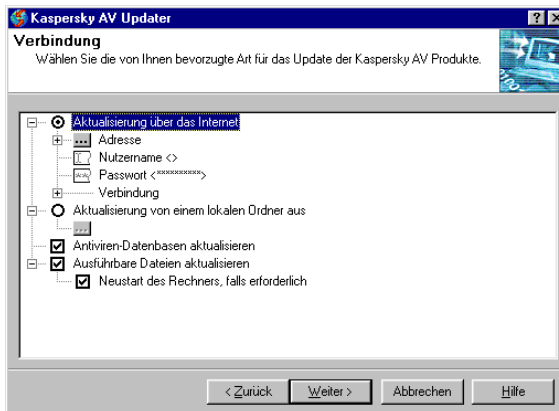


Bild 2. Fenster **Verbindung**

Im Fenster **Verbindung** können Sie die Art und das Objekt der Aktualisierung festlegen. Unten werden die Funktionen jedes Befehls auf der ersten Hierarchieebene des Einstellungsbaums erläutert (Bild 3).

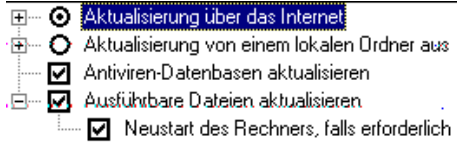


Bild 3. Allgemeine Einstellungen des Updaters

- Aktualisierung über das Internet** – Update über das Internet vornehmen.
- Aktualisierung von einem lokalen Ordner aus** – Update aus einem lokalen Ordner durchführen;
- Antiviren-Datenbanken aktualisieren** – Antiviren-Datenbanken aktualisieren.
- Ausführbare Dateien aktualisieren** – ausführbare Module des **Kaspersky Anti-Virus** aktualisieren.
 - Neustart des Rechners, falls erforderlich** – Computer neu starten, wenn dies nach der Aktualisierung ausführbarer Module des Softwarepakets erforderlich wird.

Haben Sie alle Einstellungen vorgenommen, klicken Sie auf **Weiter**.

9.3.2.1. Einstellungen für das Update aus dem Internet

Haben Sie Aktualisierung über das **Internet** gewählt, müssen Sie die entsprechenden Einstellungen vornehmen. Wechseln Sie zum Ast **Aktualisierung über das Internet** des Einstellungsbaums (Bild 4). Unten werden die einzelnen Einstellungen erläutert:

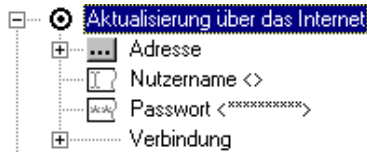


Bild 4. Einstellung der Aktualisierung über das Internet

- Adresse** – Einstellung der Update-Quelle (Protokoll, Servername usw.).
- Nutzername** – Benutzername für den Zugriff auf den Update-Server.
- Passwort** – Passwort für den Zugriff auf den Update-Server.
- Verbindung** – Einstellung der Verbindung mit dem Update-Server.

9.3.2.1.1. Auswahl der Adresse

Sie können die Aktualisierung über einen in die Liste eingetragenen Update-Server vornehmen. Um diese Liste einzusehen, wechseln Sie zum Ast **URL** des Einstellungsbaums (Bild 5).

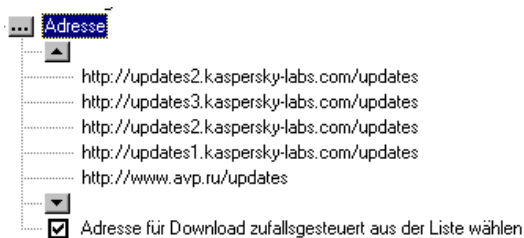



Bild 5. Einstellung der Adresse des Update-Servers

Standardmäßig wird bei der Aktualisierung die URL des ersten Servers in der Liste genutzt. Bei erfolglosem Versuch wird auf den zweiten Server gegriffen usw. Die Meldung über einen Fehler beim Zugriff auf den Server

erscheint nur, wenn zu keinem Server Verbindung hergestellt wurde. Wenn Sie die Option **Adresse für Download zufallgesteuert aus der Liste wählen** aktivieren, wird als erster Server eine beliebige URL aus der Liste genutzt.

Die Serverliste ist editierbar. Um diese zu ändern, klicken Sie auf die Schaltfläche  **Adresse**. Danach erscheint auf dem Bildschirm das Dialogfeld **Bearbeiten der Adressen-Liste** (siehe Bild 6).

Abbrechen – Dialogfenster schließen, Änderungen verwerfen.

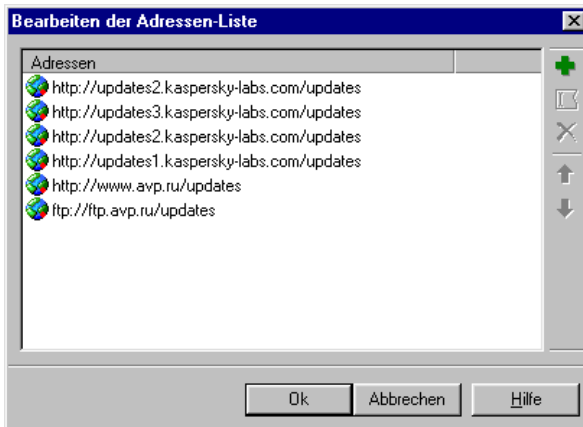






Bild 6. Dialogfeld **Bearbeiten der Adressen-Liste**

Die Bedienung der Liste erfolgt über folgende Schaltflächen im Dialogfeld oder entsprechende Menübefehle:

-  – neue Adresse in die Liste aufnehmen;
-  – aktuelle Adresse ändern;
-  – aktuelle Adresse löschen;
-  – aktuelle Adresse um eine Zeile nach oben verschieben;



– aktuelle Adresse um eine Zeile nach unten verschieben;

OK – Dialogfenster schließen, Änderungen speichern;

9.3.2.1.2. Einstellungen der IP-Verbindung

Die Einstellungen der IP-Verbindung sind abhängig von der Art der Verbindung mit dem Update-Server, die Sie wählen (Bild 7), und zwar:

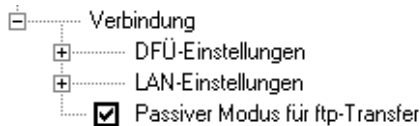


Bild 7. Einstellungen der IP-Verbindung

- DFÜ-Einstellungen** – Einrichtung der DFÜ-Verbindung zum Internet-Provider;
- LAN-Einstellungen** – Verbindung mit dem Internet-Provider, über lokales Netzwerk einstellen.
- Passiver Modus für ftp-Transfer** – Für die Verbindung mit dem FTP-Server passiven Modus verwenden (dies ist besonders wichtig für die Benutzer, die die Verbindung zu ihrem IP-Provider über ein Proxy-Server oder Firewall herstellen).

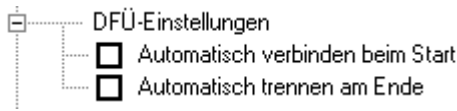


Bild 8. DFÜ-Einstellungen

Bei der Einstellung der DFÜ-Verbindung können Sie folgende Optionen aktivieren (Bild 8):

- Automatisch verbinden beim Start** – DFÜ-Verbindung zum Internet-Provider sofort nach dem Starten des Update-Vorgangs herstellen;
- Automatisch trennen am Ende** – Nach dem Abschluß des Aktualisierungsvorgangs die Verbindung automatisch trennen (Modem ausschalten).

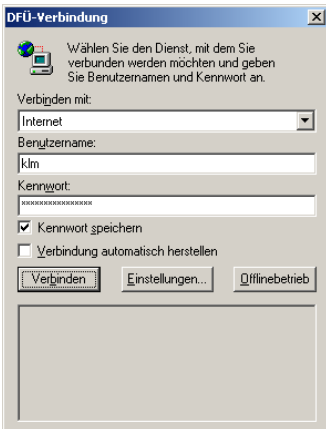


Bild 9. Dialogfeld **DFÜ-Verbindung**

Haben Sie automatische Herstellung der DFÜ-Verbindung zum Internet-Provider gewählt, wird nach dem Starten des Aktualisierungsvorgangs das standardmäßige DFÜ-Tool auf dem Bildschirm erscheinen (falls Sie kein anderes Tool gewählt haben).

Zum Herstellung der Verbindung zum Internet-Provider füllen Sie das Dialogfeld **DFÜ-Verbindung** aus (Bild 9) und klicken Sie auf **Verbinden**. Danach wird die Verbindung mit dem Fernserver hergestellt.

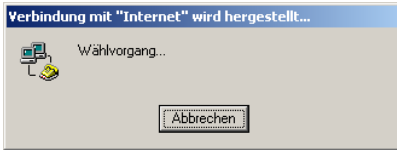


Bild 10. Dialogfeld **Verbindung mit "Internet" wird hergestellt**. Wahlvorgang

Beim Wählvorgang wird auf dem Bildschirm das Dialogfeld **Verbindung mit "Internet" wird hergestellt** mit der Meldung **Wahlvorgang** angezeigt (Bild 10). Nach Abschluß des Wählvorgangs wird der Benutzername und das Passwort geprüft.



Bild 11. Fenster **Verbindung mit Internet herstellen**

Falls der Benutzer auf Grund seiner Angaben nicht identifiziert werden kann, erscheint das Fenster **User Logon** (Bild 11), in dem die Eingabe von **Benutzername**, **Kennwort** und **Anmeldedomäne** für die Einstellung der Verbindung notwendig ist.

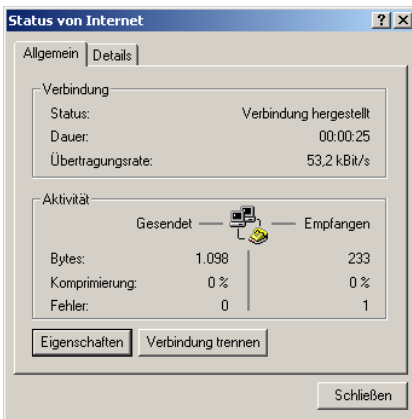


Bild 12. Dialogfeld **Status von Internet**

Wenn Sie mit dem Internet verbunden sind, erscheint ein entsprechendes Symbol in der Task-Leiste. Um die Verbindungseinstellungen anzuschauen, führen Sie einen Doppelklick auf das entsprechende Symbol in der Task-Leiste aus (Bild 12).

Wenn Sie ein lokales Netzwerk (LAN) für die IP-Verbindung verwenden, können Sie entweder die Einstellungen aus der **Systemsteuerung** verwenden, oder die Verbindung manuell konfigurieren (Bild 13)

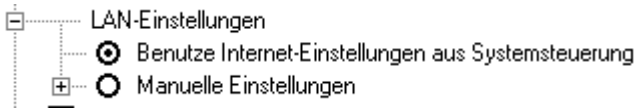


Bild 13. LAN-Einstellungen

☉ Benutze Internet-Einstellungen aus Systemsteuerung

– Einstellungen für die Verbindung aus der Systemsteuerung übernehmen;

☉ Manuelle Einstellungen – Verbindung manuell konfigurieren.



Wurde die Option **Manuelle Einstellungen** gewählt, müssen Sie folgende Einstellungen vornehmen (Bild 14):

Bild 14. Manuelle Einstellungen

☑ Proxy verwenden (Firewall) – für die Verbindung mit dem Internet-Provider Proxy-Server oder Firewall benutzen;


📄 Adresse – Adresse des Proxy-Servers (oder Firewalls), über den die Verbindung erfolgt. Die Adresse können Sie in Dezimalform (zum Beispiel 125.5.29.1) oder als vollständige Domainangabe (zum Beispiel test.russia.ru) oder als verkürzte Angabe (zum Beispiel test) eingeben;

📄 Anschluss – Port für die Verbindung mit dem Proxyserver (oder Firewall);

☑ Authentifizierung – Individuelle Benutzereinstellungen;

☑ Benutzername – Benutzer des Prozyserverns (oder des Firewalls);

 **Passwort** – Passwort für Proxyserver (oder Firewall);

 **HTTP-Proxy mit Unterstützung für FTP**– Zugriff auf FTP-Server über HTTP-Proxy-Server (CERN-Proxy);

Um eingehende Informationen über die o.g. Einstellungen der Internet-Verbindung zu erhalten, wenden Sie sich an Ihren Systemadministrator.

9.3.2.2. Aktualisierung von einem lokalen Ordner aus

Wenn Sie einen lokalen Ordner als Quelle für das Update gewählt haben, dann geben Sie die vollständige Pfadbezeichnung des Ordners an.

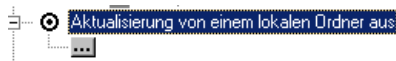


Bild 15. Aktualisierung von einem lokalen Ordner aus.

Klicken Sie auf die Schaltfläche, die auf dem Bild 15 Aktualisierung aus einem lokalen Ordner mit einem Rechteck hervorgehoben ist.

Danach wird das Dialogfeld **Durchsuchen** geöffnet, in dem der Update-Ordner gewählt werden kann.

9.3.3. Auswahl der zu aktualisierenden Objekte

Im untersten Teil des Einstellungsbaums befinden sich zwei Auswahlkästchen (Bild 16), und zwar:

- ... Antiviren-Datenbasen aktualisieren
- ... Ausführbare Dateien aktualisieren

Bild 16. Auswahl des zu aktualisierenden Objektes

- Antiviren-Datenbanken aktualisieren** – Antiviren-Datenbanken vom Update-Server kopieren und installieren;
- Ausführbare Dateien aktualisieren** – ausführbare Module vom Update-Server kopieren und installieren.
- Rechner neu starten (falls erforderlich)** – nach Installation der Software den Rechner (falls erforderlich) automatisch neu starten.

9.3.4. Fenster Optionen

Im Fenster **Optionen** können Sie zusätzliche Funktionen des Update-Programms für die Antiviren-Datenbanken einstellen (Bild 17).

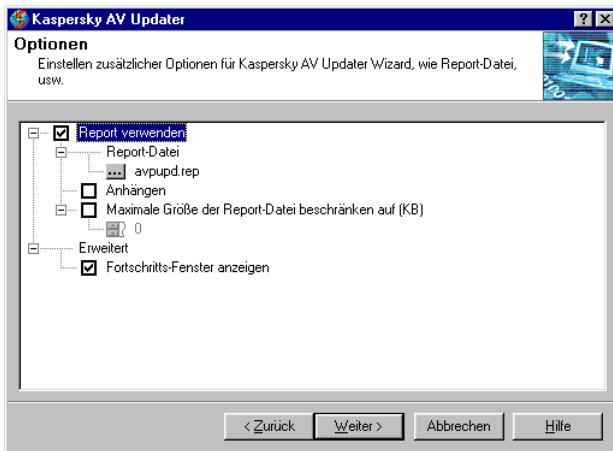


Bild 17 Fenster **Optionen**

- Report verwenden** – Update-Report erstellen.
 - Report-Datei** – hier können Sie den Namen der Report-Datei und den Pfad dazu eingeben.
 - Anhängen** – Daten in die bestehende Report-Datei anhängen

oder jedesmal eine neue Datei erstellen.

