

Kaspersky Mobile Security 9

für Microsoft Windows Mobile

KASPERSKY **lab**

Benutzerhandbuch

PROGRAMMVERSION: 9.0

Sehr geehrte Benutzerinnen und Benutzer!

Vielen Dank, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und die mit dem Produkt verbundenen Fragen beantworten wird.

Achtung! Die Rechte für dieses Dokument liegen bei Kaspersky Lab ZAO (im Weiteren auch "Kaspersky Lab") und sind durch das Urheberrecht der Russischen Föderation und durch internationale Verträge geschützt. Illegale Vervielfältigung und Verbreitung des Dokuments und seiner Teile werden nach dem jeweils gültigen Zivilrecht, Verwaltungsrecht oder Strafrecht verfolgt.

Die Materialien dürfen nur mit schriftlicher Einwilligung von Kaspersky Lab ZAO auf elektronische, mechanische oder sonstige Weise kopiert, verbreitet oder übersetzt werden.

Das Dokument und die darin enthaltenen Bilder sind ausschließlich für informative, nicht gewerbliche und persönliche Zwecke bestimmt.

Das Dokument kann zukünftig ohne besondere Ankündigung geändert werden. Die aktuelle Version des Dokuments steht auf der Seite von Kaspersky Lab unter der Adresse <http://www.kaspersky.com/de/docs> zur Verfügung.

Kaspersky Lab ZAO übernimmt keine Haftung für Inhalt, Qualität, Aktualität und Richtigkeit von in diesem Dokument verwendeten Materialien, deren Rechte bei anderen Eigentümern liegen, sowie für möglichen Schaden, der mit der Verwendung dieser Materialien verbunden ist.

In diesem Dokument werden registrierte oder nicht registrierte Markenzeichen verwendet, die Eigentum der rechtmäßigen Besitzer sind.

Redaktionsdatum: 25.01.2011

© 1997-2011 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

<http://www.kaspersky.de>
<http://support.kaspersky.de>

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESER VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.

NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. Definitionen

- 1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.
- 1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.
- 1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.
- 1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff „Sie“ weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff „Organisation“ ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.
- 1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.
- 1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.
- 1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung

- 2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.

Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben. Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der in den Lizenzen, die Sie vom Rechtsinhaber bezogen haben, bezeichneten Computern, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die Lizenzbedingungen sehen eine anderweitige Regelung vor.*

- 2.2. Wenn die Software auf einem physikalischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung oder in der Zusatzvereinbarung festgelegt ist.
- 2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software gekauft haben, bzw. jene in der Zusatzvereinbarung festgelegte Anzahl von Computern.
- 2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.
- 2.5. Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Kaufs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:
 - Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
 - Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

- 3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.
- 3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete oder in der Zusatzvereinbarung genannte Periode genutzt werden.
- 3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Kaufs oder in der Zusatzvereinbarung bezeichnete Zeitdauer genutzt werden.
- 3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (7 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung*, dass die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und technische Unterstützung über die Telefon-Hotline einräumt. Wenn der Rechtsinhaber für die einzelne geltende Evaluierungsperiode einen anderen Zeitraum festlegt, erhalten Sie darüber eine Mitteilung.
- 3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.
- 3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.
- 3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.
- 3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.
- 3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.
- 3.10. Wenn Sie die Software mit einem Aktivierungscode erworben haben, der gültig für eine Sprachversion der Software in der Region ist, in der sie vom Rechtsinhaber oder seinen Partnern erworben wurde, dann können Sie die Software nicht durch Anwendung eines Aktivierungscode aktivieren, der für eine andere Sprachversion vorgesehen ist.
- 3.11. Falls Sie Software gekauft haben, die für den Betrieb mit einem bestimmten Telekombetreiber vorgesehen ist, dann kann die Software nur für den Telekombetreiber verwendet werden, der beim Kauf angegeben wurde.
- 3.12. Im Falle von Beschränkungen, die unter den Punkten 3.10 und 3.11 spezifiziert werden, wird die entsprechende Information über diese Beschränkungen auf der Verpackung und/oder Internetseite des Rechtsinhabers und/oder seiner Partner angegeben.

4. Technische Unterstützung

Die in Klausel 2.5 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).

Technischer Support: <http://support.kaspersky.com/de>

5. Beschränkungen

- 5.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompileieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.
- 5.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend den Bestimmungen der Zusatzvereinbarung zu diesem Vertrag.
- 5.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend den Bestimmungen der Zusatzvereinbarung zu diesem Vertrag an Drittparteien übertragen dürfen.
- 5.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.
- 5.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.
- 5.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.
- 5.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

6. Eingeschränkte Garantie und Haftungsausschluss

- 6.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt*, dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.
- 6.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.
- 6.3. Sie bestätigen, akzeptieren und anerkennen, dass dem Rechteinhaber keinerlei Verantwortung oder Haftung für die von Ihnen genehmigte Löschung von Daten entsteht. Die erwähnten Daten können jedwede persönlichen oder vertraulichen Informationen beinhalten.
- 6.4. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.
- 6.5. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.5 dieses Vertrags erläutert, Updates herunterladen.
- 6.6. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.
- 6.7. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT

AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIE, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISSKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, UM IHRE VORGEGEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

7. Haftungsausschluss und Haftungsbeschränkungen

INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIRECTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDNE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

8. GNU und sonstige Drittpartei-Lizenzen

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenzieren) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

9. Geistiges Eigentum

- 9.1 Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.
- 9.2 Sie bestätigen, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüssel-Datei für die Software Eigentum des Rechtsinhabers sind und Geschäftsgeheimnisse des Rechtsinhabers konstituieren. Sie stimmen zu, den Quellcode der Software nicht zu modifizieren, abzuwandeln, zu übersetzen, zurückzuentwickeln, zu dekompileieren oder auf sonstige Weise zu versuchen, den Quellcode ausfindig zu machen.
- 9.3 Sie stimmen zu, die Software in keinsten Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

10. Geltendes Recht; Schiedsverfahren

Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 10 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

11. Zeitraum für Rechtsverfolgung.

Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

12. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht.

Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der

ursprüngliche Inhalt weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

13. Kontaktinformationen des Rechteinhabers.

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: www.kaspersky.com

© 1997-2011 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

INHALT

ÜBER DIESES HANDBUCH.....	13
In diesem Dokument.....	13
Formatierung mit besonderer Bedeutung	16
ZUSÄTZLICHE INFORMATIONSQUELLEN.....	17
Informationsquellen zur selbständigen Recherche	17
Kontaktaufnahme mit der Vertriebsabteilung.....	18
Diskussion über die Programme von Kaspersky Lab im Webforum	18
Kontakt zur Abteilung für Handbücher und Hilfesysteme	18
KASPERSKY MOBILE SECURITY 9.....	19
Neuerungen in Kaspersky Mobile Security 9.....	20
Lieferumfang.....	20
Hard- und Softwarevoraussetzungen	20
KASPERSKY MOBILE SECURITY 9 INSTALLIEREN	21
PROGRAMM DEINSTALLIEREN	22
PROGRAMM-UPDATE	25
ERSTE SCHRITTE	27
Programm aktivieren	27
Kommerzielle Version aktivieren.....	28
Aktivierung eines Abonnements für Kaspersky Mobile Security 9	29
Aktivierungscode online kaufen	30
Testversion aktivieren	30
Geheimcode festlegen.....	31
Funktion zur Geheimcode-Wiederherstellung aktivieren	32
Geheimcode-Wiederherstellung	32
Programm starten.....	33
Update der Programm-Datenbanken.....	33
Gerät auf Viren untersuchen.....	34
Programm-Infos anzeigen	34
LIZENZVERWALTUNG.....	35
Über den Lizenzvertrag	35
Über Lizenzen für Kaspersky Mobile Security 9	35
Informationen zur Lizenz anzeigen.....	36
Lizenz verlängern	37
Lizenz mit Aktivierungscode verlängern.....	37
Lizenz online verlängern	38
Lizenz durch Aktivierung eines Abonnements verlängern	39
Kündigung des Abonnements	41
Fortsetzung des Abonnements	41
PROGRAMMOBERFLÄCHE	43
Fenster für den Schutzstatus.....	43
Programm-Menü.....	45

SCHUTZ FÜR DAS DATEISYSTEM.....	47
Schutz.....	47
Schutz aktivieren / deaktivieren	47
Aktion für gefundene Objekte wählen	49
UNTERSUCHUNG DES GERÄTS.....	51
Über Scan auf Befehl	51
Untersuchung manuell starten.....	52
Untersuchung nach Zeitplan starten.....	53
Typ der Untersuchungsobjekte wählen	54
Archiv-Untersuchung anpassen.....	55
Aktion für gefundene Objekte wählen.....	56
QUARANTÄNE FÜR SCHÄDLICHE OBJEKTE.....	58
Über die Quarantäne	58
Quarantäneobjekte anzeigen.....	58
Quarantäneobjekte wiederherstellen	59
Quarantäneobjekte löschen.....	59
EINGEHENDE ANRUF UND SMS FILTERN	61
Über den Anruf- und SMS-Filter	61
Über die Modi für den Anruf- und SMS-Filter.....	62
Modus des Anruf- und SMS-Filters ändern.....	62
Schwarze Liste anlegen.....	63
Eintrag zur Schwarzen Liste hinzufügen.....	63
Eintrag in der Schwarzen Liste ändern	64
Eintrag aus der Schwarzen Liste löschen	65
Weiße Liste anlegen.....	66
Eintrag zur Weißen Liste hinzufügen	66
Eintrag in der Weißen Liste ändern.....	67
Eintrag aus der Weißen Liste löschen	68
Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen.....	69
Reaktion auf SMS von Nicht-Ziffern-Nummern.....	70
Aktion für eingehende SMS wählen.....	71
Aktion für eingehende Anrufe wählen	72
AUSGEHENDE ANRUF UND SMS EINSCHRÄNKEN. KINDERSICHERUNG.....	74
Kindersicherung.....	74
Modi der Kindersicherung.....	74
Kindersicherung aktivieren / deaktivieren	75
Schwarze Liste anlegen.....	75
Eintrag zur Schwarzen Liste hinzufügen.....	76
Eintrag in der Schwarzen Liste ändern	77
Eintrag aus der Schwarzen Liste löschen	78
Weiße Liste anlegen.....	78
Eintrag zur Weißen Liste hinzufügen	79
Eintrag in der Weißen Liste ändern.....	80
Eintrag aus der Weißen Liste löschen	80
DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS	82
Über den Diebstahlschutz.....	82
Gerät blockieren	83

Persönliche Daten löschen	85
Liste der zu löschenden Ordner erstellen	87
Wechsel der SIM-Karte auf dem Gerät überwachen	88
Geografische Koordinaten des Geräts ermitteln	89
Diebstahlschutz-Funktionen ferngesteuert starten	92
VERBERGEN SENSIBLER DATEN	94
Über die Privatsphäre	94
Über die Modi der Privatsphäre	94
Privatsphäre aktivieren / deaktivieren	95
Automatische Aktivierung der Privatsphäre	96
Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren	97
Liste der vertraulichen Nummern anlegen	99
Hinzufügen einer Nummer zur Liste der vertraulichen Nummern	100
Bearbeiten einer Nummer der Liste der vertraulichen Nummern	101
Löschen einer Nummer aus der Liste der vertraulichen Nummern	101
Auswahl der zu verbergenden Informationen: Privatsphäre	102
NETZWERKAKTIVITÄT FILTERN. FIREWALL	104
Firewall	104
Firewall aktivieren / deaktivieren	104
Firewall-Modus auswählen	105
Meldungen über Blockierung	105
PERSÖNLICHE DATEN VERSCHLÜSSELN	107
Verschlüsselung	107
Daten verschlüsseln	107
Daten entschlüsseln	109
Zugriff auf verschlüsselte Daten verbieten	110
UPDATE DER PROGRAMM-DATENBANKEN	112
Über das Update der Programm-Datenbanken	112
Datenbankinfos anzeigen	113
Manuelles Update	113
Update nach Zeitplan	114
Update im Roaming	115
PROGRAMMBERICHTE	117
Berichte	117
Berichtseinträge anzeigen	117
Einträge aus Bericht löschen	118
ERWEITERTE EINSTELLUNGEN ANPASSEN	119
Geheimcode ändern	119
Tooltips anzeigen	119
Audiosignale verwalten	120
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT	121
GLOSSAR	122
KASPERSKY LAB	125
INFORMATIONEN ZUM PROGRAMMCODE VON DRITTHERSTELLERN	126
Verteilbarer Programmcode	126

ADB	126
ADBWINAPI.DLL	126
ADBWINUSBAPI.DLL.....	126
Zusatzinformationen	128
SACHREGISTER	129

ÜBER DIESES HANDBUCH

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky Mobile Security 9. Das Dokument ist für gewöhnliche Anwender gedacht.

Das Dokument soll:

- Dem Anwender helfen, das Programm selbst auf einem mobilen Gerät zu installieren, es zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- Fragen, die sich auf das Programm beziehen, schnell beantworten.
- Auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

IN DIESEM ABSCHNITT

In diesem Dokument	13
Formatierung mit besonderer Bedeutung.....	16

IN DIESEM DOKUMENT

Dieses Dokument enthält folgende Abschnitte:

Zusätzliche Informationsquellen

Dieser Abschnitt enthält eine Beschreibung der Quellen, die zusätzliche Informationen über das Programm bieten, und verweist auf Internetressourcen, die zur Diskussion über das Programm, für Vorschläge, sowie für Fragen und Antworten dienen.

Kaspersky Mobile Security 9

Dieser Abschnitt beschreibt die Programm-Features und informiert über die Komponenten und Grundfunktionen des Programms. In diesem Abschnitt erfahren Sie mehr über den Lieferumfang. Hier werden die Hard- und Softwarevoraussetzungen genannt, welchen ein mobiles Gerät entsprechen muss, damit Kaspersky Mobile Security 9 darauf installiert werden kann.

Kaspersky Mobile Security 9 installieren

Dieser Abschnitt informiert darüber, wie das Programm auf einem mobilen Gerät installiert wird.

Programm deinstallieren

Dieser Abschnitt informiert darüber, wie das Programm von einem mobilen Gerät entfernt wird.

Programm-Update

Dieser Abschnitt informiert darüber, wie eine Vorgängerversion aktualisiert wird.

Erste Schritte

Dieser Abschnitt informiert über die ersten Schritte bei der Arbeit mit Kaspersky Mobile Security 9: Programm aktivieren, Geheimcode für das Programm festlegen, Funktion zur Geheimcode-Wiederherstellung aktivieren, Geheimcode wiederherstellen, Programm starten, Anti-Viren-Datenbanken aktualisieren und Gerät auf Viren untersuchen.

Lizenzverwaltung

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. Dieser Abschnitt informiert außerdem darüber, wie Informationen zur Lizenz von Kaspersky Mobile Security 9 angezeigt werden können und wie die Nutzungsdauer der Lizenz verlängert wird.

Programmoberfläche

Dieser Abschnitt informiert über die wichtigsten Oberflächenelemente von Kaspersky Mobile Security 9.

Schutz für das Dateisystem

Dieser Abschnitt informiert über die Komponente Schutz, die das Dateisystem Ihres Geräts vor Infektionen schützt. Außerdem wird hier beschrieben, wie der Schutz aktiviert / angehalten wird und wie die Schutzeinstellungen angepasst werden.

Untersuchung des Geräts

Dieser Abschnitt informiert über die auf Befehl gestartete Untersuchung des Geräts, mittels welcher Bedrohungen auf Ihrem Gerät erkannt und beseitigt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Untersuchung des Geräts starten, Zeitplan für die automatische Untersuchung des Dateisystems erstellen, Untersuchungsobjekte auswählen, Aktion des Programms für gefundene Schadobjekte festlegen.

Quarantäne für schädliche Objekte

Dieser Abschnitt informiert über den speziellen Speicher *Quarantäne*, in welchen potentiell gefährliche Objekte verschoben werden. Außerdem wird hier beschrieben, wie schädliche Objekte, die in diesem Ordner gespeichert sind, angezeigt, wiederhergestellt oder gelöscht werden können.

Eingehende Anrufe und SMS filtern

Dieser Abschnitt informiert über den Anruf- und SMS-Filter. Diese Komponente verhindert die Zustellung von unerwünschten Anrufen und SMS, und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste. Außerdem wird in diesem Abschnitt beschrieben, wie ein Modus ausgewählt wird, nach dem der Anruf- und SMS-Filter eingehende Anrufe und SMS untersuchen soll, wie erweiterte Einstellungen für die Filterung von eingehenden SMS und Anrufen vorgenommen werden, und wie die Schwarze und Weiße Liste erstellt werden.

Ausgehende Anrufe und SMS einschränken. Kindersicherung

Dieser Abschnitt informiert über die Komponente Kindersicherung, mit der ausgehende Anrufe und SMS-Nachrichten an bestimmte Nummern eingeschränkt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Liste für erlaubte und verbotene Nummern anlegen, Kindersicherung anpassen.

Datenschutz bei Verlust oder Diebstahl des Geräts

Dieser Abschnitt informiert über die Komponente Diebstahlschutz, die bei Diebstahl oder Verlust des Geräts die auf dem Gerät gespeicherten Informationen vor unbefugtem Zugriff schützt und das Auffinden des Geräts erleichtert.

Außerdem werden hier folgende Vorgänge beschrieben: Diebstahlschutz-Funktionen aktivieren / deaktivieren, Diebstahlschutz anpassen, Diebstahlschutz-Funktionen von einem anderen Gerät aus ferngesteuert starten.

Verbergen sensibler Daten

Dieser Abschnitt informiert über die Komponente Privatsphäre, mit der vertrauliche Benutzerinformationen verborgen werden können.

Netzwerkaktivität filtern. Firewall

Dieser Abschnitt informiert über die Firewall, die auf Ihrem Gerät die Netzwerkverbindungen überwacht. Außerdem wird hier beschrieben, wie die Firewall aktiviert / deaktiviert wird und wie ein Funktionsmodus ausgewählt wird.

Persönliche Daten verschlüsseln

Dieser Abschnitt informiert über die Komponente Verschlüsselung, mit der die Ordner auf dem Gerät verschlüsselt werden können. Außerdem wird hier beschrieben, wie ausgewählte Ordner verschlüsselt und entschlüsselt werden können.

Update der Programm-Datenbanken

Dieser Abschnitt informiert über das Update der Anti-Viren-Datenbanken des Programms. Das Update hält den Schutz Ihres Geräts auf dem neusten Stand. Außerdem werden hier folgende Vorgänge beschrieben: Informationen über die installierten Anti-Viren-Datenbanken des Programms anzeigen, Updatevorgang manuell starten, automatisches Datenbank-Update nach Zeitplan anpassen.

Programmberichte

Dieser Abschnitt informiert über die Berichte, in denen die Arbeit der einzelnen Komponenten und die Ausführung aller Aufgaben (z.B. Update der Anti-Viren-Datenbanken des Programms, Virensuche) protokolliert werden.

Erweiterte Einstellungen anpassen

Dieser Abschnitt informiert über zusätzliche Optionen von Kaspersky Mobile Security 9: Geheimcode ändern, Audiosignale des Programms und Hintergrundbeleuchtung des Bildschirms verwalten, Anzeige des Schutzsymbols und des Statusfensters aktivieren / deaktivieren.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Tipps dazu, wie Sie auf der Support-Webseite aus Mein Kaspersky Account oder telefonisch Hilfe von Kaspersky Lab erhalten können.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen der Begriffe, die in diesem Dokument vorkommen.

Kaspersky Lab

Dieser Abschnitt bietet Informationen über Kaspersky Lab ZAO.

Informationen zum Programmcode von Drittherstellern

Dieser Abschnitt informiert über den Code von Drittherstellern, der im Programm verwendet wurde.

Sachregister

Mit Hilfe dieses Abschnitts können Sie bestimmte Angaben schnell im Dokument finden.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Die Bedeutung der in diesem Dokument verwendeten Textformatierungen wird in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass...	Warnungen sind rot geschrieben und eingerahmt. Warnungen enthalten wichtige Informationen, die z.B. auf Aktionen hinweisen, die im Hinblick auf die Computersicherheit als kritisch gelten.
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise enthalten hilfreiche und informative Angaben.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Das <i>Update</i> ist...	Neue Begriffe sind kursiv geschrieben.
ALT+F4	Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die mit einem Pluszeichen verbunden sind, stehen für eine Tastenkombination.
Aktivieren	Die Namen von Elementen der Benutzeroberfläche (z.B. Eingabefelder, Menübefehle, Schaltflächen) sind halbfett geschrieben.
➡ <i>Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:</i>	Der erste Satz einer Anleitung ist kursiv geschrieben.
help	Texte in der Befehlszeile oder Meldungstexte, die das Programm auf dem Bildschirm anzeigt, werden durch spezielle Schrift hervorgehoben.
<IP-Adresse Ihres Computers>	Variable stehen in eckigen Klammern. Eine Variable muss in einem konkreten Fall durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Für Fragen zu Installation oder Verwendung von Kaspersky Mobile Security 9 stehen unterschiedliche Informationsquellen zur Verfügung. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche.....	17
Kontaktaufnahme mit der Vertriebsabteilung	18
Diskussion über die Programme von Kaspersky Lab im Webforum.....	18
Kontakt zur Abteilung für Handbücher und Hilfesysteme	18

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des technischen Supports (in der Wissensdatenbank)
- elektronisches Hilfesystem und Tooltips
- Dokumentationen

Seite auf der Webseite von Kaspersky Lab

<http://www.kaspersky.com/de/kaspersky-mobile-security> Auf dieser Seite finden Sie allgemeine Informationen über Kaspersky Mobile Security 9 sowie über die Funktionen und Besonderheiten des Programms. Außerdem können Sie Kaspersky Mobile Security 9 in unserem Online-Shop kaufen.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

<http://support.kaspersky.com/de/>

Auf dieser Seite finden Sie Artikel, die von den Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung von Kaspersky Mobile Security 9. Sie sind nach Themen wie "Datenbank-Update" oder "Beheben von Störungen bei der Arbeit" angeordnet. Die Artikel können außerdem Fragen behandeln, die neben Kaspersky Mobile Security 9 auch andere Produkte von Kaspersky Lab betreffen. Daneben können Sie Neuigkeiten über den technischen Support enthalten.

Elektronisches Hilfesystem

Bei Fragen zu einem speziellen Fenster oder zu einer Registerkarte von Kaspersky Mobile Security 9 hilft Ihnen die Kontexthilfe.

Öffnen Sie das betreffende Fenster und wählen den Punkt **Hilfe**, um die Kontexthilfe zu öffnen.

Dokumentation

Das Benutzerhandbuch informiert ausführlich über die Programmfunktionen und über die Arbeit mit Kaspersky Mobile Security 9. Außerdem bietet es Tipps für die Konfiguration des Programms.

Das Benutzerhandbuch ist als PDF im Lieferumfang von Kaspersky Mobile Security 9 enthalten.

Außerdem stehen die Dokumente auf der Webseite von Kaspersky Lab zum Download bereit.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von Kaspersky-Produkten sowie zur Verlängerung der Nutzungsdauer steht Ihnen unser Kontaktformular (<http://www.kaspersky.com/de/kontakt>) zur Verfügung:

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage nicht dringend ist, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse <http://forum.kaspersky.com> diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

KONTAKT ZUR ABTEILUNG FÜR HANDBÜCHER UND HILFESYSTEME

Wenn Sie Fragen zu dieser Dokumentation haben, einen Fehler darin gefunden haben oder Ihre Meinung über unsere Dokumentationen schreiben möchten, richten Sie sich bitte direkt an unsere Abteilung für Handbücher und Hilfesysteme. Zur Kontaktaufnahme mit der Dokumentationsgruppe senden Sie eine Nachricht an docfeedback@kaspersky.com. Geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky Mobile Security 9".

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 schützt mobile Geräte (im Folgenden "Geräte" genannt), die mit dem Betriebssystem Microsoft Windows Mobile arbeiten. Das Programm kann die Informationen auf dem Gerät vor einer Infektion durch bekannte Bedrohungen schützen, den Empfang unerwünschter SMS und Anrufe verhindern, Netzwerkverbindungen auf dem Gerät kontrollieren, Informationen verschlüsseln, Informationen für vertrauliche Kontakte verbergen und die Informationen bei Diebstahl oder Verlust des Geräts schützen. Jeder Bedrohungstyp wird von bestimmten Programmkomponenten verarbeitet. Dadurch wird es ermöglicht, die Programmeinstellungen flexibel anzupassen.

Kaspersky Mobile Security 9 umfasst folgende Schutzkomponenten:

- **Anti-Virus.** Schützt das Dateisystem des mobilen Geräts vor Viren und anderen Schadprogrammen. Anti-Virus bietet folgende Optionen: Objekte erkennen und neutralisieren; Anti-Viren-Datenbanken des Programms aktualisieren.
- **Anruf- und SMS-Filter.** Prüft alle eingehenden SMS und Anrufe auf Spam. Diese Komponente erlaubt es, das Blockieren von SMS und Anrufe, die als unerwünscht gelten, flexibel anzupassen.
- **Diebstahlschutz.** Schützt die Informationen auf dem Gerät vor unbefugtem Zugriff, wenn es verloren geht oder gestohlen wird und hilft bei der Suche nach dem Gerät. Außerdem kann der Diebstahlschutz Ihr Gerät durch einen SMS-Befehl von einem anderen Gerät aus ferngesteuert blockieren, auf dem Gerät gespeicherte Daten löschen und das Gerät orten (falls Ihr Gerät einen GPS-Empfänger besitzt). Außerdem kann der Diebstahlschutz das Gerät blockieren, falls die SIM-Karte gewechselt oder das Gerät ohne SIM-Karte eingeschaltet wird.
- **Kindersicherung.** Kontrolliert alle ausgehenden SMS und Anrufe. Mit dieser Komponente lässt sich die Filterung von ausgehenden SMS und Anrufen flexibel anpassen.
- **Privatsphäre.** Verbirgt Informationen, die mit vertraulichen Nummern aus der erstellten Kontaktliste zusammenhängen. Für diese Nummern verbirgt die Privatsphäre Einträge in den Kontakten, SMS-Korrespondenz, Einträge in der Anrufliste, neu empfangene SMS und eingehende Anrufe.
- **Firewall.** Kontrolliert die Netzwerkverbindungen auf Ihrem mobilen Gerät. Mit der Firewall können die Verbindungen festgelegt werden, die erlaubt oder verboten werden sollen.
- **Verschlüsselung.** Speichert Informationen in verschlüsselter Form. Die Komponente Verschlüsselung erlaubt es, eine beliebige Anzahl von Ordnern zu verschlüsseln. Die Ordner können sich im Gerätespeicher oder auf Speicherkarten befinden. Der Zugriff auf die Dateien aus verschlüsselten Ordnern ist erst nach der Eingabe des Geheimcodes für das Programm möglich.

Außerdem bietet das Programm eine Reihe von Servicefunktionen. Sie erlauben es, das Programm auf dem neuesten Stand zu halten, erweitern die Einsatzmöglichkeiten des Programms und unterstützen den Benutzer bei der Arbeit.

