

Seniorenportal Themen- Spezial Sicherheit

Lektion 1: „Sicherheit beginnt im Kopf“

Allgemeine Sicherheitsmaßnahmen

Wenn man nun noch einige allgemeine Regeln für die Computersicherheit befolgt kann man bedenkenlos im Internet surfen und einkaufen.

Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie vorsichtshalber beim Absender nach, ob der Anhang tatsächlich von ihm stammt.

Seien Sie vorsichtig bei Downloads von Webseiten. Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist.

Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Die Betrüger steigern ihre Erfolgsraten, indem sie individuell auf ihre Opfer zugehen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu verwandt Vertrauen zu erwecken.

Verhaltensgrundlagen beim Onlineshopping

1. Informieren Sie sich über Ihren Geschäftspartner!

Bevor Sie in einem Online-Shop einkaufen, sollten Sie genau überprüfen, ob es sich dabei auch um einen seriösen Anbieter handelt. Lesen Sie also immer die auf jeder guten Website enthaltenen Hintergrundinformationen zum betreffenden Unternehmen und die Allgemeinen Geschäftsbedingungen (AGB). Prüfen Sie auch, ob neben den elektronischen Kontaktdaten auch Adresse und Telefonnummern angegeben sind.

2. Achten Sie darauf, dass Ihre Daten verschlüsselt übertragen werden!

Stimmen Sie einer Übertragung von Kontonummern oder Passwörtern im Internet nur dann zu, wenn der Anbieter die Daten verschlüsselt. Das erkennen Sie bereits am "https" am Anfang der Internetadresse. Oft erscheinen auch ein Sicherheitsschloss oder ein Schlüssel als Symbole in der Statusleiste.

3. Sichern Sie Ihre Daten!

Stellen Sie sicher, dass Ihre Daten bei technischen Schäden auf Ihrem PC nicht verloren gehen. Insbesondere Informationen rund um Finanzen sollten Sie nicht nur auf der Festplatte Ihres PC, sondern auch auf anderen Speichermedien sichern. Sie können diese Daten beispielsweise auf CD's oder DVD's brennen, auf einem USB-Stick oder auf einer externen Festplatte zusätzlich speichern. Es ist sinnvoll, Bestellungen bzw. Rechnungen auch auszudrucken und aufzubewahren.

4. Bewahren Sie Zugangsdaten sicher auf!

Die verschiedenen Zugangsdaten wie Passwörter, PIN, TAN oder Chipkarten sollen Sie keinesfalls auf Ihrem Rechner abspeichern. Dort könnten Sie von Eindringlingen aufgespürt und dann missbräuchlich verwendet werden. Wenn Sie Zugangsdaten auf Papier notieren, so bewahren Sie diese Informationen an einem sicheren Ort auf. Zugangsdaten, die aus zwei Elementen bestehen (wie etwa Passwörter und PINs), sollten Sie niemals gemeinsam aufbewahren.

5. **Schützen Sie sich vor Internet-Schädlingen!**

Beim Surfen im Internet wird generell empfohlen, eine Firewall und Virenschutzprogramme zu verwenden. Dies gilt natürlich auch für den Online-Einkauf, bei dem sonst schnell Viren, Trojanische Pferde oder Spionagesoftware auf Ihren PC gelangen können.

6. **Prüfen Sie, ob alternative Bestellmöglichkeiten existieren!**

Ein guter Online-Shop bietet auch die Möglichkeit, Waren telefonisch oder per Fax zu bestellen. So können Sie den Weg über das Internet umgehen, wenn er Ihnen nicht sicher erscheint.

7. **Warnung vor Phishern!**

Seien Sie vorsichtig, wenn Sie E-Mails erhalten, in denen Sie zur Aktualisierung Ihrer Kundendaten aufgefordert werden. So genannte Phisher versuchen auf diese Weise, Sie auf gefälschte Seiten von Unternehmen, etwa Banken, zu locken und Ihnen persönliche Informationen zu entlocken. Wenn Sie die Website von Geschäftspartnern besuchen wollen, dann geben Sie die Internetadresse am besten jedes Mal wieder ein – dadurch können Sie vermeiden, dass Sie von Betrügern auf gefälschte Seiten gelockt werden.

Nepper- Schlepper- Bauernfänger

Mit der Zahl der Menschen die das Internet benutzen, ist auch stetig die Zahl der schwarzen Schafe gestiegen, die das Internet zum Betrügen und Erschleichen von Geld oder anderen Leistungen missbrauchen. Durch die große Anzahl an Daten und Nutzern im Internet lassen sich die Betrüger meist nur schwer verfolgen. Die Maschen der Betrüger sind hierbei immer vielfältiger und trickreicher geworden.

Beispiele

Betrugs E-mail

[mailto:support_num_9740510003044@sparkasse.de]

Gesendet: Freitag, 9. September 2005 00:05

An: ~~seniorenportal@seniorenportal.de~~

Betreff: SPARKASSE ONLINE-BANKING [Thu, 08 Sep 2005 15:10:39 -0700]



Sehr geehrte Kundin, sehr geehrter Kunde,

Der technische Dienst der Bank führt die planmassige Aktualisierung der Software durch. Für die Aktualisierung der Kundendatenbank ist es nötig, Ihre Bankdaten erneut zu bestätigen. Dafür müssen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfüllen angeboten wird.

https://www.sparkasse.de/firmenkunden/E_electronic-banking/online_banking_cud.html

Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfüllen erforderlich.

Wir bitten um Verständnis und bedanken uns für die Zusammenarbeit.

©sparkasse.de 2005
Alle Rechte vorbehalten
Vervielfältigung nur mit Genehmigung der Sparkassen-Finanzportal GmbH

Oft werden Nachrichten von Banken gefälscht mit der Bitte die persönlichen Daten erneut zu schicken da diese aufgrund eines technischen Problems verloren gegangen sind. Ein beliebter Tick ist auch das ein Anwalt aus dem Ausland schreibt er habe ein großes Erbe zu verwalten aber leider hat er nicht das nötige Geld für die Behörden. Es wird demjenigen ein Anteil des Erbes versprochen, der sich bereit erklärt die Summe für die Behörden auf ein Konto zu überweisen.