- Maximale Größe der Report-Datei beschränken auf (KB)** – maximale Größe der Report-Datei. Wird diese Größe erreicht, so wird die Datei überschrieben.
- Erweitert** – Einstellung der Benutzeroberfläche;
 - Fortschritt-Fenster anzeigen** – das Fenster **Aktualisierung läuft anzeigen** (siehe unten).

Klicken Sie auf **Weiter**, um Aktualisierung fortzusetzen.

9.3.5. Fenster Aktualisierung läuft

Dieses Fenster (Bild 18) wird nur angezeigt, wenn Sie im Fenster **Optionen** beim Element **Erweitert** das Kontrollkästchen **Fortschritt-Fenster anzeigen** aktiviert haben.

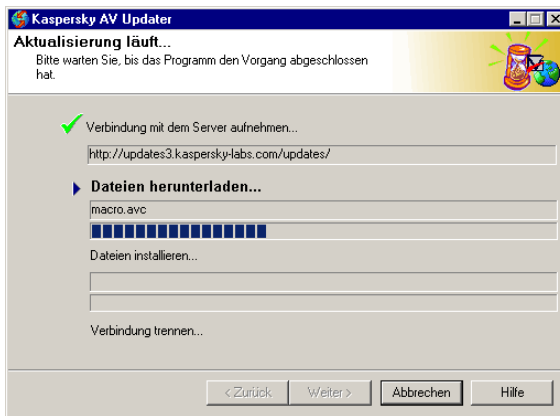




Bild 18. Fenster **Aktualisierung läuft**

Das Fenster besteht aus vier Teilen, die das jeweilige Stadium des laufenden Updates der Antiviren-Datenbanken anzeigen:

- **Verbindung mit dem Server aufnehmen** — Die Verbindung mit dem Server für den Download der Dateien wird hergestellt;
- **Dateien herunterladen ...** — Die Dateien werden vom Server auf Ihrechner kopiert (oben wird der Name der kopierten Datei und unten der Fortschrittsbalken des Aktualisierungsvorgangs angezeigt);
- **Dateien installieren ...** — Die Dateien werden auf dem Computer installiert (Oben wird der Name der installierten Datei angezeigt, unten die Fortschrittsanzeige der Installation);
- **Verbindung trennen ...** — Die Verbindung wird getrennt.

Der Status des Update-Vorgangs wird jeweils durch ein Symbol angezeigt, das sich links von den oben genannten Hinweisen befindet (Ein Symbol wird nur angezeigt, wenn der entsprechende Teil aktualisiert wird). Das

Symbol  zeigt den erfolgreichen Abschluss dieses Teils des Update-Vorgangs an, während  anzeigt, dass der Updater diesen Teil im Moment ausführt.

9.3.6. Fenster Aktualisierung abgeschlossen

Im letzten Fenster (Bild 19) können Sie den Report über das Update anzeigen (durch Anklicken der Schaltfläche **Bericht**) und das Kontrollkästchen **Homepage von DATSEC öffnen** aktivieren oder deaktivieren.

Klicken Sie auf die Schaltfläche **Beenden**, um den Update-Vorgang des Programms abzuschließen. Wenn Sie das Kontrollkästchen 'Besuch auf der Webseite von Kaspersky Lab' aktiviert haben, öffnet Internet Explorer automatisch die Internetseite von Kaspersky Lab.

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

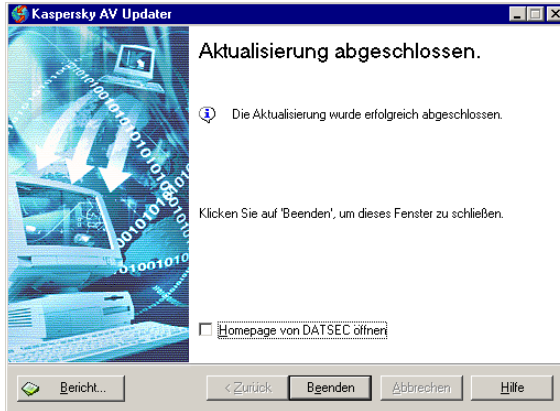


Bild 19. Fenster **Aktualisierung abgeschlossen**

Kapitel 10

10. Kaspersky Anti-Virus Control Centre

Funktionen und Start der Anwendung
Beschreibung der Oberfläche

10.1. Beschreibung von des Kaspersky Anti-Virus Control Centre

Das Kaspersky Anti-Virus Control Centre (Kaspersky AV Control Centre, Control Centre) ist Teil des Antiviren-Pakets **Kaspersky Anti-Virus**. Es dient als Kontrollzentrale und wird zur Installation und Aktualisierung von Paketkomponenten, zur Zeitsteuerung von automatisierten Tasks und zur Auswertung der Ergebnisse der Tasks verwendet.

Die Möglichkeit, mit dieser Software eine Übersicht über die installierten Komponenten und deren Versionen zu erstellen, erleichtert es dem

Benutzer, mit dem Support-Service von **Kaspersky Lab** zu kommunizieren, und erlaubt es Ihnen, sofortige Aktualisierungen vorzunehmen.

Mit dem Control Centre können Sie die Antiviren-Programme des Pakets zeitgesteuert starten. So können Sie die Produktivität steigern und gleichzeitig Ihr System nachhaltig vor Viren schützen.

Der automatisierte Start externer Programme erlaubt es, Control Centre als konventionelles Zeitsteuerungsprogramm einzusetzen. Im Allgemeinen bedarf es nicht dem Einsatz eines weiteren Werkzeugs zum automatischen Start, wodurch die Ressourcen Ihres Computers effektiv genutzt werden. Außerdem wird dadurch in Verbindung mit dem Antiviren-Sicherheitssystem und anderen Tasks die richtige Synchronisation ihrer Prozessoren gewährleistet und Konflikte werden vermieden.

10.2. Start des Kaspersky AV Control Centre

Es gibt mehrere Möglichkeiten zum Starten von Control Centre :

- Aus dem **Windows**-Hauptmenü;
- Automatischer Start beim Starten von **Windows**.
- Aus der Befehlszeile

Um Kaspersky AV Control Centre vom **Windows**-Hauptmenü aus zu starten, klicken Sie auf die Schaltfläche **Start**, zeigen Sie auf das Untermenü **Programme** und klicken Sie unter **Kaspersky Anti-Virus** auf **Kaspersky Anti-Virus Control Centre**.

Nach der Installation von **Kaspersky Anti-Virus** startet Kaspersky AV Control Centre automatisch beim Starten von **Windows** bevor der **Anmeldevorgang (logon procedure)** beginnt.




Nach dem Start des Kaspersky AV Control Centre erscheint in der Task-Leiste folgendes Symbol:  Klicken Sie darauf mit der rechten Mauskaste öffnet sich das Benutzermenü (Bild 20), das folgende Befehle beinhaltet:

Bild 20. Menü des Kaspersky AV Control Centre in der Task-Leiste

- **Kaspersky AV Control Centre...** – Programmfenster öffnen;
- **Import-Einstellungen ...** – vorher in einer Datei gespeicherten Einstellungen importieren (siehe unten);
- **Export-Einstellungen ...** – Programmeinstellungen in einer speziellen Datei mit der Erweiterung .dat speichern, später können aus dieser Datei Einstellungen importiert werden (siehe oben);
- **Hilfe** – Hilfefenster anzeigen;
- **Über ...** – Informationen über diese Software, den Lizenznamen, die Gültigkeitsdauer der Lizenz usw. (siehe Beispiel auf dem Bild 21);
- **Beenden** – Kaspersky Control Centre **verlassen**.

Die Einträge **Export-Einstellungen** und **Import-Einstellungen** dienen zur Übertragung von Einstellungen des Kaspersky AV Control Centre von einem Rechner auf einen anderen, d.h. Sie können das Programm auf einem Arbeitsplatz einrichten und dann die vorgenommenen Einstellungen in einem gemeinsam genutzten Ordner auf dem Server speichern, um später diese auf einem anderen Arbeitsplatz laden

Im oberen Teil des Benutzermenüs (oberhalb der Linie) befindet sich die Task-Liste, in deren Einstellungen die Option manueller Start aktiviert ist. Diese Tasks können über entsprechende Menüeinträge gestartet werden.

Das Hauptfenster des Kaspersky AV Control Centre muß dabei nicht geöffnet werden.

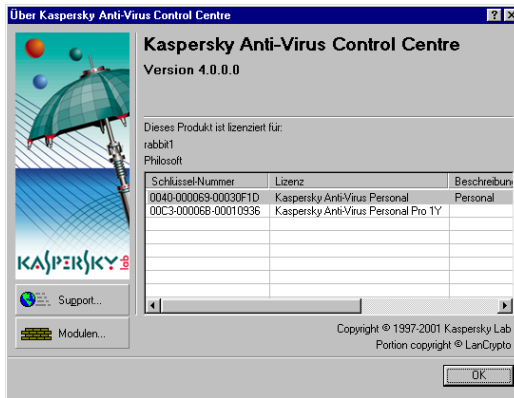


Bild 21. Über Kaspersky Anti-Virus Control Centre



Um Kaspersky AV Control Centre zu verlassen, wählen Sie den Eintrag **Beenden** aus dem Menü in der Task-Leiste.

An dieser Stelle möchten wir Sie auf einige Besonderheiten dieser Software aufmerksam machen. Kaspersky AV Control Centre besteht aus zwei Teilen: dem Serviceteil, welcher noch vor Passwortheingabe (**logon procedure**) als Systemservice startet, und einer Benutzeroberfläche, die einen grafischen Interface darstellt und die Kommunikation mit dem Benutzer gewährleistet. Sollte man auch die Benutzeroberfläche aus dem Arbeitsspeicher entfernen, werden die mit den Optionen des Kaspersky AV Control Centre festgelegten Tasks nach wie vor ausgeführt, nur kann der Anwender keine weiteren Einstellungen vornehmen und neue Tasks erstellen. Sollte man den Serviceteil ebenfalls aus dem Arbeitsspeicher entfernen, wird Kaspersky AV Control Centre die festgelegten Tasks nicht ausführen.

10.3. Die Oberfläche des Kaspersky AV Control Centre

Das Hauptfenster enthält drei Registerkarten: **Tasks**, **Komponenten**, **Einstellungen** und **Quarantäne** (die Beschreibung siehe unten).

Um eine Aktion auszuführen, benutzen Sie das Kontextmenü oder die Symbolleiste.

Im unteren Teil des Fensters sehen Sie die Schaltflächen **OK**, **Abbrechen**, **Übernehmen** und . Beim Anklicken der Schaltfläche **OK** werden alle vorgenommenen Einstellungen gespeichert. Klicken Sie auf **Abbrechen** – werden sie verworfen. In beiden Fällen wird das Hauptfenster geschlossen. Klicken Sie auf die Schaltfläche **Übernehmen**, werden die Änderungen gespeichert, das Hauptfenster bleibt dabei offen, und Sie können weitere Einstellungen vornehmen. Wenn Sie residente Tasks ausführen, werden die vorgenommenen Einstellungen sofort in das ausgeführte Modul geladen. Beim Anklicken der Schaltfläche  wird Hilfetext aufgerufen

10.3.1. Registerkarte Tasks

Die Registerkarte Tasks (Bild 22) wird zur Verwaltung der Tasks verwendet. Gemäß unserer obigen Definition bedeutet "Task" die Ausführung eines Programms. Dieses Programm wird zu einer bestimmten Zeit, auf Grund eines bestimmten Ereignisses oder durch direkte Eingabe des Benutzers mit vorgegeben Parametern und Einstellungen gestartet.

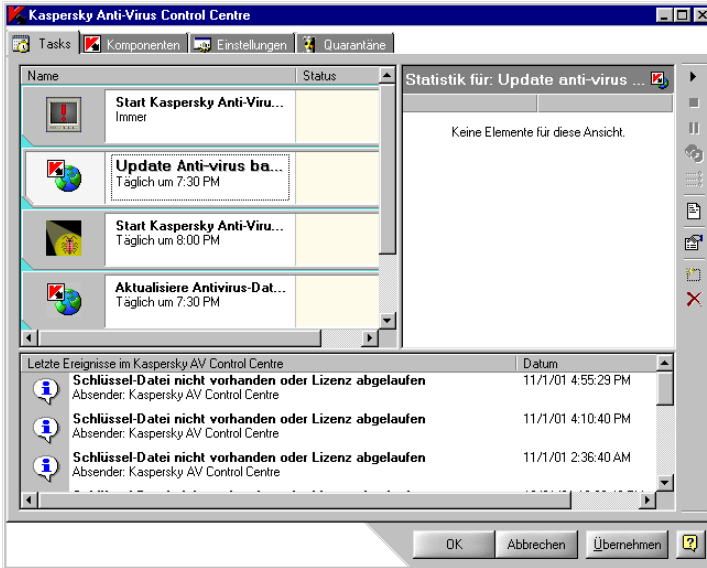


Bild 22. Registerkarte **Tasks**

Die Registerkarte besteht aus drei Teilen:

- Im linken Teil wird eine Liste der Tasks und deren Status angezeigt;
- Im rechten Teil werden die Programmstatistiken angezeigt⁴;
- Im unteren Teil finden Sie eine Liste der Ereignisse (Fehler, Warnungen, Benachrichtigungen).

Betrachten wir die einzelnen Teile der Registerkarte genauer. Die Task-Liste ist in zwei Spalten aufgeteilt: **Name** und **Status**. In der Spalte **Name** sehen Sie eine Liste der Tasks, und in der Spalte **Status** den zugehörigen Ausführungsstatus. Es gibt unterschiedliche Status-Arten:

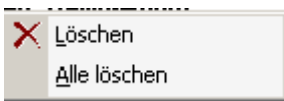
⁴ Programm-Performance Statistiken – eine Kurzform des Reports über die Programm-Performance.

- **In Betrieb** – Der Task wird momentan ausgeführt;
- **Fertig!** – Der Task wurde erfolgreich ausgeführt;
- **Erfolglos** – Die Ausführung des Tasks ist gescheitert;
- **Abgebrochen** – Der Task wurde vom Benutzer abgebrochen;
- **Pause** – Der Task wurde angehalten;
- **Start** – Der Task wurde gestartet;
- **Stopp** – Der Task wurde beendet;
- **Startfehler** – Fehler beim Starten des Tasks;
- **Erneut starten** – Der Task wird erneut gestartet.

Im rechten Teil des Fensters werden die Programmstatistiken angezeigt. Die Inhalte des Felds 'Statistik' hängen von der Art des Tasks ab.