- **Schutzstatus.** Auf dem Display werden die Status der Programmkomponenten angezeigt. Auf Basis der angezeigten Informationen können Sie den aktuellen Schutzstatus für die Informationen auf Ihrem Gerät einschätzen.
- **Update der Anti-Viren-Datenbanken des Programms.** Diese Funktion hält die Anti-Viren-Datenbanken von Kaspersky Mobile Security 9 aktuell.
- **Ereignisbericht.** Das Programm führt für jede Komponente einen separaten Ereignisbericht, der die Arbeit der Komponente dokumentiert (z.B. ausgeführte Operation, Daten über ein blockiertes Objekt, Untersuchungs- oder Updatebericht).
- **Lizenz.** Beim Kauf von Kaspersky Mobile Security 9 wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, der die Bedingungen für die Nutzung des Programms und den Zugriff auf der Anti-Viren-Datenbanken des Programms und auf den technischen Support festlegt. Die Gültigkeitsdauer der Lizenz und sonstige Informationen, die für die volle Funktionsfähigkeit des Programms erforderlich sind, sind in der Lizenz enthalten.

Mit der Funktion **Lizenz** können Sie sich ausführlich über die von Ihnen verwendete Lizenz informieren und deren Gültigkeit verlängern.

Kaspersky Mobile Security 9 führt keine Datensicherung und Datenwiederherstellung aus.

IN DIESEM ABSCHNITT

Neuerungen in Kaspersky Mobile Security 9..... [20](#)

Lieferumfang [20](#)

Hard- und Softwarevoraussetzungen [20](#)

NEUERUNGEN IN KASPERSKY MOBILE SECURITY 9

Ausführliche Beschreibung der Neuerungen in Kaspersky Mobile Security 9.

Kaspersky Mobile Security 9 bietet folgende neue Möglichkeiten:

- Der Zugriff auf das Programm wird durch einen Geheimcode geschützt.
- Die Komponente Privatsphäre erlaubt es, für vertrauliche Kontakte aus der Kontaktliste folgende Informationen zu verbergen: Einträge in den Kontakten, SMS-Korrespondenz, Anrufliste sowie neu eingegangene SMS und eingehende Anrufe. Vertrauliche Informationen können angezeigt werden, wenn das Verbergen deaktiviert ist.
- Die Komponente Verschlüsselung erlaubt es, Ordner zu verschlüsseln, die sich im Gerätespeicher oder auf einer Speicherkarte befinden. Die Komponente speichert vertrauliche Daten in verschlüsselter Form und erlaubt den Zugriff auf verschlüsselte Informationen erst nach Eingabe des Geheimcodes für das Programm.
- Es wurde eine neue Servicefunktion für die Anzeige von Tooltips hinzugefügt: Kaspersky Mobile Security 9 zeigt eine kurze Beschreibung für eine Komponente an, wenn diese angepasst werden soll.
- Der Kauf eines Aktivierungscode und die Lizenzverlängerung sind nun mit einer Abonnementsfunktion oder im Online-Modus direkt vom mobilen Gerät aus möglich.

LIEFERUMFANG

Kaspersky Mobile Security 9 kann über das Internet bezogen werden (Programm und Dokumentation werden in elektronischer Form geliefert). Außerdem wird Kaspersky Mobile Security 9 über die Niederlassungen von Mobilfunkanbietern vertrieben. Eine genaue Beschreibung der Bezugsmöglichkeiten und des Lieferumfangs erhalten Sie durch unsere Vertriebsabteilung, nach Ausfüllen des Kontaktformulars unter <http://www.kaspersky.com/de/kontakt...>

HARD- UND SOFTWAREVORAUSSETZUNGEN

Kaspersky Mobile Security 9 kann auf mobilen Geräten installiert werden, die mit den folgenden Betriebssystemen arbeiten:

- Microsoft Windows Mobile 5.0
- Microsoft Windows Mobile 6.0, 6.1, 6.5

KASPERSKY MOBILE SECURITY 9 INSTALLIEREN

Die Installation des Programms auf einem mobilen Gerät umfasst mehrere Schritte.

Es wird empfohlen, vor Beginn der Installation alle anderen Programme auf dem mobilen Gerät zu schließen.

➤ Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9 zu installieren:

1. Um das mobile Gerät mit dem Computer zu verbinden, verwenden Sie das Programm Microsoft ActiveSync.
2. Führen Sie eine der folgende Aktionen aus:
 - Wenn Sie das Programm auf CD erworben haben, starten Sie auf der CD die automatische Installation von Kaspersky Mobile Security 9.
 - Wenn Sie das Programm über das Internet bezogen haben, kopieren Sie die Installationsdatei auf das mobile Gerät. Dazu stehen folgende Methoden zur Verfügung:
 - Von der Webseite von Kaspersky Lab
 - Mit dem Programm Microsoft ActiveSync
 - Mit einer Speicherkarte

Starten Sie anschließend die Installation (öffnen Sie das CAB-Archiv auf dem mobilen Gerät).
3. Lesen Sie den Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab abgeschlossen wird. Klicken Sie auf **OK**, wenn Sie die Vertragsbedingungen akzeptieren. Danach wird Kaspersky Mobile Security 9 auf dem Gerät installiert. Klicken Sie auf **Abbrechen**, wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen.
4. Wählen Sie eine Sprache für die Oberfläche von Kaspersky Mobile Security 9 und klicken auf **OK**.
5. Starten Sie das Gerät neu, um die Installation abzuschließen. Klicken Sie dazu auf **Neustart**.

Das Programm wird mit den von Kaspersky Lab empfohlenen Einstellungen installiert.

PROGRAMM DEINSTALLIEREN

➔ Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9 zu deinstallieren.

1. Entschlüsseln Sie die Daten auf Ihrem Gerät, wenn diese mit Kaspersky Mobile Security 9 verschlüsselt wurden (s. Abschnitt "Daten entschlüsseln" auf S. 109).
2. Deaktivieren Sie die Privatsphäre (s. Abschnitt "Privatsphäre aktivieren / deaktivieren" auf S. 95).
3. Beenden Sie Kaspersky Mobile Security 9. Gehen Sie dazu auf **Menü** → **Beenden**.
4. Entfernen Sie Kaspersky Mobile Security 9. Gehen Sie dazu folgendermaßen vor:
 - a. Klicken Sie auf **Start** → **Einstellungen**.
 - b. Wählen Sie auf der Registerkarte **System** den Punkt **Programme entfernen** (s. Abb. unten).



Abbildung 1: Registerkarte **System**

- c. Wählen Sie in der Liste der installierten Programme **Kaspersky Mobile Security** und klicken Sie auf **Entfernen** (s. Abb. unten).



Abbildung 2: Programm zur Deinstallation wählen

- d. Bestätigen Sie die Programmeinstellung im folgenden Fenster mit **Ja**.
- e. Geben Sie den Geheimcode ein und klicken Sie auf **OK**.
- f. Legen Sie fest, ob Programmeinstellungen und Quarantäneobjekte gespeichert werden sollen: (s. Abb. unten):
- Wenn Sie die Programmeinstellungen und Quarantäneobjekte speichern möchten, klicken Sie auf **Speichern**.

- Klicken Sie auf **Löschen**, um das Programm vollständig zu deinstallieren.

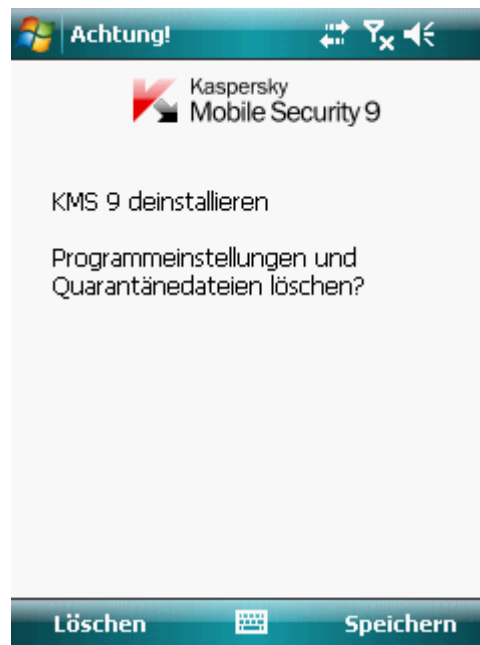


Abbildung 3: Programmeinstellungen löschen

5. Starten Sie das Gerät neu, um die Deinstallation des Programms abzuschließen.

PROGRAMM-UPDATE

Sie können Kaspersky Mobile Security 9 aktualisieren, wenn Sie eine Vorgängerversion dieser Programmgeneration installiert haben (z.B. Update der Version 9.0 auf Version 9.2).

Wenn Sie Kaspersky Mobile Security 8.0 verwenden, können Sie ein Upgrade auf Kaspersky Mobile Security 9 vornehmen.

➤ *Gehen Sie folgendermaßen vor, um das Programm auf die neue Version zu aktualisieren:*

1. Deaktivieren Sie die Verschlüsselung – entschlüsseln Sie alle Daten (s. Abschnitt "Daten entschlüsseln" auf S. [109](#)).
2. Deaktivieren Sie die Privatsphäre (s. Abschnitt "Privatsphäre aktivieren / deaktivieren" auf S. [95](#)).
3. Beenden Sie die aktuelle Version von Kaspersky Mobile Security. Gehen Sie dazu auf **Menü** → **Beenden**.
4. Kopieren Sie die Distribution auf das Gerät. Dazu stehen folgende Methoden zur Verfügung:
 - Von der Webseite von Kaspersky Lab
 - Mit dem Programm Microsoft ActiveSync
 - Mit einer Speicherkarte
5. Starten Sie auf dem Gerät das Setup für Kaspersky Mobile Security 9.
6. Lesen Sie den Lizenzvertrag genau. Wenn Sie den Vertragsbestimmungen zustimmen, klicken Sie auf **Akzeptieren**. Ihnen wird vorgeschlagen, zuerst die installierte Programmversion zu entfernen.
7. Bestätigen Sie die Deinstallation der vorherigen Programmversion durch Betätigen von **OK**.
8. Geben Sie den Geheimcode ein.
9. Legen Sie fest, ob Programmeinstellungen und Quarantäneobjekte gespeichert werden sollen:
 - Wenn Sie die Programmeinstellungen und Quarantäneobjekte speichern möchten, klicken Sie auf **Speichern**.
 - Klicken Sie auf **Löschen**, um das Programm vollständig zu deinstallieren.
10. Starten Sie das Gerät neu, um den Deinstallationsvorgang abzuschließen. Klicken Sie dazu auf **Neustart**.
11. Starten Sie nach dem Neustart des Geräts die Installation von Kaspersky Mobile Security 9.0 (s. Abschnitt "Kaspersky Mobile Security 9 installieren" auf S. [21](#)).

Wenn die aktuelle Lizenz noch nicht abgelaufen ist, wird das Programm automatisch aktiviert. Wenn die Lizenz abgelaufen ist, führen sie eine Programmaktivierung durch (s. Abschnitt "Programm aktivieren" auf S. [27](#)).

➤ *Zum Upgrade von Kaspersky Mobile Security 8.0 auf Version 9, gehen Sie bitte wie folgt vor:*

1. Entschlüsseln Sie alle Daten, die mit Kaspersky Mobile Security 8.0 verschlüsselt wurden.
2. Beenden Sie Kaspersky Mobile Security 9. Gehen Sie dazu auf **Menü** → **Beenden**.
3. Entfernen Sie Kaspersky Mobile Security 9. Gehen Sie dazu folgendermaßen vor:
 - a. Klicken Sie auf **Start** → **Einstellungen**.

- b. Wählen Sie auf der Registerkarte **System** den Punkt **Programme entfernen**.
 - c. Wählen Sie in der Liste der installierten Programme **Kaspersky Mobile Security** und klicken Sie auf **Entfernen**.
 - d. Bestätigen Sie die Programmdeinstallation im folgenden Fenster mit **Ja**.
 - e. Geben Sie den Geheimcode aus der Vorgängerversion des Programms ein und betätigen Sie **OK**.
 - f. Löschen Sie die Einstellungen von Kaspersky Mobile Security 8.0 vollständig, da diese nicht mit den Einstellungen von Version 9 kompatibel sind. Klicken Sie dazu auf **Löschen**.
4. Starten Sie das Gerät neu, um die Deinstallation von Kaspersky Mobile Security 8.0 abzuschließen.
 5. Gehen Sie weiter zur Installation von Kaspersky Mobile Security 9 (s. Abschnitt "Kaspersky Mobile Security 9 installieren" auf S. [21](#)).
 6. Wechseln Sie zur Programmaktivierung (s. Abschnitt "Programm aktivieren" auf S. [27](#)).

Wenn die Lizenz für Kaspersky Mobile Security 8.0 noch gültig ist, aktivieren Sie die Programmversion 9 mit dem Aktivierungscode von Version 8.0.

ERSTE SCHRITTE

Dieser Abschnitt informiert über die ersten Schritte bei der Arbeit mit Kaspersky Mobile Security 9: Programm aktivieren, Geheimcode für das Programm festlegen, Funktion zur Geheimcode-Wiederherstellung aktivieren, Geheimcode wiederherstellen, Programm starten, Anti- Viren-Datenbanken aktualisieren und Gerät auf Viren untersuchen.

IN DIESEM ABSCHNITT

Programm aktivieren	27
Geheimcode festlegen	31
Funktion zur Geheimcode-Wiederherstellung aktivieren	32
Geheimcode-Wiederherstellung	32
Programm starten	33
Update der Programm-Datenbanken	33
Gerät auf Viren untersuchen	34
Programm-Infos anzeigen	34

PROGRAMM AKTIVIEREN

Um mit der Arbeit von Kaspersky Mobile Security 9 zu beginnen, muss das Programm aktiviert werden.

Um Kaspersky Mobile Security 9 auf einem Gerät zu aktivieren, ist eine Internetverbindung erforderlich.

Stellen Sie vor der Programmaktivierung sicher, dass Datum und Uhrzeit des Gerätesystems korrekt eingestellt sind.

Das Programm kann auf folgende Weise aktiviert werden:

- **Testversion aktivieren.** Bei der Aktivierung einer Testversion empfängt das Programm eine kostenlose Testlizenz. Die Gültigkeitsdauer der Testlizenz wird nach der Aktivierung auf dem Bildschirm angezeigt. Nach Ablauf der Testlizenz werden die Programmfunktionen eingeschränkt. Es stehen nur folgende Funktionen zur Verfügung:
 - Programm aktivieren
 - Programmlizenzen verwalten
 - Hilfesystem für Kaspersky Mobile Security 9.
 - Verschlüsselung deaktivieren
 - Privatsphäre deaktivieren

Es ist nicht möglich, eine weitere Testlizenz zu aktivieren.

- **Kommerzielle Version aktivieren.** Für die Aktivierung einer kommerziellen Version wird der Aktivierungscode verwendet, den Sie beim Kauf des Programms erhalten. Bei der Aktivierung einer kommerziellen Version

empfängt das Programm eine kommerzielle Lizenz, die Zugriff auf alle Programmfunktionen verleiht. Die Gültigkeitsdauer der Lizenz wird auf dem Bildschirm angezeigt. Nach Ablauf der Lizenzgültigkeit wird die Programmfunktionalität eingeschränkt. Das Programm wird nicht mehr aktualisiert.

Ein Aktivierungscode kann folgendermaßen erworben werden:

- Online, durch Aufrufen der speziellen Website von Kaspersky Lab für mobile Geräte direkt aus Kaspersky Mobile Security 9.
- Im Internet-Shop von Kaspersky Lab (<http://www.kaspersky.com/de/store>);
- Im Fachhandel
- **Abonnement aktivieren.** Bei der Aktivierung eines Abonnements empfängt das Programm eine kommerzielle Lizenz mit Abonnement. Die Gültigkeitsdauer einer Lizenz mit Abonnement ist auf 30 Tage beschränkt. Durch ein Abonnement verlängert das Programm die Gültigkeitsdauer der Lizenz alle 30 Tage. Bei einer Verlängerung der Lizenzgültigkeit wird für die Nutzung des Programms von Ihrem Konto die in den Abonnementsbedingungen festgelegte Summe abgebucht. Dieser Betrag wird durch Senden einer kostenpflichtigen SMS abgebucht. Nachdem der Betrag abgebucht wurde, erhält das Programm vom Aktivierungsserver eine neue Lizenz mit einem Abonnement. Diese Lizenz ermöglicht die Nutzung aller Programmfunktionen. Das Abonnement für Kaspersky Mobile Security 9 ist nicht verpflichtend. In diesem Fall wird die Programmfunktionalität nach Ablauf der Lizenz eingeschränkt und die Antiviren-Datenbanken des Programms werden nicht mehr aktualisiert.

IN DIESEM ABSCHNITT

Kommerzielle Version aktivieren	28
Aktivierung eines Abonnements für Kaspersky Mobile Security 9.....	29
Aktivierungscode online kaufen.....	30
Testversion aktivieren	30

KOMMERZIELLE VERSION AKTIVIEREN

➡ *Gehen Sie folgendermaßen vor, um eine kommerzielle Programmversion mit einem Aktivierungscode zu aktivieren:*

1. Gehen Sie auf **Start** → **Programme**.
2. Wählen Sie **KMS 9** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

Das Fenster **Aktivieren** wird geöffnet.

3. Gehen Sie auf **Code eingeben**.

Das Aktivierungsfenster für Kaspersky Mobile Security 9 wird geöffnet (s. Abb. unten).

4. Geben Sie den Code in die entsprechenden vier Felder ein und klicken Sie dann auf **Weiter**.



Abbildung 4: Kommerzielle Version aktivieren

5. Bestätigen Sie die Internetverbindung mit **Ja**.

Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab und erhält eine Lizenz. Wurde eine Lizenz empfangen, werden die Lizenzinformationen auf dem Bildschirm angezeigt.

Wenn der von Ihnen eingegebene Aktivierungscode ungültig ist, erscheint eine entsprechende Meldung auf dem Bildschirm des mobilen Geräts. Prüfen Sie in diesem Fall, ob der Aktivierungscode richtig eingegeben wurde, und wenden Sie sich dann an die Firma, bei der Sie den Aktivierungscode für Kaspersky Mobile Security 9 gekauft haben.

Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Lizenz fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

6. Gehen Sie weiter zum Festlegen des Geheimcodes (s. Abschnitt "Geheimcode festlegen" auf S. 31).

AKTIVIERUNG EINES ABONNEMENTS FÜR KASPERSKY MOBILE SECURITY 9

Um das Abonnement zu aktivieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

➔ Gehen Sie folgendermaßen vor, um ein Abonnement für Kaspersky Mobile Security 9 zu aktivieren:

1. Wählen Sie **Start** → **Programme**.
2. Wählen Sie **KMS 9** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

Das Fenster **Aktivieren** wird geöffnet.

3. Wählen Sie Sofort **kaufen** aus.

- Bestätigen Sie die Internetverbindung mit **Ja**.

Das Programm überprüft, ob der Abonnementdienst für Ihren Mobilfunkanbieter verfügbar ist. Wenn der Abonnementdienst verfügbar ist, dann öffnet sich der Bildschirm **Aktivierung** mit den Abonnementbedingungen.

Wenn der Abonnementdienst nicht verfügbar ist, informiert Sie das Programm darüber und kehrt zu dem Fenster zurück, in dem Sie eine andere Aktivierungsmethode für das Programm auswählen können.

- Lesen Sie sich die Abonnementbedingungen durch und bestätigen Sie mit **Ja** die Aktivierung des Abonnements für Kaspersky Mobile Security 9.

Das Programm verschickt eine kostenpflichtige SMS und erhält dann vom Kaspersky-Lab-Aktivierungsserver eine Lizenz. Sie werden von Kaspersky Mobile Security 9 benachrichtigt, sobald das Abonnement aktiviert wurde.

Falls auf Ihrer Karte nicht genügend Guthaben vorhanden ist, um die kostenpflichtige SMS zu versenden, wird die Aktivierung des Abonnements abgebrochen.

Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Lizenz fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

Wenn Sie mit den Abonnementbestimmungen nicht einverstanden sind, klicken Sie auf **Abbrechen**. In diesem Fall bricht das Programm die Aktivierung des Abonnements ab und kehrt zu dem Fenster zurück, in dem Sie die Aktivierungsmethode für das Programm auswählen können.

- Gehen Sie weiter zur Eingabe des Geheimcodes (s. Abschnitt "Geheimcode festlegen" auf S. [31](#)).

AKTIVIERUNGSCODE ONLINE KAUFEN

➤ Gehen Sie folgendermaßen vor, um im Online-Shop einen Aktivierungscode zu kaufen:

- Gehen Sie auf **Start** → **Programme**.
- Wählen Sie **KMS 9** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

Das Fenster **Aktivieren** wird geöffnet.

- Wählen Sie **Online kaufen**.

Das Fenster **Online kaufen** wird geöffnet.

- Klicken Sie auf **Öffnen**.

Die Webseite von Kaspersky Lab für mobile Geräte wird geöffnet. Hier können Sie eine Bestellung für eine Lizenzverlängerung aufgeben.

- Folgen Sie den einzelnen Schritten der Anweisung.
- Nachdem Sie einen Aktivierungscode gekauft haben, fahren Sie fort mit der Aktivierung einer kommerziellen Programmversion (s. Abschnitt "Kommerzielle Version aktivieren" auf S. [28](#)).

TESTVERSION AKTIVIEREN

➤ Gehen Sie folgendermaßen vor, um eine Testversion von Kaspersky Mobile Security 9 zu aktivieren:

- Wählen Sie **Start** → **Programme**.

2. Wählen Sie **KMS 9** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

Das Fenster **Aktivieren** wird geöffnet.

3. Wählen Sie **Testversion**.
4. Bestätigen Sie die Internetverbindung mit **Ja**.

Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab und erhält eine Lizenz.

Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Lizenz fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

5. Gehen Sie zur Eingabe des Geheimcodes des Programms (s. Abschnitt "Geheimcode festlegen" auf S. [31](#)).

GEHEIMCODE FESTLEGEN

Nachdem das Programm gestartet wurde, werden Sie aufgefordert, den Geheimcode des Programms einzugeben. Der *Geheimcode des Programms* verhindert einen unautorisierten Zugriff auf die Programmeinstellungen.

Der aktuelle Geheimcode des Programms kann später geändert werden.

Kaspersky Mobile Security 9 fragt in folgenden Fällen nach dem Geheimcode:

- beim Zugriff auf das Programm
- beim Zugriff auf verschlüsselte Ordner
- wenn von einem anderen mobilen Gerät aus ein SMS-Befehl gesendet wird, um folgende Funktionen ferngesteuert zu starten: SMS-Block, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.
- bei der Deinstallation des Programms

Der Geheimcode des Programms besteht aus Ziffern und muss aus mindestens vier Zeichen bestehen.

Falls Sie den Geheimcode für das Programm vergessen sollten, können Sie diesen wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. [32](#)). Dazu muss vorher die Funktion zur Geheimcode-Wiederherstellung aktiviert werden (s. Abschnitt "Funktion zur Geheimcode-Wiederherstellung aktivieren" auf S. [32](#)).

➔ *Gehen Sie folgendermaßen vor, um den Geheimcode festzulegen:*

1. Nach der Aktivierung des Programms geben Sie im Feld **Code installieren** Ihren Geheimcode ein.
2. Wiederholen Sie die Eingabe im Feld **Code bestätigen**.

Ein eingegebener Code wird automatisch auf seine Sicherheit geprüft.

3. Wenn die Prüfung ergibt, dass ein Code unsicher ist, erscheint eine Warnung auf dem Bildschirm und das Programm erfragt eine Bestätigung. Klicken Sie auf **OK**, um den Code zu verwenden. Klicken Sie auf **Nein**, um einen neuen Code festzulegen.
4. Klicken Sie auf **OK**.

FUNKTION ZUR GEHEIMCODE-WIEDERHERSTELLUNG AKTIVIEREN

Die Funktion zur Geheimcode-Wiederherstellung kann nach der ersten Aktivierung des Programms aktiviert werden. So können Sie später den Geheimcode des Programms wiederherstellen, falls Sie ihn vergessen sollten.

Wenn Sie die Funktion nach der ersten Aktivierung des Programms nicht aktiviert haben, können Sie sie aktivieren, nachdem Kaspersky Mobile Security 9 neu auf dem Gerät installiert wurde.

Der Geheimcode für das Programm lässt sich nur dann wiederherstellen (s. Abschnitt "Geheimcode-Wiederherstellung" auf S. 32), wenn die Funktion zur Geheimcode-Wiederherstellung aktiviert ist. Wenn Sie das Kennwort vergessen haben und die Funktion zur Geheimcode-Wiederherstellung deaktiviert ist, können die Funktionen von Kaspersky Mobile Security 9 nicht mehr verwaltet werden und es ist nicht mehr möglich, auf verschlüsselte Dateien zuzugreifen und das Programm zu entfernen.

➤ Gehen Sie folgendermaßen vor, um die Funktion zur Geheimcode-Wiederherstellung zu aktivieren:

1. Nachdem Sie einen Geheimcode für das Programm festgelegt haben, bestätigen Sie mit **Ja**, dass die Funktion zur Geheimcode-Wiederherstellung aktiviert werden soll.
2. Tragen Sie im Feld **Ihre E-Mail-Adresse** eine E-Mail-Adresse ein und klicken Sie auf **Weiter**.

Die angegebene Adresse wird zur Geheimcode-Wiederherstellung verwendet.

Das Programm stellt eine Internetverbindung mit dem Geheimcode-Wiederherstellungsserver her, übermittelt die eingegebenen Daten und aktiviert die Funktion zur Geheimcode-Wiederherstellung.

GEHEIMCODE-WIEDERHERSTELLUNG

Der Geheimcode lässt sich nur wiederherstellen, wenn vorher die Funktion zur Geheimcode-Wiederherstellung aktiviert wurde (s. Abschnitt "Funktion zur Geheimcode-Wiederherstellung aktivieren" auf S. 32).

➤ Gehen Sie folgendermaßen vor, um den Geheimcode für das Programm wiederherzustellen:

1. Wählen Sie **Start** → **Programme**.
2. Wählen Sie **KMS 9** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.

Ein Fenster für die Eingabe des Geheimcodes wird geöffnet.

3. Klicken Sie auf **Abbrechen**.
4. Klicken Sie auf **Ja**, um zur Geheimcode-Wiederherstellung weiterzugehen.

Unter **Code-Wiederherstellung** werden folgende Informationen angezeigt:

- Webseite von Kaspersky Lab, die für die Geheimcode-Wiederherstellung dient.
 - ID-Code des Geräts
5. Gehen Sie auf die Webseite <http://mobile.kaspersky.com/recover-code>, um den Geheimcode wiederherzustellen.
 6. Füllen Sie die entsprechenden Felder aus:

- E-Mail-Adresse, die Sie zuvor für die Geheimcode-Wiederherstellung festgelegt haben.
- ID-Code des Geräts

Anschließend wird ein Wiederherstellungscode an die von Ihnen hinterlegte E-Mail-Adresse geschickt.

7. Klicken Sie im Fenster **Code-Wiederherstellung** auf **Fortsetzen** und tragen Sie den Wiederherstellungscode ein, den Sie empfangen haben.
8. Legen Sie einen neuen Geheimcode für das Programm fest. Tragen Sie dazu den neuen Geheimcode in die Felder **Code installieren** und **Code bestätigen** ein.
9. Klicken Sie auf **OK**.