Auch e-mails von Behörden wurden schon gefälscht. In einer vermeintlichen Nachricht des Bundeskriminalamts wurden die Empfänger der e-mail bezichtigt sie seien beim illegalen downloaden von Musik ertappt worden. Die dafür fällige Strafe sollte sofort überwiesen werden.

Betrug - Internetseiten

Auch ganze Internetseiten dienen nur zum ausspionieren persönlicher Daten hier ein Beispiel einer gefälschten Seite der Sparkasse



In der Regel geht es bei diesen Internetseiten meist darum das man seine persönlichen Daten eingibt.

Oft werben Internetseiten auch mit kostenlosen Angeboten die aber nach kurzer Zeit kostenpflichtig werden und monatlich Geld kosten.

Wenn man allerdings einige Sicherheitsregeln befolgt, wenn man im Internet einkauft oder andere Geschäfte abwickelt, kann man sich gut vor Internetbetrug schützen.

TIPP: Wenn sie unsicher sind, stellen Sie Ihre Fragen im Seniorenportal.de Forum

Seniorenportal Themen- Spezial Sicherheit

Lektion 2: Technische Schutzmaßnahmen

Welche Gefahren gibt es am Computer?	1
Welchen Schutz gibt es gegen all diese Gefahren?	1
Welches Schutzprogramm ist das richtige?	2
Installationsanleitung 5 Grundregeln (unbedingt einhalten)	2
Installation von Kaspersky Internet Security 2010	3
Glossar	8

Welche Gefahren gibt es am Computer?

Viren, Würmer, Trojaner.. all das sind Begriffe die inzwischen fast täglich in den Medien zu hören sind, doch was hat es mit diesen Gefahren wirklich auf sich? Und vor allem wie kann man sich davor schützen?

Der Überbegriff für alle schädlichen Programme für Computer ist „Malware“. Damit werden alle Programme bezeichnet, die Funktionen, welche unerwünscht und evtl. sogar schädlich sind, auf Computern ausführen. Dies geschieht meist im Hintergrund und wird vom Nutzer erst dann bemerkt wenn bereits Schaden angerichtet wurde. Die angerichteten Schäden sind je nach Malware sehr unterschiedlich: Während in den Anfängen (Mitte der 80'er Jahre) meist Dateien gelöscht oder zerstört wurden, zielen die meisten Programme heutzutage auf das ausspionieren persönlicher Daten über das Internet ab. Eine genauere Unterscheidung der einzelnen Schadprogramme finden sie am Ende dieser Lektion im Glossar.

Deshalb ist es wichtig sich von Anfang an mit Programmen gegen diese Gefahren zu schützen.

Welchen Schutz gibt es gegen all diese Gefahren?

Prinzipiell lassen sich zwei Arten von Schutzprogrammen am Computer unterscheiden:

Antivirusprogramme

Diese Programme werden auf dem Computer installiert, und laufen dann ständig im Hintergrund mit um nach Viren zu suchen. Immer wenn ein Schadprogramm versucht sich im Computer zu auszubreiten schlagen diese Programme Alarm und blockieren bzw. löschen die Malware. Um dies gewährleisten zu können müssen die Antivirusprogramme aber immer alle neuen Viren „kennen“, um sie auch eindeutig identifizieren zu können. Dies geschieht in der Regel über Aktualisierungen aus dem Internet. Je nach Qualität des Programms geschieht diese Aktualisierung einmal täglich bis zu mehrmals stündlich.

ACHTUNG: Ein nicht aktualisiertes Antivirenprogramm kann neue Bedrohungen nicht erkennen und bietet somit keinen ausreichenden Schutz!

Firewalls

Eine Firewall (dt.: „Feuerwand“) ist auch ein Programm das auf einem Computer installiert sein muss, um sich umfassend gegen Schadprogramme zu schützen. Man kann sich dieses Programm wirklich wie eine Wand zwischen dem eigenen Computer und dem Internet vorstellen. In dieser Wand gibt es „Türen“ durch die Daten entweder ins Internet, oder auf den eigenen Computer gelangen können. Allerdings werden diese „Türen“ nur dann geöffnet, wenn die Daten auch durch die Wand dürfen, d.h. in den Einstellungen der Firewall muss konfiguriert sein welche Programme Daten mit dem Internet austauschen dürfen. Alle Daten die Schadprogramme ans Internet senden wollen bleiben so an der Firewall hängen.

Welches Schutzprogramm ist das richtige?

Für den Laien ist bei der großen Anzahl der am Markt befindlichen Schutzprogramme die Auswahl nicht ganz einfach.

Reicht der vom Nachbarn empfohlene, kostenlose Virenschutz aus?

Benötige ich ein Schutzprogramm mit Firewall und muss ich die Aktualisierungen selbst überwachen?

Peter Knapp vom Mediacenter 50plus hat sich seit sechs Jahren ausgiebig mit Schutzsoftware und deren Eignung, speziell für nicht so versierte Internetnutzer beschäftigt und gibt folgende Tipps:

1. Nutzen Sie unbedingt Programme, die bei den gängigen Tests ganz vorne liegen. Wie z.B. seit Jahren die Kaspersky – Schutzsoftware
2. Wer beim Schutz spart zahlt oft doppelt und dreifach!
3. Wenn Sie kein Onlinebanking und Onlineshopping machen, reicht ein gutes Antivirenprogramm. Die Bedienung ist hier extrem einfach.
4. Wenn Sie Zahlungen und Transaktionen über das Internet vornehmen ist eine Firewall Pflicht. Sie sollte Bestandteil eines kompletten Sicherheitspaketes sein. Nicht zwei separate Programme verwenden.

Installationsanleitung 5 Grundregeln (unbedingt einhalten)

Beachten Sie bei der Installation eines Schutzprogrammes bitte unbedingt folgende 5 Grundregeln!