So sind zum Beispiel für den Task "Automatisiertes Update" folgende Zeilen im Feld 'Statistik' zu sehen: **Datum**, **Zeit**, **Aktion**, **Ergebnis** und **Objekt**, die jeweils anzeigen, an welchem Datum und zu welcher Zeit der Task gestartet wurde, welche Aktionen ausgeführt wurden, deren Ergebnisse, und auf welche Objekte die Aktionen angewandt wurden.

Im unteren Teil des Fensters finden Sie eine Liste der Ereignisse mit Angabe des Datums und der Zeit, wenn diese eingetreten sind, sowie von welcher Komponente sie gestartet wurden. Die Ereignisse werden von allen laufenden Komponenten des Softwarepakets an das Kaspersky AV Control Centre geschickt. Sie können die Ereignisse nach Namen oder Datum sowohl aufwärts, als auch abwärts sortieren. In diese Liste werden nur kritische Ereignisse aufgenommen. Wählen Sie ein Ereignis aus der Liste aus, wird das Programm, von dem es ausging, hervorgehoben.



Die Liste besitzt ein Kontextmenü (Bild 23). Die Elemente des Kontextmenüs werden für folgende Aktionen benutzt:

Bild 23. Kontextmenü in der Ereignisliste.

- **Löschen** – Löscht das ausgewählte Ereignis (nach Bestätigung);
- **Alles löschen** – Löscht alle Ereignisse aus der Liste (nach Bestätigung).

Zur Verwaltung der Tasks (beispielsweise erstellen, konfigurieren, entfernen, starten und beenden) werden das Kontextmenü und die Schaltflächen der Symbolleiste (Bild 24) verwendet.

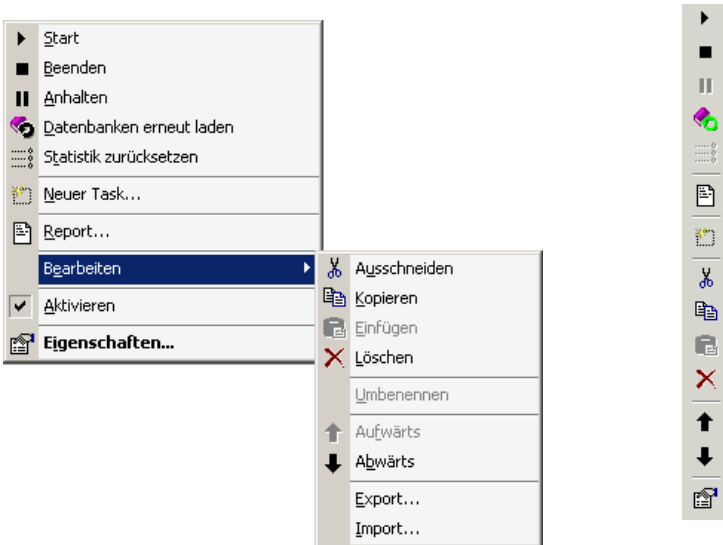


Bild 24. Kontextmenü der Task-Liste und Symbolleiste auf der Registerkarte **Tasks**

Um das Kontextmenü zu öffnen, klicken Sie mit der rechten Maustaste in den linken Teil des Fensters, d.h. dort, wo sich Task-Liste und Statusanzeige befinden.

- **Start** – Task starten;
- **Beenden** – Ausführung beenden und den Task aus dem Arbeitsspeicher entfernen;

- **Anhalten** – Ausführung des Tasks anhalten. Dabei bleibt der Task im Arbeitsspeicher. Die Ausführung wird angehalten;
- **Datenbanken erneut laden** – Antiviren-Datenbanken neu laden. Dieser Befehl wird nur für residente Tasks benötigt, in die neue Antiviren-Datenbanken zu laden sind, ohne den Task neu zu starten;
- **Statistik zurücksetzen** – Statistiken der Task-Ausführung löschen (nur für residente Programme);
- **Neuer Task** – Neuen Task erstellen. Wenn Sie diesen Eintrag auswählen, wird ein Task-Assistent gestartet (siehe **Ошибка! Источник ссылки не найден.**);
- **Report** – Im Fenster des Kaspersky Report Viewer (siehe Kapitel 11) den Task-Report anzeigen;
- **Aktivieren** – Einen Task in den Zeitplaner aufnehmen / aus dem Zeitplaner ausschließen. Wenn Sie den Task aus dem Zeitplaner ausschließen, wird er zwar in der Liste angezeigt, aber vom Zeitplaner nicht mehr gestartet;
- **Eigenschaften** – Einstellungen des Tasks anzeigen;
- **Bearbeiten** – Task-Einstellungen anpassen (dieses Element besteht aus einem Untermenü mit folgenden Einträgen:
 - **Ausschneiden** – einen Task aus der Liste "ausschneiden" und in der internen Zwischenablage des Kaspersky AV Control Centre speichern; dabei wird der Name des Tasks, die Einstellungen und der Zeitplan zum Starten gespeichert;
 - **Kopieren** – einen Task in die interne Zwischenablage kopieren;
 - **Einfügen** – einen Task aus der internen Zwischenablage in die Task-Liste aufnehmen;
 - **Löschen** – einen Task aus der Liste löschen;
 - **Umbenennen** – einen Task umbenennen;
 - **Aufwärts** – einen Task in der Liste um eine Zeile nach oben verschieben;







- **Abwärts** – einen Task in der Liste um eine Zeile nach unten verschieben;
- **Export** – einen Task in einer Datei speichern. Wenn Sie diesen Eintrag wählen, öffnet sich ein Fenster zum Speichern der Task-Einstellungen in einer Datei mit der Erweiterung .tsk;
- **Import** – einen Task aus einer Datei laden.

Die Befehle **Export** und **Import** dienen zum Austausch von Tasks zwischen Rechnern, d.h. Sie können einen Task auf einem Computer erstellen, in einem gemeinsamen Ordner auf dem Server ablegen und ihn auf einem anderen Arbeitsplatz laden.

Einige Befehle können für bestimmte Tasks nicht verfügbar sein.

Die Position der Tasks in der Liste bestimmt die Reihenfolge, in der sie gestartet werden.

Die Tasks werden, wie oben erwähnt, mithilfe von Schaltflächen in der Symbolleiste verwaltet. Diese Schaltflächen entsprechen folgenden Einträgen im Kontextmenü:

Schaltfläche	Eintrag im Kontextmenü
	Starten
	Abbrechen
	Anhalten
	Datenbanken erneut laden
	Statistik zurücksetzen
	Report anzeigen

Schaltfläche	Eintrag im Kontextmenü
--------------	------------------------



	Neuer Task
--	-------------------



	Eigenschaften
--	----------------------



	Löschen
--	----------------


Wenn Sie den Mauszeiger auf eine Schaltfläche bewegen, erscheint ein Popup-Tipp, der die Funktion der Schaltfläche erläutert.

 Zur Bearbeitung der Tasks gibt es verschiedene Funktionen:


Drücken Sie eine Buchstabentaste auf der Tastatur, gelangen Sie zu den Listeneinträgen, die mit dem gewählten Buchstaben beginnen.

Es gibt noch andere Tasten zum schnellen Zugriff.

- **Einfügen** – einen neuen Task erstellen. Wenn sie diese Taste anklicken, wird das Fenster "Neuer Task" geöffnet (Näheres siehe Punkt **Ошибка! Источник ссылки не найден.**).
- **Entfernen** – einen Task aus der Liste entfernen (nach Bestätigung).
- **Leertaste** –Eigenschaften des ausgewählten Tasks anzeigen. Wenn Sie diese Taste anklicken, wird das Fenster "Eigenschaften" geöffnet (Näheres siehe Punkt 10.3.1.1).

Wenn zum Beispiel ein Task **Automatisiertes Update** in der Liste vorhanden ist, und Sie die Taste  auf der Tastatur drücken, wählen sie damit diesen Task aus.

10.3.1.1. Fenster **Eigenschaften**

Dieses Fenster erscheint, wenn Sie auf die Schaltfläche  klicken oder **Eigenschaften** im Kontextmenü auswählen. Das Erscheinungsbild des Fensters hängt von der Art des Tasks ab, den es beschreibt.

In dieser Version des Softwareprodukts gibt es folgende Fenster des Kaspersky Anti-Virus Updater.

Das Fenster **Eigenschaften** für Tasks des Kaspersky AV Updater besteht aus einer Reihe von Registerkarten mit Einstellungen Bild 25.

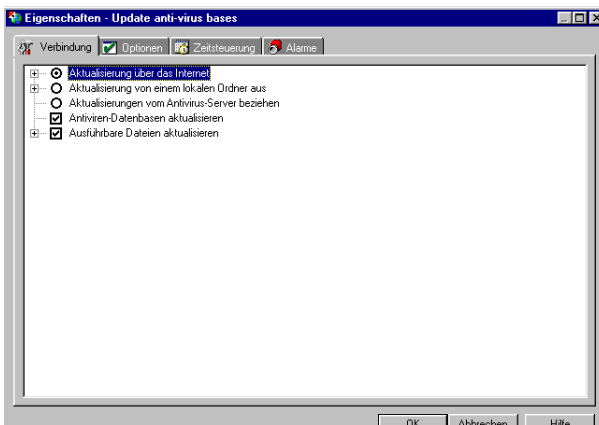


Bild 25. Fenster **Eigenschaften** für
Tasks des Kaspersky AV Updater

Registerkarte	Beschreibung
Verbindung	Siehe Punkt 9.3.2
Optionen	Siehe Punkt 9.3.4
Benutzerkonto	Siehe Punkt 10.4.4

Registerkarte	Beschreibung
Zeitplan	Siehe Punkt 10.4.2
Warnungen	Siehe Punkt 10.4.3

📁 Die Registerkarte **Verbindung** im Fenster "Eigenschaften" enthält eine zusätzliche Option, mit der Sie Ihre Antiviren-Datenbanken und ausführbare Module über einen Ordner auf dem Kaspersky AV Server aktualisieren können. Dies ist die Option "Vom Kaspersky AV Server aktualisieren".

10.3.2. Registerkarte Komponenten

In der Registerkarte **Komponenten** (Bild 26) befindet sich die Liste der Komponenten⁵ der **Kaspersky Anti-Virus Software**.

⁵ Eine Komponente ist ein Programm, ein Hilfsprogramm, eine Bibliothek, eine Bibliothek oder eine Datenbank aus dem Kaspersky Anti-Virus Paket, das jeweils für ein genau abgegrenztes Aufgabengebiet zuständig ist.

KASPERSKY ANTI-VIRUS FÜR LOTUS NOTES/DOMINO

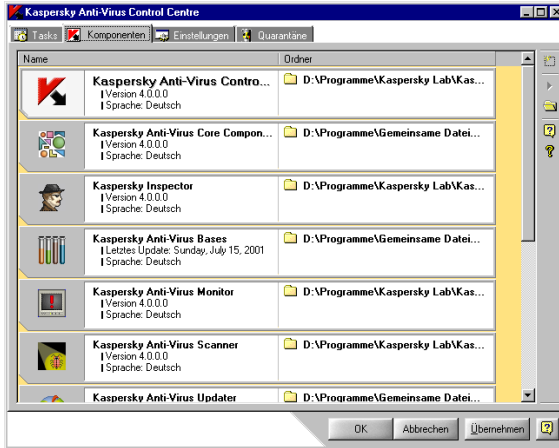


Bild 26. Registerkarte **Komponenten**

Im rechten Teil der Registerkarte befindet sich die Symbolleiste (Bild 27). Wenn sie mit der rechten Maustaste klicken, erscheint das Kontextmenü.

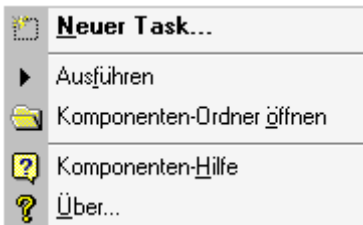







Bild 27. Kontextmenü und Symbolleiste auf der Registerkarte
Komponenten

Die Schaltflächen der Symbolleiste entsprechen genau den Einträgen im Kontextmenü (siehe unten).

Schaltfläche	Eintrag im Kontextmenü	Beschreibung
	Neuer Task...	Erstellt basierend auf der ausgewählten Komponente einen neuen Task. Wenn Sie auf diese Schaltfläche klicken oder diesen Menüeintrag wählen, wird das Fenster Neuer Task geöffnet (Näheres siehe im Punkt Ошибка! Источник ссылки не найден..)
	Ausführen...	Startet die Task-Ausführung.
	Komponenten-Ordner öffnen	Zeigt in einem Standarddialogfeld des MS Windows die Komponentenordner an.
	Komponenten-Hilfe	Startet das Hilfesystem für die gewünschte Komponente-
	Über...	Anzeigen der Informationen über die Produktversion, das letzte Update der Antiviren-Datenbanken und anderes. Wenn sie auf diese Schaltfläche klicken oder diesen Menüeintrag auswählen, öffnet sich das Fenster Über das Programm

10.3.3. Registerkarte **Einstellungen**

Die Registerkarte **Einstellungen** (Bild 28) dient zur Auswahl der Einstellungen des Kaspersky AV Control Centre. Die Einstellungen sind in

vier Kategorien unterteilt. Jede Kategorie fasst die Einstellungen für eine genau abgegrenzte Art von Funktionen zusammen.

Die Liste Einstellungskategorien befindet sich im linken Fensterteil. Wenn Sie eine oder andere Kategorie wählen, wird rechts der entsprechende Einstellungsbaum angezeigt (Näheres über Einstellungsbaum siehe Kapitel 12).

☞ Falls alle Kategorien im Fenster nicht untergebracht werden können, erscheinen an ihrer Stelle die Schaltflächen ▲ und ▼, mit denen Sie die Liste blättern können.

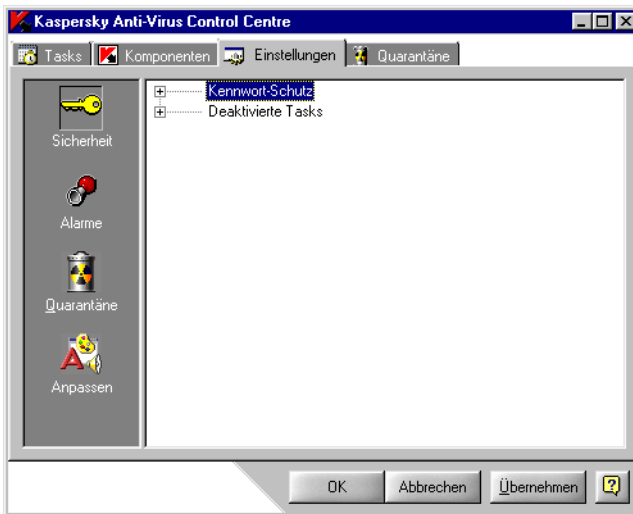


Bild 28. Registerkarte **Einstellungen**

☞ Wenn das Fenster zu klein ist, erscheinen in der Liste der Kategorien die Schaltflächen ▲ und ▼, mit denen man aufwärts und abwärts blättern kann.