PROGRAMM STARTEN

➤ *Gehen Sie folgendermaßen vor, um Kaspersky Mobile Security 9 zu starten:*

1. Wählen Sie **Start** → **Programme**.
2. Wählen Sie **KMS 9** und starten Sie das Programm. Verwenden Sie dazu den Stylus oder die mittlere Joystick-Taste.
3. Geben Sie den Geheimcode des Programms ein und klicken Sie auf **OK**.

Ein Fenster mit dem Schutzstatus von Kaspersky Mobile Security 9 wird geöffnet (s. Abschnitt "Fenster für den Schutzstatus" auf S. [43](#)). Klicken Sie auf **Menü**, um zu den Optionen des Programms zu wechseln.

UPDATE DER PROGRAMM-DATENBANKEN

Bei der Suche nach Bedrohungen verwendet Kaspersky Mobile Security 9 die Anti-Viren-Datenbanken des Programms, die eine Beschreibung aller derzeit bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Die Anti-Viren-Datenbanken, die zum Lieferumfang von Kaspersky Mobile Security 9 gehören, können zum Zeitpunkt der Installation bereits veraltet sein.

Es wird empfohlen, die Anti-Viren-Datenbanken des Programms sofort nach der Programminstallation zu aktualisieren.

Um die Anti-Viren-Datenbanken des Programms zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

➤ *Gehen Sie folgendermaßen vor, um das Update der Anti-Viren-Datenbanken des Programms zu starten:*

1. Wählen Sie **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Wählen Sie **Update**.
Das Fenster **Update** wird geöffnet.
3. Wählen Sie **Update starten**.

Das Programm startet das Update der Anti-Viren-Datenbanken des Programms von einem Kaspersky-Lab-Server. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

GERÄT AUF VIREN UNTERSUCHEN

Es wird empfohlen, Ihr mobiles Gerät nach der Programminstallation vollständig auf schädliche Objekte zu untersuchen.

Die erste Untersuchung erfolgt mit von Kaspersky Lab vordefinierten Einstellungen.

➤ *Gehen Sie folgendermaßen vor, um eine vollständige Untersuchung des Geräts zu starten:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie **Alles scannen**.

PROGRAMM-INFOS ANZEIGEN

Sie können allgemeine Informationen über das Programm Kaspersky Mobile Security 9 und über seine Version anzeigen.

➤ *Gehen Sie folgendermaßen vor, um Informationen über das Programm anzuzeigen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Programm-Infos**.

LIZENZVERWALTUNG

Im Zusammenhang mit der Lizenzierung von Kaspersky-Lab-Programmen sind folgende Begriffe wichtig:

- Lizenzvertrag
- Lizenz.

Diese drei Begriffe sind miteinander verbunden und bilden ein einheitliches Lizenzierungsschema. Es folgt eine ausführliche Erklärung.

Dieser Abschnitt informiert außerdem darüber, wie Informationen zur Lizenz von Kaspersky Mobile Security 9 angezeigt werden können und wie die Nutzungsdauer der Lizenz verlängert wird.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag	35
Über Lizenzen für Kaspersky Mobile Security 9	35
Informationen zur Lizenz anzeigen	36
Lizenz verlängern	37

ÜBER DEN LIZENZVERTRAG

Der *Lizenzvertrag* ist ein Vertrag zwischen einer natürlichen oder juristischen Person, die rechtmäßiger Besitzer eines Exemplars von Kaspersky Mobile Security 9 ist, und der Kaspersky Lab ZAO. Der Lizenzvertrag gehört zum Lieferumfang jedes Kaspersky-Lab-Programms. Er legt die Rechte und Einschränkungen für die Nutzung von Kaspersky Mobile Security genau fest.

In Übereinstimmung mit dem Lizenzvertrag erhalten Sie durch den Erwerb und die Installation eines Kaspersky-Lab-Programms das unbefristete Besitzrecht an einer Kopie.

Kaspersky Lab bietet Ihnen folgende Zusatzleistungen an:

- Technischen Support
- Update der Anti-Viren-Datenbanken für Kaspersky Mobile Security 9
- Update der Programm-Module für Kaspersky Mobile Security 9.0

Um diese Leistungen zu nutzen, muss eine Lizenz gekauft und aktiviert werden (s. Abschnitt "Über Lizenzen für Kaspersky Mobile Security 9" auf S. [35](#)).

ÜBER LIZENZEN FÜR KASPERSKY MOBILE SECURITY 9

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky Mobile Security 9 und der zum Programm gehörenden Zusatzleistungen (s. Abschnitt "Über den Lizenzvertrag" auf S. [35](#)), die von Kaspersky Lab und seinen Partnern angeboten werden.

Jede Lizenz wird durch Gültigkeitsdauer und Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen.

- technischer Support;
- Update der Anti-Viren-Datenbanken für Kaspersky Mobile Security 9
- Update der Programm-Module für Kaspersky Mobile Security 9

Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen:

- *Test* – Kostenlose Lizenz mit begrenzter Gültigkeitsdauer (z.B. 7 Tage) zum Kennenlernen von Kaspersky Mobile Security 9.

Eine Testlizenz kann nur einmal verwendet werden.

Wenn Sie eine Testlizenz verwenden, ist der technische Support auf Fragen über die Programmaktivierung und den Kauf einer kommerziellen Lizenz beschränkt. Nach Ablauf der Gültigkeitsdauer einer Testlizenz stellt Kaspersky Mobile Security 9 alle Funktionen ein. Um mit dem Programm weiterzuarbeiten, ist eine Aktivierung notwendig (s. Abschnitt "Kommerzielle Version aktivieren" auf S. [28](#)).

- *Kommerziell* – Gekaufte Lizenz, die eine begrenzte Gültigkeitsdauer (z.B. 1 Jahr) besitzt und beim Kauf von Kaspersky Mobile Security 9 zur Verfügung gestellt wird.

Während der Laufzeit einer kommerziellen Lizenz sind alle Programmfunktionen und zusätzliche Services verfügbar.

Nach Ablauf der kommerziellen Lizenz stehen bestimmte Funktionen von Kaspersky Mobile Security 9 nicht mehr zur Verfügung und die Anti-Viren-Datenbanken des Programms werden nicht mehr aktualisiert. Sieben Tage vor Ablauf der Lizenz werden Sie vom Programm entsprechend benachrichtigt, so dass Sie die Lizenz rechtzeitig verlängern können.

- *Kommerziell mit Abonnement* – kostenpflichtige Lizenz mit Möglichkeit der automatischen oder manuellen Verlängerung. Eine Lizenz mit Abonnement wird von Dienstleistern angeboten.

Das Abonnement gilt für einen begrenzten Zeitraum (30 Tage). Nach Ablauf dieses Zeitraums kann es manuell oder automatisch verlängert werden. Die Verlängerungsmethode hängt von der Gesetzgebung und dem jeweiligen Mobilfunkanbieter ab. Ein Abonnement wird automatisch verlängert, falls der erforderliche Betrag rechtzeitig an den Dienstleister überwiesen wird.

Bei Verlängerung des Abonnements wird die in den Abonnementsbedingungen festgelegte Summe von Ihrem Konto abgebucht. Die Kosten werden durch den Versand einer kostenpflichtigen SMS an die Nummer Ihres Mobilfunkanbieters abgebucht.

Wenn das Abonnement nicht verlängert wird, stellt Kaspersky Mobile Security 9 die Aktualisierung der Anti-Viren-Datenbanken des Programms ein und die Funktionen des Programms werden eingeschränkt.

Bei Verwendung des Abonnements können Sie die kommerzielle Lizenz mit Hilfe des Aktivierungscodes aktivieren. In diesem Fall wird das Abonnement automatisch beendet.

Bei Verwendung der kommerziellen Lizenz können Sie das Abonnement aktivieren. Wenn im Augenblick der Abonnementsaktivierung eine Lizenz mit beschränkter Gültigkeitsdauer aktiviert war, wird diese durch eine neue Lizenz mit Abonnement ersetzt.

INFORMATIONEN ZUR LIZENZ ANZEIGEN

Sie können folgende Informationen zur Lizenz erhalten: Nummer und Typ der Lizenz, Anzahl der verbleibenden Tage und Gerätenummer.

➤ Gehen Sie folgendermaßen vor, um Informationen zur Lizenz anzuzeigen:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

3. Wählen Sie **Lizenz-Info**.

LIZENZ VERLÄNGERN

Kaspersky Mobile Security 9 erlaubt es, die Programmlizenz zu verlängern.

Eine Lizenz kann auf folgende Weise verlängert werden:

- Aktivierungscode eingeben – Programm mit einem Aktivierungscode aktivieren. Den Aktivierungscode können Sie auf der Seite <http://www.kaspersky.de/store> oder bei den Vertriebspartnern von Kaspersky Lab erwerben.
- Online-Kauf einer Aktivierungscode – gehen Sie über Ihr mobiles Gerät auf die Website und kaufen Sie einen Aktivierungscode online.
- Abonnieren von Kaspersky Mobile Security 9 – Aktivieren eines Abonnements, um die Lizenz alle 30 Tage zu verlängern.

Um das Programm zu aktivieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

IN DIESEM ABSCHNITT

Lizenz mit Aktivierungscode verlängern	37
Lizenz online verlängern	38
Lizenz durch Aktivierung eines Abonnements verlängern	39
Kündigung des Abonnements	41
Fortsetzung des Abonnements	41

LIZENZ MIT AKTIVIERUNGSCODE VERLÄNGERN

➤ Gehen Sie folgendermaßen vor, um die Lizenz mit einem Aktivierungscode zu verlängern:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

3. Wählen Sie den Punkt **Verlängerung**.

Das Fenster **Verlängerung** wird geöffnet.

- Geben Sie den Code in die entsprechenden vier Felder ein und klicken Sie dann auf **Weiter** (s. Abb. unten).

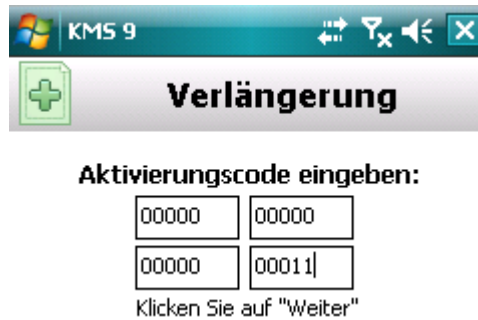


Abbildung 5: Lizenz mit Aktivierungscode verlängern

- Bestätigen Sie die Internetverbindung mit **Ja**.

Das Programm sendet eine Anfrage an den Aktivierungsserver von Kaspersky Lab und erhält eine Lizenz. Wurde eine Lizenz empfangen, werden die Lizenzinformationen auf dem Bildschirm angezeigt.

Wenn der von Ihnen eingegebene Aktivierungscode ungültig ist, erscheint eine entsprechende Meldung auf dem Bildschirm des mobilen Geräts. Prüfen Sie in diesem Fall, ob der Aktivierungscode richtig eingegeben wurde, und wenden Sie sich dann an die Firma, bei der Sie den Aktivierungscode für Kaspersky Mobile Security 9 gekauft haben.

Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Lizenz fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

- Klicken Sie zum Abschluss auf **OK**.

LIZENZ ONLINE VERLÄNGERN

➤ Gehen Sie folgendermaßen vor, um eine Lizenz online zu verlängern:

- Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

- Wählen Sie den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

- Wählen Sie den Punkt **Online kaufen**.

Das Fenster **Online kaufen** wird geöffnet.

4. Klicken Sie auf **Öffnen** (s. Abb. unten).



Abbildung 6: Lizenz online verlängern

Es wird eine Website geöffnet, auf der Sie ein Formular zur Lizenzverlängerung ausfüllen können.

Wenn die Lizenz abgelaufen ist, öffnet sich die spezielle Webseite von Kaspersky Lab für mobile Geräte, auf der Sie online einen Aktivierungscode kaufen können.

5. Folgen Sie den einzelnen Schritten der Anweisung.
6. Nachdem die Bestellung für die Lizenzverlängerung abgeschlossen wurde, geben Sie den neuen Aktivierungscode ein (s. Abschnitt "Lizenz mit Aktivierungscode verlängern" auf S. [37](#)).

LIZENZ DURCH AKTIVIERUNG EINES ABONNEMENTS VERLÄNGERN

Zur Verlängerung der Gültigkeit der Programmlizenz können Sie ein Abonnement aktivieren (s. Abschnitt "Über Lizenzen für Kaspersky Mobile Security 9" auf S. [35](#)) für Kaspersky Mobile Security 9 aktivieren. Besteht ein Abonnement, so verlängert Kaspersky Mobile Security 9 alle 30 Tage die Lizenz. Bei jeder Verlängerung der Lizenz wird die in den Abonnementsbedingungen festgelegte Summe von Ihrem Konto abgebucht.

Um ein Abonnement für Kaspersky Mobile Security 9 zu aktivieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

➤ Gehen Sie folgendermaßen vor, um ein Abonnement für Kaspersky Mobile Security 9 zu aktivieren:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

Wählen Sie den Punkt **Sofort kaufen** (s. Abb. unten).

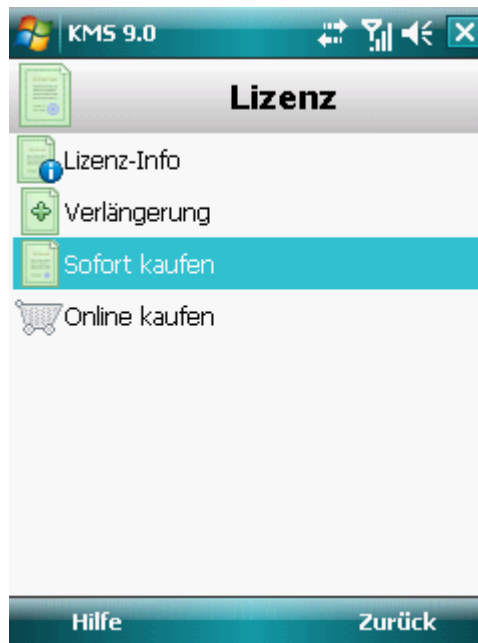


Abbildung 7: Abonnement aktivieren

3. Bestätigen Sie die Internetverbindung mit **Ja**.

Das Programm überprüft, ob der Abonnementdienst für Ihren Mobilfunkanbieter verfügbar ist.

Wenn der Abonnementdienst verfügbar ist, dann öffnet sich der Bildschirm **Aktivierung** mit den Abonnementbedingungen.

Ist der Abonnementdienst nicht verfügbar, informiert Sie das Programm hierüber und kehrt zu dem Fenster zurück, in dem Sie eine andere Methode für die Lizenzverlängerung auswählen können. Die Aktivierung des Abonnements wird abgebrochen.

4. Lesen Sie sich die Abonnementbedingungen durch und bestätigen Sie mit **Ja** die Aktivierung des Abonnements für Kaspersky Mobile Security 9.

Das Programm verschickt eine kostenpflichtige SMS und erhält dann vom Kaspersky-Lab-Aktivierungsserver eine Lizenz. Sie werden von Kaspersky Mobile Security 9 benachrichtigt, sobald das Abonnement aktiviert wurde.

Falls auf Ihrer Karte nicht genügend Guthaben vorhanden ist, um die kostenpflichtige SMS zu versenden, wird die Aktivierung des Abonnements abgebrochen.

Wenn bei der Verbindung mit dem Server Fehler aufgetreten sind und der Download einer Lizenz fehlschlägt, wird die Aktivierung abgebrochen. In diesem Fall sollten die Einstellungen der Internetverbindung geprüft werden. Sollte es nicht gelingen, den Fehler zu beheben, wenden Sie sich an den technischen Support.

Wenn Sie mit den Abonnementbestimmungen nicht einverstanden sind, klicken Sie auf **Abbrechen**. In diesem Fall bricht das Programm die Aktivierung des Abonnements ab und kehrt zu dem Fenster zurück, in dem Sie eine andere Methode für die Lizenzverlängerung auswählen können.

5. Klicken Sie zum Abschluss auf **OK**.

KÜNDIGUNG DES ABONNEMENTS

Das Abonnement für Kaspersky Mobile Security 9 ist nicht verpflichtend. In diesem Fall verlängert Kaspersky Mobile Security 9 die Lizenz nicht alle 30 Tage. Nach Ablauf der bestehenden Lizenz wird die Programmfunktionalität eingeschränkt und die Anti-Viren-Datenbanken des Programms werden nicht mehr aktualisiert.

Wenn das Abonnement gekündigt wurde, können Sie es fortsetzen (s. Abschnitt "Fortsetzung des Abonnements" auf S. [41](#)).

➔ Gehen Sie folgendermaßen vor, um das Abonnement für Kaspersky Mobile Security 9 zu kündigen:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

3. Wählen Sie den Punkt **Abonnement kündigen** (s. Abb. unten).

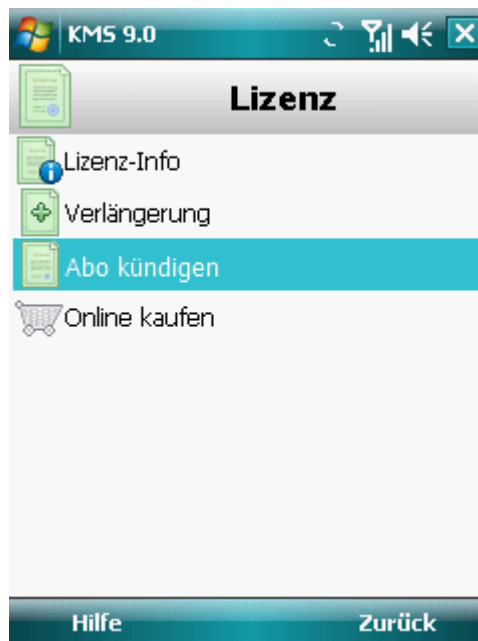


Abbildung 8: Kündigung des Abonnements

4. Bestätigen Sie die Kündigung des Abonnements mit **Ja**.

Kaspersky Mobile Security 9 teilt Ihnen mit, dass das Abonnement gekündigt wurde.

FORTSETZUNG DES ABONNEMENTS

Wenn das Abonnement gekündigt wurde (s. Abschnitt "Kündigung des Abonnements" auf S. [41](#)), können Sie es fortsetzen. In diesem Fall verlängert Kaspersky Mobile Security 9 alle 30 Tage die Lizenz.

Bei Fortsetzung des Abonnements werden die Kosten erst dann von Ihrem Konto abgebucht, wenn die aktuelle Lizenz in weniger als drei Tagen endet.

➤ *Gehen Sie folgendermaßen vor, um das Abonnement fortzusetzen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Lizenz**.

Das Fenster **Lizenz** wird geöffnet.

3. Wählen Sie die Option **Sofort kaufen**.

Wenn die bestehende Lizenz abgelaufen ist, schlägt Kaspersky Mobile Security 9 vor, das Abonnement wieder zu aktivieren (s. Abschnitt "Lizenz verlängern" auf S. [37](#)).

Wenn die aktuelle Lizenz noch nicht abgelaufen ist, setzt Kaspersky Mobile Security 9 das Abonnement fort und verlängert nach Ablauf der aktuellen Lizenz die Lizenzgültigkeit alle 30 Tage.

PROGRAMMOBERFLÄCHE

Dieser Abschnitt informiert über die wichtigsten Oberflächenelemente von Kaspersky Mobile Security 9.

IN DIESEM ABSCHNITT

Fenster für den Schutzstatus	43
Programm-Menü	45

FENSTER FÜR DEN SCHUTZSTATUS

Der Status der wichtigsten Programmkomponenten wird im Fenster für den Schutzstatus angezeigt.

Es gibt drei Statusvarianten. Jeder Status wird durch eine Farbe signalisiert. Die Farben entsprechen den Signalen einer Ampel. Grün bedeutet, dass der Schutz Ihres Geräts dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass bestimmte Sicherheitsrisiken vorliegen. Als Bedrohung gelten nicht nur veraltete Anti-Viren-Datenbanken, sondern beispielsweise auch deaktivierte Schutzkomponenten oder die Auswahl einer niedrigen Sicherheitsstufe.

Das Fenster für den Schutzstatus ist sofort nach dem Programmstart verfügbar und bietet folgende Informationen:

- **Schutz** – Status des Echtzeitschutzes (s. Abschnitt "Schutz für das Dateisystem" auf S. [47](#)).

Grün bedeutet, dass der Schutz aktiviert ist und dem erforderlichen Niveau entspricht. Die Anti-Viren-Datenbanken des Programms sind aktuell.

Gelb zeigt an, dass die Datenbanken seit mehreren Tagen nicht aktualisiert wurden.

Rot signalisiert Probleme, die zu Datenverlust oder zur Infektion des Geräts führen können. Beispiel: Der Schutz ist deaktiviert. Möglicherweise wurden die Anti-Viren-Datenbanken des Programms seit über 15 Tagen nicht mehr aktualisiert.

- **Firewall** – Stufe für den Schutz des Geräts vor unerwünschter Netzwerkaktivität (s. Abschnitt "Filterung der Netzwerkaktivität. Firewall" auf S. [104](#)).

Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Es wurde eine Sicherheitsstufe für die Firewall ausgewählt.

Rot deutet drauf hin, dass die Netzwerkaktivität nicht gefiltert wird.

- **Diebstahlschutz** – Status des Datenschutzes für den Fall eines Diebstahls oder Verlusts des Geräts (s. Abschnitt "Datenschutz bei Verlust oder Diebstahl des Geräts" auf S. [82](#)).

Das grüne Statussymbol bedeutet, dass die Diebstahlschutz-Funktionen, die unter dem Status der Komponente angezeigt werden, aktiviert sind.

Rot deutet drauf hin, dass alle Funktionen des Diebstahlschutzes deaktiviert sind.

- **Privatsphäre** – Status des Schutzes für vertrauliche Daten (s. Abschnitt "Verbergen sensibler Daten" auf S. [94](#)).

Das grüne Statussymbol bedeutet, dass die Komponente aktiviert ist. Vertrauliche Daten werden verborgen.

Gelb warnt davor, dass die Komponente deaktiviert ist. Persönliche Daten werden angezeigt und sind zur Anzeige verfügbar.

- **Lizenz** – Gültigkeitsdauer der Lizenz (s. Abschnitt "Lizenzverwaltung" auf S. 35).

Das grüne Statussymbol bedeutet, dass die Lizenz noch mehr als 14 Tage gültig ist.

Gelb warnt davor, dass die Lizenz weniger als 14 Tage gültig ist.

Rot signalisiert, dass die Gültigkeit der Lizenz abgelaufen ist.



Abbildung 9: Fenster Status der Programmkomponenten

Sie können auch in das Fenster für den Schutzstatus wechseln. Wählen Sie dazu **Menü** → **Schutzstatus**.

PROGRAMM-MENÜ

Die Programmkomponenten sind logisch angeordnet und stehen im Programm-Menü zur Verfügung. Die einzelnen Menüpunkte erlauben es, die Einstellungen einer ausgewählten Komponente zu öffnen oder Schutzaufgaben zu wählen (s. Abb. unten).



Abbildung 10: Programm-Menü

Das Menü von Kaspersky Mobile Security 9 enthält folgende Punkte:

- **Anti-Virus** – Virenschutz für das Dateisystem, Untersuchung und Update der Anti-Viren-Datenbanken des Programms.
- **Diebstahlschutz** – Bei Diebstahl oder Verlust das Gerät blockieren und Daten löschen.
- **Privatsphäre** – vertrauliche Daten auf dem Gerät verbergen.
- **Verschlüsselung** – Datenverschlüsselung zum Schutz der Informationen auf dem Gerät.
- **Anruf- und SMS-Filter** – Filterung von unerwünschten eingehenden Anrufen und SMS.
- **Kindersicherung** – Kontrolle über ausgehende Anrufe und SMS.
- **Firewall** – Netzwerkschutz für das Gerät.
- **Erweitert** – allgemeine Programmeinstellungen, Informationen zum Programm, den verwendeten Anti-Viren-Datenbanken und der Lizenz.
- **Schutzstatus** – Informationen über den Schutzstatus des Geräts.
- **Beenden** – Programm beenden.

➔ Um das Programm-Menü zu öffnen,

wählen Sie **Menü**.

Verwenden Sie zur Navigation innerhalb des Programm-Menüs den Joystick des Geräts oder den Stylus.

- *Gehen Sie folgendermaßen vor, um zum Statusfenster für die Programmkomponenten zurückzukehren:*
wählen Sie **Menü** → **Schutzstatus**.
- *Gehen Sie folgendermaßen vor, um das Programm zu beenden:*
wählen Sie **Menü** → **Beenden**.

SCHUTZ FÜR DAS DATEISYSTEM

Dieser Abschnitt informiert über die Komponente Schutz, die das Dateisystem Ihres Geräts vor Infektionen schützt. Außerdem wird hier beschrieben, wie der Schutz aktiviert / angehalten wird und wie die Schutzeinstellungen angepasst werden.

IN DIESEM ABSCHNITT

Schutz	47
Schutz aktivieren / deaktivieren.....	47
Aktion für gefundene Objekte wählen	49

SCHUTZ

Der Schutz startet beim Hochfahren des Betriebssystems und befindet sich permanent im Arbeitsspeicher des Geräts. Der Schutz untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden. Der Untersuchungsvorgang für eine Datei wird nach folgendem Algorithmus ausgeführt:

1. Der Schutz untersucht jede Datei, auf die Sie zugreifen.
2. Der Schutz analysiert eine Datei auf schädliche Objekte. Schädliche Objekte werden auf Basis der Anti-Viren-Datenbanken des Programms erkannt. Die Anti-Viren-Datenbanken des Programms enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte sowie entsprechende Desinfektionsmethoden.
3. Aufgrund der Analyseergebnisse sind folgende Varianten für das Verhalten des Schutzes möglich:
 - Wenn in einer Datei Schadcode gefunden wird, sperrt der Schutz die Datei und führt die festgelegte Aktion aus.

Wenn in einer Datei kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff auf die Datei. Informationen über die Untersuchungsergebnisse werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

SCHUTZ AKTIVIEREN / DEAKTIVIEREN

Wenn der Schutz aktiviert ist, werden alle Aktionen in Ihrem System permanent kontrolliert.

Der Schutz vor Viren und anderen Bedrohungen beansprucht die Ressourcen des Geräts. Wenn mehrere Aufgaben ausgeführt werden, kann der Schutz vorübergehend beendet werden, um die Auslastung des Geräts zu senken.

Die Kaspersky-Lab-Spezialisten warnen davor, den Schutz zu deaktivieren, weil dies zur Infektion Ihres mobilen Gerätes und zu Datenverlust führen kann.

Das Deaktivieren des Schutzes beeinflusst die Ausführung von Aufgaben zur Virensuche und zum Update der Anti-Viren-Datenbanken des Programms nicht.

Der aktuelle Schutzstatus wird im Fenster **Anti-Virus** neben dem Menüpunkt **Schutz** angezeigt.

Der Schutz kann folgendermaßen aktiviert / deaktiviert werden:

- aus dem Menü für die Einstellungen der Komponente
- aus dem Menü **Anti-Virus**

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

➔ *Gehen Sie folgendermaßen vor, um den Schutz zu aktivieren:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Schutz**.