Diese Reihenfolge sollten Sie unbedingt einhalten:

1. Wenn Sie keine Installations- CD/DVD besitzen, laden Sie sich zuerst die neue Schutzsoftware aus dem Internet. Z.B. unter www.kaspersky.de
2. Trennen sie anschließend unbedingt die Internetverbindung!!!
3. Deinstallieren Sie vor der Neuinstallation unbedingt vorhandene Schutzprogramme über die Systemsteuerung. Mehrere Schutzprogramme dürfen nicht gleichzeitig auf dem System vorhanden sein.
4. Installieren Sie nun die neue Schutzsoftware
5. Stellen Sie jetzt die Internetverbindung her und aktivieren Sie das Programm

Installation von Kaspersky Internet Security 2010

Dieses Programm der Firma Kaspersky Labs besteht sowohl aus einem Antivirusprogramm, als auch aus einer Firewall. Dies erhöht die Benutzerfreundlichkeit, da man nicht lernen muss mit zwei unterschiedlichen Programmen umzugehen. Im folgenden werden sie lernen wie man dieses Programm installiert und richtig benutzt.

Die Installation

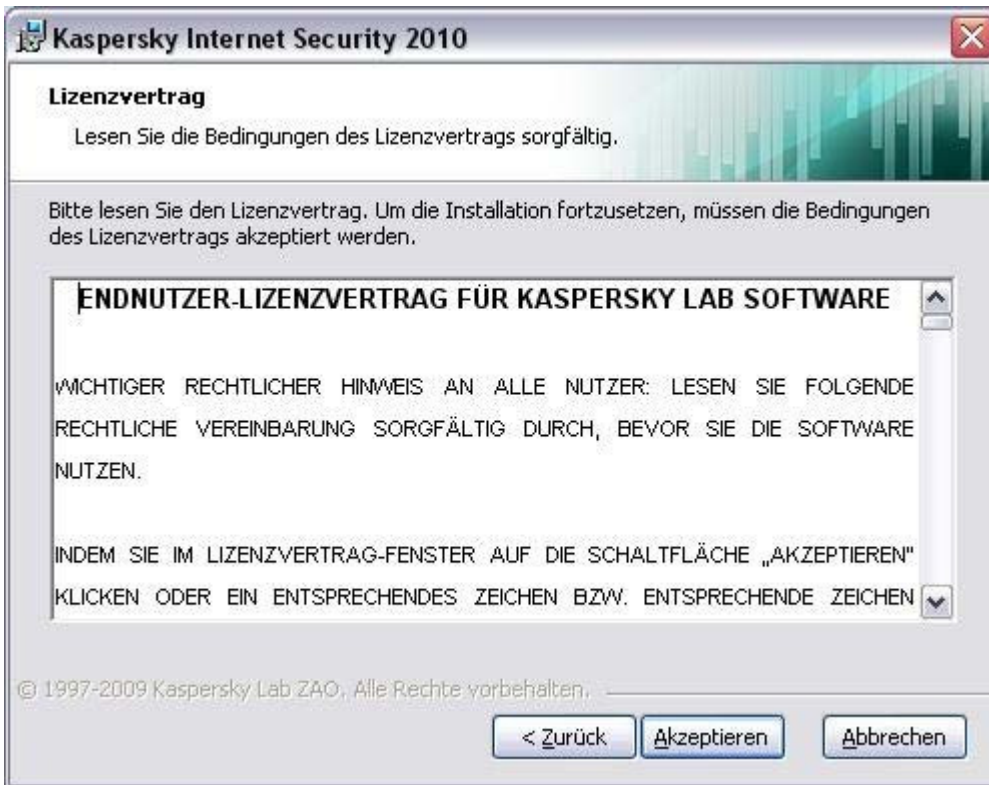
Schritt 1

Legen sie die Kaspersky Internet Security 2010 CD in ihr Laufwerk ein, die Installation startet automatisch.



Klicken Sie auf Weiter, um die Schnellinstallation zu starten.

Schritt 2



Lesen Sie nun bitte den Lizenzvertrag durch. Wenn Sie mit den Bedingungen einverstanden sind, klicken Sie auf Akzeptieren. Die Installation wird fortgesetzt. Um die Installation abzubrechen, auf Abbrechen klicken.

Schritt 3



Der Installations Assistent bietet die Teilnahme am Kaspersky Security Network (KSN) an. Wenn Sie am KSN teilnehmen erhält das Kaspersky Labor Informationen über neue Schadprogramme, die auf Ihrem PC entdeckt wurden, Systeminformationen und eine

einzigartige Identifikationsnummer, die von Kaspersky Internet Security vergeben wurde. Es wird garantiert, dass keine persönlichen Daten gesendet werden. Lesen Sie die Erklärung zur Datensammlung zur Nutzung von Kaspersky Security Network. Wenn Sie mit den Bedingungen einverstanden sind, setzen Sie einen Haken bei Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network und klicken Sie auf Weiter. Die Installation wird fortgesetzt.

Schritt 4

Das Programm beginnt nun mit der Installation, dies kann einige Minuten dauern.



Schritt 5



Bitte geben sie nun den Aktivierungscode ein, den sie auf einem Zettel in der Verpackung finden. Klicken sie anschließend auf Weiter.

Schritt 6



Wenn sie den Aktivierungscode richtig eingegeben haben sehen sie nun die Gültigkeitsdauer ihrer Lizenz. Klicken sie auf Weiter.

Schritt 7



Die Installation ist nun abgeschlossen klicken sie auf Beenden um das Programm zu starten.

Erstes Update und Überprüfung ob alles ordnungsgemäß funktioniert

Das Programm benötigt direkt nach der Installation eine Liste der aktuellen Bedrohungen im Internet. Dies wird durch eine Warnmeldung unten rechts auf dem Monitor angezeigt. (Warnmeldungen werden in Lektion 2 noch genauer behandelt.)



Klicken sie auf Jetzt aktualisieren damit das automatische Update gestartet wird



Sie können anhand eines kleinen Symbols in der Taskleiste ganz unten rechts im Bildschirm erkennen ob Kaspersky Internet Security aktiv ist.