Kategorie

Funktion



Sicherheit

Diese Kategorie enthält Optionen, die die Sicherheit des Systems gewährleisten und den Zugriff auf Einstellungen und Komponenten des Kaspersky AV Control Centre einschränken;



Alarme

Diese Kategorie enthält Optionen, die die Behandlung kritischer Ereignisse bei Ausführung der Tasks des Kaspersky AV Control Centre bestimmen;



Quarantäne

Diese Kategorie enthält Optionen zum Einrichten des Quarantäne-Ordners auf einem Arbeitsplatz oder auf dem Server (wichtig nur für Arbeit unter Kaspersky Administration Kit); Näheres über Quarantäne siehe unten.



Anpassen

Diese Kategorie enthält Optionen zum Einrichten der Benutzeroberfläche des Kaspersky AV Control Centre.

10.3.3.1. Kategorie Sicherheit

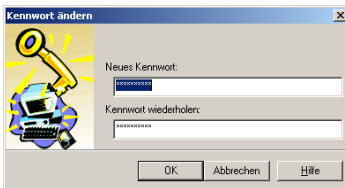


Diese Kategorie (Bild 29) enthält Einstellungen, die mit der Sicherheit des Systems zusammenhängen. Hier wird der Passwortschutz und die Verweigerung des Zugriffs auf einige Arten von Tasks eingestellt.

Bild 29. Registerkarte
Einstellungen. Kategorie
Sicherheit

Dieses Element verfügt über folgende Optionen:

- ☰ **Kennwort** – Passworteingabe zur Verwaltung des **Kaspersky Anti-Virus** mithilfe des Kaspersky Anti-Virus Control Centre sowie zu Beschränkung des Zugriffs bestimmte Programmfunktionen (die Auflistung der Funktionen bedingt sich auf der unteren Ebene der Einstellungsbaums). Klicken Sie auf die Schaltfläche ☰, erscheint das Fenster **Passwort ändern**.



Dieses Dialogfeld (Bild 30) dient zur Eingabe und Änderung des Passwortes. Geben Sie in das Feld **Neues Kennwort** Ihr Passwort ein, dann wiederholen Sie die Eingabe im Feld **Kennwort wiederholen**.

Bild 30. Dialogfeld
Kennwort ändern

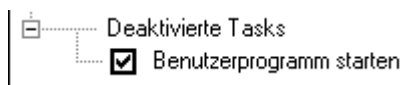
- Schutz vor Unterbrechung residenter Tasks** – Um Ausführung eines Tasks abzubrechen, müssen Sie ein Passwort eingeben. Wenn beispielsweise auf Ihrem Rechner der Anti-Virus Monitor läuft und diese Funktion aktiviert ist, müssen Sie sich mit seinem Passwort anmelden, um die Arbeit des Monitors abzubrechen.
- Schutz vor Unterbrechung nicht residenter Tasks** –

Um Ausführung eines nicht residenten Tasks wie Starten vom Kaspersky AV Scanner oder Kaspersky AV Updater abzubrechen, müssen Sie ein Passwort eingeben.

- ☑ **Änderung der Einstellungen des Kaspersky AV Control Centre** – Öffnen des entsprechenden Dialogfeldes und Änderung der Einstellungen des Kaspersky AV Control Centre sind passwortgeschützt.
- ☑ **Beenden der Arbeit mit Kaspersky AV Control Centre** – um Kaspersky AV Control Centre aus dem Arbeitsspeicher zu entfernen, müssen Sie ein Passwort eingeben.

📁 Bei der Auswahl der zu schützenden Aktionen vergessen Sie nicht, das Passwort in das Feld **Passwort** einzugeben!

Ferner können Sie auf dieser Registerkarte die Ausführung einiger Tasks verbieten, die im Falle eines unerlaubten Zugriffs (Systemeinbruchs) gefährlich sein können.



Diese Option kann im Element **Deaktivierte Tasks** (Bild 31) gewählt werden.

Bild 31. Element **Deaktivierte Tasks**

In dieser Version der Software gibt es nur einen solchen Task:

- ☑ **Benutzeranwendung starten** – Ist diese Option aktiviert, können die Benutzeranwendungen als Tasks des Kaspersky AV Control Centre nicht mehr gestartet werden.

10.3.3.2. Kategorie Alarme

Mit dieser Kategorie (Bild 32) können Sie festlegen, wie von den Tasks erzeugte Warnungen zu behandeln sind.

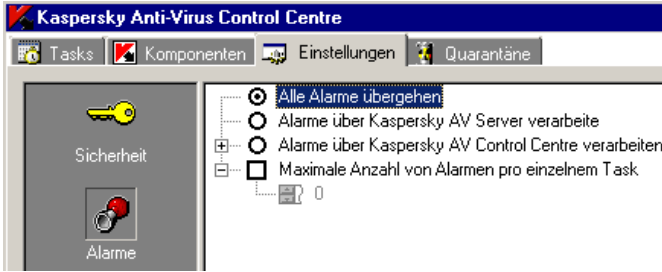


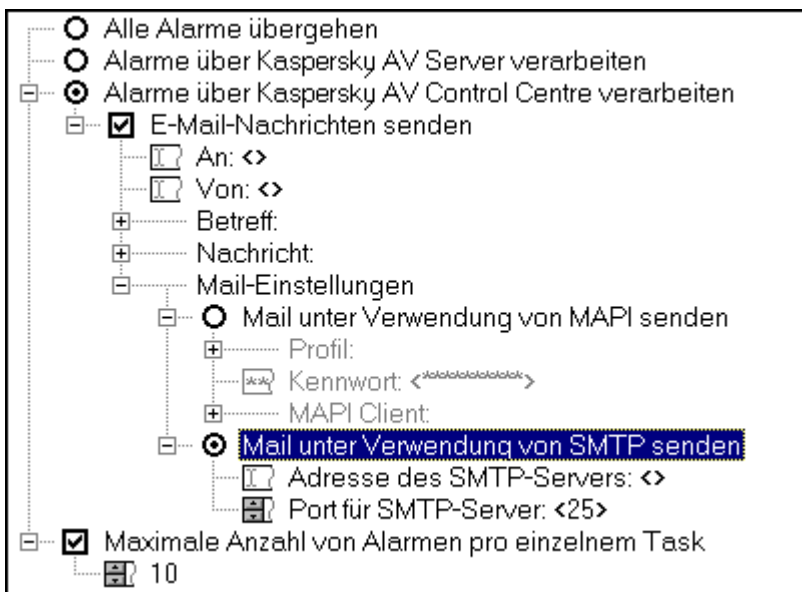
Bild 32. Registerkarte **Einstellungen**. Kategorie **Alarme**

Die Alarme können wie folgt behandelt werden:

- ☉ **Alle Alarme übergehen** – Generieren von Meldungen verbieten.
- ☉ **Alarme über Kaspersky AV Server verarbeiten** – Warnungen über Kaspersky AV **Server senden**.– Kaspersky AV Server ist eine Komponente, die die Verwaltung des Softwarepakets **Kaspersky Anti-Virus** über ein Netzwerk erlaubt.
- ☉ **Alarme über Kaspersky AV Control Centre verarbeiten**– Warmmeldungen über Kaspersky AV Control Centre senden;.

Um die Anzahl der von einem Task zu generierenden Meldungen einzuschränken, aktivieren Sie die Option **Maximale Anzahl von Alarmen pro individuelm Task** und geben dann den gewünschten Wert ein.

📁 So ist beispielsweise auf dem Bild 33. Option Warmmeldungen über Kaspersky AV Control Centre senden eine Situation dargestellt, wenn die maximale Anzahl von Warmmeldungen pro Task auf 10 begrenzt ist. Dies bedeutet, dass wenn Kaspersky AV Control Centre eine elfte Warmmeldung empfängt, wird die Liste eingegangener Warmmeldungen automatisch gelöscht.

Bild 33. Option **E-Mail-Nachrichten senden**

Haben Sie die Option **Alarme über Kaspersky AV Control Centre verarbeiten** aktiviert, so müssen Sie die auch die notwendigen Einstellungen vornehmen. Um Warnmeldungen per E-Mail zu empfangen, aktivieren Sie die Option **E-Mail-Nachrichten senden**. Stellen Sie dann folgende Parameter ein:

An: Tragen Sie hier die E-Mail-Adresse des Empfängers ein;

Von: Tragen Sie hier den Namen oder die Adresse ein, die in der Zeile "Von" der E-Mail-Nachricht erscheinen soll. Hier kann eine beliebige Zeichenkette stehen. Diese Einstellung wird für die Zusammenarbeit mit einigen SMTP Servern benötigt und wird zur Benutzerauthentifizierung verwendet;

Betreff: Betreff der E-Mail-Nachricht;

Nachricht: Der Text, den die E-Mail enthalten soll;

Mail-Einstellungen Legen Sie die Einstellungen des E-Mail-Systems zum Senden von Alarmen fest. Es gibt zwei Methoden zum Senden:

- unter Verwendung von MAPI;
- unter Verwendung von SMTP.

 **Kontaktieren Sie ihren Netzwerkadministrator für weitere Informationen über SMTP und MAPI.**

10.3.3.2.1. Mail unter Verwendung von SMTP senden

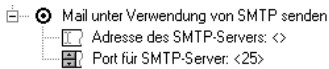


Bild 34. SMTP-Einstellungen.

Um Alarme unter Verwendung von SMTP zu senden, wählen sie die Option **Mail unter Verwendung von SMTP senden** (Bild 34) aus und tragen sie die folgenden Angaben ein:

Adresse des SMTP-Servers

Gibt die Adresse des SMTP-Servers an, die in dezimaler Schreibweise (z. B. 125.5.29.1), als vollständige Domäne (z. B. test.mail.ru) oder in Kurzschreibweise (z. B. test) eingetragen werden kann;

Port für SMTP-Server

Gibt den Port des SMTP-Servers an. Der voreingestellte Wert ist 25.

Wir wollen an einem Beispiel verdeutlichen, wie die Einstellungen der Registerkarte **Alarme** verwendet werden. Wir wollen beispielsweise einstellen, dass SMS-Nachrichten über kritische Ereignisse an das Mobiltelefon eines Systemadministrators mittels eines E-Mail-Gateways geschickt werden.

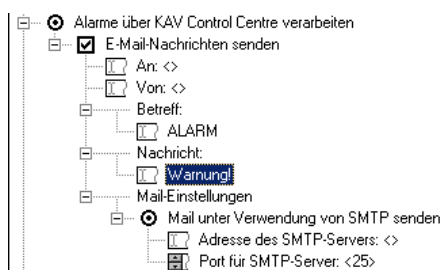
Geben Sie folgende Daten ein:

- Handynummer des Administrators – **1234567 (direkte Rufnummer)**;

- Netzbetreiber – z.B. “Beeline GSM” (d.h. die Netzvorwahl der direkten Rufnummer – 7 901);
- Adresse des SMTP Servers – **mysmtp.home.ru**;
- Port für SMTP Server – **25**.

Vergewissern Sie sich, dass

- die Nachricht von **Control Centre** gesendet wurde,
- die Nachricht den Betreff **Alarm** hatte,
- die Nachricht folgenden Text beinhaltet: **Warnung! Kritisches Ereignis eingetreten!**



Dafür aktivieren Sie folgende Einstellungen (Siehe Bild 35).

Bild 35. Einstellungen für das Senden von Warnungen bei kritischen Ereignissen.

Die Adresse des E-Mail-Gateways sowie die Netzvorwahl des Mobilnetzbetreibers können je nach Standort variieren.

10.3.3.2.2. Mails unter Verwendung von MAPI senden

Wenn auf ihrem Computer das Betriebssystem **Windows 95/98** läuft, können Sie mit Control Centre das Senden von Nachrichten mittels MAPI festlegen.

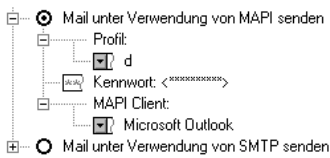


Bild 36. MAPI Einstellungen

Zum Setup der MAPI Parameter, wählen Sie die Option **Mail unter Verwendung von MAPI senden** (Bild 36) und aktivieren folgende Einstellungen:

Profil

Name des Profils (Konfigurations-Datei) des MAPI Clients;

Kennwort

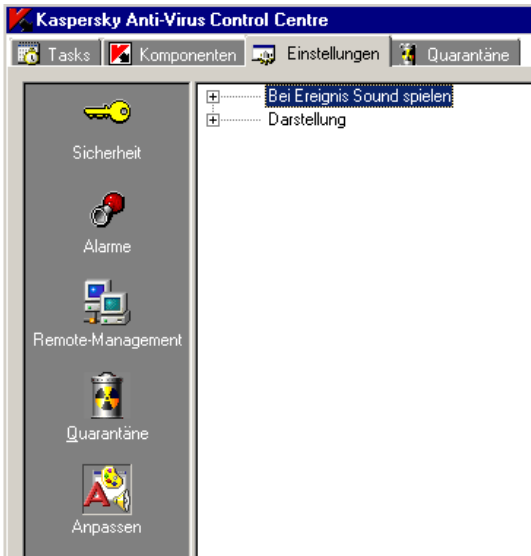
Passwort zum Zugriff auf das Profil;

MAPI Client

Name des MAPI Clients, der verwendet wird, um Warnmeldungen zu senden.

Einige MAPI Clients benutzen keine Profile. Lassen Sie in diesem Fall die Zeilen **Konfiguration** und **Profil-Kennwort** leer.

10.3.3.3. Kategorie Anpassen



Die Kategorie **Anpassen** (Bild 37) beinhaltet die Einstellungen der Programmoberfläche. In dieser Kategorie können sie die akustischen Signale, die bei bestimmten Aktionen abgespielt werden, und die Farbeinstellungen des Programms festlegen.

Bild 37. Die Registerkarte **Einstellungen**.
Kategorie **Anpassen**

Die Kategorie **Anpassen** enthält zwei Elemente: **Bei Ereignis Sound spielen** und **Darstellung**. Es folgt eine kurze Beschreibung dieser Elemente:

Bei Ereignis Sound spielen Einstellung der akustischen Signale, die nach dem Start (oder Beenden) bestimmter Operationen ausgegeben werden) (Siehe Punkt "Sound" für nähere Erläuterungen);

Darstellung

Einstellung der Farben der Programmoberfläche (Siehe Punkt "Farbeinstellungen" für nähere Erläuterungen)

10.3.3.3.1. Sound-Einstellungen

Control Centre erlaubt es, akustische Signale bestimmten Ereignissen zuzuordnen. Dies verleiht ihrem Programm zusätzliche Servicefunktionen.



Die Sound-Einstellungen werden wie oben erwähnt im Element **Bei Ereignis Sound spielen** vorgenommen (Bild 38).

Bild 38. Sound-Einstellungen.