Das Fenster **Schutz** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Schutz aktivieren** (s. Abb. unten).

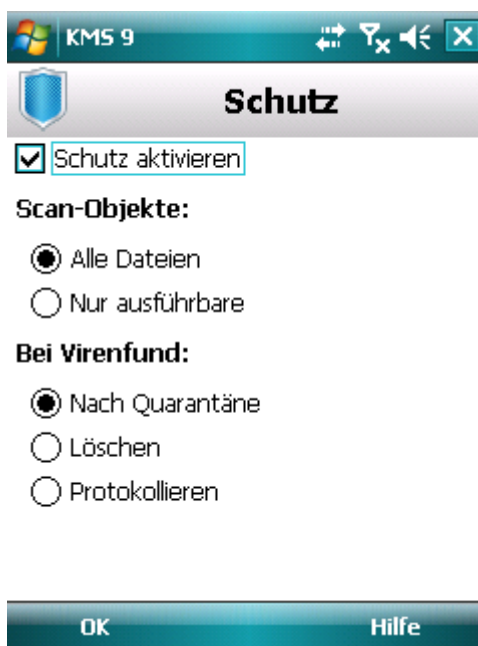


Abbildung 11: Schutz aktivieren

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

➔ *Gehen Sie folgendermaßen vor, um den Schutz zu deaktivieren:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Schutz**.

Das Fenster **Schutz** wird geöffnet.

3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

➤ Gehen Sie folgendermaßen vor, um den Schutz schnell zu aktivieren / deaktivieren:

1. Wählen Sie **Menü** → Anti-Virus.
2. Das Fenster **Anti-Virus** wird geöffnet.
3. Klicken Sie auf **Aktivieren** / **Deaktivieren**. Die Beschriftung der Schaltfläche ändert sich abhängig vom aktuellen Schutzstatus in das jeweilige Gegenteil.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

In der Grundeinstellung werden gefundene schädliche Objekte von Kaspersky Mobile Security 9 in die Quarantäne verschoben. Sie können eine Aktion auswählen, die Kaspersky Mobile Security 9 mit gefundenen schädlichen Objekten ausführen soll.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

Um die Schutzeinstellungen zu ändern, vergewissern Sie sich, dass der Schutz aktiviert ist.

➤ Gehen Sie folgendermaßen vor, um die Reaktion des Programms auf ein schädliches Objekt einzustellen (s. Abb. unten):

1. Wählen Sie **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Wählen Sie **Schutz**.
Das Fenster **Schutz** wird geöffnet.
3. Legen Sie fest, welche Aktion das Programm beim Fund eines schädlichen Objekts ausführen soll. Wählen Sie dazu einen Wert für **Bei Virenfund** (s. Abb. unten):
 - **Nach Quarantäne** – Objekte in die Quarantäne verschieben.
 - **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.

- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Zugriffsversuche auf ein Objekt (z.B. Kopieren oder Öffnen) blockieren.

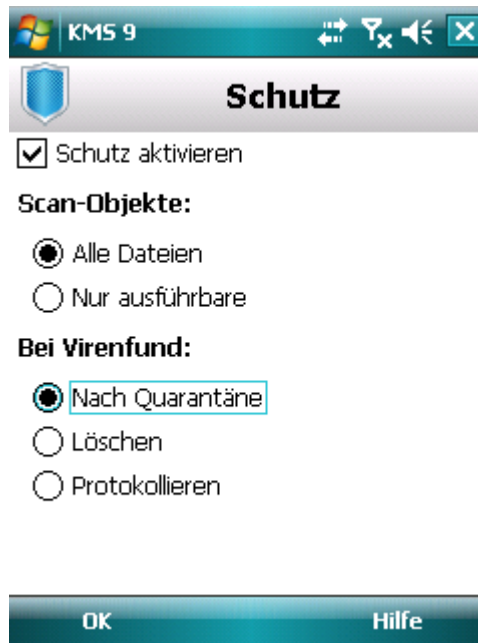


Abbildung 12: Aktion für Objekt wählen

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

UNTERSUCHUNG DES GERÄTS

Dieser Abschnitt informiert über die auf Befehl gestartete Untersuchung des Geräts, mit der Bedrohungen auf Ihrem Gerät erkannt und beseitigt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Untersuchung des Geräts starten, Zeitplan für die automatische Untersuchung des Dateisystems erstellen, Untersuchungsobjekte auswählen, Aktion des Programms für gefundene Schadobjekte festlegen.

IN DIESEM ABSCHNITT

Über Scan auf Befehl	51
Untersuchung manuell starten	52
Untersuchung nach Zeitplan starten	53
Typ der Untersuchungsobjekte wählen	54
Archiv-Untersuchung anpassen	55
Aktion für gefundene Objekte wählen	56

ÜBER SCAN AUF BEFEHL

Mit der Untersuchung des Geräts lassen sich schädliche Objekte erkennen und neutralisieren. Mit Kaspersky Mobile Security 9 kann der Inhalt des Geräts vollständig oder teilweise untersucht werden, d.h. die Untersuchung lässt sich auf den Inhalt des internen Gerätespeichers oder eines bestimmten Ordners (auch eines Ordners auf einer Speicherkarte) beschränken.

Die Untersuchung des Geräts wird nach folgendem Algorithmus ausgeführt:

1. Kaspersky Mobile Security 9 untersucht Dateien der festgelegten Typen (s. Abschnitt "Typ der Untersuchungsobjekte wählen" auf S. [54](#)).
2. Bei der Untersuchung wird die Datei auf schädliche Objekte analysiert. Schädliche Objekte werden auf Basis der Anti-Viren-Datenbanken des Programms erkannt. Die Anti-Viren-Datenbanken des Programms enthalten eine Beschreibung aller momentan bekannten schädlichen Objekte und entsprechende Desinfektionsmethoden.

Aufgrund der Analyseergebnisse bestehen folgende Varianten für das Verhalten von Kaspersky Mobile Security 9:

- Wenn in einer Datei schädlicher Code gefunden wird, sperrt Kaspersky Mobile Security 9 die Datei und führt die in den Einstellungen festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. [56](#)).
- Wenn kein schädlicher Code gefunden wird, wird die Datei sofort zum Zugriff freigegeben.

Eine Untersuchungsaufgabe kann manuell oder automatisch nach einem zuvor erstellten Zeitplan (s. Abschnitt "Untersuchung nach Zeitplan starten" auf S. [53](#)) gestartet werden.

Informationen über die Ergebnisse des Scan auf Befehl werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

UNTERSUCHUNG MANUELL STARTEN

Sie können eine Untersuchung manuell starten, wenn der Prozessor des Geräts nicht mit anderen Aufgaben beschäftigt ist.

➔ Gehen Sie folgendermaßen vor, um die Virenuntersuchung manuell zu starten:

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie einen Untersuchungsbereich für das Gerät (s. Abb. unten):

- **Alles scannen** – das gesamte Dateisystem des Geräts untersuchen. Standardmäßig werden folgende Objekte untersucht: Gerätespeicher und Speicherkarten.
- **Speicher scannen** – im Systemspeicher laufende Prozesse und die dazu gehörenden Dateien untersuchen.
- **Ordner scannen** – einzelnes Objekt im Dateisystem des Geräts oder auf einer eingelegten Speicherkarte untersuchen. Durch Klick auf **Ordner scannen** öffnet sich ein Fenster, in dem das Dateisystem des Geräts dargestellt ist. Verwenden Sie zur Navigation im Dateisystem die Joystick-Tasten oder den Stylus. Um die Untersuchung eines Ordners zu starten, markieren Sie den entsprechenden Ordner und klicken Sie auf **Scannen**.

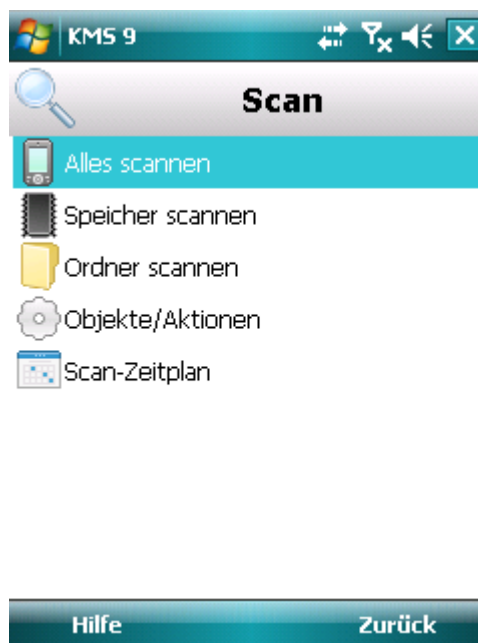


Abbildung 13: Untersuchungsbereich wählen

Nach dem Start der Untersuchung öffnet sich das Untersuchungsfenster, in dem der aktuelle Status angezeigt wird: Anzahl der untersuchten Objekte und Pfad zum Objekt, das gerade untersucht wird.

Beim Fund eines schädlichen Objekts führt Kaspersky Mobile Security 9 die in den Untersuchungseinstellungen festgelegte Aktion aus (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. 56).

Wenn Kaspersky Mobile Security 9 eine Bedrohung findet, verschiebt er diese standardmäßig in die Quarantäne.

Nach Abschluss der Untersuchung erscheint auf dem Bildschirm eine Statistik mit folgendem Inhalt:

- Anzahl der untersuchten Objekte
 - Anzahl der gefundenen, unter Quarantäne gestellten und gelöschten Viren
 - Anzahl der übersprungenen Objekte (Dateien werden beispielsweise übersprungen, wenn sie vom Betriebssystem verwendet werden oder sich bei einer ausschließlichen Untersuchung von ausführbaren Dateien als nicht ausführbar erweisen).
 - Zeitpunkt der Untersuchung
4. Klicken Sie zum Abschluss auf **OK**.

UNTERSUCHUNG NACH ZEITPLAN STARTEN

Mit Kaspersky Mobile Security 9 kann ein Zeitplan eingerichtet werden, nach dem die Untersuchung automatisch zur angegebenen Zeit startet. Die Untersuchung erfolgt im Hintergrund. Wenn ein infiziertes Objekt gefunden wird, führt das Programm die Aktion aus, die in den Untersuchungseinstellungen festgelegt wurde (s. Abschnitt "Aktion für gefundene Objekte wählen" auf S. [56](#)).

Die Untersuchung nach Zeitplan ist standardmäßig deaktiviert.

➡ *Gehen Sie folgendermaßen vor, um einen Zeitplan für die Untersuchung anzupassen:*

1. Wählen Sie **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Wählen Sie **Scan**.
Das Fenster **Scan** wird geöffnet.
3. Wählen Sie **Scan-Zeitplan**.
Das Fenster **Zeitplan** wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen **Scan nach Zeitplan** (s. Abb. unten).
5. Wählen Sie einen Wert für **Frequenz**:
 - **Täglich**: Die Untersuchung erfolgt jeden Tag. Geben Sie im Eingabefeld die **Zeit** ein.

- **Wöchentlich:** Die Untersuchung erfolgt einmal pro Woche. Geben Sie **Zeit** und **Wochentag** an.

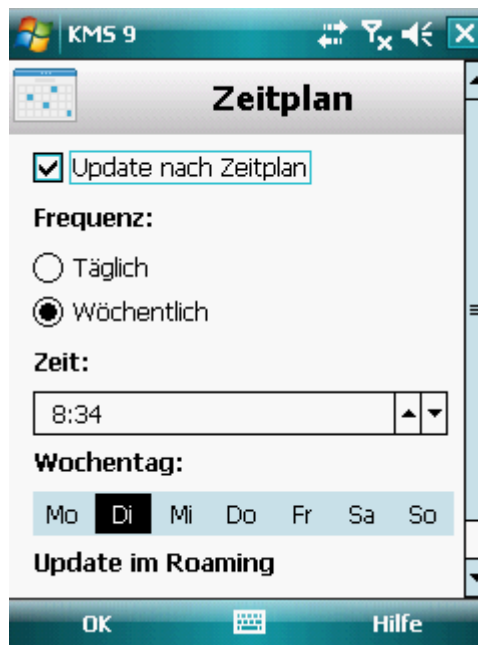


Abbildung 14: Automatischen Start der Untersuchung anpassen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

TYP DER UNTERSUCHUNGSOBJEKTE WÄHLEN

Sie können festlegen welche Objekttypen auf Schadcode untersucht werden sollen.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

➔ Gehen Sie folgendermaßen vor, um Untersuchungsobjekte zu wählen:

1. Wählen Sie auf **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie auf **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie auf **Objekte/Aktionen**.

Das Fenster **Objekte/Aktionen** wird geöffnet.

4. Wählen Sie im Block **Untersuchungsobjekte** die zu scannenden Objekte (s. Abb. unten):

- **Alle Dateien** – alle Dateitypen untersuchen.
- **Nur ausführbare** – Es werden nur ausführbare Programmdateien der folgenden Formate untersucht: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS.

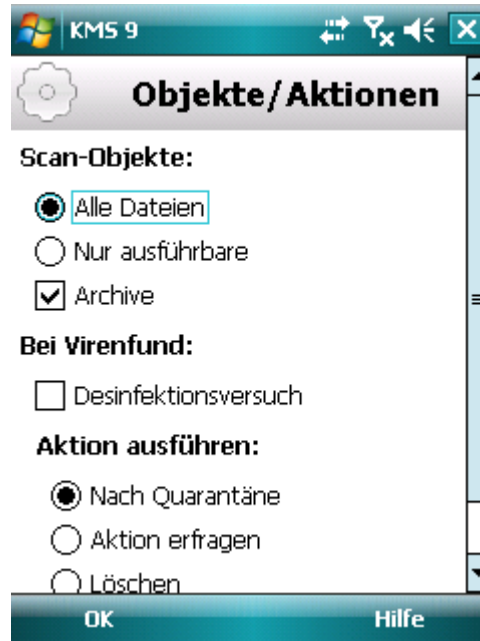


Abbildung 15: Schutzobjekte wählen

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

ARCHIV-UNTERSUCHUNG ANPASSEN

Viren werden häufig in Archiven versteckt. Das Programm kann Archive der folgenden Formate scannen: ZIP, JAR, JAD und CAB. Archive werden bei der Untersuchung entpackt, wodurch die Geschwindigkeit der Virensuche wesentlich sinken kann.

Die Untersuchung von Archiven auf schädlichen Code, die während einer Virensuche ausgeführt wird, kann aktiviert / deaktiviert werden.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

➤ Gehen Sie folgendermaßen vor, um die Untersuchung von Archiven zu aktivieren:

1. Wählen Sie **Menü** → **Anti-Virus**.
Das Fenster **Anti-Virus** wird geöffnet.
2. Wählen Sie **Scan**.
Das Fenster **Scan** wird geöffnet.
3. Wählen Sie **Objekte/Aktionen**.
Das Fenster **Objekte/Aktionen** wird geöffnet.
4. Aktivieren Sie im Block **Untersuchungsobjekte** das Kontrollkästchen **Archive**.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR GEFUNDENE OBJEKTE WÄHLEN

In der Grundeinstellung werden gefundene infizierte Objekte von Kaspersky Mobile Security 9 in die Quarantäne verschoben. Die Aktion, die das Programm beim Fund eines schädlichen Objekts ausführen soll, kann geändert werden.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

➔ *Gehen Sie folgendermaßen vor, um die Reaktion des Programms auf ein schädliches Objekt einzustellen (s. Abb. unten):*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Scan**.

Das Fenster **Scan** wird geöffnet.

3. Wählen Sie **Objekte/Aktionen**.

Das Fenster **Objekte/Aktionen** wird geöffnet.

4. Damit das Programm versucht, infizierte Objekte zu desinfizieren, aktivieren Sie für **Bei Virenfund** das Kontrollkästchen **Desinfektionsversuch** (s. Abb. unten).

5. Legen Sie eine Aktion für gefundene schädliche Objekte fest. Wählen Sie dazu einen Wert für **Aktion ausführen**:

Wenn das Kontrollkästchen **Desinfektionsversuch** aktiviert ist, heißt diese Einstellung **Wenn irreparabel**. Diese Einstellung legt fest, welche Aktion das Programm ausführen soll, wenn sich ein Objekt nicht desinfizieren lässt.

- **Nach Quarantäne** – Objekte in die Quarantäne verschieben.
- **Aktion erfragen** – beim Fund von schädlichen Objekten den Benutzer nach einer Aktion fragen.
- **Löschen** – schädliche Objekte löschen, ohne den Benutzer zu benachrichtigen.

- **Protokollieren** – schädliche Objekte überspringen und Fund in den Programmbericht eintragen. Zugriffsversuche auf ein Objekt (z.B. Kopieren oder Öffnen) blockieren.

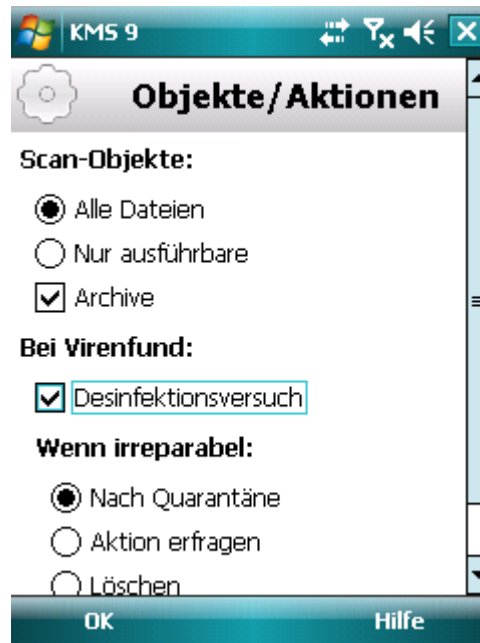


Abbildung 16: Aktion für schädliches Objekt wählen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

QUARANTÄNE FÜR SCHÄDLICHE OBJEKTE

Dieser Abschnitt informiert über den speziellen Speicher *Quarantäne*, in den potentiell gefährliche Objekte verschoben werden. Außerdem wird hier beschrieben, wie schädliche Objekte, die in diesem Ordner gespeichert sind, angezeigt, wiederhergestellt oder gelöscht werden können.

IN DIESEM ABSCHNITT

Über die Quarantäne.....	58
Quarantäneobjekte anzeigen	58
Quarantäneobjekte wiederherstellen.....	59
Quarantäneobjekte löschen	59

ÜBER DIE QUARANTÄNE

Während einer Untersuchung des Geräts oder im Rahmen des Schutzes verschiebt das Programm die gefundenen Schadobjekte in die *Quarantäne* (spezieller Isolationsordner). Schädliche Objekte werden in der Quarantäne in gepackter Form gespeichert, sodass deren Aktivierung ausgeschlossen ist und von ihnen keine Gefahr mehr für das Gerät ausgeht.

Sie können Dateien, die sich in der Quarantäne befinden, anzeigen, löschen oder wiederherstellen.

QUARANTÄNEOBJEKTE ANZEIGEN

Sie können eine Liste der Objekte, die vom Programm in die Quarantäne verschoben wurden, anzeigen lassen. Für jedes Objekt in der Liste werden der vollständige Name und das Funddatum angezeigt.

Sie können sich auch Zusatzinformationen über das ausgewählte infizierte Objekt anzeigen lassen: Den Pfad eines Objekts auf dem Gerät, bevor das Objekt vom Programm in die Quarantäne verschoben wurde, sowie den Namen der Bedrohung.

➤ *Gehen Sie folgendermaßen vor, um eine Liste der Quarantäneobjekte anzuzeigen:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet. Es enthält eine Liste der in die Quarantäne verschobenen Objekte (s. Abb. unten).

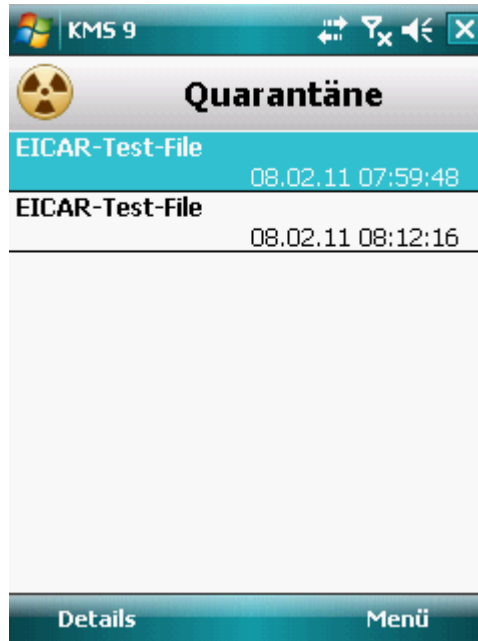


Abbildung 17: Liste der in die Quarantäne verschobenen Objekte

- Um Informationen über ein infiziertes Objekt anzuzeigen,

klicken Sie auf **Details**.

Das Fenster **Details** wird geöffnet.

Unter **Details** werden folgende Informationen über das Objekt angezeigt: Dateipfad, unter dem das Programm das Objekt auf dem Gerät gefunden hat, und Name des Virus.

QUARANTÄNEOBJEKTE WIEDERHERSTELLEN

Wenn Sie sicher sind, dass ein gefundenes Objekt keine Gefahr für das Gerät darstellt, können Sie es aus der Quarantäne wiederherstellen. Ein wiederhergestelltes Objekt wird in den ursprünglichen Ordner verschoben.

- Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne wiederherzustellen:

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet.

3. Wählen Sie ein Objekt, das wiederhergestellt werden soll, und wechselndann zu **Menü** → **Wiederherstellen**.

Das markierte Objekt wird aus der Quarantäne im ursprünglichen Ordner wiederhergestellt.

QUARANTÄNEOBJEKTE LÖSCHEN

Sie können entweder ein einzelnes Objekt oder alle Objekte aus der Quarantäne löschen.

➤ *Gehen Sie folgendermaßen vor, um ein Objekt aus der Quarantäne zu löschen:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet.

3. Wählen Sie ein zu löschendes Objekt und klicken Sie dann auf **Menü** → **Löschen**.

Das markierte Objekt wird aus der Quarantäne gelöscht.

➤ *Gehen Sie folgendermaßen vor, um alle Quarantäneobjekte zu löschen:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Quarantäne**.

Das Fenster **Quarantäne** wird geöffnet.

3. Klicken Sie auf **Menü** → **Alle löschen**.

Alle Quarantäneobjekte werden gelöscht.

EINGEHENDE ANRUF- UND SMS FILTERN

Dieser Abschnitt informiert über den Anruf- und SMS-Filter. Diese Komponente verhindert die Zustellung von unerwünschten Anrufen und SMS und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste. Außerdem wird in diesem Abschnitt beschrieben, wie ein Modus ausgewählt wird, nach dem der Anruf- und SMS-Filter eingehende Anrufe und SMS untersuchen soll, wie erweiterte Einstellungen für die Filterung von eingehenden SMS und Anrufen vorgenommen werden, und wie die Schwarze und Weiße Liste erstellt werden.

IN DIESEM ABSCHNITT

Über den Anruf- und SMS-Filter	61
Über die Modi für den Anruf- und SMS-Filter	62
Modus des Anruf- und SMS-Filters ändern	62
Schwarze Liste anlegen	63
Weißer Liste anlegen	66
Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen	69
Reaktion auf SMS von Nicht-Ziffern-Nummern	70
Aktion für eingehende SMS wählen	71
Aktion für eingehende Anrufe wählen	72

ÜBER DEN ANRUF- UND SMS-FILTER

Der Anruf- und SMS-Filter verhindert die Zustellung von unerwünschten Anrufen und SMS und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste.

Die Listen bestehen aus Einträgen. Jeder Listeneintrag enthält folgende Informationen:

- Telefonnummer, aufgrund welcher der Anruf- und SMS-Filter für die Schwarze Liste Informationen blockieren und für die Weiße Liste zustellen soll.
- Typ der Ereignisse, aufgrund welcher der Anruf- und SMS-Filter für die Schwarze Liste blockieren und für die Weiße Liste erlauben soll. Folgende Informationstypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, aufgrund welcher der Anruf- und SMS-Filter erwünschte und unerwünschte SMS unterscheidet. Für die Schwarze Liste blockiert der Anruf- und SMS-Filter die SMS-Nachrichten, die diese Phrase enthalten, und stellt SMS zu, in denen diese Schlüsselphrase nicht enthalten ist. Für die Weiße Liste stellt der Anruf- und SMS-Filter die SMS zu, die diese Phrase enthalten, und blockiert die SMS, in denen diese Schlüsselphrase nicht enthalten ist.

Der Anruf- und SMS-Filter filtert die eingehenden SMS und Anrufe nach dem ausgewählten Modus (s. Abschnitt "Über die Modi für den Anruf- und SMS-Filter" auf S. [62](#)). Nach diesem Modus untersucht der Anruf- und SMS-Filter alle eingehenden Anrufe und Nachrichten, und stuft sie als erwünscht oder unerwünscht (Spam) ein. Sobald der Anruf- und SMS-Filter einen Anruf oder eine SMS als erwünscht oder unerwünscht einstuft, wird die Untersuchung abgeschlossen.

Informationen über blockierte SMS und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

ÜBER DIE MODI FÜR DEN ANRUF- UND SMS-FILTER

Der Modus bestimmt die Regeln, nach welchen der Anruf- und SMS-Filter die eingehenden Anrufe und SMS filtert.

Für den Anruf- und SMS-Filter sind folgende Modi vorgesehen:

- **Aus** - Alle eingehenden SMS-Nachrichten und Anrufe werden zugestellt.
- **Weißer Liste erlauben** – Anrufe und SMS werden nur von Nummern aus der Weißen Liste zugestellt.
- **Schwarze Liste blockieren** – Anrufe und SMS werden von allen Nummern unter Ausnahme der Schwarzen Liste zugestellt.
- **Beide Listen** – Eingehende Anrufe und SMS-Nachrichten werden aufgrund von Nummern aus der Weißen Liste zugestellt und aufgrund von Nummern aus der Schwarzen Liste blockiert. Nach einem Gespräch oder nach dem Empfang einer SMS von einer Nummer, die auf keiner Liste steht, schlägt der Anruf- und SMS-Filter vor, die Nummer in eine der Listen aufzunehmen.

Sie können den Modus des Anruf- und SMS-Filters ändern (s. Abschnitt "Modus des Anruf- und SMS-Filters ändern" auf S. 62). Der aktuelle Modus des Anruf- und SMS-Filters wird auf dem Display **Anruf- und SMS-Filter** neben dem Menüpunkt **Modus** angezeigt.

MODUS DES ANRUF- UND SMS-FILTERS ÄNDERN

➔ Gehen Sie folgendermaßen vor, um den Modus des Anruf- und SMS-Filters zu ändern:

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

3. Wählen Sie einen Wert für den **Modus für Anruf- und SMS-Filter** aus (s. Abb. unten).



Abbildung 18: Modus des Anruf- und SMS-Filters ändern

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Die Schwarze Liste enthält Einträge über verbotene Nummern, d.h. jene Nummern, von denen Anrufe und SMS durch den Anruf- und SMS-Filter blockiert werden. Jeder Eintrag enthält folgende Informationen:

- Telefonnummer, von welcher der Anruf- und SMS-Filter Anrufe und / oder SMS blockieren soll.
- Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer blockieren soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach welcher der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter zugestellt.