Je nach Aktion die gerade vom Programm ausgeführt wird ändert sich das Symbol:

Während eines Updates sieht es z.B.: so aus:

Öffnen sie das Programmfenster, indem sie einen Doppelklick auf dieses Symbol machen. Falls das Update beendet ist und das Programm ordnungsgemäß arbeitet sollte das Fenster folgendermaßen aussehen:



Glossar

Hier werden die wichtigsten Schadprogramme für Computer unterschieden und genauer erklärt.

Glossar

Adware wird Software genannt, die ohne Nachfrage Funktionen startet, die der Werbung oder auch der Marktforschung dienen.

Backdoor (dt. Hintertür) bezeichnet Programme die Unbefugten Zugang auf den eigenen Rechner verschaffen. Dadurch kann der Computer unbemerkt z.B. als Verteiler für Werbe e-mails missbraucht werden.

Phishing ist eine Art des Internetbetrugs. Hier wird versucht, über gefälschte Internetseiten und e-mails an die Daten oder an Geld der Benutzer zu gelangen.

Rootkits sind Programme, die meist dazu dienen, Prozesse oder Dateien im System zu verstecken. Dies kann z.B. dazu genutzt werden Viren zu tarnen, damit sie nicht von Sicherheitsprogrammen entdeckt werden.

Spyware sammelt Daten über das Nutzerverhalten der Anwender und versendet diese über das Internet

Trojaner oder auch Trojanische Pferde sind augenscheinlich harmlose oder sogar nützliche Programme die aber ein verstecktes Schadprogramm enthalten (meist Spyware oder eine Backdoor).

Viren sind Programme die sich ständig selbst kopieren und in Programmen, Dokumenten oder anderen Daten einnisten und diese beschädigen können.

Würmer sind den Viren ähnliche Programme. Auch sie reproduzieren sich selbst allerdings versenden sie sich auch selbst über das Internet und verbreiten sich deshalb in rasanter Geschwindigkeit.

Seniorenportal Themen- Spezial Sicherheit

Lektion 3: Die Schutzsoftware besser kennen lernen

Untersuchung	2
Update	2
Lizenzverlängerung	3
Einstellungen	5
Grundeinstellungen wieder herstellen.....	6
Berichte abrufen	10

In dieser Lektion werden sie lernen wie das Programm Kaspersky Internet Security 2010 (KIS 2010) zu benutzen ist und wie sie selbständig Wartungsaufgaben durchführen können. Sie können das Programmfenster öffnen indem sie einen **Doppelklick** auf das **Kaspersky- Symbol** in der rechten unteren Ecke ihres Bildschirms machen:



Nun können sie das **Programmfenster von Kaspersky** sehen:



Im oberen Bereich des Fensters können sie die Statusmeldungen von KIS 2010 sehen. Wenn alles ordnungsgemäß funktioniert sollte die Leiste grün sein und den Text: „Der Computer ist sicher“ enthalten. Sobald Probleme mit dem Programm auftreten sollten ändert die Leiste die Farbe in gelb bzw. rot und die Probleme werden gemeldet. Falls dies der Fall sein sollte erscheint in derselben Zeile ein Knopf mit der Aufschrift: „Korrigieren“ Wenn sie dies anklicken behebt das Programm eventuelle Fehler. Auf der linken Seite des Fensters gibt es sogenannte Registerkarten wenn sie diese anklicken ändert sich jeweils der Inhalt des Fensters: Für den Anfang sind hier erstmal nur die beiden Registerkarten Untersuchung und Update von Belang.

Untersuchung

Eine Untersuchung des Computers wird immer dann fällig, wenn entweder das Programm neu installiert wurde und/oder sie den Verdacht haben auf ihrem System könnte sich ein Schadprogramm eingenistet haben.

Um die Untersuchung von Hand zu starten öffnen sie das Programmfenster, klicken sie einmal auf Untersuchung und anschließend auf „Vollständige Untersuchung starten“. Nun beginnt das Programm damit sämtliche Teile ihres Systems auf Schadprogramme zu untersuchen.

Eine schnelle Untersuchung kann zwar viel Zeit sparen, wenn sich allerdings Schadprogramme bereits länger auf ihrem Computer ausbreiten kann es sein, das nicht alle Bedrohungen erkannt und beseitigt werden können.

Update

Wie in Lektion 2 bereits beschrieben kann ein Antivirenprogramm nur dann ordnungsgemäß arbeiten, wenn es immer über eine Liste der aktuellen Bedrohungen verfügt. Diese Listen bekommt KIS 2010 über das automatische Update aus dem Internet. In der Regel geschieht dieses Update automatisch ohne das sie etwas dafür tun müssen, allerdings können manchmal Probleme auftreten die nur durch ein manuell gestartetes Update behoben werden können. (Zum Beispiel wenn sie Probleme mit ihrer Internetverbindung hatten)

Um das Update von Hand zu starten öffnen sie das Programmfenster klicken sie auf Update und dann auf „Update ausführen“ Nun lädt sich KIS 2010 selbständig die aktuellen Bedrohungslisten aus dem Internet und installiert diese auf ihrem Computer.

(Details Siehe Abbildung nächste Seite)

[TIPP: Download Kaspersky Internet Security als kostenlose 30-Tage Testversion unter www.kaspersky.de](http://www.kaspersky.de)

Kaspersky Internet Security 2010

Quarantäne | Bericht | Einstellungen

Der Computer ist sicher
Anti-Spam: Ein Training ist erforderlich

Schutz-Center
Komplexer Schutz für Ihren Computer

Programmkontrolle
Programme und Zugriff auf Daten kontrollieren

Untersuchung
Computer und Dateien untersuchen

Update
Datenbanken und Programm-Module aktualisieren

Sicherheit+
Tools für einen erweiterten Schutz

Update
Die regelmäßige Aktualisierung der Datenbanken und Programm-Module von Kaspersky Internet Security ist Voraussetzung für einen effektiven Schutz.