Um eine Option auszuwählen, markieren Sie das Kontrollkästchen neben dem Namen und klicken Sie auf die Schaltfläche **...** zum Öffnen des Fensters für die Auswahl der Audio-Datei. Diese Datei sollte im Format WAV vorliegen. Die einzelnen Sounds haben folgende Bedeutung:

Task starten

Diesen Sound sofort nach dem Start des Tasks abspielen (unabhängig von der Art des Tasks);

Task erfolgreich beendet

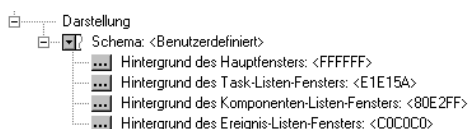
Diesen Sound nach erfolgreichem Abschluss des Tasks abspielen, d.h. falls der Task nicht vom Benutzer abgebrochen wurde und nicht mit einem Fehler beendet wurde;

Task vom Benutzer abgebrochen Diesen Sound abspielen, wenn der Task vom Benutzer abgebrochen wurde;

Task fehlgeschlagen Gibt einen Sound aus, der auf das Scheitern des Tasks hinweist;

10.3.3.3.2. Farbeinstellungen

Mithilfe von Kaspersky AV Control Centre können Sie die farbliche Gestaltung der Benutzeroberfläche ändern.



Die Farbeinstellung der Elemente der Oberfläche werden, wie oben erwähnt, im Element **Darstellung** verändert (Bild 39).

Bild 39. Darstellung

Um dem Benutzer die Einstellung der Farben zu erleichtern, enthält die Anwendung eine Auswahl an standardmäßigen Farbschemata. Um ein Farbschema auszuwählen, gehen Sie zur Liste **Schema <...>**. Jedes Schema ist durch die folgenden Einstellungen gekennzeichnet:

Hintergrund des Hauptfensters Die Hintergrundfarbe des Hauptfensters der Anwendung;

Hintergrund des Task-Listen-Fensters Die Hintergrundfarbe des Task-Listen-Fensters auf der Registerkarte **Tasks**

Hintergrund des Komponenten-Listen-Fensters Die Hintergrundfarbe der Registerkarte **Komponenten**

Hintergrund des Ereignis-Listen-Fensters Die Hintergrundfarbe der Registerkarte **Tasks**

Auf den folgenden Abbildungen (Bild 40) als Beispiel das Farbschema **Lila** dargestellt und dessen Einstellungen werden angezeigt.

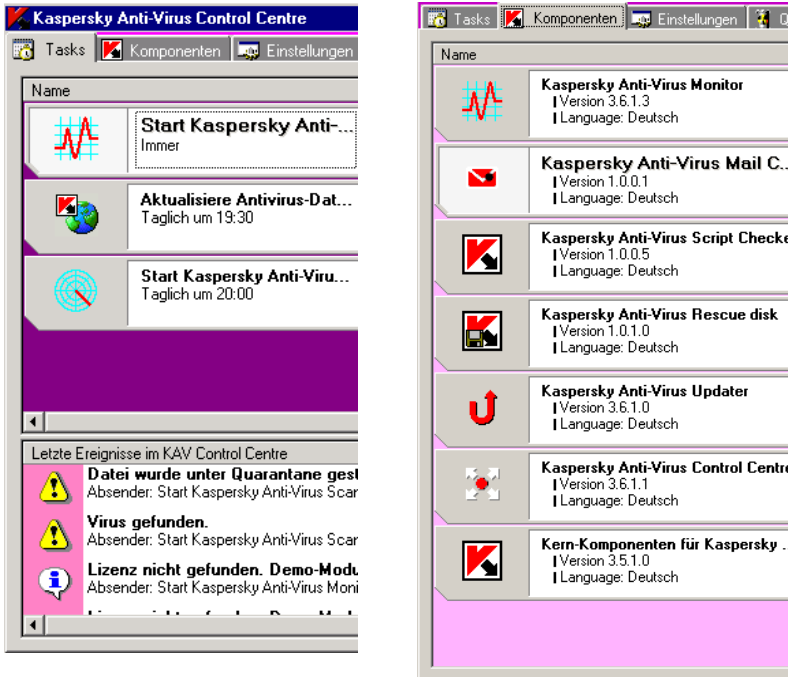



Bild 40 KAV Control Centre. Registerkarte **Komponenten**

10.4. Task-Assistent

Die zeitgesteuerte Ausführung einer bestimmten Anwendung mit einer vorgegebenen Liste von Parametern und Einstellungen kann als ein gesonderter Task des Zeitplaners festgelegt werden werden.

Der Wizard Neuer Task wird gestartet, wenn Sie **Neuer Task** im Kontextmenü auswählen oder auf die Schaltfläche  in der Symbolleiste der Registerkarten **Tasks** oder **Komponenten** klicken.

Das Erstellen eines neuen Tasks in Control Centre gleicht einem **Windows Wizard** und besteht aus einer Folge von Fenstern (Schritten), von denen jedes einzelne bestimmte Aktionen erfordert.

Um von einem Wizard-Fenster zum anderen zu gelangen, klicken Sie auf die Schaltflächen **Weiter** (einen Schritt vorwärts) und **Zurück** (einen Schritt rückwärts). Um das Erstellen des Tasks abzuschließen, klicken Sie auf **Fertigstellen**. Um das Erstellen des Tasks abubrechen, klicken Sie auf **Abbrechen**. Um zu dem jeweiligen Schritt Hilfe zu erhalten, klicken Sie auf **Hilfe**.

10.4.1. Fenster Tasks

In Abhängigkeit von ihren Aufgaben, den gestarteten Programmen und ihren Einstellungen können Tasks in zwei Gruppen eingeteilt werden:

- Tasks, die während ihrer Ausführung Anwendungen aus dem Paket **Kaspersky Anti-Virus** starten;
- andere Tasks.

Geben Sie im Fenster **Neuer Task** Name und Typ des Tasks an (Bild 41).

Es gibt folgende Task-Typen:

- **Scannen von Arbeitsspeicher und Laufwerken** – Starten des Kaspersky AV Scanner mit der Möglichkeit für jeden Task andere Scan-Parameter einzustellen. Der Task kann automatisch zeitgesteuert, auf Grund des Eintretens eines bestimmten Ereignisses oder durch direkte Benutzereingabe gestartet werden;

- **Online scannen** – Startet den Kaspersky Anti-Virus Monitor und/oder nimmt zeitbedingte Änderungen an seinen Einstellungen vor, ohne den Computer neu zu starten. Der Startzeitpunkt für jede Einstellung kann entweder mit der Zeitsteuerung genau festgelegt werden, oder durch das Eintreten bestimmter Systemereignisse bestimmt werden, oder er wird dadurch bestimmt, dass der Benutzer von einer Tätigkeit zu einer anderen übergeht (zum Beispiel während des Installierens neuer Software, Kopieren von importierten Programmen und Dokumenten, Empfangen von E-Mail und so weiter);

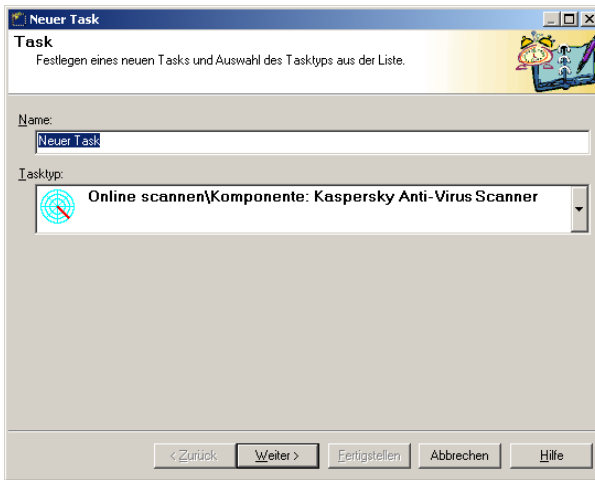


Bild 41. Fenster **Task**.

- **Update der Antiviren-Datenbanken** – Automatisiertes Update der Datenbank mit den neuen Virendaten. Das Update kann über das Internet oder über ein lokales Netzwerk vorgenommen werden, was die Verbindungskosten verringert, die Geschwindigkeit des Updateprozesses erhöht und die Administration des Pakets vereinfacht;
- **Benutzerprogramm starten** – Jede Anwendung, die von Control Centre aus gestartet werden kann;

- **Installation neuer Programme** – Start des Wizards zum Einrichten neuer Anwendungen.

10.4.2. Fenster Zeitsteuerung für Kaspersky Anti-Virus Updater

Beim Erstellen eines Kaspersky Anti-Virus Updater Tasks sollten Sie im Fenster **Zeitsteuerung** die Voraussetzungen und die Häufigkeit des Starts angeben (Bild 42).

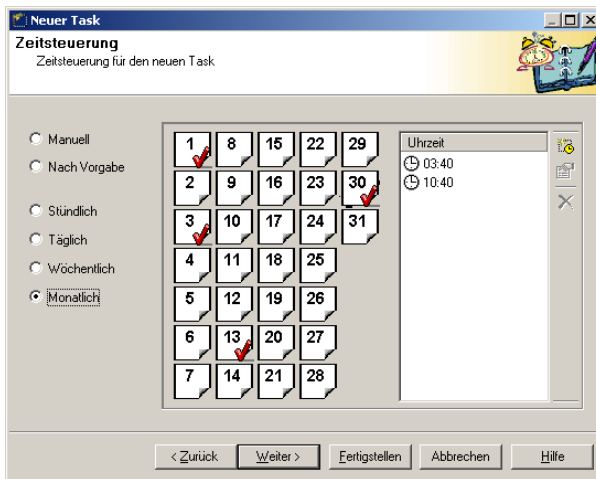


Bild 42. Dialogfeld **Zeitsteuerung** für Tasks des Kaspersky AV Updater

Es gibt folgende Möglichkeiten zum Starten:

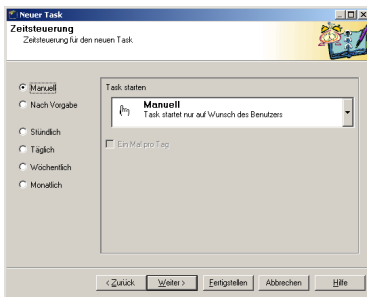
Manuell Start des Tasks auf Grund eines Ereignisses oder durch Benutzereingabe (Siehe "Start von Tasks");

- Nach Vorgabe** Start des Tasks in Abhängigkeit davon, ob die angegebene Bedingung beim Beenden einer Task-Art erfüllt ist (Siehe "Bedingungsgesteuerter Start von Tasks")
- Stündlich** Start des Tasks zum angegebenen Zeitpunkt im Abstand von einer Stunde (Siehe "Task jede Stunde starten");
- Täglich** Täglicher Start des Tasks zum angegebenen Zeitpunkt (Siehe "Task jeden Tag starten");
- Wöchentlich** Wöchentlicher Start des Tasks zum angegebenen Zeitpunkt (Siehe "Task jede Woche starten");
- Monatlich** Monatlicher Start des Tasks am angegebenen Tag zum angegebenen Zeitpunkt (Siehe "Task jeden Monat starten").

Wählen Sie im linken Teil des Dialogfeldes den gewünschten Startintervall aus und stellen Sie die Zeitsteuerung wie in den folgenden Kapiteln beschrieben ein.

10.4.2.1. Start von Tasks nach Eintreten bestimmter Ereignisse

Kaspersky AV Control Centre erlaubt es, den Task durch das Eintreten eines Ereignisses im System oder durch Benutzereingabe zu starten.



Um diese Art des Starts auszuwählen, aktivieren Sie **Manuell**, dann erscheint im rechten Teil des Fensters **Zeitsteuerung** die Liste der Bedingungen (Bild 43).

Bild 43. Zeitsteuerung.
Einstellung des Manuellen Starts.

Wählen Sie eine Startbedingung aus der Liste aus. Es gibt mehrere Möglichkeiten:

Manuell

Der Task wird manuell durch Benutzereingabe in Control Centre gestartet;

Beim Start von Control Centre

Der Task wird beim Start von Control Centre ausgeführt, d.h. bei der Anmeldung des Benutzers;

Beim Start des Bildschirmschoners

Der Task wird beim Start des Bildschirmschoners ausgeführt;

Beim Start von Control Centre System Service

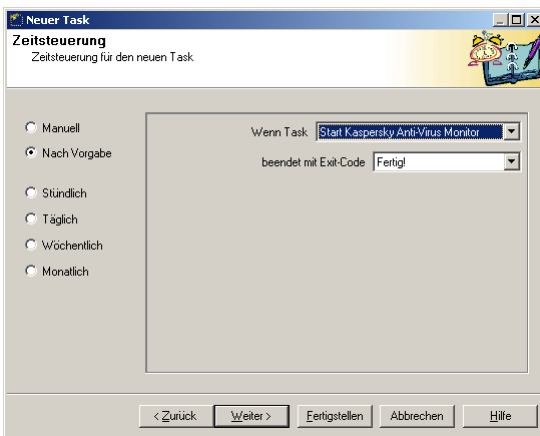
Der Task wird beim Starten von Control Centre System Service ausgeführt, d.h. beim Systemstart.

Alle Arten von Tasks können einmal täglich oder bei jedem Eintreten des Ereignisses gestartet werden.

10.4.2.2. Bedingungsgesteuerter Start von Tasks

Kaspersky AV Control Centre erlaubt es, die Ausführung eines Tasks davon abhängig zu machen, ob eine bestimmte Bedingung erfüllt ist, nachdem eine Komponente des Pakets seine Arbeit beendet hat.

In dieser Version des Produkts geschieht dies folgendermaßen: der Benutzer kann einen Task erstellen, der gestartet wird wenn ein **Kaspersky Anti-Virus** Task mit einem bestimmten Exit-Code beendet wird.



Wählen Sie im linken Teil des Fensters **Zeitsteuerung** die Option **Nach Vorgabe**, um den Task auf diese Art zu starten (Bild 44).

Bild 44. Zeitsteuerung nach Vorgabe.

Wählen Sie danach im Eingabefeld **Wenn Task** den Task-Status, von dem die Bedingung abhängen soll, und stellen Sie in der Liste **beendet mit Exit-Code** den Rückgabewert des Tasks ein.

Der Task-Status, von dem die Bedingung abhängt, wird als Haupttask bezeichnet, und der Rückgabewert des Haupttasks als Ergebnis des Haupttasks.

Es gibt folgende Haupttypen von Task **Viren-Datenbanken aktualisieren**.

Das Programm bearbeitet folgende Ergebnisse des Haupttasks:

- **Beliebiges Ergebnis** – Der erstellte Task wird sofort nach der Ausführung des Haupttasks ungeachtet des Ergebnisses gestartet;
- **Fertig** – Der erstellte Task wird nur gestartet, wenn der Haupttask erfolgreich beendet wurde;
- **Störung** – Der erstellte Task wird nur gestartet, wenn bei der Ausführung des Haupttasks ein Fehler auftritt;
- **Vom Benutzer abgebrochen** – Der erstellte Task startet, falls die Ausführung des Haupttasks vom Benutzer abgebrochen wurde.