Der Anruf- und SMS-Filter blockiert die Anrufe und SMS, die alle Kriterien eines Eintrags aus der Schwarzen Liste erfüllen. Anrufe und SMS-Nachrichten, die auch nur ein Kriterium eines Eintrags aus der Schwarzen Liste nicht erfüllen, werden vom Anruf- und SMS-Filter zugestellt.

Eine Telefonnummer mit identischen Filterkriterien kann nicht gleichzeitig zur Schwarzen und Weißen Liste hinzugefügt werden.

Informationen über blockierte SMS und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen	63
Eintrag der Schwarzen Liste ändern	64
Eintrag aus Schwarzer Liste löschen	65

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für den Anruf- und SMS-Filter stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9 eine entsprechende Meldung an.

➤ Zum Hinzufügen eines Eintrags zur Schwarzen Liste des Anruf- und SMS-Filters:

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie **Menü** → **Hinzufügen**.

Das Fenster **Neuer Eintrag** wird geöffnet.

4. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):

- **Eingehende verbieten** – Typ von Ereignissen einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Schwarzen Liste blockiert werden:
 - **Anrufe und SMS** – eingehende SMS und Anrufe blockieren.
 - **Nur Anrufe** – nur eingehende Anrufe blockieren.
 - **Nur SMS** - nur eingehende SMS blockieren.
- **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Schwarzen Liste. Der Anruf- und SMS-Filter blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS unerwünscht (Spam) ist. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Alle übrigen SMS werden zugestellt.

Wenn alle SMS von einer beliebigen Nummer aus der Schwarzen Liste blockiert werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

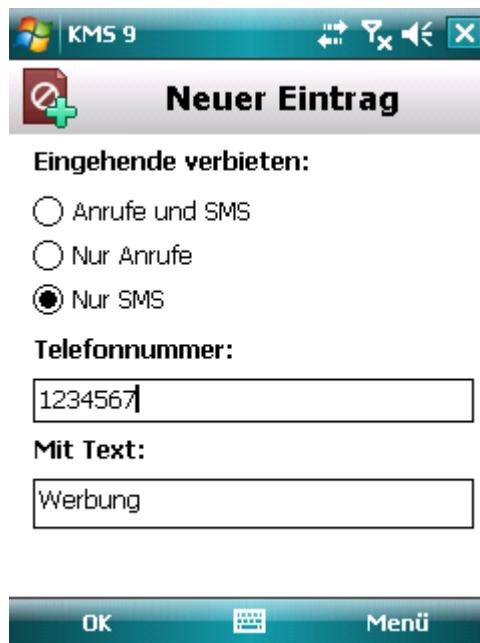


Abbildung 19: Einstellungen eines Eintrags

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG IN DER SCHWARZEN LISTE ÄNDERN

Alle Einstellungswerte der Einträge aus der Schwarzen Liste für verbotene Nummern können geändert werden.

➤ *Zum Ändern eines Eintrags in der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie aus der Liste ein Element, das geändert werden soll, und wechseln Sie dann zu **Menü** → **Ändern**.

Das Fenster **Ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Einstellungen:

- **Eingehende verbieten** – Typ von Ereignissen einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Schwarzen Liste blockiert werden:
 - **Anrufe und SMS** – eingehende SMS und Anrufe blockieren.
 - **Nur Anrufe** – nur eingehende Anrufe blockieren.
 - **Nur SMS** - nur eingehende SMS blockieren.
- **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Schwarzen Liste. Der Anruf- und SMS-Filter blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS unerwünscht (Spam) ist. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Alle übrigen SMS werden zugestellt.

Wenn alle SMS von einer beliebigen Nummer aus der Schwarzen Liste blockiert werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS DER SCHWARZEN LISTE LÖSCHEN

Eine Nummer kann aus der Schwarzen Liste gelöscht werden. Außerdem können Sie die Schwarze Liste des Anruf- und SMS-Filters leeren, d.h. alle Einträge daraus löschen.

- *Zum Löschen eines Eintrags aus der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Markieren Sie den zu löschenden Eintrag in der Liste und wechseln Sie dann zu **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen des Eintrags. Klicken Sie dazu auf **Ja**.

- *Zum Leeren der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie **Menü** → **Alle löschen**.

Die Liste wird geleert.

WEIßE LISTE ANLEGEN

Die Weiße Liste enthält Einträge über erlaubte Nummern, d.h. jene Nummern, von denen Anrufe und SMS durch den Anruf- und SMS-Filter zugestellt werden. Jeder Eintrag enthält folgende Informationen:

- Telefonnummer, von welcher der Anruf- und SMS-Filter Anrufe und / oder SMS zustellen soll.
- Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer zustellen soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter blockiert.

Der Anruf- und SMS-Filter stellt nur die Anrufe und SMS zu, die alle Kriterien eines Eintrags aus der Weißen Liste erfüllen. Anrufe und SMS-Nachrichten, die auch nur ein Kriterium eines Eintrags aus der Weißen Liste nicht erfüllen, werden vom Anruf- und SMS-Filter blockiert.

IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen	66
Eintrag der Weißen Liste ändern.....	67
Eintrag aus Weißer Liste löschen.....	68

EINTRAG ZUR WEIßEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für den Anruf- und SMS-Filter stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9 eine entsprechende Meldung an.

➔ *Zum Hinzufügen eines Eintrags zur Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Weiße Liste**.

Das Fenster **Weiße Liste** wird geöffnet.

3. Wählen Sie **Menü** → **Hinzufügen**.

Das Fenster **Neuer Eintrag** wird geöffnet.

4. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):

- **Eingehende erlauben** – Typ von Ereignissen von einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Weißen Liste erlaubt werden:
 - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
 - **Nur Anrufe** – nur eingehende Anrufe erlauben.
 - **Nur SMS** - nur eingehende SMS erlauben.
- **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Weißen Liste. Der Anruf- und SMS-Filter stellt Anrufe und SMS von einer Nummer zu, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS erwünscht ist. Für Nummern aus der Weißen Liste stellt der Anruf- und SMS-Filter nur die SMS zu, die die Schlüsselphrase enthalten. Alle übrigen SMS von dieser Nummer werden blockiert.

Wenn alle SMS von einer beliebigen Nummer aus der Weißen Liste zugestellt werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

KMS 9 Neuer Eintrag

Eingehende erlauben:

Anrufe und SMS

Nur Anrufe

Nur SMS

Telefonnummer:

987654321

Mit Text:

Zahlung

OK Menü

Abbildung 20: Einstellungen eines Eintrags

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG IN DER WEIßEN LISTE ÄNDERN

Alle Einstellungen für Einträge aus der Weißen Liste können geändert werden.

➡ *Zum Ändern eines Eintrags in der Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Weißer Liste**.

Das Fenster **Weißer Liste** wird geöffnet.

3. Wählen Sie aus der Liste ein Element aus, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

Das Fenster **Ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Einstellungen:

- **Eingehende erlauben** – Typ von Ereignissen von einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Weißen Liste erlaubt werden:
 - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
 - **Nur Anrufe** – nur eingehende Anrufe erlauben.
 - **Nur SMS** - nur eingehende SMS erlauben.
- **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer *1234? aus der Weißen Liste. Der Anruf- und SMS-Filter stellt Anrufe und SMS von einer Nummer zu, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS erwünscht ist. Für Nummern aus der Weißen Liste stellt der Anruf- und SMS-Filter nur die SMS zu, die die Schlüsselphrase enthalten. Alle übrigen SMS von dieser Nummer werden blockiert.

Wenn alle SMS von einer beliebigen Nummer aus der Weißen Liste zugestellt werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS DER WEIßEN LISTE LÖSCHEN

Sie können einen Eintrag aus der Weißen Liste löschen oder die Liste vollständig leeren.

➔ *Zum Löschen eines Eintrags aus der Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Weißer Liste**.

Das Fenster **Weißer Liste** wird geöffnet.

3. Markieren Sie den zu löschenden Eintrag in der Liste und wechseln Sie dann zu **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen des Eintrags. Klicken Sie dazu auf **Ja**.

➔ *Zum Leeren der Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Weißer Liste**.

Das Fenster **Weißer Liste** wird geöffnet.

3. Wählen Sie **Menü** → **Alle löschen**.

Die Liste wird geleert.

REAKTION AUF SMS-NACHRICHTEN UND ANRUF VON KONTAKTEN, DIE NICHT IM TELEFONBUCH STEHEN

Im Modus **Beide Listen** oder **Weißer Liste** (s. Abschnitt "Über die Modi für den Anruf- und SMS-Filter" auf S. 62) können Sie zusätzlich festlegen, wie der Anruf- und SMS-Filter auf SMS und Anrufe von Nummern reagieren soll, die sich nicht in den Kontakten befinden. Die Weiße Liste des Anruf- und SMS-Filters lässt sich durch Aufnahme der Nummern aus den Kontakten erweitern.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

- ➔ *Gehen Sie folgendermaßen vor, um festzulegen, wie der Anruf- und SMS-Filter auf eine Nummer reagieren soll, die nicht im Telefonbuch des Geräts steht:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

3. Wählen Sie einen Wert für **Kontakte erlauben** (s. Abb. unten):

- Damit Anruf- und SMS-Filter die Nummern des Telefonbuchs als zusätzliche Weiße Liste betrachtet und SMS und Anrufe von Nummern blockiert, die nicht im Telefonbuch stehen, aktivieren Sie das Kontrollkästchen **Kontakte erlauben**.

- Wählen Sie **Kontakte erlauben**, damit der Anruf- und SMS-Filter die Anrufe und Nachrichten nur nach dem festgelegten Modus filtert.



Abbildung 21: Reaktion des Anruf- und SMS-Filters auf Nummern, die nicht in den Kontakten stehen.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

REAKTION AUF SMS VON NICHT-ZIFFERN-NUMMERN

Für den Modus des Anruf- und SMS-Filters **Beide Listen** oder **Schwarze Liste** (s. Abschnitt "**Modus des Anruf- und SMS-Filters ändern**" auf S. 62) können Sie die Schwarze Liste durch Aufnahme aller Nicht-Ziffern-Nummern (Nummern, die Buchstaben enthalten) erweitern. In diesem Fall blockiert der Anruf- und SMS-Filter den Empfang von SMS, die von Nicht-Ziffern-Nummern stammen.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

- ➔ *Gehen Sie folgendermaßen vor, um festzulegen, wie der Anruf- und SMS-Filter auf eingehende SMS von Nicht-Ziffern-Nummern reagieren soll:*

1. Wählen Sie **Menü** → **Anruf- und SMS-Filter**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

3. Wählen Sie einen Wert für die Option **Nicht-Ziffern-Nummern blockieren** (s. Abb. unten):

- Wählen Sie den Wert **Nicht-Ziffern-Nummern blockieren**, damit der Anruf- und SMS-Filter Nachrichten von Nicht-Ziffern-Nummern automatisch löscht.

- Deaktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**, damit der Anruf- und SMS-Filter Nachrichten von Nicht-Ziffern-Nummern nur auf Basis des für den Anruf- und SMS-Filter ausgewählten Modus filtert.



Abbildung 22: Aktion des Anruf- und SMS-Filters für eingehende SMS von Nicht-Ziffern-Nummern anpassen

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

AKTION FÜR EINGEHENDE SMS WÄHLEN

Im Modus **Beide Listen** (s. Abschnitt "**Über die Modi für den Anruf- und SMS-Filter**" auf S. [62](#)) prüft der Anruf- und SMS-Filter eingehende SMS auf Übereinstimmungen mit der Schwarzen und Weißen Liste.

Wenn die Nummer des Absenders auf keiner der beiden Listen steht, werden Sie vom Anruf- und SMS-Filter darüber informiert. Sie können auswählen, welche der vorgeschlagenen Aktionen der Anruf- und SMS-Filter mit der eingehenden SMS ausführen soll (s. Abb. unten).



Abbildung 23: Meldung vom Anruf- und SMS-Filter über den Empfang einer Nachricht

Sie können eine der folgenden Aktionen für eine SMS wählen:

- Um eine SMS zu blockieren und die Telefonnummer des Absenders in die Schwarze Liste aufzunehmen, wählen Sie **Menü → Zur Schwarzen Liste**.
- Um eine SMS zu erlauben und die Telefonnummer des Absenders in die Weiße Liste aufzunehmen, wählen Sie **Menü → Zur Weißen Liste**.
- Um eine SMS zu erlauben und die Telefonnummer des Absenders in keine der Listen einzutragen, wählen Sie **Überspringen**.

Informationen über blockierte SMS werden in einem Programmbericht erfasst (s. Abschnitt "Programmierberichte" auf S. [117](#)).

AKTION FÜR EINGEHENDE ANRUFTE WÄHLEN

Im Modus **Beide Listen** (s. Abschnitt "**Über die Modi für den Anruf- und SMS-Filter**" auf S. [62](#)) prüft der Anruf- und SMS-Filter eingehende Anrufe auf Übereinstimmungen mit der Schwarzen und Weißen Liste.

Wenn die Nummer des Absenders auf keiner der beiden Listen steht, werden Sie vom Anruf- und SMS-Filter nach Gesprächsende darüber informiert und Sie können eine Aktion für den eingehenden Anruf wählen (s. Abb. unten).

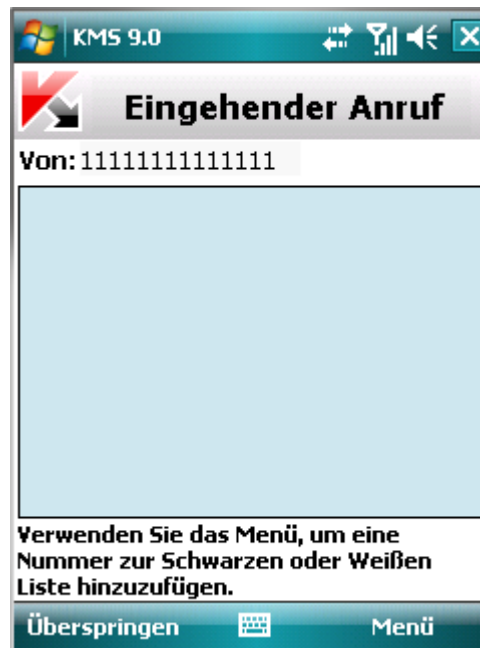


Abbildung 24: Meldung vom Anruf- und SMS-Filter über einen angenommenen Anruf

Für eine Nummer, von der ein Anruf erfolgte, können Sie eine der folgenden Aktionen wählen:

- Um die Telefonnummer des Anrufers in die Schwarze Liste aufzunehmen, wechseln Sie zu **Menü** → **Zur Schwarzen Liste**.
- Um die Telefonnummer des Anrufers in die Weiße Liste aufzunehmen, wechseln Sie zu **Menü** → **Zur Weißen Liste**.
- Damit die Telefonnummer des Anrufers in keine der Listen eingetragen wird, wählen Sie **Überspringen**.

Informationen über blockierte Anrufe werden in einem Programmbericht erfasst.

AUSGEHENDE ANRUFE UND SMS EINSCHRÄNKEN. KINDERSICHERUNG

Dieser Abschnitt informiert über die Komponente Kindersicherung, mit der ausgehende Anrufe und SMS an bestimmte Telefonnummern eingeschränkt werden können. Außerdem werden hier folgende Vorgänge beschrieben: Liste für erlaubte und verbotene Nummern anlegen, Kindersicherung anpassen.

IN DIESEM ABSCHNITT

Kindersicherung	74
Modi der Kindersicherung	74
Kindersicherung aktivieren / deaktivieren	75
Schwarze Liste anlegen	75
Weißer Liste anlegen	78

KINDERSICHERUNG

Die Kindersicherung ermöglicht die Kontrolle ausgehender SMS-Nachrichten und Anrufe unter Verwendung einer Schwarzen und Weißen Liste von Telefonnummern. Die Funktion der Komponente wird durch den Modus festgelegt.

Im Modus **Schwarze Liste** blockiert die Kindersicherung ausgehende SMS-Nachrichten oder Anrufe an Nummern aus der Schwarzen Liste. Alle übrigen ausgehenden SMS-Nachrichten und Anrufe werden erlaubt. Im Modus **Weißer Liste** erlaubt die Kindersicherung ausgehende SMS-Nachrichten oder Anrufe nur an Nummern aus der Weißen Liste. Alle übrigen SMS-Nachrichten und Anrufe werden von der Kindersicherung blockiert. Im Modus **"Aus"** kontrolliert die Kindersicherung die ausgehenden SMS und Anrufe nicht.

Die Kindersicherung blockiert nur ausgehende SMS, die mit Hilfe der Standardmittel des Geräts gesendet werden. Die Kindersicherung erlaubt ausgehende SMS, die mit Programmen von Drittherstellern gesendet werden.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

MODI DER KINDERSICHERUNG

Der Modus Kindersicherung legt die Regel fest, nach der die Kontrolle der ausgehenden SMS und Anrufe erfolgt.

Es sind die folgenden Optionen für die Kindersicherung vorgesehen:

- **Aus** – Kindersicherung deaktivieren. Ausgehende SMS und Anrufe nicht kontrollieren.
Dieser Modus gilt als Standard.
- **Weißer Liste** – SMS und / oder Anrufe werden nur an Nummern aus der Weißen Liste erlaubt (s. Abschnitt "Weiße Liste anlegen" auf S. [78](#)). Alle übrigen Nachrichten und Anrufe werden blockiert.
- **Schwarze Liste** – SMS und / oder Anrufe werden nur an Nummern aus der Schwarzen Liste verboten (s. Abschnitt "Schwarze Liste anlegen" auf S. [75](#)). Alle übrigen Nachrichten und Anrufe werden erlaubt.

Sie können den Modus der Kindersicherung ändern (s. Abschnitt "Kindersicherung aktivieren / deaktivieren" auf S. 75). Der aktuelle Modus der Kindersicherung wird im Fenster **Kindersicherung** neben dem Menüpunkt **Modus** angezeigt.

KINDERSICHERUNG AKTIVIEREN / DEAKTIVIEREN

➤ Gehen Sie folgendermaßen vor, um einen Modus für die Kindersicherung zu ändern:

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Kinder sicherung** wird geöffnet.

3. Wählen Sie einen Modus für die Kindersicherung (s. Abb. unten).

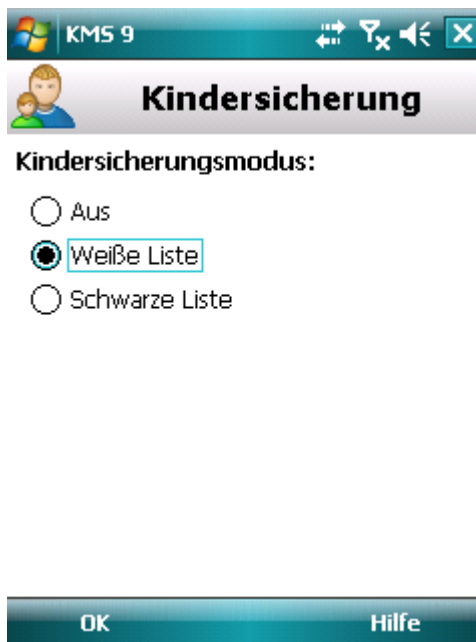


Abbildung 25: Modus für die Kindersicherung ändern

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

SCHWARZE LISTE ANLEGEN

Sie können eine Schwarze Liste anlegen, nach der die Kindersicherung ausgehende SMS und Anrufe blockieren soll. Die Liste enthält Telefonnummern, an die ausgehende SMS und Anrufe verboten werden.

Informationen über blockierte SMS und Anrufe werden in einem Programmbericht (s. Abschnitt "Programmberichte" auf S. 117).

IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen	76
Eintrag der Schwarzen Liste ändern	77
Eintrag aus Schwarzer Liste löschen	78

EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für die Kindersicherung stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9 eine entsprechende Meldung an.

➔ *Zum Hinzufügen eines Eintrags zur Schwarzen Liste der Kindersicherung:*

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie **Menü** → **Hinzufügen**.

Das Fenster **Neuer Eintrag** wird geöffnet.

4. Legen Sie die Werte für folgende Optionen fest (s. Abb. unten):

- **Ausgehende verbieten** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer blockiert werden soll:
 - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe blockieren.
 - **Nur Anrufe** – nur ausgehende Anrufe blockieren.
 - **Nur SMS** - nur ausgehende SMS-Nachrichten blockieren.

- **Telefonnummer** – Telefonnummer, für die der Versand von SMS-Nachrichten und/oder Anrufe gesperrt wird. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

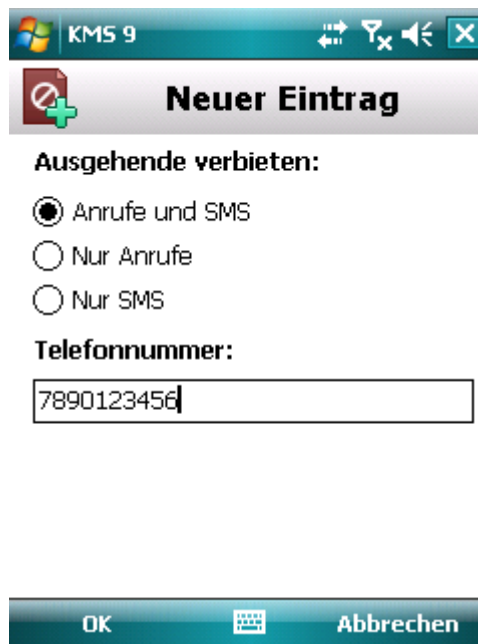


Abbildung 26: Einstellungen eines Eintrags

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG IN DER SCHWARZEN LISTE ÄNDERN

Alle Einstellungswerte der Einträge aus der Schwarzen Liste für verbotene Nummern können geändert werden.

➤ *Zum Ändern eines Eintrags in der Schwarzen Liste der Kindersicherung:*

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.

Das Fenster **Ändern** wird geöffnet.

4. Ändern Sie die erforderlichen Optionen:

- **Ausgehende verbieten** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer blockiert werden soll:
 - **Anrufe und SMS** – ausgehende SMS-Nachrichten und Anrufe blockieren.
 - **Nur Anrufe** – nur ausgehende Anrufe blockieren.
 - **Nur SMS** - nur ausgehende SMS-Nachrichten blockieren.

- **Telefonnummer** – Telefonnummer, für die der Versand von SMS-Nachrichten und/oder Anrufe gesperrt wird. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht und "?" für ein beliebiges Einzelzeichen).

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS DER SCHWARZEN LISTE LÖSCHEN

Es kann vorkommen, dass eine Nummer versehentlich zur Schwarzen Liste der verbotenen Nummern hinzugefügt wurde. Eine solche Nummer kann aus der Liste gelöscht werden. Außerdem können Sie die Schwarze Liste der Kindersicherung leeren, d.h. alle Einträge daraus löschen.

➔ *Zum Löschen eines Eintrags aus der Schwarzen Liste der Kindersicherung:*

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Markieren Sie den zu löschenden Eintrag in der Liste und gehen Sie dann auf **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

➔ *Zum Leeren der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Schwarze Liste**.

Das Fenster **Schwarze Liste** wird geöffnet.

3. Wählen Sie **Menü** → **Alle löschen**.

Die Liste wird geleert.

WEIßE LISTE ANLEGEN

Sie können eine Weiße Liste anlegen, nach der der Anruf- und SMS-Filter eingehende SMS und Anrufe erlauben soll.

IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen	79
Eintrag der Weißen Liste ändern.....	80
Eintrag aus Weißer Liste löschen.....	80

EINTRAG ZUR WEIßEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für die Kindersicherung stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Mobile Security 9 eine entsprechende Meldung an.

➔ Zum Hinzufügen eines Eintrags zur Weißen Liste der Kindersicherung:

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Weiße Liste**.

3. Das Fenster **Weiße Liste** wird geöffnet.

4. Wählen Sie **Menü** → **Hinzufügen**.

Das Fenster **Neuer Eintrag** wird geöffnet.

5. Legen Sie die Werte für folgende Optionen fest (s. Abb. unten):

- **Ausgehende erlauben** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer erlaubt werden soll:
 - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
 - **Nur Anrufe** – nur ausgehende Anrufe erlauben.
 - **Nur SMS** – nur ausgehende SMS erlauben.
- **An Telefonnummer** – Telefonnummer, an die Kindersicherung ausgehende SMS und / oder Anrufe erlauben soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

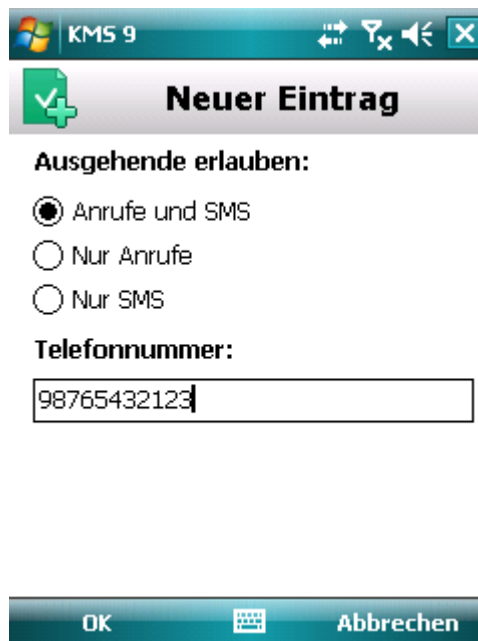


Abbildung 27: Parameter eines Eintrags

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG IN DER WEIßEN LISTE ÄNDERN

Alle Einstellungswerte der Einträge aus der Weißen Liste für erlaubte Nummern können geändert werden.

➤ Zum Ändern eines Eintrags in der Weißen Liste der Kindersicherung:

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Weiße Liste**.

3. Das Fenster **Weiße Liste** wird geöffnet.

4. Wählen Sie aus der Liste ein Element, das geändert werden soll, und wechseln dann zu **Menü** → **Ändern**.

Das Fenster **Ändern** wird geöffnet.

5. Ändern Sie die erforderlichen Optionen:

- **Ausgehende erlauben** – Typ der ausgehenden Informationen, der von der Kindersicherung für eine Nummer erlaubt werden soll:
 - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
 - **Nur Anrufe** – nur ausgehende Anrufe erlauben.
 - **Nur SMS** – nur ausgehende SMS erlauben.
- **An Telefonnummer** – Telefonnummer, an die Kindersicherung ausgehende SMS und / oder Anrufe erlauben soll. Die Nummer kann mit einer Ziffer, mit einem Buchstaben oder mit dem Zeichen "+" beginnen und darf Ziffern / Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "*" und "?" möglich (wobei "*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen).

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

EINTRAG AUS DER WEIßEN LISTE LÖSCHEN

Sie können einen Eintrag löschen oder die Weiße Liste vollständig leeren.

➤ Zum Löschen eines Eintrags aus der Weißen Liste der Kindersicherung:

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Weiße Liste**.

3. Das Fenster **Weiße Liste** wird geöffnet.

4. Markieren Sie den zu löschenden Eintrag in der Liste und wechseln dann zu **Menü** → **Löschen**.

5. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

➤ Zum Leeren der Weißen Liste des Anruf- und SMS-Filters:

1. Wählen Sie **Menü** → **Kindersicherung**.

Das Fenster **Kinder sicherung** wird geöffnet.