Datenbank-Status: aktuell
Datenbanken vom: 29.11.2009 16:18:00

Bedrohungstypen:	Insgesamt:	Datenbanken vom:
Schädliche Programme	3291353	29.11.2009 16:18:00
Banner	23491	28.11.2009 09:02:00
Phishing-Seiten	12383	29.11.2009 17:16:00
Spam	97283	29.11.2009 16:43:00
Schädliche Skripts	11524	10.07.2009 09:24:00
Verdächtige Seiten	121479	29.11.2009 13:02:00
Netzwerkangriffe	1096	29.10.2009 11:26:00
Regeln für Sicherheitsanalyse	2836	23.11.2009 20:03:00

Überblick über die Virenaktivität

Update ausführen
Wurde abgeschlossen vor 2 Minuten
Startmodus: automatisch

Rollback zu den vorherigen Datenbanken
Wenn bei einer Aktualisierung die Datenbanken aufgrund einer Störung teilweise beschädigt wurden, können Sie zur vorherigen Version der Datenbanken zurückkehren.

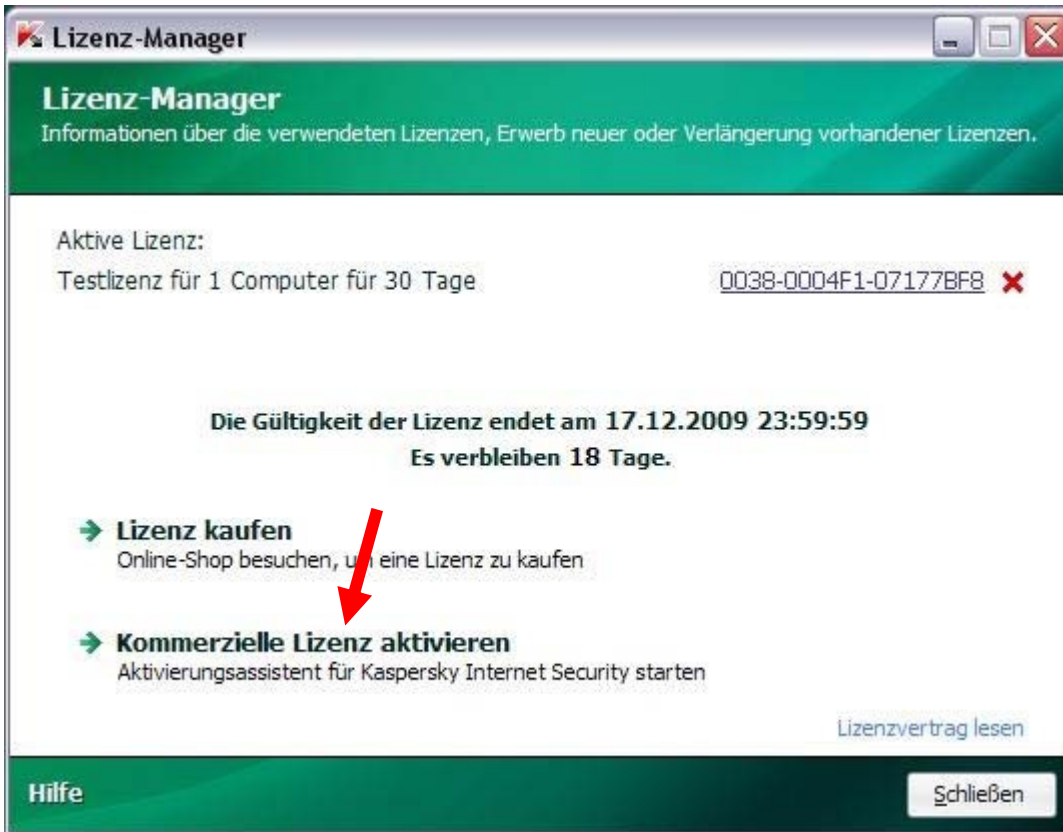
Hilfe | Mein Kaspersky Account | Support | Lizenz: Es verbleiben 18 Tage | Lizenz kaufen

Lizenzverlängerung

Da Virenprogramme ständig über das Internet aktuell gehalten werden müssen, sind die Lizenzen (die Berechtigung das Programm zu benutzen) mit einer zeitlichen Beschränkung. Wenn sie Kaspersky Internet Security 2010 kaufen, erwerben sie eine Lizenz für ein Jahr. Wenn diese Zeit abgelaufen ist müssen sie eine Verlängerung für ein Jahr erwerben. Diese können sie entweder persönlich im Fachhandel erwerben oder über das Internet im Onlineshop bestellen.

Bevor ihre Lizenz endet meldet sich KIS 2010 rechtzeitig damit sie genügend Zeit haben sich um eine Verlängerung zu kümmern. Sie können die Gültigkeitsdauer ihrer Lizenz in Erfahrung bringen indem sie das Programmfenster öffnen. Im unteren Bereich steht neben dem Wort Lizenz die Restgültigkeitsdauer.

Wenn sie bereits eine Verlängerung erworben haben, müssen sie diese noch über das Programm aktivieren. Dies können sie tun indem sie das Programmfenster öffnen und im unteren Bereich auf das Wort Lizenz klicken. Ein neues Fenster öffnet sich:



Klicken sie auf „Kommerzielle Lizenz aktivieren“



Geben sie im nächsten Fenster den Aktivierungscode, den sie beim Kauf der Verlängerung erhalten haben, ein und klicken sie anschließend auf „Weiter“ nun gleicht das Programm die Lizenzdaten mit dem Internet ab. Wenn sie alles richtig eingegeben

haben sollte nun ein Fenster mit „Ihre Lizenz wurde verlängert“ erscheinen. Im unteren Teil des Programmfensters sollte außerdem die neue Gültigkeitsdauer erscheinen.