10.4.2.3. Task jede Stunde starten

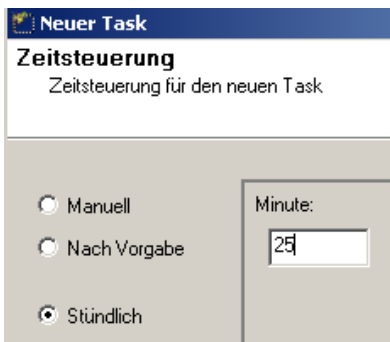


Bild 45. Task jede Stunde starten

Um den erstellten Task jede Stunde zu starten, wählen Sie die Option **Stündlich** im linken Teil des Fensters **Zeitsteuerung** (Bild 45), und stellen dann die Startzeit im rechten Teil des Fensters ein.

Bild 45 zeigt die Einstellung des stündlichen Starts der Zeitsteuerung jeweils zu Minute 25 einer Stunde. Wenn Sie beispielsweise um 12:00 Uhr den Wert **25** eintragen, startet der Task um 12:25, 13:25, 14:25 und so weiter.

10.4.2.4. Task jeden Tag starten

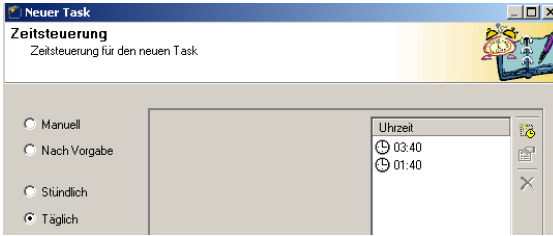


Bild 46. Task jeden Tag starten

Um den Task täglich zu einer bestimmten Zeit zu starten, wählen Sie die Option **Täglich** im Fenster **Zeitsteuerung** aus (Bild 46) und stellen dann die Startzeit ein.

Die Einstellung der Startzeit wird in der Liste **Uhrzeit** vorgenommen. Benutzen Sie dazu Control Centre und das Kontextmenü. Sie können diese folgendermaßen verwenden.

Schaltfläche der Symbolleiste	Eintrag im Kontextmenü	im Zweck
-------------------------------------	------------------------------	-------------



Erstellen...

Eine neue Startzeit eintragen. Wenn Sie diesen Eintrag auswählen und das Fenster **Zeit** aktiviert wird, geben Sie die Startzeit des Tasks ein. Dieses Dialogfeld können Sie mit einem Doppelklick an beliebiger freier Stelle in der Liste **Zeit** aufrufen, oder wenn Sie die Taste **Einfügen** in der Tastatur drücken.

Schaltfläche der Symbolleiste

Eintrag im Zweck Kontextmenü



Ändern...

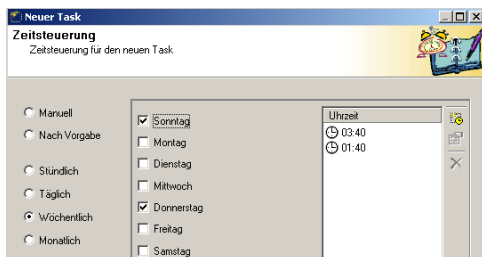
Ändern der Startzeit des Tasks. Wenn Sie diesen Eintrag auswählen und das Fenster **Zeit** aktiviert wird, geben Sie die neue Startzeit ein. Sie können einen Doppelklick auf die zu ändernde Zeile ausführen oder die **Leertaste** drücken.



Löschen...

Löschen der Startzeit aus der Liste. Sie können auch die Taste **Entf.** Bei gewählter Zeile drücken.

10.4.2.5. Task jede Woche starten



Der Auswahlschalter **Wöchentlich** auf der linken Seite des Fensters **Zeitsteuerung** erlaubt es Ihnen, den Task wöchentlich zu starten: an festgelegten Tagen und zu festgelegten Zeitpunkten.

Bild 47. Task jede Woche starten

Die Angabe der Tage und Stunden, zu denen der Task gestartet werden soll erfolgt, indem Sie Wochentage markieren und die Uhrzeit im Fenster **Zeit** eintragen. Siehe "Task jeden Tag starten" für nähere Erläuterungen zum Einstellen der Startzeit.

Bild 47 zeigt die Einstellung zum Starten des Tasks montags (3:40 a.m. und 10:40 p.m.) und freitags (3:40 a.m. und 10:40 p.m.).

10.4.2.6. Task jeden Monat starten

Um den Task jeden Monat an festgelegten Tagen und zu festgelegten Zeiten zu starten, wählen Sie die Option **Monatlich** auf der Registerkarte **Zeitsteuerung** (Bild 48).

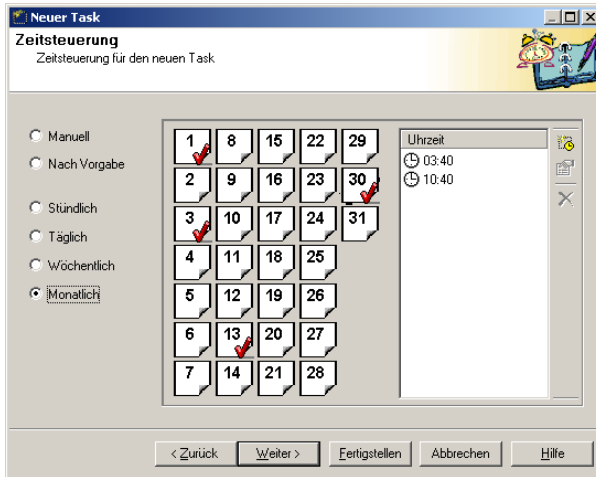

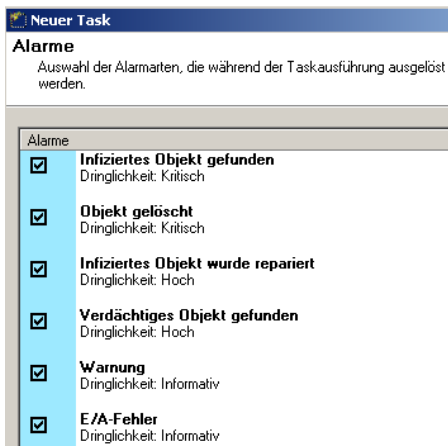


Bild 48. Task jeden Monat starten.

Benutzen Sie Ihre Maus, um die Tage zu markieren, an denen die erstellten Tasks gestartet werden sollen, und geben Sie den Startzeitpunkt im Element **Zeit** an (Siehe "Task jeden Tag starten" für nähere Erläuterungen zum Einstellen der Startzeit).

Die Tage, an denen der Task gestartet wird, sind mit  markiert. Bild 48 zeigt die Einstellung zum Starten des Tasks am ersten, dritten, dreizehnten und dreißigsten jeden Monats um 3:40 a.m. und 10:40 p.m.

10.4.3. Fenster Alarme



Wählen Sie im Fenster **Alarme** (Bild 49) die Warnmeldungen aus, die von diesem Task erzeugt werden.

Wie oben erwähnt sind Warnungen Nachrichten, die von Tasks erzeugt werden.

Um eine Warnmeldung auszuwählen, aktivieren Sie das entsprechende Kontrollkästchen.

Bild 49. Auswahl der Alarmarten.

10.4.4. Fenster Benutzerkonto

Control Centre kann als **Windows** Systemdienst vor der Benutzeranmeldung ausgeführt werden. Geben Sie in diesem Fall das Benutzerkonto an, das von diesem Task benutzt werden soll.

Benutzerkonto enthält Informationen (wie vollständiger Name, Passwort und mehr) über den Benutzer.

Um das Konto zu konfigurieren, wechseln Sie zum Fenster **Benutzerkonto** (Bild 50). Wenn ein Task unter einem anderen Benutzerkonto gestartet wird, das sich vom aktuellen Konto unterscheidet, so werden die vom Task generierten Meldungen nur dann angezeigt, wenn Sie die Option **Zugriff auf Arbeitsplatz** aktivieren.

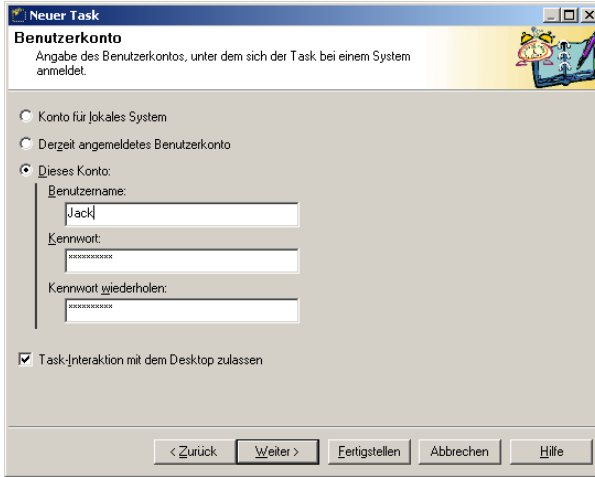


Bild 50. Benutzerkonto für den Task-Start.

Sie können folgende Konten benutzen:

**Konto für Windows-Konto
lokales
System**

**Derzeit angemeldetes
Benutzerkonto** Das aktuelle Benutzerkonto

Dieses Konto Konto des Benutzers, dessen
Einstellungen in den Zeilen
Benutzername, **Wennwort** und
Kennwort wiederholen angegeben
werden.

Um einem Task den Zugriff auf den Desktop zu gewähren, aktivieren Sie die Option **Task-Interaktion mit dem Desktop zulassen**.

10.4.5. Task-Einstellungen

In diesem Schritt der Task-Erstellung geben Sie die für diesen Task spezifischen Parameter an. Grundsätzlich gleichen diese Einstellungen den Registerkarten.

Folgende Task-Typen und Fenster werden in diesem Schritt aktiviert:

Task-Typ	Fenster Reihenfolge	Beschreibung
Kaspersky Anti- Virus Updater	1. Verbindung	Siehe Beschreibung in Kapitel 9.3.2. Es gibt in diesem Fenster zwei zusätzliche Optionen, die es erlauben, die Antiviren-Datenbanken und die ausführbaren Module im angegebenen Ordner des Kaspersky Anti-Virus Servers zu installieren.
	2. Einstellungen	Siehe Beschreibung im Punkt 9.3.4.

11. Kaspersky Report Viewer

*Funktion des Programms. Aktivierung
Beschreibung der Benutzeroberfläche*

11.1. Wofür wird Kaspersky Report Viewer verwendet?

Kaspersky Report Viewer ist ein Programm zur Ansicht und Verwaltung von Reports, die von Komponenten des Softwarepakets **Kaspersky Anti-Virus** generiert werden.







11.2. Aktivierung der Report- Anzeige

Um **Kaspersky Report Viewer** zu aktivieren, klicken Sie im Fenster **Fertigstellen** auf **Bericht**.

Rechts oben im Report-Fenster befindet sich die Symbolleiste, die die Schaltflächen zur Steuerung der Kaspersky Report Viewer enthält. Die Schaltflächen besitzen eine Direkthilfe. Um auf diese zuzugreifen, zeigen Sie mit dem Mauszeiger auf die entsprechende Schaltfläche. Neben der Schaltfläche wird dann ein kleines Fenster mit einem kurzen Hilfetext eingeblendet.

Im oberen Teil des Fensters sehen Sie das Hauptmenü. Es ist zu erwähnen, dass bestimmte Schaltflächen der Symbolleiste über analoge Menübefehle verfügen.


Unten finden Sie eine vergleichende Tabelle über die Korrespondenz zwischen Schaltflächen und Menübefehlen und deren Funktionen.

Symbolleiste	Menü	Funktion
	Ansicht Maximieren	→ Positioniert ein Anwendungs-fenster über alle anderen Programmfenster auf dem Windows -Desktop.
	Datei→Öffnen	Öffnet eine gespeicherte Reportdatei.
	Datei→ Speichern unter...	Speichert den Report in einer Datei mit einem anderen Namen.
	Datei→ Report löschen	Löscht alle Daten in der Report-Datei.
	Datei→ Drucken	Druckt den Report aus
	Ansicht→ Aktualisieren	Wiederholt den letzten Ladevorgang des Reports aus einer Datei
	Bearbeiten→ Suchen	Suche einer Zeile oder eines Teils davon im Report. Wenn Sie auf diese Schaltfläche klicken, dann wird das Such-Fenster geöffnet

Symbolleiste	Menü	Funktion
	Bearbeiten→ Weitersuchen	Suche der nächsten Zeile (oder eines Teils davon), die mit dem Suchmuster übereinstimmt.
	Ansicht→Report verfolgen	Report verfolgen (wenn Sie diese Option aktivieren, wird beim Eingang neuer Daten der Report automatisch auf die letzte Zeile positioniert).
	Ansicht→Letzte Session	Report-Vorschau für die letzte Session.
	Ansicht→Nur Statistik	Zeigt nur Statistiken an
	Ansicht→ Nur Kommentar	Zeigt nur Kommentare an
	Hilfe	Hilfetext



Bild 52. Fenster **Suchen im Report**



Suchfenster (Bild 52) erscheint, wenn Sie die Schaltfläche  in der Symbolleiste anklicken oder den Eintrag **Suchen** im Menü **Bearbeiten** wählen. Um eine Zeile (oder einen Teil davon zu suchen) geben Sie diese ins Feld **Zeile finden** ein, geben Sie die Suchkriterien an und klicken Sie auf **Ok**.

Für die Suche sind folgende Einstellungen möglich:

- **Nur ganzes Wort suchen** – Suche im Report nach allen Wörtern, die dem angegebenen Muster entsprechen;
- **Groß-/Kleinschreibung beachten** – Zwischen Groß- und Kleinschreibung unterscheiden;

- **Mit Mustervergleich** – Suche nach Reportzeilen, die dem Muster entsprechen.

Um das Fenster zu schließen, klicken Sie auf **Abbrechen**. Um Hilfe zu erhalten, klicken Sie auf **Hilfe**.

 Nachdem Sie die erste Zeile (oder einen Teil davon) eines gewissen Musters gefunden haben, können Sie den Rest der Zeichenkette (oder Unterzeile) suchen. Klicken Sie dazu auf , oder wählen Sie im Menü Bearbeiten den Befehl Weitersuchen.

12. Tree-Chart™


Beschreibung und Arbeitsweise des Bedienungselements Tree-Chart.

12.1. Was ist Tree-Chart?



Die Benutzeroberfläche von Kaspersky Anti-Virus verwendet die sogenannte **Tree-Chart™** Technologie.

Tree-Chart™ ist eine universelle Technologie zur interaktiven Darstellung von Daten. Diese Technologie wurde von Spezialisten des Kaspersky Lab entwickelt und eignet sich sowohl für Einsteiger als auch für erfahrene Anwender. Dabei werden alle Daten in Form eines Baums dargestellt. Die Knoten des Baums sind Standard-Bedienungselemente (Schaltflächen, Listen, Schalter, usw.).