2. Wählen Sie **Weiß e Liste**.
3. Das Fenster **Weiß e Liste** wird geöffnet.
4. Wählen Sie **Menü** → **Alle löschen**.

Die Liste wird geleert.

DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS

Dieser Abschnitt informiert über die Komponente Diebstahlschutz, die bei Diebstahl oder Verlust des Geräts die auf dem Gerät gespeicherten Informationen vor unbefugtem Zugriff schützt und das Auffinden des Geräts erleichtert.

Außerdem werden hier folgende Vorgänge beschrieben: Diebstahlschutz-Funktionen aktivieren / deaktivieren, Diebstahlschutz anpassen, Diebstahlschutz-Funktionen von einem anderen Gerät aus ferngesteuert starten.

IN DIESEM ABSCHNITT

Diebstahlschutz.....	82
Gerät blockieren.....	83
Persönliche Daten löschen.....	85
Liste der zu löschenden Ordner erstellen.....	87
Wechsel der SIM-Karte auf dem Gerät überwachen.....	88
Geografische Koordinaten des Geräts ermitteln	89
Diebstahlschutz-Funktionen ferngesteuert starten.....	92

ÜBER DEN DIEBSTAHLSCHEUTZ

Der Diebstahlschutz schützt die Informationen, die auf Ihrem mobilen Gerät gespeichert sind, vor unbefugtem Zugriff.

Der Diebstahlschutz umfasst folgende Funktionen:

- **SMS-Block** erlaubt es, das Gerät ferngesteuert zu blockieren und einen Text festzulegen, der auf dem Display des blockierten Geräts angezeigt wird.
- **SMS-Clean** erlaubt es, die persönlichen Benutzerdaten (Einträge in den Kontakten, SMS, Bilder, Kalender, Berichte, Internet-Einstellungen) sowie Daten auf Speicherkarten und von Dateien aus der Lösch-Liste per Fernsteuerung vom Gerät zu löschen.
- **SIM-Watch** erlaubt es, die aktuelle Telefonnummer zu ermitteln, wenn die SIM-Karte gewechselt wurde. Außerdem kann das Gerät automatisch blockiert werden, wenn die SIM-Karte gewechselt oder das Gerät ohne SIM eingeschaltet wird. Informationen über die neue Telefonnummer werden als Nachricht an die von Ihnen angegebene Telefonnummer und / oder E-Mail-Adresse geschickt.
- Mit **GPS-Find** kann ein Gerät geortet werden. Die geografischen Koordinaten des Geräts werden als Nachricht an die Telefonnummer, von der der spezielle SMS-Befehl stammte, und an eine E-Mail-Adresse geschickt.

Alle Diebstahlschutz-Funktionen sind nach der Installation von Kaspersky Mobile Security 9 deaktiviert.

Die Diebstahlschutz-Funktionen von Kaspersky Mobile Security 9 lassen sich durch einen SMS-Befehl von einem anderen Gerät aus starten (s. Abschnitt "Diebstahlschutz-Funktionen ferngesteuert starten" auf S. [92](#)).

Um die Diebstahlschutz-Funktionen ferngesteuert zu starten, ist der Geheimcode des Programms erforderlich, der beim ersten Start von Kaspersky Mobile Security 9 auf Ihrem Gerät festgelegt wird.

Der aktuelle Status der einzelnen Funktionen wird im Fenster **Diebstahlschutz** neben der jeweiligen Funktion angezeigt.

Informationen über die Arbeit einer Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

GERÄT BLOCKIEREN

Nach Empfang eines speziellen SMS-Befehls kann die Funktion SMS-Block per Fernsteuerung den Zugriff auf das Gerät und die darauf gespeicherten Daten sperren. Das Gerät kann nur durch Eingabe des Geheimcodes entsperrt werden.

Diese Funktion blockiert das Gerät nicht: Sie aktiviert eine Option für das ferngesteuerte Blockieren.

➤ Gehen Sie folgendermaßen vor, um die Funktion SMS-Block zu aktivieren:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Wählen Sie **SMS-Block**.

Das Fenster **SMS-Block** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SMS-Block aktivieren**.

4. Ändern Sie im Feld **Text beim Blockieren** den Text, der auf dem Display des blockierten Geräts angezeigt werden soll (s. Abb. unten). In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Telefonbesitzers hinzufügen können.



Abbildung 28: Einstellungen der Funktion SMS-Block

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Ein anderes Gerät, auf dem die Funktion SMS-Block aktiviert ist, kann auf folgende Weise gesperrt werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Mobile Security 9) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Um einen speziellen SMS-

Befehl zu erstellen, verwenden Sie bitte die Funktion Befehl senden. Dadurch erhält Ihr Gerät unbemerkt eine SMS und das Gerät wird blockiert.

- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät unbemerkt eine SMS und das Gerät wird blockiert.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um ein Gerät per Fernzugriff zu blockieren, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall wird der Geheimcode für das Programm in verschlüsselter Form gesendet.

Um ein Gerät per Fernzugriff zu blockieren, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall werden Befehl und Geheimcode in verschlüsselter Form gesendet.

➤ Gehen Sie folgendermaßen vor, um den SMS-Befehl mit Hilfe der Funktion Befehl senden an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie die Option **SMS-Befehl auswählen** auf **Gerät blockieren** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.



Abbildung 29: Gerät per Fernsteuerung blockieren

6. Klicken Sie auf **Senden**.

- Um mit Hilfe der SMS-Standardfunktionen eines Telefons eine SMS zu erstellen,

schicken Sie an das andere Gerät eine SMS mit dem Text `block:<Code>`, wobei `<Code>` der Geheimcode ist, der auf dem anderen Gerät hinterlegt ist. Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

PERSÖNLICHE DATEN LÖSCHEN

Nach Erhalt des speziellen SMS-Befehls ermöglicht es die Funktion SMS-Clean, die folgenden, auf dem Gerät gespeicherten Informationen zu löschen:

- persönliche Benutzerdaten (Einträge in den Kontakten und auf der SIM- Karte, SMS, Bilder, Kalender, Internet-Einstellungen)
- Informationen auf einer Speicherkarte
- Die Dateien aus dem Ordner **Eigene Dateien** und aus anderen Ordnern der Liste **Zu löschende Ordner**.

Diese Funktion löscht die auf dem Gerät gespeicherten Daten nicht, sondern aktiviert eine Option zur Datenlöschung.

- Gehen Sie folgendermaßen vor, um die Funktion SMS-Clean zu aktivieren:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Wählen Sie **SMS-Clean**.

Das Fenster **SMS-Clean** wird geöffnet.

3. Wählen Sie **Modus**.

Das Fenster **SMS-Clean** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **SMS-Clean aktivieren**.

5. Wählen Sie die zu löschenden Informationen aus. Aktivieren Sie dazu im Block **Löschen** die entsprechenden Kontrollkästchen (s. Abb. unten):

- Aktivieren Sie das Kontrollkästchen **Persönliche Daten**, damit persönliche Daten gelöscht werden.

- Aktivieren Sie das Kontrollkästchen **Zu löschende Ordner**, damit die Dateien aus dem Ordner **Eigene Dateien** und aus der Liste **Zu löschende Ordner** gelöscht werden.



Abbildung 30: Typ der zu löschenden Daten wählen

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.
7. Wechseln Sie zur Erstellung der Liste **Zu löschende Ordner** (s. Abschnitt "**Liste der zu löschenden Ordner erstellen**" auf S. [87](#)).

Wenn die Funktion aktiviert ist, können persönliche Daten auf folgende Weise vom Gerät gelöscht werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Mobile Security 9) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion **Befehl senden**. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die Informationen werden gelöscht.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese.

Um per Fernsteuerung Daten vom Gerät zu löschen, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall werden **Befehl** und **Geheimcode** in verschlüsselter Form gesendet.

➔ Gehen Sie folgendermaßen vor, um einen Befehl an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie die Option **SMS-Befehl auswählen** auf **Daten löschen** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.

Abbildung 31: Löschen persönlicher Daten per Fernsteuerung starten

6. Klicken Sie auf **Senden**.

- Um mit Hilfe der SMS-Standardfunktionen eines Telefons eine SMS zu erstellen,

schicken Sie an das andere Gerät eine SMS mit dem Text `wipe:<Code>` (wobei `<Code>` der Geheimcode des anderen Geräts ist). Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER ZU LÖSCHENDEN ORDNER ERSTELLEN

Die Funktion SMS-Clean erlaubt es, eine Liste mit Ordnern anzulegen, die nach dem Empfang einer speziellen SMS gelöscht werden sollen.

Damit der Diebstahlschutz die Ordner aus der Liste nach Eingang des speziellen SMS-Befehls löscht, müssen Sie sich vergewissern, dass im Menüpunkt **Modus** das Kontrollkästchen **Ordner** aktiviert ist.

- Gehen Sie folgendermaßen vor, um einen Ordner zur Liste der zu löschenden Ordner hinzuzufügen:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Wählen Sie **SMS-Clean**.

Das Fenster **SMS-Clean** wird geöffnet.

3. Wählen Sie **Zu löschende Ordner**.

Das Fenster **Zu löschende Ordner** wird geöffnet.

4. Wählen Sie **Menü** → **Hinzufügen** (s. Abb. unten).

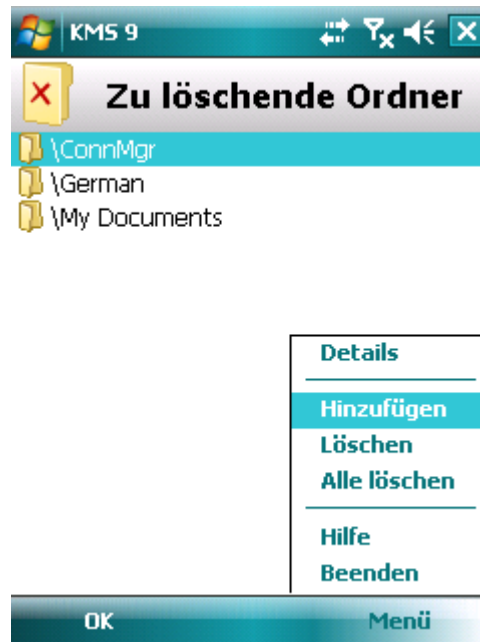


Abbildung 32: Zu löschende Ordner wählen

5. Wählen Sie in der Ordnerstruktur den entsprechenden Ordner aus und klicken Sie auf **Auswählen**.

Der Ordner wird zur Liste hinzugefügt.

➤ Gehen Sie folgendermaßen vor, um einen Ordner aus der Liste zu löschen:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Wählen Sie **SMS-Clean**.

Das Fenster **SMS-Clean** wird geöffnet.

3. Wählen Sie **Zu löschende Ordner**.

Das Fenster **Zu löschende Ordner** wird geöffnet.

4. Wählen Sie einen Ordner aus der Liste und gehen Sie auf **Menü** → **Löschen**.

WECHSEL DER SIM-KARTE AUF DEM GERÄT ÜBERWACHEN

Wenn die SIM-Karte ausgetauscht wird, kann SIM-Watch die neue Telefonnummer an eine vorgegebene Telefonnummer und / oder E-Mail-Adresse schicken und das Gerät blockieren.

➤ Gehen Sie folgendermaßen vor, um die Funktion SIM-Watch zu aktivieren und den Wechsel der SIM-Karte auf dem Gerät zu überwachen:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Wählen Sie **SIM-Watch**.

Das Fenster **SIM-Watch** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SIM-Watch aktivieren**.

4. Passen Sie folgende Optionen an, um den Wechsel der SIM-Karte auf dem Gerät zu kontrollieren (s. Abb. unten):

- Um automatisch eine Nachricht über die neue Nummer Ihres Telefons zu erhalten, geben Sie unter **Neue Nummer senden** im Feld **SMS an Telefonnummer** die Nummer ein, die benachrichtigt werden soll.
Die Nummer kann mit einer Ziffer oder dem Zeichen "+" beginnen und darf nur Ziffern enthalten.
- Wenn Sie per E-Mail über die neue Nummer des Telefons informiert werden möchten, geben Sie die entsprechende Adresse unter **Neue Nummer senden** im Feld **Nachricht an E-Mail-Adresse** ein.
- Aktivieren Sie unter **Erweitert** das Kontrollkästchen **Gerät blockieren**, damit das Gerät blockiert wird, wenn die SIM-Karte ausgetauscht oder das Gerät ohne SIM eingeschaltet wird. Das Gerät kann durch Eingabe des Geheimcodes entsperrt werden.
- Damit auf dem Display des blockierten Geräts eine Nachricht angezeigt wird, füllen Sie das Feld **Text beim Blockieren** aus. In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Besitzers hinzufügen können.



Abbildung 33: Einstellungen die Funktion SIM-Watch

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

GEOGRAFISCHE KOORDINATEN DES GERÄTS ERMITTELN

Nach Empfang eines speziellen SMS-Befehls kann die Funktion GPS-Find die geografischen Koordinaten des Geräts ermitteln und diese mit einer SMS oder E-Mail an das anfragende Gerät und an eine E-Mail-Adresse schicken.

Für das Senden einer SMS fallen die tarifgemäßen Gebühren an.

Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger. Der GPS-Empfänger wird automatisch aktiviert, nachdem das Gerät einen speziellen SMS-Befehl erhalten hat. Wenn sich das Gerät im Empfangsbereich von Satelliten befindet, empfängt die Funktion GPS-Find die Gerätekoordinaten und leitet sie weiter. Besteht im Augenblick der Anfrage kein Satellitenempfang, dann versucht GPS-Find in regelmäßigen Abständen, das Gerät zu orten und die Suchergebnisse zu übermitteln.

➔ Gehen Sie folgendermaßen vor, um GPS-Find zu aktivieren:

1. Wählen Sie **Menü** → **Diebstahlschutz**.

Das Fenster **Diebstahlschutz** wird geöffnet.

2. Wählen Sie **GPS-Find**.

Das Fenster **GPS-Find** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **GPS-Find aktivieren**.

In der Grundeinstellung sendet Kaspersky Mobile Security 9 die Koordinaten des Geräts mit einer Antwort-SMS.

4. Wenn die Koordinaten des Geräts per E-Mail gesendet werden sollen, geben Sie für die Option **Nachricht an E-Mail-Adresse** die entsprechende E-Mail-Adresse an (s. Abb. unten).



Abbildung 34: Einstellungen der Funktion GPS-Find

5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Wenn GPS-Find aktiviert ist, können die Koordinaten des Geräts auf folgende Weise ermittelt werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Mobile Security 9) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät eine SMS und das Programm sendet die Gerätekoordinaten. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion Befehl senden.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät eine SMS und das Programm sendet die Gerätekoordinaten.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um die Gerätekoordinaten zu erhalten, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall wird der Geheimcode in verschlüsselter Form gesendet.

Um ein Gerät per Fernsteuerung zu orten, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall werden **Befehl** und **Geheimcode** in verschlüsselter Form gesendet.

➔ Gehen Sie folgendermaßen vor, um einen Befehl an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie die Option **SMS-Befehl auswählen** auf **GPS-Find** (s. Abb. unten).
4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.
5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.

Abbildung 35: Gerät orten

6. Klicken Sie auf **Senden**.

➔ Um mit Hilfe der Standardfunktionen eines Telefons eine SMS zu erstellen,

senden Sie an das andere Gerät eine SMS mit dem Text `find:<Code>`, wobei `<Code>` der Geheimcode ist, der auf dem anderen Gerät hinterlegt ist. Groß- und Kleinschreibung von Buchstaben sowie Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

Eine SMS-Nachricht mit den Gerätekoordinaten wird an die Telefonnummer gesendet, von der der SMS-Befehl stammte, sowie an eine E-Mail-Adresse, sofern eine solche in den Einstellungen für GPS-Find hinterlegt wurde.

DIEBSTAHLSCHUTZ-FUNKTIONEN FERNGESTEUERT

STARTEN

Das Programm ermöglicht den Versand eines speziellen SMS-Befehls, um auf einem anderen Gerät, auf dem Kaspersky Mobile Security installiert ist, die Diebstahlschutz-Funktionen ferngesteuert zu starten. Der SMS-Befehl wird in Form einer verschlüsselten SMS gesendet und enthält den Geheimcode für das Programm, das auf dem anderen Geräts installiert ist. Der Empfang des SMS-Befehls bleibt auf dem anderen Gerät unbemerkt.

Für die SMS fallen die tarifgemäßen Gebühren an.

➔ Gehen Sie folgendermaßen vor, um einen Befehl an das andere Gerät zu senden:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Wählen Sie einen der folgenden Werte für **SMS-Befehl auswählen** (s. Abb. unten):

- **SMS-Block.**
- **SMS-Clean.**
- **GPS-Find.**
- **Privatsphäre** (s. Abschnitt "**Verbergen sensibler Daten**" auf S. [94](#)).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

5. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.

KMS 9

Befehl senden

SMS-Befehl auswählen:

Gerät blockieren

SMS-Clean

GPS-Find

Privatsphäre

Telefonnummer:

123456789

Code des Remote-Geräts:

Senden Menü

Abbildung 36: Diebstahlschutz-Funktionen ferngesteuert starten

6. Klicken Sie auf **Senden**.

VERBERGEN SENSIBLER DATEN

Dieser Abschnitt informiert über die Komponente Privatsphäre, mit der vertrauliche Benutzerinformationen verborgen werden können.

IN DIESEM ABSCHNITT

Über die Privatsphäre.....	94
Über die Modi der Privatsphäre.....	94
Privatsphäre aktivieren / deaktivieren	95
Automatische Aktivierung der Privatsphäre.....	96
Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren	97
Liste der vertraulichen Nummern erstellen.....	99
Auswahl der zu verbergenden Informationen: Privatsphäre.....	102

ÜBER DIE PRIVATSPHÄRE

Die Privatsphäre verbirgt vertrauliche Informationen. Dazu dient eine festgelegte Kontaktliste, die vertrauliche Nummern enthält. Für vertrauliche Nummern verbirgt die Privatsphäre Einträge in den Kontakten, Eingehende, Entwürfe, weitergeleitete SMS sowie Einträge der Anrufliste. Die Privatsphäre blockiert das Signal, das über den Empfang einer neuen SMS-Nachricht informiert und verbirgt die SMS im Eingangsordner. Die Privatsphäre blockiert einen von einer vertraulichen Nummer eingehenden Anruf und zeigt auf dem Display keine Informationen über den Anruf an. Der Anrufer hört in diesem Fall das "Besetzt"-Zeichen. Um die Anrufe und SMS-Nachrichten anzuzeigen, die eingegangen sind, während das Verbergen sensibler Daten aktiviert war, deaktivieren Sie diese Funktion. Wenn das Verbergen wieder aktiviert wird, werden die Informationen verborgen.

Sie können die Funktion zum Verbergen sensibler Daten in Kaspersky Mobile Security 9 oder ferngesteuert von einem anderen mobilen Gerät aus aktivieren. Das Deaktivieren der Funktion zum Verbergen sensibler Daten ist nur vom Programm aus möglich.

Informationen über die Arbeit der Privatsphäre werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

ÜBER DIE MODI DER PRIVATSPHÄRE

Sie können den Privatsphären-Modus durch verschiedene Einstellungsmöglichkeiten steuern. Dieser Modus legt fest, ob das Verbergen vertraulicher Informationen aktiviert oder deaktiviert ist.

Standardmäßig ist das Verbergen deaktiviert.

Es sind die folgenden Privatsphären-Modi vorgesehen:

- **Anzeigen** – vertrauliche Informationen werden angezeigt. Die Einstellungen der Privatsphäre können geändert werden.
- **Verbergen** – vertrauliche Informationen werden verborgen. Die Einstellungen der Privatsphäre können nicht geändert werden.

Sie können entweder eine automatische Aktivierung des Verbergens sensibler Daten (s. Abschnitt "Automatische Aktivierung der Privatsphäre" auf S. 96) oder eine ferngesteuerte Aktivierung dieser Funktion von einem anderen Gerät aus einrichten (s. Abschnitt "Funktion zum Verbergen von sensiblen Daten ferngesteuert aktivieren" auf S. 97).

Der aktuelle Status des Verbergens sensibler Daten wird im Fenster **Privatsphäre** neben dem Menüpunkt **Modus** angezeigt.

Es kann eine gewisse Zeit beanspruchen, bis eine Modusänderung der Privatsphäre wirksam wird.

PRIVATSPHÄRE AKTIVIEREN / DEAKTIVIEREN

Der Privatsphären-Modus kann folgendermaßen geändert werden:

- aus dem Menü für die Einstellungen der Komponente
- aus dem Menü für **Privatsphäre**

➔ Gehen Sie folgendermaßen vor, um den Privatsphären-Modus zu ändern:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Privatsphäre** wird geöffnet.

3. Wählen Sie einen Wert für **Privatsphären -Modus**. (s. Abb. unten).

4. Klicken Sie auf **OK**.

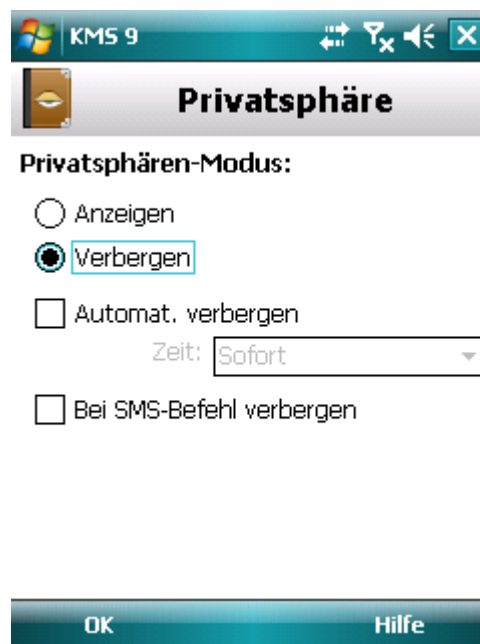


Abbildung 37: Privatsphären-Modus ändern

5. Bestätigen Sie, dass der Privatsphären-Modus geändert werden soll. Klicken Sie dazu auf **Ja**.

➤ *Gehen Sie folgendermaßen vor, um den Privatsphären-Modus schnell zu ändern:*

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Klicken Sie auf **Verbergen / Anzeigen**. Die Beschriftung der Schaltfläche ändert sich abhängig vom aktuellen Modus der Privatsphäre in das jeweilige Gegenteil.
3. Bestätigen Sie, dass der Privatsphären-Modus geändert werden soll. Klicken Sie dazu auf **Ja**.

AUTOMATISCHE AKTIVIERUNG DER PRIVATSPHÄRE

Sie können eine automatische Aktivierung des Verbergens vertraulicher Informationen nach Ablauf einer bestimmten Zeit einrichten. Diese Funktion wird aktiviert, nachdem das Gerät in den Energiesparmodus wechselt.

Deaktivieren Sie die Funktion zum Verbergen von sensiblen Daten, bevor die Einstellungen der Privatsphäre geändert werden sollen.

➤ *Gehen Sie folgendermaßen vor, um festzulegen, dass das Verbergen sensibler Daten nach Ablauf eines bestimmten Zeitraums automatisch aktiviert wird:*

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Privatsphäre** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Automatisch verbergen** (s. Abb. unten).
4. Legen Sie einen Zeitraum fest, nach dem das Verbergen sensibler Daten automatisch aktiviert werden soll. Wählen Sie dazu einen der folgenden Werte für **Zeit**:

- **Sofort**
- **In 1 Minute**
- **In 5 Minuten**
- **In 15 Minuten**

- In 1 Stunde

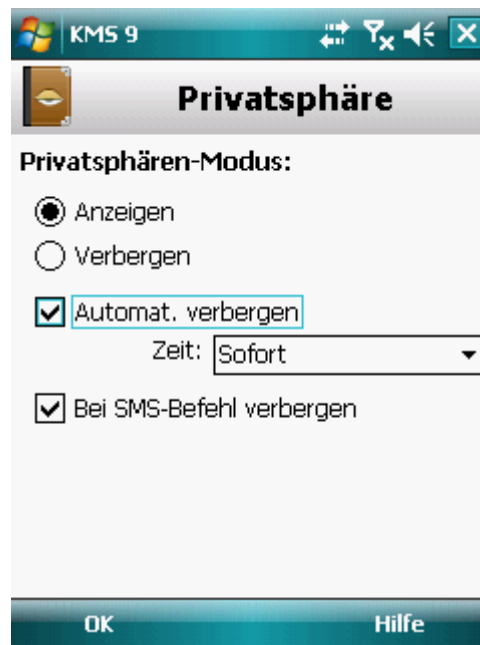


Abbildung 38: Einstellungen für den automatischen Start der Privatsphäre

5. Klicken Sie auf **OK**.

FUNKTION ZUM VERBERGEN VON SENSIBLEN DATEN FERNGESTEUERT AKTIVIEREN

Kaspersky Mobile Security 9 erlaubt es, das Verbergen sensibler Daten ferngesteuert von einem anderen mobilen Gerät aus zu aktivieren. Dazu muss zuvor auf Ihrem Gerät die Funktion "Bei SMS-Befehl verbergen" aktiviert werden.

- *Um eine ferngesteuerte Aktivierung des Verbergens vertraulicher Informationen zu ermöglichen, gehen Sie wie folgt vor:*

1. Gehen Sie auf **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Gehen Sie auf **Modus**.

Das Fenster **Privatsphäre** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Bei SMS-Befehl verbergen** (s. Abb. unten).

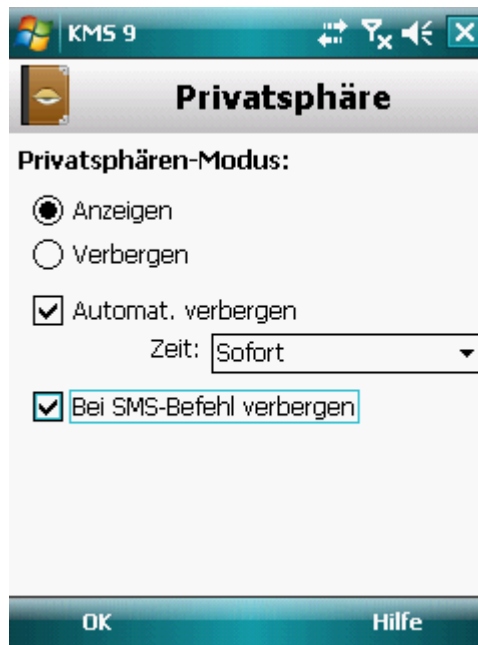


Figure 39: Einstellungen für das ferngesteuerte Aktivieren der Privatsphäre

4. Klicken Sie auf **OK**.

Für die ferngesteuerte Aktivierung des Verbergens vertraulicher Informationen stehen Ihnen folgende Methoden zur Verfügung:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Mobile Security 9) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die vertraulichen Daten werden verborgen. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion **Befehl senden**.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Programms auf Ihrem Gerät, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät eine SMS und die vertraulichen Daten werden verborgen.

Für das Senden einer SMS-Nachricht fallen auf dem Telefon, von dem der SMS-Befehl gesendet wird, die tarifgemäßen Gebühren an.