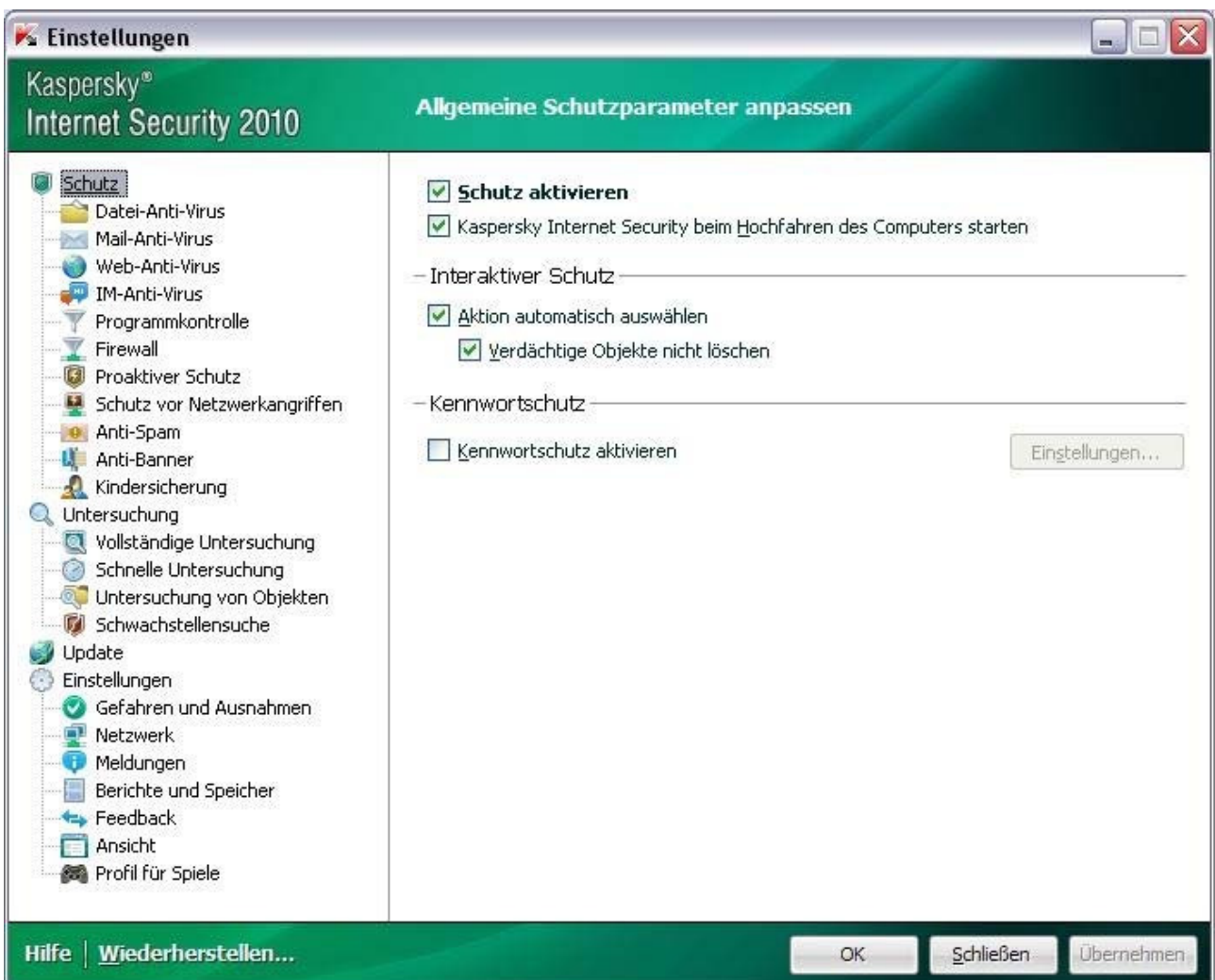
ACHTUNG: Wenn ihre Lizenz nicht mehr gültig ist, arbeitet das Programm nicht mehr ordnungsgemäß. Es ist kein ausreichender Schutz mehr vorhanden.

Einstellungen

KIS 2010 bietet ihnen eine Reihe von Möglichkeiten das Programm genau auf ihre Bedürfnisse zuzuschneiden, allerdings erfordert dies Erfahrungen im Umgang mit Virenprogrammen und Firewalls. Wenn sie dennoch etwas an den Einstellungen des Programms ändern wollen können sie dies indem sie im **oben rechts im Programmfenster auf Einstellungen klicken**.



Es öffnet sich das Einstellungsfenster:



Sie können im linken Bereich des Fensters auswählen für welchen Programmteil sie die Einstellungen ändern wollen, im rechten Bereich erscheinen dann die jeweiligen Parameter die sie einstellen können.

Wenn sie etwas geändert haben müssen sie zum bestätigen unten rechts auf „Übernehmen“ klicken und anschließend erst auf „OK“ ansonsten werden die veränderten Einstellungen wieder verworfen.

Grundeinstellungen wieder herstellen

In der Regel sind die Voreinstellungen die Kaspersky vornimmt in Ordnung und es muss nichts mehr geändert werden.

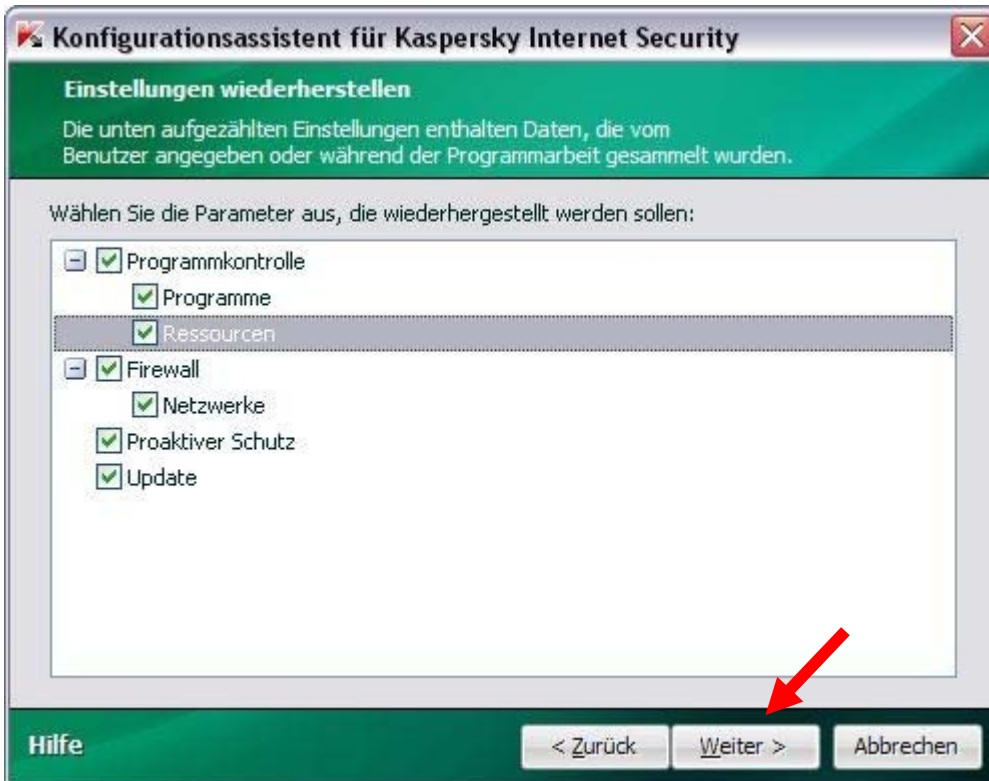
Falls sie einmal aus Versehen etwas verändert haben und nicht mehr wissen was es war bietet ihnen KIS 2010 eine Möglichkeit die Grundeinstellungen des Programms wieder herzustellen. Dazu klicken sie im Programmfenster auf „Einstellungen“ im neu geöffneten Einstellungsfenster klicken sie unten links auf „Wiederherstellen“.