Diese Technologie bietet ein klares und leicht verständliches Bild der Wechselbeziehungen zwischen verschiedenen Einstellungen und macht es einfach, das Programm zu verstehen.







 In diesem Handbuch sind alle Bedienungselemente mit Abbildungen versehen, um das Aussehen der Elemente im Programmfenster zu illustrieren.

12.2. Einstellungsbaum

Jeder Knoten des Baums kann Äste besitzen. Wenn ein Ast geöffnet ist, dann enthält der entsprechende Knoten das Symbol . Ist ein Ast geschlossen, dann enthält der Knoten das Symbol .

Zum Ändern der Einstellungen muss der Ast sichtbar sein.

Um einen Ast anzuzeigen oder auszublenden, können folgende Methoden verwendet werden:

Aktion	Aktivierung
Öffnen eines Knotens (Aussehen des Knotens: )	Die Taste  auf der Tastatur. Der Befehl  Anzeige erweitern im Kontextmenü. Die Taste "+" auf Ihrem numerischen Ziffernblock (alle Äste des Knotens werden angezeigt).
Ausblenden eines Astes (Aussehen des Knotens: )	Die Taste  auf der Tastatur. Der Befehl  Anzeige reduzieren im Kontextmenü. Die Taste - auf Ihrem numerischen Ziffernblock (alle Äste des Knotens werden ausgeblendet).

12.3. Bedienelemente


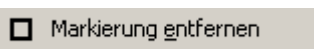
Zum Ändern von Einstellungen können verschiedene Bedienelemente verwendet werden.

12.3.1. Kontrollkästchen

Ein **Kontrollkästchen**, das

- Alle Dateien — deaktiviert bzw. nicht markiert ist, bedeutet, dass der betreffende Typ einer Virus-Untersuchung nicht durchgeführt wird.
- Alle Dateien — aktiviert bzw. markiert ist, bedeutet, dass der betreffende Typ einer Virus-Untersuchung vom Programm durchgeführt wird.

Sie können folgende Methoden anwenden, um eine Kästchen zu aktivieren oder zu deaktivieren:

Funktion	Aufruf
Aktivieren eines Kästchens	<p>Die Taste LEERZEICHEN auf Ihrer Tastatur.</p> <p>Der Befehl  im Kontextmenü.</p> <p>Klicken mit der Maus.</p>
Deaktivieren eines Kästchens	<p>Die Taste LEERZEICHEN auf Ihrer Tastatur.</p> <p>Der Befehl  im Kontextmenü.</p> <p>Klicken mit der Maus.</p>

12.3.2. Options-Schaltfläche

Eine **Options-Schaltfläche** ist ein Element einer Gruppe. Eine Gruppe von Options-Schaltflächen kann aus zwei oder mehr Schaltflächen bestehen. Sie können diese Schaltflächen verwenden, um eine bestimmte Option auszuwählen. Es gibt folgende Options-Schaltflächen:

- Int 13h — nicht markiert (deaktiviert);
- Int 13h — markiert (aktiviert).

Innerhalb einer Gruppe kann nur eine Options-Schaltfläche aktiviert werden.


Zur Auswahl und Abwahl einer Options-Schaltfläche gibt es folgende Methoden:

Funktion

Aufruf

Auswahl der Options-Schaltfläche

Die Taste **Leerzeichen** auf der Tastatur.

Der Befehl  im Kontextmenü.


Die Options-Schaltfläche mit der Maus anklicken.

Abwahl der Options-Schaltfläche

Auswahl einer anderen Options-Schaltfläche aus dieser Gruppe.

12.3.3. Textfeld

Zur Bearbeitung eines Werts in einem **Textfeld** wird die Tastatur verwendet. Der aktuelle Wert des Textfelds wird in eckigen Klammern rechts vom Namen des Textfelds angezeigt.


 Referenzname der Tabellendateien <KAVITAB> — Das Textfeld.

Zur Bearbeitung eines Werts in einem Textfeld gibt es folgende Methoden:

Funktion

Aufruf

Bearbeiten eines Feldwerts Anklicken des Feldsymbols mit der Maus.


Der Befehl  im Kontextmenü.

Die Taste **F2** auf der Tastatur. Das Textfeld ändert sein Aussehen wie folgt .

Nach dem Bearbeiten des Werts in einem Textfeld klicken Sie die Taste **Eingabe** auf der Tastatur oder klicken Sie mit der Maus außerhalb des Textfelds. Um alten Wert wiederherzustellen, drücken Sie die **Esc**,-Taste.

12.3.4. Eingabefeld: Festlegen eines Pfades für ...

Zur Bearbeitung eines Werts in einem **Pfadfeld** verwenden Sie den konventionellen Windows-Dialog, der zur Auswahl eines Ordners oder einer Datei dient.

 D:\Programme\Kaspersky Lab\Kaspersky Anti-Virus Personal Pro — Das Eingabefeld für einen Pfad.

Zum Bearbeiten eines Feldwerts für einen Pfad gibt es folgende Methoden:

Funktion	Aufruf
-----------------	---------------


Bearbeiten eines Feldwerts	Mit der Maus auf das Feldsymbol klicken.
----------------------------	--

Der Befehl  im Kontextmenü.

Die Taste **F2** auf der Tastatur.

12.3.5. Eingabefeld: Festlegen von Zahlenwerten für ...

Zur Eingabe eines neuen Werts tippen Sie diesen über Ihre Tastatur in das **Zahlenfeld** ein oder benutzen Sie zur Bedienung der Pfeilelemente den Mauszeiger, um den bestehenden Wert zu verändern. Der aktuelle Wert des Zahlenfelds wird in eckigen Klammern rechts vom Zahlenfeld angezeigt.

 Minimale gefährliche Veränderung der Dateigröße (Byte) <100> — Das Eingabefeld für Zahlen.

Zum Ändern von Zahlen innerhalb eines Felds gibt es folgende Methoden:

Funktion	Aufruf
-----------------	---------------

Bearbeiten eines Feldwerts	Mit der Maus auf das Feldsymbol klicken.
----------------------------	--

Der Befehl  im Kontextmenü.

Die Taste **F2** auf der Tastatur.

12.3.6. Dropdown-Liste

Die Dropdown-Liste erlaubt Ihnen die Auswahl eines Elements aus einer Liste (Bild 53). Um eine Liste zu durchsuchen, verwenden Sie die Tasten \uparrow und \downarrow auf der Tastatur. Um die Liste automatisch aufwärts- bzw. abwärts zu scrollen, verwenden die Tastenkombinationen **STRG+** \uparrow bzw. **STRG+** \downarrow .



Bild 53. Dropdown-Liste

12.4. Kontrollindikatoren

Bei der Einstellung des Programms zur Virus-Suche werden in der Laufwerkshierarchie sogenannte Folge-Regeln verwendet. Das heißt, wenn Sie bestimmte Einstellungen für das Objekt **Arbeitsplatz** festlegen (Bild 54), dann werden diese automatisch für alle Laufwerke auf Ihrem Computer angewendet.



Bild 54. Laufwerkshierarchie

Jedem Hierarchieelement entspricht ein *Kontrollindikator*, den Sie aktivieren oder deaktivieren können, und *Regeln*, die zum Element angewendet werden. Der Kontrollindikator zeigt, ob für ein Hierarchieelement der Überprüfungsmodus aktiviert bzw. deaktiviert ist. Die Regeln bestimmen die Überprüfungsart.

Als Vorgabe *vererben die Elemente die für ihre Gruppe geltenden Regeln* (für Gruppe, der sie angehören). Werden die Regeln für die Gruppe gewählt, so ändern sich auch automatisch die Regeln für die Behandlung ihrer Elemente.

Sie können für einige Elemente eigene Regelfestlegen oder den Zustand ihrer Kontrollindikatoren ändern. Diese Elemente werden dann *nach eigenen Regeln behandelt*. Werden dann die Regeln für die Gruppe geändert, bleiben die für diese Elemente festgesetzten Regeln unverändert. Wird aber der Zustand des Kontrollindikators einer Gruppe geändert, so wird für die Elemente dieser Gruppe erneut der Vererbungsmodus aktiviert.

Sie können den Vererbungsmodus für ein Element ganz abschalten. Wählen Sie dazu im Kontextmenü den Eintrag **Feste Regel aufstellen**. Danach wird der Kontrollindikator als rotes Kästchen mit schwarzem Häkchen aussehen. Diese Elemente werden dann *nach festn eigenen Regeln behandelt*. Diese Elemente werden auch dann eigene Regeln behalten, wenn Kontrollindikatoren für ihrer Gruppe geändert werden. Sie können den vererbungsmodus wieder aktivieren, wenn im Kontextmenü den Eintrag **Feste Regel aufheben** wählen.

Der Kontrollindikator kann wie folgt aussehen:

Indikator	Beschreibung	Bedeutung
<input checked="" type="checkbox"/>	Ein Quadrat mit einem eingeschlossenen Häkchen Das Quadrat kann rot oder schwarz sein.	Der Such-Modus ist aktiviert. Das Quadrat ist rot — der Erbmodus ist deaktiviert. Das Quadrat ist schwarz — der Erbmodus ist aktiviert.

Indikator	Beschreibung	Bedeutung
<input checked="" type="checkbox"/>	<p>Ein Quadrat mit eingeschlossenem Häkchen und einem Dreieck in der rechten unteren Ecke. Das Dreieck kann rot oder schwarz sein.</p>	<p>Der Erbmodus ist aktiviert, aber einige Objekte sind aus der Gruppe ausgeschlossen und besitzen ihre eigenen Einstellungen.</p> <p>Das Dreieck ist rot — der Erbmodus ist für ein oder mehrere Objekte deaktiviert.</p> <p>Das Dreieck ist schwarz — die Regel wurde für ein oder mehrere Objekte geändert.</p>
<input type="checkbox"/>	<p>Ein Quadrat ohne Häkchen aber mit einem Dreieck in der rechten unteren Ecke. Das Dreieck kann rot oder schwarz sein.</p>	<p>Der Such-Modus ist deaktiviert, aber für ein oder mehrere Objekte ist dieser Modus aktiviert.</p> <p>Das Dreieck ist rot — der Erbmodus ist für ein oder mehrere Objekte deaktiviert.</p> <p>Das Dreieck ist schwarz — die Regel wurde für ein oder mehrere Objekte geändert.</p>

13. Anhang A.

Klassifikation der Computerviren

Beschreibung der Typen von Computerviren.

Ein **Computervirus** ist ein Programm (eine bestimmte Auswahl ausführbarer Codes und/oder Befehle), das fähig ist, Kopien von sich selbst anzufertigen (die nicht unbedingt vollständig mit dem Original übereinstimmen) und diese ohne Wissen des Benutzers in unterschiedliche Objekte und/oder Ressourcen von Computersystemen bzw. Netzwerken einzufügen. Dabei behalten die Kopien die Fähigkeit zur weiteren Ausbreitung.

Viren können nach folgenden Hauptmerkmalen in Klassen unterteilt werden:

- Aufenthaltsort;
- Betriebssystem (OS);
- Besonderheiten des Funktionsalgorithmus;
- Destruktive Fähigkeiten.

Nach dem **Aufenthaltsort** können folgende Arten von Viren unterschieden werden:

- **Dateiviren** – Dateien, die auf unterschiedliche Weise in ausführbare Dateien eindringen (der am weitesten verbreiteten Virustyp), oder Kopien von sich selbst erstellen (Companion-Viren), oder Besonderheiten der Organisation eines Dateisystems ausnutzen (Link-Viren);
- **Bootviren** – Viren, die sich in einen Bootsektor der Festplatte oder in den Master-Bootsektor (Master Boot Record) schreiben, oder aber eine Verknüpfung mit dem aktiven Bootsektor ändern;

- **Makroviren** – Viren, die Dateien mit Dokumenten und elektronischen Tabellen bestimmter populärer Textverarbeitungsprogramme infizieren;
- **Netzviren** – Viren, die zu ihrer Verbreitung Protokolle oder Befehle von Computernetzen und E-Mails verwenden.

Es existiert eine große Anzahl von Verbindungen: z.B. **Datei-Bootviren**, die sowohl Dateien als auch Bootsektoren von Festplatten infizieren. Solche Viren besitzen in der Regel recht schwierige Funktionsalgorithmen, verwenden häufig originelle Methoden zum Eindringen in ein System, und benutzen Stealth- und polymorphe Technologien. Ein anderes Beispiel einer Verbindung ist ein **Netz-Makrovirus**, der nicht nur veränderbare Dokumente infiziert, sondern seine Kopien auch per E-Mail verschickt.

Die zweite Klassifikationsebene der Virustypen stellt das infizierbare **Betriebssystem** (das Betriebssystem, dessen Objekte durch Infektion beschädigt werden können) dar. Jeder Datei- oder Netzvirus infiziert Dateien eines oder mehrerer Betriebssysteme (DOS, Windows, Win95/NT, OS/2 usw.). Makroviren infizieren Dateien der Formate Word, Excel und Office97. Bootviren sind auf konkrete Positionsformate von Systemdaten in den Bootsektoren von Festplatten ausgerichtet.

Unter den **Besonderheiten des Funktionsalgorithmus** von Viren sind folgende Punkte zu erwähnen:

- Residenz;
- Verwendung von Stealth-Algorithmen;
- Selbstverschlüsselung und polymorphe Struktur;
- Verwendung von originellen Methoden.

Ein RESIDENTER Virus hinterlässt bei der Infektion eines Computers seinen residenten Teil im Arbeitsspeicher. Der residente Teil fängt dann Aufrufe des Betriebssystems an infizierbare Objekte ab und dringt in diese ein. Residente Viren befinden sich im Arbeitsspeicher und sind bis zum Ausschalten des Computers oder bis zum Neustart des Betriebssystems aktiv. Nicht residente Viren infizieren den Arbeitsspeicher des Computers nicht und besitzen nur eine zeitlich begrenzte Aktivität. Bestimmte Viren hinterlassen im Arbeitsspeicher kleine residente Programme, die keine Viren verbreiten. Solche Viren gelten als nicht resident.

Makroviren können als resident bezeichnet werden, da sie sich während der gesamten Arbeitszeit eines infizierten Textverarbeitungsprogramms ständig im Arbeitsspeicher des Computers aufhalten. Dabei übernimmt das Textverarbeitungsprogramm die Rolle des Betriebssystems und dem Begriff "Neustart des Betriebssystems" kommt hier das Beenden des Textverarbeitungsprogramms gleich.

In multifunktionalen Betriebssystemen kann die "Lebenszeit" eines residenten DOS-Virus auch durch den Zeitpunkt bestimmt werden, zu dem ein infiziertes DOS-Fenster geschlossen wird. In bestimmten Betriebssystemen wird die Aktivität von Bootviren durch den Zeitpunkt der Installation von Festplattentreibern des Betriebssystems begrenzt.