➔ Um das Verbergen vertraulicher Informationen mit Hilfe eines speziellen SMS-Befehls ferngesteuert zu aktivieren, gehen Sie wie folgt vor:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Befehl senden**.

Das Fenster **Befehl senden** wird geöffnet.

3. Setzen Sie die Option **SMS-Befehl auswählen** auf **Privatsphäre** (s. Abb. unten).

4. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.

- Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode des Geräts ein, an das der SMS-Befehl gerichtet ist.

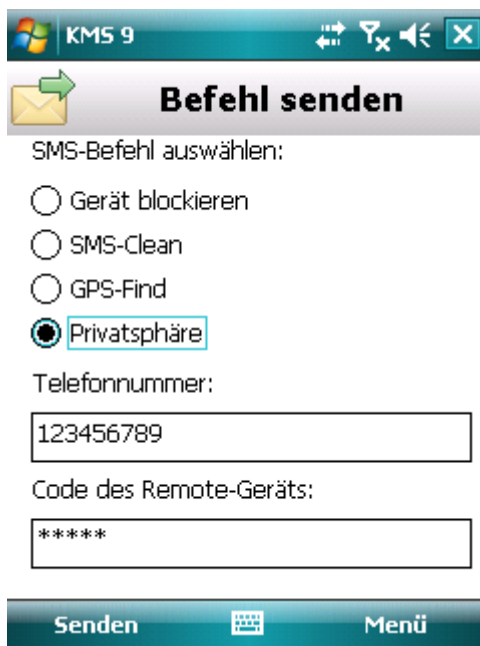


Figure 40: Privatsphäre ferngesteuert starten

- Klicken Sie auf **Senden**.

Wenn das Gerät den SMS-Befehl erhält, wird das Verbergen vertraulicher Informationen automatisch aktiviert.

- Um das Verbergen sensibler Daten mit Hilfe der Standard-SMS-Funktionen des Telefons ferngesteuert zu aktivieren:

schicken Sie an das andere Gerät eine SMS mit dem Text `hide:<Code>`, wobei `<Code>` der Geheimcode für das Programm ist, der auf dem anderen Gerät festgelegt wurde. Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

LISTE DER VERTRAULICHEN NUMMERN ANLEGEN

Die Kontaktliste enthält vertrauliche Nummern, für die die Privatsphäre Informationen verbirgt. Eine neue Nummer kann entweder manuell zur Liste hinzugefügt oder aus den Kontakten oder von der SIM-Karte importiert werden.

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

IN DIESEM ABSCHNITT

Hinzufügen einer Nummer zur Liste der vertraulichen Nummern.....	100
Bearbeiten einer Nummer der Liste der vertraulichen Nummern	101
Löschen einer Nummer aus der Liste der vertraulichen Nummern	101

HINZUFÜGEN EINER NUMMER ZUR LISTE DER VERTRAULICHEN NUMMERN

Sie können der Kontaktliste eine Nummer (z.B. +12345678) manuell hinzufügen, oder sie aus den Kontakten oder von der SIM-Karte importieren.

Deaktivieren Sie die Funktion zum Verbergen von sensiblen Daten, bevor die Einstellungen der Privatsphäre geändert werden sollen.

➔ Gehen Sie folgendermaßen vor, um eine Nummer zur Kontaktliste hinzuzufügen:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Führen Sie im nächsten Fenster eine der folgenden Aktionen aus (s. Abb. unten):

- Um eine Nummer aus den Kontakten hinzuzufügen, wählen Sie **Menü** → **Hinzufügen** → **Outlook-Kontakt**. Wählen Sie im folgenden Fenster **Outlook-Kontakte** den entsprechenden Eintrag und klicken Sie dann auf **Auswählen**.
- Wählen Sie **Menü** → **Hinzufügen** → **Von SIM hinzufügen**, um eine Nummer hinzuzufügen, die auf der SIM-Karte gespeichert ist. Wählen Sie im folgenden Fenster **Kontakt von SIM** den entsprechenden Eintrag und klicken Sie dann auf **OK**.
- Um eine Nummer manuell hinzuzufügen, wählen Sie **Menü** → **Hinzufügen** → **Nummer**. Füllen Sie im folgenden Fenster **Hinzufügen** das Feld **Telefonnummer** aus und klicken Sie auf **OK**.



Abbildung 41: Eintrag zur Liste der geschützten Kontakte hinzufügen

Die Nummer wird zur Kontaktliste hinzugefügt.

BEARBEITEN EINER NUMMER DER LISTE DER VERTRAULICHEN NUMMERN

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

Es können nur Nummern aus der Kontaktliste geändert werden, die manuell hinzugefügt wurden. Nummern, die aus den Kontakten oder aus der SIM-Nummernliste übernommen wurden, können nicht geändert werden.

➤ Gehen Sie folgendermaßen vor, um eine Nummer in der Kontaktliste zu ändern:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Markieren Sie in der Kontaktliste die Nummer, die Sie ändern möchten, und gehen Sie dann auf das **Menü** → **Ändern**.

Das Fenster **Ändern** wird geöffnet.

4. Ändern Sie die Daten im Feld **Telefonnummer**.

5. Klicken Sie nach Abschluss der Änderungen auf **OK**.

Die Nummer wird geändert.

LÖSCHEN EINER NUMMER AUS DER LISTE DER VERTRAULICHEN NUMMERN

Sie können eine Nummer aus der Liste der vertraulichen Kontakte löschen oder die gesamte Kontaktliste leeren.

Deaktivieren Sie das Verbergen von sensiblen Daten, bevor die Kontaktliste erstellt werden soll.

➤ Gehen Sie folgendermaßen vor, um eine Nummer aus der Kontaktliste zu löschen:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Wählen Sie eine Nummer, die gelöscht werden soll, und gehen Sie dann auf **Menü** → **Löschen**.

4. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

➤ Gehen Sie folgendermaßen vor, um die Kontaktliste zu leeren:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Kontaktliste**.

Das Fenster **Kontaktliste** wird geöffnet.

3. Wählen Sie **Menü** → **Alle löschen**.
4. Bestätigen Sie das Löschen. Klicken Sie dazu auf **Ja**.

Die Kontaktliste wird geleert.

AUSWAHL DER ZU VERBERGENDEN INFORMATIONEN: PRIVATSPHÄRE

Die Privatsphäre erlaubt es, für Nummern aus der Kontaktliste die folgenden Informationen zu verbergen: Kontakte, SMS-Korrespondenz, Einträge in den Anruflisten, eingehende SMS und Anrufe. Sie können die Informationen und Ereignisse auswählen, die von der Privatsphäre für vertrauliche Nummern verborgen werden sollen.

Deaktivieren Sie die Funktion zum Verbergen von sensiblen Daten, bevor die Einstellungen der Privatsphäre geändert werden sollen.

➔ Gehen Sie folgendermaßen vor, um die zu verbergenden Informationen und Ereignisse für vertrauliche Nummern auszuwählen:

1. Wählen Sie **Menü** → **Privatsphäre**.

Das Fenster **Privatsphäre** wird geöffnet.

2. Wählen Sie **Verborgene Objekte**.

Es öffnet sich das Fenster **Zu verbergende Objekte** (s. Abb. unten).

3. Wählen Sie im Block **Informationen verbergen** die Informationen aus, die für vertrauliche Nummern verborgen werden sollen. Folgende Einstellungen sind vorgesehen:
 - **Kontakte** – Alle Informationen über vertrauliche Nummern in den Kontakten ausblenden.
 - **SMS** – SMS-Nachrichten in den Ordnern **Eingang**, **Ausgang** und **Weitergeleitet** für vertrauliche Nummern verbergen.
 - **Anrufliste** – Anrufe von vertraulichen Nummern werden angenommen. Die Nummer des Anrufers wird aber nicht ermittelt und in der Anrufliste werden Infos über vertrauliche Nummern (Angenommen, Gewählt, Unbeantwortet) verborgen.
4. Wählen Sie im Block **Ereignisse verbergen** die Ereignisse aus, die für vertrauliche Nummern verborgen werden sollen. Folgende Einstellungen sind vorgesehen:
 - **Eingehende SMS** – Der Empfang eingehender SMS wird verborgen (auf dem Display erscheint kein Signal darüber, dass eine neue SMS von einer vertraulichen Nummer empfangen wurde). Alle SMS, die von vertraulichen Nummern empfangen wurden, können gelesen werden, wenn das Verbergen sensibler Daten deaktiviert wird.

- **Eingehende Anrufe** – Anrufe von vertraulichen Nummern werden blockiert (Der Anrufer hört in diesem Fall ein "Besetzt"-Zeichen). Informationen über eingegangene Anrufe werden angezeigt, wenn das Verbergen sensibler Daten deaktiviert wird.

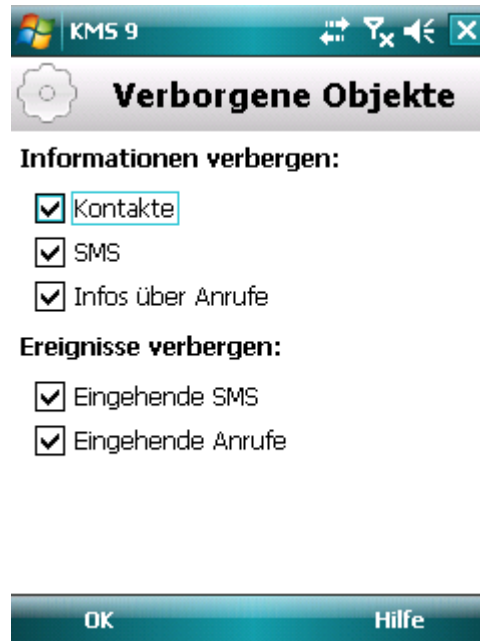


Abbildung 42: Verborgene Objekte wählen

5. Klicken Sie auf **OK**.

NETZWERKAKTIVITÄT FILTERN. FIREWALL

Dieser Abschnitt informiert über die Firewall, die auf Ihrem Gerät die Netzwerkverbindungen überwacht. Außerdem wird hier beschrieben, wie die Firewall aktiviert / deaktiviert wird und wie ein Funktionsmodus ausgewählt wird.

IN DIESEM ABSCHNITT

Firewall.....	104
Firewall aktivieren / deaktivieren	104
Firewall-Modus auswählen.....	105
Meldungen über Blockierung.....	105

FIREWALL

Die Firewall richtet sich bei der Kontrolle von Netzwerkverbindungen auf Ihrem Gerät nach dem ausgewählten Modus. Mit der Firewall lassen sich erlaubte Verbindungen (z.B. für die Synchronisierung mit dem System für die Remote-Administration) und verbotene Verbindungen (z.B. für Suche im Internet, Datei-Download) festlegen.

Die Firewall ist nach der Installation von Kaspersky Mobile Security 9 standardmäßig deaktiviert.

Die Firewall erlaubt es, die Meldungen über blockierte Verbindungen anzupassen (s. Abschnitt "Firewall aktivieren / deaktivieren" auf S. [104](#)).

Informationen über die Arbeit der Firewall werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

FIREWALL AKTIVIEREN / DEAKTIVIEREN

Sie können einen Modus auswählen, nach dem die Firewall erlaubte und verbotene Verbindungen ermittelt. Es sind die folgenden Firewall-Modi vorgesehen:

- **Aus** – jede Netzwerkaktivität erlauben. Diese Sicherheitsstufe gilt als Standard.
- **Minimaler Schutz** – nur eingehende Verbindungen blockieren. Ausgehende Verbindungen werden erlaubt.
- **Maximaler Schutz** – alle eingehenden Verbindungen blockieren. Prüfen eines E-Mail-Postfachs, Anzeige von Webseiten und Download von Dateien sind erlaubt. Ausgehende Verbindungen können nur über die Ports SSH, HTTP, HTTPS, IMAP, SMTP, POP3 erfolgen.
- **Alle blockieren** – jede Netzwerkaktivität außer Update die Anti-Viren-Datenbanken und Lizenzverlängerung blockieren.

Sie können den Modus der Firewall ändern (s. Abschnitt "Firewall-Modus auswählen" auf S. [105](#)). Der aktuelle Modus wird im Fenster **Firewall** neben dem Menüpunkt **Modus** angezeigt.

FIREWALL-MODUS AUSWÄHLEN

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

➤ Gehen Sie folgendermaßen vor, um eine Sicherheitsstufe für die Firewall zu wählen:

1. Wählen Sie **Menü** → **Firewall**.

Das Fenster **Firewall** wird geöffnet.

2. Wählen Sie **Modus**.

Das Fenster **Modus** wird geöffnet.

3. Wählen Sie einen Modus für die Firewall (s. Abb. unten).

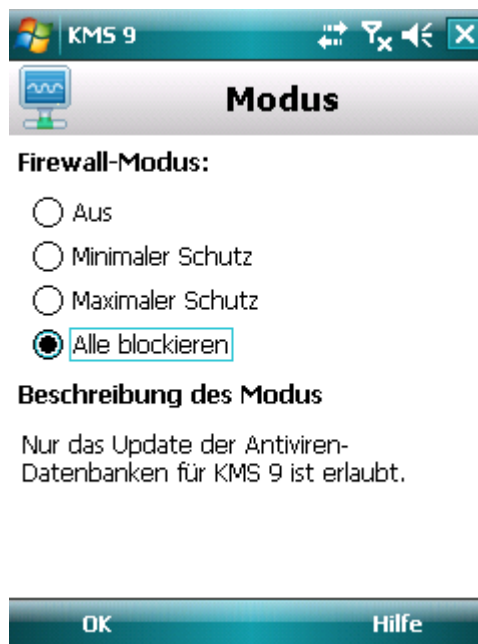


Abbildung 43: Sicherheitsstufe für Firewall wählen

4. Klicken Sie auf **OK**.

MELDUNGEN ÜBER BLOCKIERUNG

Die Firewall erlaubt den Empfang von Meldungen über blockierte Verbindungen. Sie können die Meldungen der Firewall steuern.

In der Grundeinstellung ist das Senden von Meldungen über Blockierungen deaktiviert.

➤ Gehen Sie folgendermaßen vor, um den Versand von Meldungen über Blockierungen zu verwalten:

1. Wählen Sie **Menü** → **Firewall**.

Das Fenster **Firewall** wird geöffnet.

2. Wählen Sie **Benachrichtigungen**.

Das Fenster **Benachrichtigungen** wird geöffnet (s. Abb. unten).

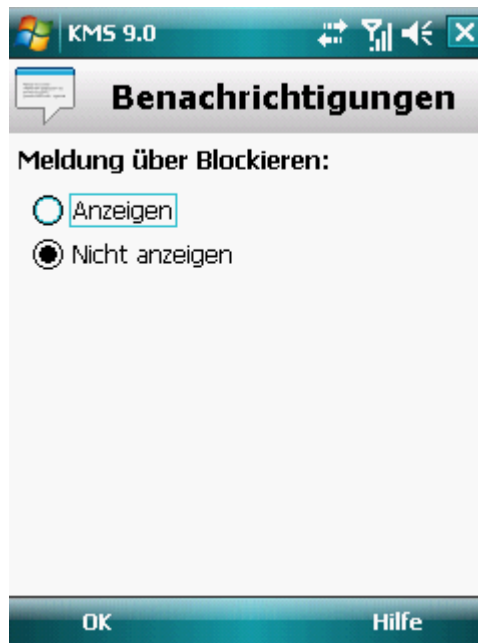


Abbildung 44: Einrichtung des Versandes von Meldungen über Blockierungen

3. Wählen Sie im Block **Meldungen über Blockieren** eine der folgenden Aktionen aus:
 - **Anzeigen** – der Versand von Meldungen wird aktiviert. Die Firewall informiert über blockierte Verbindungen.
 - **Verbergen** – der Versand von Meldungen wird deaktiviert. Die Firewall informiert nicht über blockierte Verbindungen.
4. Klicken Sie auf **OK**.

PERSÖNLICHE DATEN VERSCHLÜSSELN

Dieser Abschnitt informiert über die Komponente Verschlüsselung, mit der die Ordner auf dem Gerät verschlüsselt werden können. Außerdem wird hier beschrieben, wie ausgewählte Ordner verschlüsselt und entschlüsselt werden können.

IN DIESEM ABSCHNITT

Verschlüsselung	107
Daten verschlüsseln	107
Daten entschlüsseln	109
Zugriff auf verschlüsselte Daten verbieten	110

VERSCHLÜSSELUNG

Die Funktion Verschlüsselung chiffriert die Informationen, die sich in den von Ihnen ausgewählten Ordnern befinden. Die Verschlüsselungsfunktion basiert auf einer analogen Funktion, die in das Betriebssystem Ihres Geräts integriert ist. Die Chiffrierfunktion erlaubt es, Ordner eines beliebigen Typs zu verschlüsseln. Eine Ausnahme bilden Systemdateien. Zur Verschlüsselung können Sie Ordner auswählen, die sich im Gerätespeicher oder auf einer Speicherkarte befinden. Um auf verschlüsselte Informationen zuzugreifen, muss der Geheimcode des Programms eingegeben werden, der beim ersten Start des Programms festgelegt wurde.

Um ausführbare exe-Dateien aus einem verschlüsselten Ordner zu starten, müssen diese vorher entschlüsselt werden. Dazu muss der Geheimcode des Programms eingegeben werden.

Um mit verschlüsselten Ordnern zu arbeiten, geben Sie den Geheimcode für das Programm ein (s. Abschnitt "Geheimcode festlegen" auf S. [31](#)). Wenn das Gerät in den Stromsparmmodus gewechselt hat und die festgelegte Zeitspanne abgelaufen ist (s. Abschnitt "Zugriff auf verschlüsselte Daten verbieten" auf S. [110](#)), wird der Datenzugriff automatisch blockiert.

Die Dateien in einem Ordner werden durch den Befehl **Verschlüsseln** chiffriert. Künftig werden die Daten automatisch ver- und entschlüsselt, wenn Dateien in dem Ordner gespeichert oder daraus gelesen werden oder wenn auf die Dateien zugegriffen wird.

Um ausführbare exe-Dateien aus einem verschlüsselten Ordner zu starten, müssen diese vorher entschlüsselt werden.

Die Komponente Verschlüsselung ist nach der Installation von Kaspersky Mobile Security 9 deaktiviert.

Informationen über die Arbeit der Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

DATEN VERSCHLÜSSELN

Die Verschlüsselung erlaubt es, eine beliebige Anzahl von Ordnern, die nicht zum System gehören, zu verschlüsseln. Die Ordner können sich im Gerätespeicher oder auf einer Speicherkarte befinden.

Eine Liste aller bisher verschlüsselten und entschlüsselten Ordner befindet sich im Fenster **Verschlüsselung** unter dem Menüpunkt **Ordnerliste**.

Außerdem können Sie einen einzelnen Ordner oder alle Ordner, die in der Ordnerliste stehen, verschlüsseln.

➤ *Gehen Sie folgendermaßen vor, um Daten zu verschlüsseln:*

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Wählen Sie **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet.

3. Klicken Sie auf **Menü** → **Hinzufügen**.

Ein Fenster mit einer Übersicht des Dateisystems Ihres Geräts wird geöffnet.

4. Wählen Sie den Ordner, der verschlüsselt werden soll, und klicken Sie dann auf **Verschlüsseln** (s. Abb. unten).

Verwenden Sie zur Navigation im Dateisystem den Stylus oder die Joystick-Tasten des Geräts.

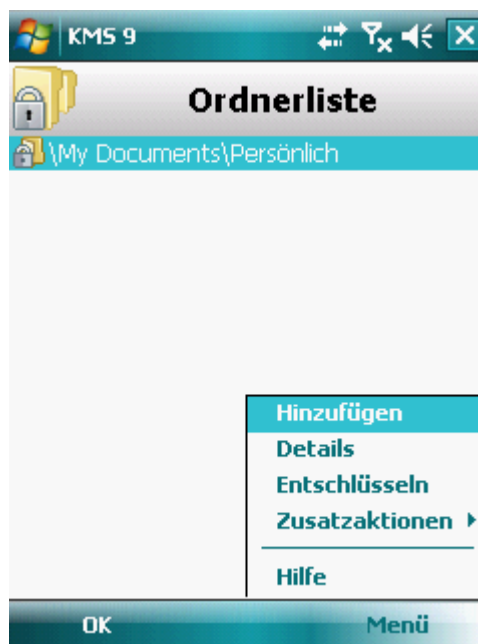


Abbildung 45: Daten verschlüsseln

Sie werden von Kaspersky Mobile Security 9 benachrichtigt, wenn der Verschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

5. Klicken Sie auf **OK**.

Für einen verschlüsselten Ordner ändert sich im **Menü** der Punkt **Verschlüsseln** in **Entschlüsseln**.

Nach der Verschlüsselung werden Daten automatisch ent- und verschlüsselt, wenn Sie mit den Daten in einem verschlüsselten Ordner arbeiten, Daten aus einem verschlüsselten Ordner entnehmen oder neue Daten darin speichern.

➤ *Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu verschlüsseln:*

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Wählen Sie **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet.

3. Wählen Sie **Menü** → **Zusatzaktionen** → **Alle verschlüsseln**.

Sie werden von Kaspersky Mobile Security 9 benachrichtigt, wenn der Verschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

DATEN ENTSCHLÜSSELN

Sie können zuvor verschlüsselte Daten vollständig entschlüsseln (s. Abschnitt "Datenverschlüsselung" auf S. [107](#)). Sie können einen oder alle Ordner entschlüsseln, die auf dem Gerät chiffriert wurden.

➔ *Gehen Sie folgendermaßen vor, um einen zuvor verschlüsselten Ordner zu entschlüsseln:*

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Wählen Sie **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet. Es enthält eine Liste aller bisher ver- und entschlüsselten Ordner.

3. Wählen Sie aus der Liste einen verschlüsselten Ordner aus und gehen Sie auf **Menü** → **Entschlüsseln** (s. Abb. unten).



Abbildung 46: Funktion aktivieren

Sie werden von Kaspersky Mobile Security 9 benachrichtigt, wenn der Entschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

Für einen verschlüsselten Ordner ändert sich im **Menü** der Punkt **Entschlüsseln** in **Verschlüsseln**. Sie können die Datenverschlüsselung erneut verwenden (s. Abschnitt "Daten verschlüsseln" auf S. [107](#)).

➤ Gehen Sie folgendermaßen vor, um alle Ordner der Liste auf einmal zu entschlüsseln:

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Wählen Sie **Ordnerliste**.

Das Fenster **Ordnerliste** wird geöffnet.

3. Wählen Sie **Menü** → **Zusatzaktionen** → **Alle entschlüsseln**.

Sie werden von Kaspersky Mobile Security 9 benachrichtigt, wenn der Entschlüsselungsvorgang abgeschlossen wurde. Es erscheint ein Meldungsfenster.

4. Klicken Sie auf **OK**.

ZUGRIFF AUF VERSCHLÜSSELTE DATEN VERBIETEN

Die Verschlüsselung erlaubt es, eine Zeitspanne festzulegen, nach deren Ablauf das Zugriffsverbot für verschlüsselte Ordner automatisch aktiviert werden soll. Diese Funktion wird aktiviert, nachdem das Gerät in den Energiesparmodus wechselt. Um mit verschlüsselten Informationen zu arbeiten, muss der Geheimcode des Programms eingegeben werden. Um danach mit verschlüsselten Daten zu arbeiten, muss der Geheimcode eingegeben werden (s. Abschnitt "Geheimcode festlegen" auf S. [31](#)).

Außerdem können Sie den Zugriff auf verschlüsselte Daten sofort verbieten und die Abfrage des Geheimcodes aktivieren.

➤ Gehen Sie folgendermaßen vor, um den Zugriff auf einen Zugriff zeitverzögert zu verbieten:

1. Wählen Sie **Menü** → **Verschlüsselung**.

Das Fenster **Verschlüsselung** wird geöffnet.

2. Wählen Sie **Zugriff verbieten**.

Das Fenster **Zugriff verbieten** wird geöffnet.

3. Legen Sie fest, wie lange die Daten noch verfügbar sein sollen, nachdem das Gerät in den Stromsparmodus gewechselt hat. Wählen Sie dazu für **Zugriff verweigern** einen der folgenden Werte (s. Abb. unten):

- **Sofort**
- **In 1 Minute**
- **In 5 Minuten**
- **In 15 Minuten**

- In 1 Stunde

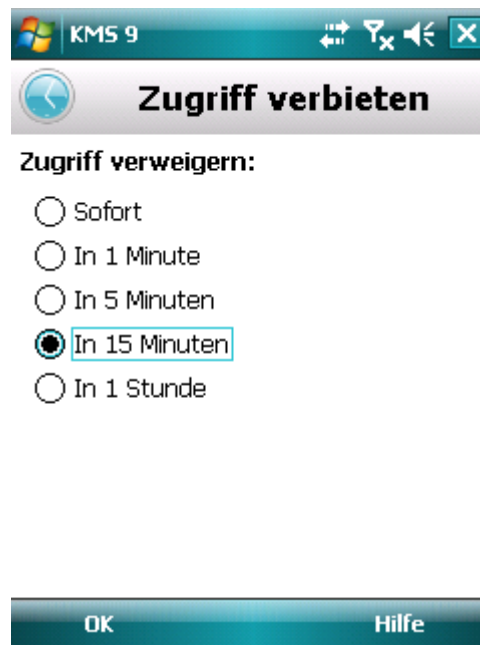


Abbildung 47: Zugriff auf verschlüsselte Daten blockieren

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

- ➔ Um den Zugriff auf einen Ordner sofort zu blockieren,

klicken Sie in der Taskleiste des Geräts auf das Symbol von Kaspersky Mobile Security 9.0 und wählen Sie den Punkt **Daten blockieren** (s. Abb. unten).



Abbildung 48: Kontextmenü des Programms in der Taskleiste des Geräts

UPDATE DER PROGRAMM-DATENBANKEN

Dieser Abschnitt informiert über das Update der Anti-Viren-Datenbanken des Programms. Das Update hält den Schutz Ihres Geräts auf dem neusten Stand. Außerdem werden hier folgende Vorgänge beschrieben: Informationen über die installierten Anti-Viren-Datenbanken des Programms anzeigen, Updatevorgang manuell starten, automatisches Datenbank-Update nach Zeitplan anpassen.

IN DIESEM ABSCHNITT

Über das Update der Programm-Datenbanken.....	112
Datenbankinfos anzeigen.....	113
Manuelles Update	113
Update nach Zeitplan	114
Update im Roaming	115

ÜBER DAS UPDATE DER PROGRAMM-DATENBANKEN

Die Suche erfolgt auf Basis von Anti-Viren-Datenbanken des Programms, die eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden sowie eine Beschreibung sonstiger unerwünschter Objekte enthalten. Es ist sehr wichtig, die Anti-Viren-Datenbanken des Programms auf dem neuesten Stand zu halten.

Es wird empfohlen, die Anti-Viren-Datenbanken des Programms regelmäßig zu aktualisieren. Die Anti-Viren-Datenbanken des Programms gelten als veraltet, wenn seit dem letzten Update mehr als 15 Tage vergangen sind. In diesem Fall sinkt das Schutzniveau.