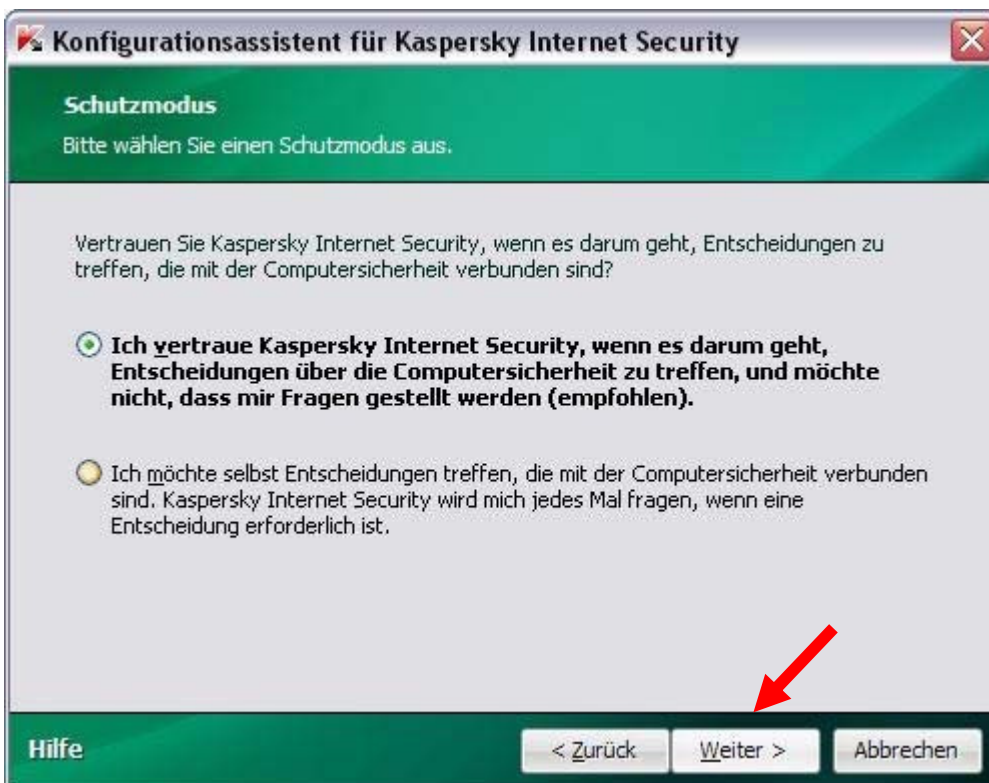
Es öffnet sich ein neues Fenster:



Klicken sie auf „Weiter“ um die Wiederherstellung zu starten



Im nächsten Fenster werden sie gefragt für welchen Teil des Programms die Einstellungen wiederhergestellt werden sollen. Machen sie Häkchen in **allen Kästchen** indem sie darauf klicken. Anschließend klicken sie auf „Weiter“

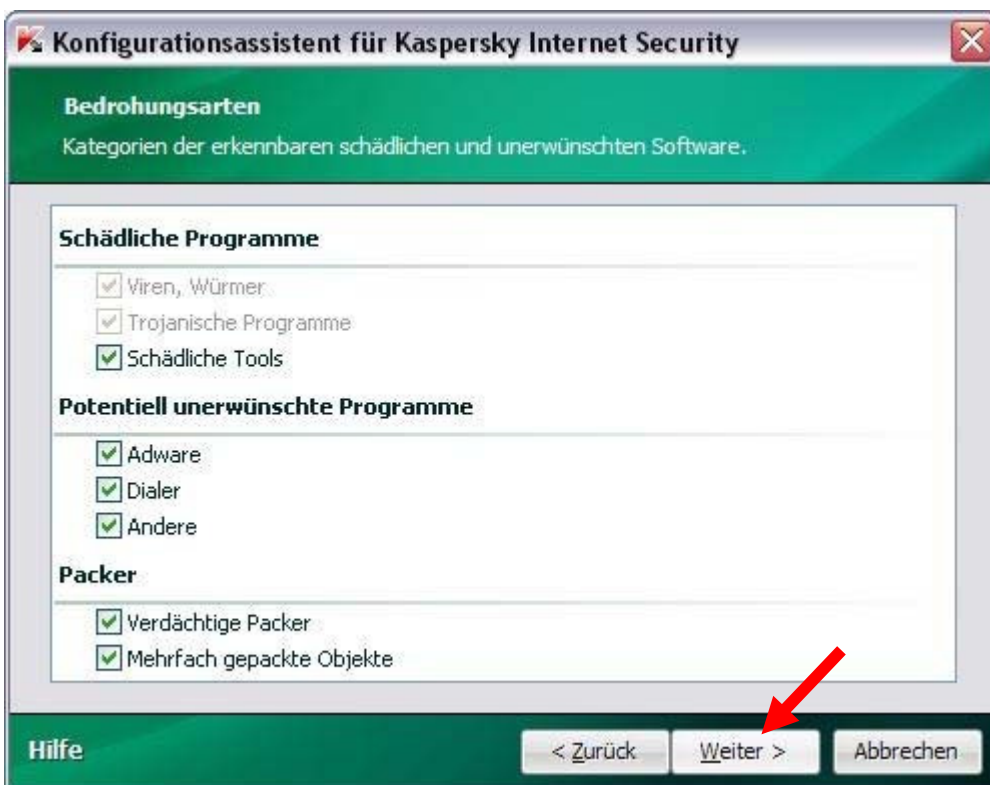


Dieses Fenster dient der Abfrage ob sie selbst entscheiden wollen wie ihr Computer geschützt wird, oder ob die Einstellungen wie von Kaspersky empfohlen vorgenommen

werden sollen. Sie sollten die Einstellung lassen wie sie ist und nur auf „Weiter“ klicken.