Die VERWENDUNG VON STEALTH-ALGORITHMEN erlaubt es Viren, sich vollständig oder teilweise im System zu verstecken. Der am weitesten verbreitete Stealth-Algorithmus ist das Abfangen von Anfragen des Betriebssystems nach dem Lesen/Schreiben infizierter Objekte. Dabei reparieren Stealth-Viren diese entweder vorübergehend oder sie "schieben" an ihrer Stelle virusfreie Datenbestandteile "unter". Im Fall von Makroviren ist die populärste Methode das Verbot des Aufrufs für das Menü zu Makrovorschau. Einer der bekanntesten Datei-Stealth-Viren ist der Virus "Frodo", der bekannteste Boot-Stealth-Virus heißt "Brain".

SELBSTVERSCHLÜSSELUNG und POLYMORPHE STRUKTUREN werden praktisch von allen Virustypen dazu benutzt, das Vorgehen zum Auffinden eines Virus maximal zu erschweren. Polymorphe Viren (polymorphic) sind schwer auffindbare Viren, die keine Signatur besitzen. Das heißt, sie enthalten keinen stabilen Code-Bestandteil. In den meisten Fällen verfügen zwei Varianten ein und desselben polymorphen Virus über keinerlei Gemeinsamkeiten. Das wird durch die Verschlüsselung des Basisvirkörpers und Modifikationen des Entschlüsselungsprogramms erreicht.

Häufig werden in Viren unterschiedliche ORIGINELLE METHODEN verwendet, um die Viren tiefer im Kern des Betriebssystems verstecken zu können (wie dies der Virus "SARASA" tut), um das Entdecken der residenten Kopie zu verhindern (wie die Viren "TPVO" und "Trout2"), oder um die Desinfektion eines Virus zu erschweren (dazu wird z.B. eine Kopie des Virus im Flash-BIOS untergebracht), usw.

Hinsichtlich der **destruktiven Fähigkeiten** von Viren kann folgende Klassifikation vorgenommen werden:

- **unschädliche Viren**: diese Viren üben keinen Einfluss auf die Funktion des Computers aus (außer der Verringerung des verfügbaren Speichers auf der Festplatte in Folge ihrer Verbreitung);
- **ungefährliche Viren**, deren Einfluss sich auf die Verringerung des verfügbaren Speichers auf der Festplatte und Grafik-, Sound- und andere Effekte beschränkt;
- **gefährliche Viren**, die zu ernststen Zwischenfällen bei der Funktion des Computers führen können;
- **sehr gefährliche Viren**, deren Funktionsalgorithmen bewusst Prozeduren enthalten, die folgende Schäden anrichten können: Verlust von Programmen, Vernichten von Daten, Löschen von Informationen, die für die Funktion des Computers nötig sind und in den Systembereichen des Arbeitsspeichers gespeichert sind, und sogar – wie eine nicht nachprüfbare Computerlegende besagt – der schnelle Verschleiß beweglicher mechanischer Teile, was durch Resonanz zu der Zerstörung bestimmter Festplattentypen führen soll.

Doch auch wenn im Algorithmus eines Virus keine Komponenten gefunden werden, die dem System Schaden zufügen können, kann ein Virus nicht mit letzter Sicherheit als unschädlich bezeichnet werden. Sein Eindringen in den Computer kann unvorhersehbare und manchmal katastrophale Folgen haben. Ein Virus kann wie jedes Programm Fehler aufweisen, als deren Folge sowohl Dateien als auch Festplattensektoren beschädigt werden können (so funktioniert zum Beispiel der auf den ersten Blick völlig harmlose Virus "DenZuk" mit 360K Disketten so gut wie korrekt, kann aber auf Disketten mit größerer Kapazität Informationen vernichten). Weiterhin treten Viren auf, die nicht nach ihrem internen Dateiformat als "COM oder EXE" definiert werden, sondern nach ihrer Endung. Es ist klar, dass bei einer Differenz zwischen Format und Namensendung eine Datei nach der Infektion nicht mehr funktionsfähig ist. Außerdem ist die gegenseitige Beeinflussung von residenten Viren und System bei der Verwendung neuer DOS-Versionen, bei der Arbeit mit Windows und mit anderen leistungsfähigen Programmsystemen möglich.

14. Anhang B.

Kaspersky Lab Ltd.

Kaspersky Lab. Antiviren-Produkte. Unsere Adresse

14.1. Über die Firma "Kaspersky Lab"

Kaspersky Lab Ltd. ist eine internationale Software-Entwicklungsfirma mit Vertretungen in Moskau (Russland), Cambridge (Großbritannien) und Pleasanton (USA), die sich in privater Hand befindet. Kaspersky Lab wurde 1997 gegründet. Es beschäftigt sich vor allem mit Entwicklung, Vermarktung und Vertrieb von Datensicherheitstechnologien und Computersoftware höchster Qualität.

Kaspersky Lab nimmt weltweit eine führende Position in den Bereichen Datensicherheit und Antiviren-Technologien ein. Zahlreiche funktionelle Details in fast allen modernen Antiviren-Programmen wurden erstmalig in unserem Unternehmen entwickelt: eine externe Antiviren-Datenbank mit speziellen eingebetteten Modulen, eine Suchfunktion in archivierten und komprimierten Dateien, integrierter Antiviren-Schutz für Linux, u.a. Neben Antiviren-Software beschäftigt sich Kaspersky Lab auch mit der Entwicklung von allgemeiner Datensicherheitssoftware. Unsere aktuelle Produktpalette schließt Kaspersky Inspector und Kaspersky WEB Inspector ein, deren einzigartige Funktionen den Benutzern erlauben, jede unautorisierte Modifikation im Dateisystem und Inhalt eines Webservers völlig unter Kontrolle zu halten.

Durch Zusatzfunktionen bietet Kaspersky Personal Firewall umfassenden Arbeitsplatzschutz gegen jeden Hackerangriff und die Kaspersky Access Control - eine zuverlässige Verwaltung der Zugriffsrechte auf Computer.

Das Flaggschiff von Kaspersky Lab – Kaspersky Anti-Virus (AVP)– wird seit 1989 ständig weiterentwickelt und von zahlreichen Computerfachzeitschriften und Virus-Forschungszentren mehrfach das beste Antiviren-Produkt auf dem Markt genannt.

Kaspersky Anti-Virus umfasst alle zuverlässigen Methoden für den Antiviren-Schutz: Antiviren-Scanner, ein residentes Werkzeug, welches die Viren "im Flug abfängt", Integritätsprüfer und Behaviour-Blocker. Kaspersky Anti-Virus unterstützt alle gängigen Betriebssysteme und Anwendungen und gewährleistet eine sichere Antiviren-Abwehr für Mail-Gateways (MS Exchange Server, Lotus Notes/Domino, Sendmail, Qmail, und Postfix), Firewalls und WEB-Server. Alle Produkte von Kaspersky Anti-Virus arbeiten mit der eigenen Datenbank von Kaspersky, die 55.000 bekannte Viren und schädliche Codes umfasst. Das System ist außerdem mit einer einzigartigen Technologie versehen, die sogar zukünftige Bedrohungen bekämpft: Der eingebaute heuristische Code Analyser entdeckt bis zu 92 % unbekannter Viren und der einzige Behaviour-Blocker für MS Office 2000 garantiert den 100-prozentigen Schutz gegen alle Makroviren.

14.2. Andere Antiviren-Produkte von "Kaspersky Lab."

Kaspersky Anti-Virus Personal/Personal Pro. Ein Paket, das speziell für den umfassenden Virenschutz von Heimcomputern ausgearbeitet wurde, die mit den Betriebssystemen Windows 95/98/ME, Windows 2000/NT, Business-Applications der MS Office 2000 Suite, sowie mit den Mailprogrammen Outlook und Outlook Express arbeiten. Kaspersky Anti-Virus Personal/Personal Pro umfasst ein Programm zur täglichen Aktualisierung über das Internet, integrierte Steuerungsmodule und einen automatisierten Virenschutz. Das einzigartige System zur heuristischen Datenanalyse der zweiten Generation ist zur effektiven Neutralisierung unbekannter Viren in der Lage. Die übersichtliche und bequeme Benutzeroberfläche erlaubt das schnelle Anpassen der Konfiguration und macht die Arbeit mit dem Programm sehr komfortabel.

Kaspersky Anti-Virus Personal umfasst:

- Antiviren-Scanner zum Durchführen der vollständigen Untersuchung lokaler und Netzlaufwerke nach den Anforderungen des Benutzers;
- Antiviren-Monitor, der in Echtzeit automatisch alle ausführbaren Dateien überwacht;
- E-Mail-Filter, der im Hintergrund die Untersuchung aller eingehenden und ausgehenden E-Mail-Nachrichten durchführt;
- Control Center, das zeitgesteuert und automatisch den Start von Kaspersky Anti-Virus, die zentralisierte Programmkontrolle und das automatische Versenden von Benachrichtigungen über Virusangriffe verwaltet.

Kaspersky Anti-Virus Personal Pro umfasst außer den genannten noch zwei zusätzliche Komponenten:

- Inspector, der die zuverlässige Kontrolle über alle unbefugten Modifikationen der Festplatte bietet und nötigenfalls veränderte Dateien und Bootsektoren wiederherstellt;
- Behaviour Blocker, der den hundertprozentigen Schutz vor Makroviren garantiert.

Kaspersky Anti-Virus Business Optimal. Ein Paket, das dem Kampf gegen Viren aller Art in kleinen und mittleren Unternehmensnetzwerken dient, die aus bis zu 100 Workstations bestehen und überwiegend einheitliche Betriebssysteme verwenden.

Kaspersky Anti-Virus Business Optimal bietet einen kompletten Virenschutz für:

- Workstations mit Windows 95/98/ME, Windows NT/2000 Workstation, Linux, OS/2;
- Datei-Server und Application-Server mit Windows NT/2000 Server, Linux, Novell NetWare, FreeBSD, BSDi, OpenBSD;
- E-Mail-Gateways wie MS Exchange Server, Lotus Notes/Domino, Sendmail, Postfix, Qmail, Exim.

In Abhängigkeit der verwendeten Betriebssysteme und spezifischen Anforderungen können Sie aus den Antiviren-Programmen selbst ein Paket zusammenstellen.

Kaspersky Anti-Virus Corporate Suite. Das Paket bietet umfassende Computerdatensicherheit für große Unternehmensnetzwerke. Sein Hauptvorteil ist das Schaffen einer zentral gesteuerten, plattformunabhängigen Struktur zum Schutz vor Viren und externen Invasionen für jede Art von Unternehmensnetzwerken mit beliebiger topologischer Komplexität, das die Möglichkeit der Integration von Remote-Netzen bietet, die sich an jedem Punkt der Erde befinden können.

Dieses Produkt kann optimal in Ihr Unternehmensnetzwerk integriert werden, völlig unabhängig von der verwendeten Software und Hardware anderer Hersteller. Die Flexibilität dieser Lösung erlaubt es, ein effektives System für die Computersicherheit aufzubauen, das der Konfiguration Ihres Netzwerks entspricht.

Kaspersky Anti-Virus Corporate Suite bietet einen globalen Virenschutz für:

- Workstations mit Windows 95/98/ME, Windows NT/2000 Workstation, Linux, OS/2;
- Datei-Server und Application-Server mit Windows NT/2000 Server, Linux, Novell NetWare, FreeBSD, BSDi;
- E-Mail-Gateways wie MS Exchange Server, Lotus Notes/Domino, Sendmail, Postfix.
- CVP-kompatible Firewalls;
- Web-Server.

In Abhängigkeit der verwendeten Betriebssysteme und spezifischen Anforderungen können Sie aus den Antiviren-Programmen selbst ein Paket zusammenstellen.

Kaspersky Web Inspector. Kaspersky WEB Inspector ist ein unikaler Sicherheitskomplex, der WEB-Servern mit einem hermetischen Schutz gegen mögliche Beschädigungen und nicht sanktionierte Modifikationen ihres Inhalts ausstattet. Kontinuierlich überwacht das

Programm in Echtzeit (im Hintergrund) die Vollständigkeit des Serverinhalts und verfolgt Modifikationen. Werden beliebige nicht sanktionierte Veränderungen entdeckt, dann sendet Kaspersky WEB Inspector eine Warnung an die angegebene Adresse und gewährleistet die Möglichkeit zur hundertprozentigen Wiederherstellung des Originalinhalts eines Servers.

14.3. Unsere Adresse

Technischer Support	Informationen über technischen Support finden Sie unter folgender Adresse: <u>www.kaspersky.com.buyoffline.asp</u>
Allgemeine Informationen	WWW: <u>http://www.kaspersky.com</u> <u>http://www.viruslist.com</u> E-mail: <u>sales@kaspersky.com</u>

15. Anhang C. Index

Index der Grundbegriffe.

Allgemeine Programm-Optionen	43	Öffnen von Datenbanken mit Hilfe von	
Analyse-Datenbank.....	80	Lotus Notes Client	30
Antiviren-Datenbanken.....	10	Parameter für das Ereignisjournals.....	67
Arten der Journaleinträge.....	89	Parameter für das Scannen von	
Auswahl der Quarantäne-Datenbank.....	83	Datenbanken	
Auswahl von zu scannenden Objekten.....	61	Parameter für das Scannen von Anlagen	
Bearbeitungsarten für die zu scannenden		51
Objekte.....	68	Planung der Überprüfungen	49
Desinfektion.....	71	Parameter für das Scannen von	
Löschen.....	72	Datenbanken	46
Verschieben nach Quarantäne.....	69	Anfrage auf Überprüfung	53
Weiterleiten.....	74	Desinfektion von Objekten	48
Beenden der Antiviren-Überprüfung.....	76	Planung der Überprüfungen	50
Benutzeroberfläche der Konfigurations-		Parameter für das Scannen von Mails	
Datenbank	35	Auswahl von zu scannenden Objekten	57
Deinstallation des Programms mit Hilfe des		Parameter für das Scannen von Anlagen	
Deinstallationsprogramms.....	93	58
Funktionsschema von Kaspersky Anti-Virus		Parameter für das Versenden von	
für Lotus Domino/Notes	24	Benachrichtigungen	64
Modul zum Abfangen von Mails Hook	26	Parameter für den Überprüfungsvermerk	66
Modul zum Abfangen von Mails Scan	26	Parameter für die Bearbeitung von zu	
Modul zum Abfangen von Mails		scannenden Objekten	62
Scheduler	26	Parameter für die Überprüfung von Mails	55
Installations-CD	11	Quarantäne-Datenbank für Dokumente.....	87
Kaspersky Anti-Virus für Lotus		Quarantäne-Datenbank für Mail-	
Domino/Notes.....	8	Nachrichten.....	84
Lizenzvertrag	11	Start der Antiviren-Überprüfung	76
Manuelle Deinstallation des Programms..	95	Systemvoraussetzungen	18
Öffnen von Datenbanken mit Hilfe eines		Technische Unterstützung	16
Web-Browsers	29	Zugriff auf die Datenbanken	33