Kaspersky Mobile Security 9 lädt die Updates der Anti-Viren-Datenbanken des Programms von Kaspersky-Lab-Updateservern herunter. Dabei handelt es sich um spezielle Internetseiten, auf welchen Updates der Datenbanken für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Um die Anti-Viren-Datenbanken des Programms zu aktualisieren, muss auf dem mobilen Gerät eine Internetverbindung eingerichtet sein.

Die Aktualisierung der Anti-Viren-Datenbanken des Programms wird nach folgendem Algorithmus ausgeführt:

1. Die Anti-Viren-Datenbanken des Programms auf Ihrem mobilen Gerät werden mit den Datenbanken verglichen, die sich auf dem Kaspersky-Lab-Updateserver befinden.
2. Kaspersky Mobile Security 9 führt eine der folgenden Aktionen aus:
 - Wenn Ihre Anti-Viren-Datenbanken des Programms aktuell sind, wird eine entsprechende Meldung angezeigt.
 - Wenn sich die installierten Anti-Viren-Datenbanken von den angebotenen unterscheiden, wird ein neues Updatepaket heruntergeladen und installiert.

Die Verbindung wird nach Abschluss des Updatevorgangs automatisch getrennt. Eine Verbindung, die bereits vor dem Update aufgebaut wurde, bleibt bestehen.

Sie können die Updateaufgabe entweder manuell starten, wenn das Gerät nicht für andere Aufgaben benötigt wird, oder einen Zeitplan für das automatische Update einstellen.

Ausführliche Informationen über die verwendeten Anti-Viren-Datenbanken stehen im Fenster **Erweitert** unter dem Menüpunkt **Datenbankinfos** zur Verfügung.

Informationen über das Update der Anti-Viren-Datenbanken werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [117](#)).

DATENBANKINFOS ANZEIGEN

Sie können folgende Informationen über die installierten Anti-Viren-Datenbanken des Programms anzeigen: Datum des letzten Updates, Erscheinungsdatum der Datenbanken, Größe der Datenbanken und Anzahl der Einträge in den Datenbanken.

➤ *Gehen Sie folgendermaßen vor, um Informationen über die installierten Datenbanken anzuzeigen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Datenbankinfos**.

Das folgende Fenster **Datenbankinfos** informiert über die installierten Anti-Viren-Datenbanken des Programms

MANUELLES UPDATE

Sie können das Update der Anti-Viren-Datenbanken manuell starten.

➤ *Gehen Sie folgendermaßen vor, um das Update der Programm-Datenbanken zu starten:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Update**.

Das Fenster **Update** wird geöffnet.

3. Wählen Sie **Update starten** (s. Abb. unten):

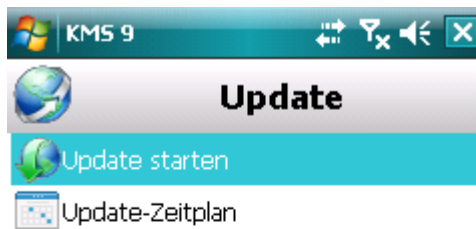


Abbildung 49: Update manuell starten

Das Programm startet das Update die Anti-Viren-Datenbanken des Programms von einem Kaspersky-Lab-Server. Informationen über den Updatevorgang werden auf dem Bildschirm angezeigt.

UPDATE NACH ZEITPLAN

Eine wichtige Voraussetzung für die Sicherheit des Geräts besteht darin, den Schutz auf dem neusten Stand zu halten. Sie können das automatische Update der Anti-Viren-Datenbanken festlegen.

- *Gehen Sie folgendermaßen vor, um einen Zeitplan einzurichten, nach dem die Anti-Viren-Datenbanken automatisch aktualisiert werden:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Update**.

Das Fenster **Update** wird geöffnet.

3. Wählen Sie den Punkt **Update-Zeitplan**.

Das Fenster **Zeitplan** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Update nach Zeitplan** (s. Abb. unten).

5. Erstellen Sie einen Zeitplan für das Update. Wählen Sie dazu einen Wert für die Option **Frequenz**:

- **Täglich:** Die Anti-Viren-Datenbanken des Programms werden jeden Tag aktualisiert. Legen Sie dann einen Wert für **Zeit** fest.

- **Wöchentlich:** Die Anti-Viren-Datenbanken des Programms werden ein Mal in der Woche aktualisiert. Legen Sie dann Werte für **Zeit** und **Wochentag** fest.

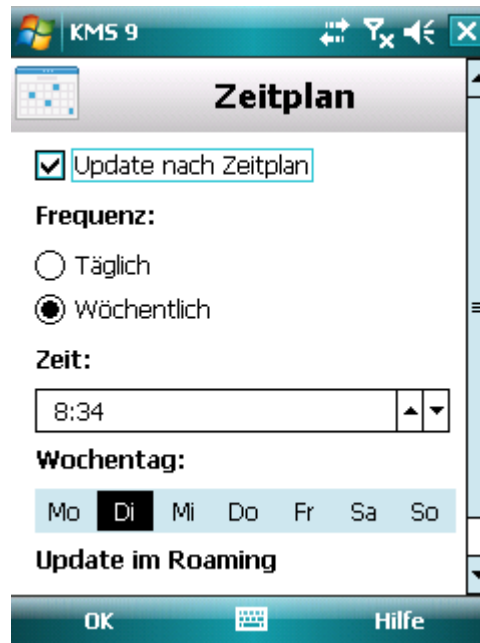


Abbildung 50: Einstellungen für automatisches Update

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

UPDATE IM ROAMING

Sie können festlegen, dass das geplante Update der Anti-Viren-Datenbanken des Programms im Roaming erlaubt / verboten wird. Falls im Roaming ein geplantes Update verboten wird, ist eine manuelle Aktualisierung im gewöhnlichen Modus möglich.

- *Gehen Sie folgendermaßen vor, um das geplante Update der Anti-Viren-Datenbanken des Programms im Roaming zu erlauben:*

1. Wählen Sie **Menü** → **Anti-Virus**.

Das Fenster **Anti-Virus** wird geöffnet.

2. Wählen Sie **Update**.

Das Fenster **Update** wird geöffnet.

3. Wählen Sie den Punkt **Update-Zeitplan**.

Das Fenster **Zeitplan** wird geöffnet.

- Aktivieren Sie im Block **Update im Roaming** das Kontrollkästchen **Update im Roaming**.

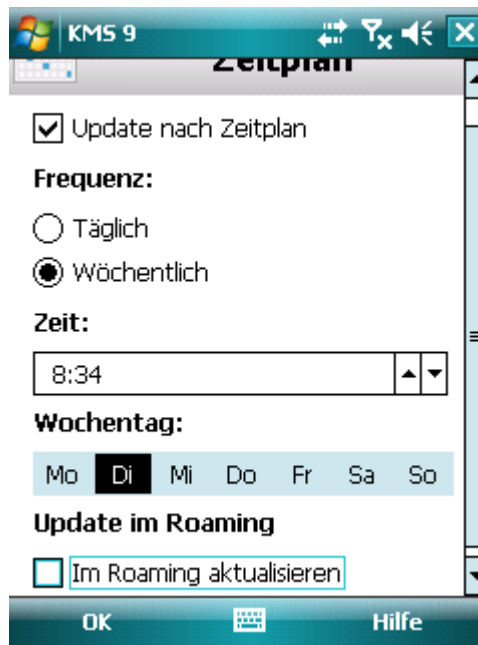


Abbildung 51: Update im Roaming anpassen

- Klicken Sie auf **OK**, um die Änderungen zu speichern.

PROGRAMMBERICHTE

Dieser Abschnitt informiert über die Berichte, in welchen die Arbeit der einzelnen Komponenten und die Ausführung aller Aufgaben (z.B. Update der Anti-Viren-Datenbanken des Programms, Virensuche) protokolliert werden.

IN DIESEM ABSCHNITT

Berichte.....	117
Berichtseinträge anzeigen.....	117
Einträge aus Bericht löschen.....	118

BERICHTE

In Berichten werden Ereignisse gespeichert, die bei der Arbeit der einzelnen Komponenten von Kaspersky Mobile Security 9 auftreten. Die Einträge sind in absteigender Reihenfolge nach dem Zeitpunkt der Ereignisse angeordnet.

Für jede Komponente wird ein eigener Ereignisbericht geführt.

BERICHTSEINTRÄGE ANZEIGEN

➤ *Gehen Sie folgendermaßen vor, um alle Einträge anzuzeigen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Berichte**.

Das Fenster **Berichte** wird geöffnet.

3. Wählen Sie die Komponente, für die ein Ereignisbericht angezeigt werden soll.

Der Ereignisbericht der gewählten Komponente wird geöffnet.

➤ *Um ausführliche Informationen über einen Berichtseintrag anzuzeigen,*

wählen Sie einen Eintrag und klicken Sie auf **Details**.

Im Fenster **Details** werden die Informationen zu der vom Programm ausgeführten Aktion detailliert angezeigt. So wird für die Aktion "Objekt in Quarantäne verschoben" zum Beispiel auch angezeigt, unter welchem Pfad die infizierte Datei auf dem Gerät gefunden wurde.

➤ *Um zur Berichtsliste zurückzukehren,*

klicken Sie auf **Menü** → **Zurück**.

EINTRÄGE AUS BERICHT LÖSCHEN

Sie können alle Berichte leeren. Die Informationen über die Arbeit aller Komponenten von Kaspersky Mobile Security 9 werden gelöscht.

➤ Gehen Sie folgendermaßen vor, um alle Berichte zu leeren:

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie den Punkt **Berichte**.

Das Fenster **Bericht** wird geöffnet.

3. Öffnen Sie den Bericht einer beliebigen Komponente.

4. Gehen Sie auf **Menü** → **Alle löschen** (s. Abb. unten).



Abbildung 52: Einträge löschen

5. Bestätigen Sie die Deinstallation mit **Ja**.

Es werden alle Einträge im Bericht aller Komponenten gelöscht.

ERWEITERTE EINSTELLUNGEN ANPASSEN

Dieser Abschnitt informiert über zusätzliche Optionen von Kaspersky Mobile Security 9: Geheimcode ändern, Audiosignale des Programms verwalten, Anzeige von Tooltips aktivieren / deaktivieren.

IN DIESEM ABSCHNITT

Geheimcode ändern.....	119
Tooltips anzeigen	119
Audiosignale verwalten	120

GEHEIMCODE ÄNDERN

Der Geheimcode für das Programm, der nach der Programmaktivierung festgelegt wurde, kann geändert werden.

➤ *Gehen Sie folgendermaßen vor, um den Geheimcode zu ändern:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Einstellungen**.

Das Fenster **Einstellungen** wird geöffnet.

3. Wählen Sie den Punkt **Code eingeben**.

4. Geben Sie den aktuellen Code im Feld **Geheimcode eingeben** ein.

5. Geben Sie in den Feldern **Code installieren** und **Code bestätigen** einen neuen Code ein und klicken Sie auf **OK**, um die Änderungen zu speichern.

TOOLTIPS ANZEIGEN

Während Sie die Einstellungen der Komponenten anpassen, zeigt Kaspersky Mobile Security 9 standardmäßig kurze Tooltips für die jeweilige Funktion an. Die Anzeige von Tooltips für Kaspersky Mobile Security 9 lässt sich anpassen.

➤ *Gehen Sie folgendermaßen vor, um die Anzeige von Tooltips anzupassen:*

1. Wählen Sie **Menü** → **Erweitert**.

Das Fenster **Erweitert** wird geöffnet.

2. Wählen Sie **Einstellungen**.

Das Fenster **Einstellungen** wird geöffnet.

3. Wählen Sie **Tooltips**.

Das Fenster **Tooltips** wird geöffnet.

4. Wählen Sie einen Wert für **Tooltips**:
 - **Anzeigen** – Tooltips anzeigen, bevor eine Funktion angepasst wird.
 - **Verbergen** – keine Tooltips anzeigen.
5. Klicken Sie auf **OK**.

AUDIOSIGNALE VERWALTEN

Bei der Arbeit des Programms treten unterschiedliche Ereignisse auf. Dazu zählen beispielsweise der Fund eines infizierten Objekts oder eines Virus, der Ablauf der Lizenz usw. Damit das Programm Sie über solche Ereignisse informiert, können Sie entsprechende Audiosignale aktivieren.

In der Grundeinstellung aktiviert Kaspersky Mobile Security 9 die Audiosignale nur entsprechend dem für das Gerät festgelegten Modus.

Verwenden Sie die Joystick-Tasten des Geräts, um die Einstellungswerte zu ändern.

➡ *Gehen Sie folgendermaßen vor, um die Audiosignale des Programms zu verwalten:*

1. Wählen Sie **Menü** → **Erweitert**.
Das Fenster **Erweitert** wird geöffnet.
2. Wählen Sie **Einstellungen**.
Das Fenster **Einstellungen** wird geöffnet.
3. Wählen Sie **Ton**.
Das Fenster **Ton** wird geöffnet.
4. Wählen Sie einen Wert für **Audiosignale** (s. Abb. unten):
 - **Aktivieren** – unabhängig vom Geräteprofil immer Audiosignale verwenden.
 - **Deaktivieren** – keine Audiosignale verwenden.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie Kaspersky Mobile Security bereits erworben haben, werden Sie per Telefon oder über das Internet von den Spezialisten des technischen Supports unterstützt.

Die Support-Spezialisten beantworten Ihre Fragen zur Installation und Verwendung des Programms und helfen Ihnen dabei, die Folgen von Virenangriffen zu beheben, wenn Ihr Computer infiziert wurde.

Bitte lesen Sie die Supportrichtlinien (<http://support.kaspersky.de/support/rules>), bevor Sie sich an den Technischen Support wenden.

E-Mail-Anfrage an den Technischen Support

Zur Kontaktaufnahme mit dem Technischen Support dient ein Kontaktformular.

Anfragen können in deutscher oder, englischer Sprache gestellt werden.

Um eine E-Mail-Anfrage zu stellen, ist die Angabe der **Kundennummer**, die Sie bei der Anmeldung auf der Support-Webseite erhalten haben, und des **Keywords** erforderlich.

Beschreiben Sie das aufgetretene Problem im Webformular möglichst genau. Machen Sie in den Pflichtfeldern folgende Angaben:

- **Problemart.** Wählen Sie das Thema, zu dem Ihr Problem gehört (z.B. "Problem bei der Installation/Deinstallation des Produkts" oder "Problem bei der Suche/Desinfektion von Viren". Wenn keine der Kategorien zutrifft, wählen Sie "Allgemeine Frage".
- **Name und Versionsnummer des Programms.**
- **Anfragetext.** Beschreiben Sie das Problem möglichst genau.
- **E-Mail-Adresse.** An diese Adresse werden die Support-Spezialisten Ihre Anfrage beantworten.

Technischer Support am Telefon

Bei dringenden Problemen können Sie Ihren lokalen technischen Support anrufen. Wenn Sie sich an den deutschsprachigen (http://www.kaspersky.de/technischer_support) oder internationalen (<http://support.kaspersky.ru/support/international>) Support wenden, halten Sie bitte die Informationen (<http://support.kaspersky.com/de/support/details>) über Ihr Gerät und das installierte Anti-Viren-Programm bereit. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

GLOSSAR

A

ANTI-VIREN-DATENBANKEN

Die Datenbanken werden von den Kaspersky-Lab-Spezialisten erstellt und enthalten eine detaillierte Beschreibung aller im Moment bekannten Bedrohungen für die Computersicherheit und der dafür notwendigen Erkennungs- und Desinfektionsmethoden. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen.

ARCHIV

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

D

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die beiden wichtigsten Zeichen in Dateimasken sind * und ? (wobei * für eine beliebige Anzahl von beliebigen Zeichen steht und ? für ein beliebiges Einzelzeichen). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Anti-Viren-Datenbanken von den Kaspersky-Lab-Updateservern auf das Gerät kopiert und automatisch von der Anwendung übernommen.

DESINFEKTION VON OBJEKTEN

Verarbeitungsmethode für infizierte Objekte, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder sich ergibt, dass eine Desinfektion unmöglich ist. Objekte werden auf Basis von Datenbank-Einträgen desinfiziert. Beim Desinfektionsvorgang können Daten teilweise verloren gehen.

G

GEHEIMCODE FÜR DAS PROGRAMM

Der Geheimcode des Programms verhindert einen unautorisierten Zugriff auf die Programmeinstellungen und auf die geschützten Informationen auf dem Gerät. Er wird beim ersten Start des Programms vom Benutzer festgelegt und besteht aus mindestens vier Ziffern. Der Geheimcode des Programms wird in folgenden Fällen abgefragt:

Für den Zugriff auf die Programmeinstellungen,

Für den Zugriff auf verschlüsselte Ordner,

Wenn von einem anderen mobilen Gerät aus ein SMS-Befehl gesendet wird, um folgende Funktionen ferngesteuert zu starten: SMS-Block, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.

Bei der Deinstallation des Programms

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, alle Funktionen des Kaspersky-Lab-Programms zu nutzen. Bei Ablauf der Lizenz wechselt das Programm in den eingeschränkten Funktionsmodus. In diesem Modus sind im Programm folgende Aktionen verfügbar:

Deaktivierung aller Komponenten;

Entschlüsselung eines oder mehrerer Ordner

Deaktivierung des Verbergens von sensiblen Daten

Deaktivierung des automatischen Verbergens von sensiblen Daten

Anzeige des Hilfesystems für das Programm

I

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Geräts führen kann.

L

LÖSCHEN VON SMS

Verarbeitungsmethode für SMS, die Spam-Merkmale aufweisen. Dabei wird die Nachricht physikalisch gelöscht. Diese Methode wird für SMS empfohlen, die eindeutig als Spam gelten.

N

NICHT-ZIFFERN-NUMMERN

Eine Nicht-Ziffern-Nummer (auch Buchstabenwahl-, Wortwahlrufnummer oder Vanity-Rufnummer) ist eine Telefonnummer, die teilweise oder vollständig aus Buchstaben besteht.

O

OBJEKT BLOCKIEREN

Der Zugriff auf ein Objekt wird für externe Programme verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Verarbeitungsmethode für ein Objekt, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde. Diese Verarbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion nicht möglich ist.

OBJEKT WIEDERHERSTELLEN

Ein Originalobjekt wird aus der Quarantäne entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

P

PROGRAMM AKTIVIEREN

Freischaltung aller Programmfunktionen. Zur Aktivierung des Programms ist eine installiert Lizenz erforderlich.

Q**QUARANTÄNE**

Die Quarantäne ist ein besonderer Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die während der Untersuchung des Geräts oder im Laufe des Schutzes erkannt werden.

QUARANTÄNE (OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN)

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Ort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

S**SCAN AUF BEFEHL**

Funktionsmodus von Kaspersky-Lab-Programmen, der vom Benutzer initiiert wird und der Untersuchung bestimmter Dateien dient.

SCHWARZE LISTE

Die Einträge dieser Liste enthalten folgende Informationen:

Telefonnummer, von der der Anruf- und SMS-Filter Anrufe und / oder SMS blockieren soll.

Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer blockieren soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.

Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter zugestellt.

W**WEIßE LISTE**

Die Einträge dieser Liste enthalten folgende Informationen:

Telefonnummer, von der der Anruf- und SMS-Filter Anrufe und / oder SMS zustellen soll.

Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer zustellen soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.

Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter blockiert.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Das Unternehmen ist heute der bekannteste Hersteller für Datenschutz-Software in Russland und bietet eine breite Palette von Programmen zum Schutz vor Viren, Spam und Hackerangriffen an.

Kaspersky Lab ist ein international tätiger Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, den Benelux-Ländern, China, Polen, Rumänien und den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Dokortitel besitzen. Die führenden Viren-Analytiker von Kaspersky Lab gehören zu der anerkannten Computer Anti-Virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind einzigartiges Wissen und Erfahrung, die von den Mitarbeitern im Laufe des über vierzehnjährigen permanenten Kampfes gegen Viren gesammelt wurden. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen in der Malware-Entwicklung vorhersagen und unseren Anwendern frühzeitig einen zuverlässigen Schutz vor neuen Angriffen bieten. Dieser Vorsprung bildet die Basis der Produkte und Services von Kaspersky Lab. Wir sind unseren Konkurrenten stets einen Schritt voraus und bieten unseren Kunden den Schutz von höchster Qualität.

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Kaspersky Lab ist ein wichtiger Wegbereiter für neue Standards von Anti-Viren-Programmen. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Intuitiv bedienbare Verwaltungstools ermöglichen es, den Antivirenschutz von Computern und Firmennetzwerken maximal zu automatisieren. Viele internationale Developer verwenden in ihrer Software den Kernel von Kaspersky Anti-Virus. Zu ihnen zählen Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien) und BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die eine störungsfreie Funktion der Produkte und präzise Kompatibilität mit spezifischen Business-Vorgaben garantieren. Wir planen, realisieren und begleiten komplexe Antiviren-Lösungen für Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Für unsere Benutzer haben wir einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gerne am Telefon oder per E-Mail. Alle Ihre Fragen werden ausführlich beantwortet.

Webseite von Kaspersky Lab: <http://www.kaspersky.de>

Viren-Enzyklopädie: <http://www.securelist.com/de/>

Antiviren-Labor: newvirus@kaspersky.com
(nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)

Webforum von Kaspersky Lab: <http://forum.kaspersky.com>

INFORMATIONEN ZUM PROGRAMMCODE VON DRITHTHERSTELLERN

Bei der Entwicklung des Programms wurde der Code von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

Verteilbarer Programmcode	126
Zusatzinformationen.....	128

VERTEILBARER PROGRAMMCODE

Mit diesem Programm wird unabhängiger Code von Drittanbietern unverändert als Quellcode oder in Binärform verteilt.

IN DIESEM ABSCHNITT

ADB.....	126
ADBWINAPI.DLL	126
ADBWINUSBAPI.DLL	126

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

ZUSATZINFORMATIONEN

Informationen zum Programmcode von Drittherstellern.

Für das Erstellen und die Überprüfung elektronischer digitaler Signaturen wird die Programmbibliothek für den Informationsschutz (PBSI) "Crypto-C" verwendet, die von CryptoEx OOO entwickelt wurde.

Webseite von CryptoEx OOO: <http://www.cryptoex.ru>

SACHREGISTER

A

Aktionen	
Virensuche.....	56
Aktionen für Objekte.....	49, 56
Aktivieren	
Anruf- und SMS-Filter.....	62
Firewall.....	104, 105
Kindersicherung.....	74, 75
Privatsphäre.....	95
Verschlüsselung.....	107

Ä

Ändern	
Liste der vertraulichen Kontakte für die Privatsphäre.....	101
Schwarze Liste der Kindersicherung.....	77
Schwarze Liste des Anruf- und SMS-Filters.....	64
Weiße Liste der Kindersicherung.....	80
Weiße Liste des Anruf- und SMS-Filters.....	67

A

Anruf- und SMS-Filter.....	61
Aktion für Anruf.....	72
Aktion für SMS.....	71
Modi.....	62
Nicht-Ziffern-Nummern.....	70
Nummer, die nicht in den Kontakten steht.....	69
Schwarze Liste.....	63
Weiße Liste.....	66
Archive	
Virensuche.....	54, 55

B

Bildschirm	
Fenster für den Schutzstatus.....	43

C

Code	
Aktivierungscode.....	27, 28, 30
Geheimcode für das Programm.....	31

D

Daten	
Entschlüsselung.....	109
Verschlüsselung.....	107
Zugriff mit Geheimcode.....	110
DATEN	
VERTRAULICHE INFORMATIONEN.....	94
Deaktivieren	
Kindersicherung.....	74, 75
Privatsphäre.....	94, 95
Verschlüsselung.....	109
Diebstahlschutz.....	82
GPS-Find.....	89
SIM-Watch.....	88
SMS-Block.....	83

SMS-Clean	85
E	
Eintrag	
Schwarze Liste des Anruf- und SMS-Filters	63
Weiße Liste der Kindersicherung.....	79
Weiße Liste des Anruf- und SMS-Filters	66
Ereignisbericht	117
Ereignisberichte	
Einträge anzeigen.....	117
Einträge löschen.....	118
Erlauben	
ausgehende Anrufe	78
ausgehende SMS-Nachrichten.....	78
eingehende Anrufe	66
eingehende SMS	66
Netzwerkverbindungen	105
F	
FILTERUNG	
EINGEHENDE ANRUFE	61
EINGEHENDE SMS	61
G	
Geheimcode für das Programm	31, 32
H	
Hinzufügen	
Liste der vertraulichen Nummern für die Privatsphäre.....	100
Schwarze Liste der Kindersicherung	76
Schwarze Liste des Anruf- und SMS-Filters	63
Weiße Liste der Kindersicherung.....	79
Weiße Liste des Anruf- und SMS-Filters	66
K	
Kindersicherung	
Modi	74
Schwarze Liste	75
Weiße Liste.....	78
L	
Lizenz.....	35
Informationen.....	36
Lizenzvertrag	35
Programm aktivieren	27
Verlängerung.....	37
Lizenz verlängern.....	37
Lizenzvertrag.....	35
Löschen	
Berichtseinträge.....	118
Quarantäneobjekt.....	59
Schwarze Liste des Anruf- und SMS-Filters	65
Schwarze Liste für die Kindersicherung	78
Weiße Liste der Kindersicherung.....	80
Weiße Liste des Anruf- und SMS-Filters	68
LÖSCHEN	
PROGRAMM	22
Löschen Liste der vertraulichen Kontakte für die Privatsphäre	101

M

Modi	
Anruf- und SMS-Filter	62
Kindersicherung	74
Privatsphäre	94, 95

O

Objekt wiederherstellen	59
-------------------------------	----

P

Privatsphäre	
Auswahl der zu verbergenden Informationen und Ereignisse	102
automatischer Start	96
Liste der vertraulichen Kontakte	99
Modi	94
PRIVATSPHÄRE	94
Programm aktivieren	27
Lizenz	35
PROGRAMM INSTALLIEREN	21
Programm-Menü	45
PROGRAMMOBERFLÄCHE	43

Q

Quarantäne	
Objekt löschen	59
Objekt wiederherstellen	59
Objekte anzeigen	58
QUARANTÄNE	58

S

Schutzstatus	43
Schwarze Liste	
Anruf- und SMS-Filter	63
Kindersicherung	75
Sicherheitsstufe	
Firewall	105
Sicherheitsstufe der Firewall wählen	105
SMS-Befehl senden	92
SMS-Block	
ausgehende Anrufe	75
ausgehende SMS-Nachrichten	75
Eingehende Anrufe	63, 66
eingehende SMS	63
Informationen verschlüsseln	110
Start	
Programm	33
Update	113
Virensuche	52

U

Update	
Manuell starten	113
Start nach Zeitplan	114
UPDATE	
PROGRAMMVERSION	25

V

Verbieten	
ausgehende Anrufe	76
ausgehende SMS-Nachrichten.....	76
Netzwerkverbindungen.....	105
Verschlüsselung	
Daten entschlüsseln	109
Daten verschlüsseln	107
Zugriff automatisch blockieren.....	110
Virensuche	
Aktionen für Objekte	56
Archive.....	55
Manuell starten	52
Start nach Zeitplan	53
Untersuchungsobjekte.....	54

W

Weißer Liste	
Anruf- und SMS-Filter.....	66
Kindersicherung.....	78

Z

Zeitplan	
Update	114
Virensuche.....	53
Zugriff auf verschlüsselte Daten verbieten	110