In diesem Fenster werden die Einstellungen für das Update vorgenommen, sie sollten die Einstellung auf „Automatisches Update“ lassen und auf „Weiter“ klicken.



Jetzt wird festgelegt welche Arten von Schadprogrammen KIS 2010 bekämpfen soll.

Achten sie darauf das hier in allen Kästchen ein Häkchen ist und klicken sie danach auf „Weiter“. Das Programm startet nun mit dem analysieren des Systems und dem Wiederherstellen der ursprünglichen Einstellungen.



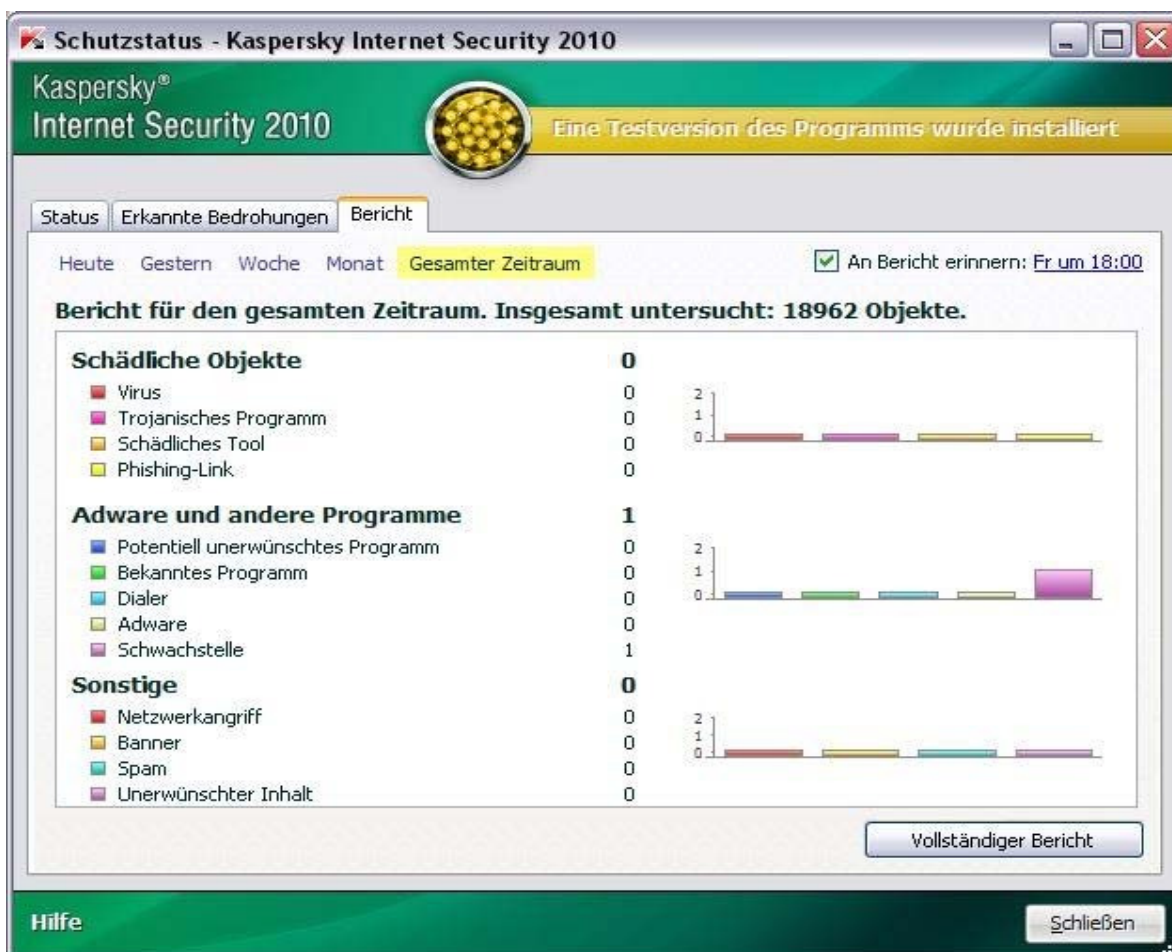
Wenn sie dieses Fenster sehen können ist KIS 2010 wieder auf die empfohlenen Einstellungen zurückgesetzt, klicken sie auf „Beenden“ um das Fenster zu schließen.

Berichte abrufen

KIS 2010 bietet Ihnen die Möglichkeit Berichte anzuzeigen in denen Sie erkennen können wie viele Bedrohungen das Programm schon erkannt bzw. bekämpft hat. Wenn Sie sich dafür interessieren klicken Sie im oberen Teil des Programmfensters einfach auf „Bericht“

Es öffnet sich ein neues Fenster in dem Sie genau aufgeschlüsselt sehen können welche Schadprogramme Ihren Computer bereits befallen haben.

Standard mäßig werden Sie jeden Freitag um 18 Uhr an den aktuellen Bericht von KIS 2010 erinnert falls Sie diese Funktion ausschalten möchten öffnen Sie das Berichtsfenster und entfernen Sie in der rechten oberen Ecke des Fensters das Häkchen vor „An Bericht erinnern“



[TIPP: Download Kaspersky Internet Security als kostenlose 30-Tage Testversion unter www.kaspersky.de](http://www.kaspersky.de)