IKARUS anti.virus
Handbuch

https://www.ikarussecurity.com

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Inhaltsverzeichnis

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

1

Einleitung

Vielen Dank, dass Sie sich für IKARUS anti.virus von IKARUS Security Software entschieden haben.

IKARUS anti.virus schützt Ihre persönlichen Daten und Ihren PC vor allen Arten von Malware. Zusätzlich schützt Sie das AntiSPAM Modul vor SPAM E-Mails. Beim Erkennen neuer und existierender Bedrohungen jeder Art gehört die integrierte IKARUS scan.engine zu den Besten der Welt.

Einfache Installation, ein intuitives User-Interface und regelmäßige Updates der Virendatenbank sind nur einige der vielen Vorteile.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

2

Installation von anti.virus

In diesem Kapitel erfahren Sie, wie man IKARUS anti.virus installiert und erfolgreich in Betrieb nimmt. Jeder Installationsschritt ist mit Bildern dokumentiert und kann 1:1 nachvollzogen werden.

2.1 Systemvoraussetzungen

Damit Sie die IKARUS anti.virus problemlos verwenden können, sind folgende Systemvoraussetzungen notwendig:

Hardware:

- Prozessor ab 2 GHz (Intel/AMD)
- 2 GB RAM
- Mind. 500 MB freier Speicherplatz
- Bildschirmauflösung mind. 1024 x 575

Betriebssystem:

- Windows 7 und höher (32/64 Bit)
- Windows Server 2008 R2 und höher (32/64 Bit)
- Windows Embedded Versionen (konfigurationsabhängig)
- Microsoft Outlook 2007 und höher

ACHTUNG: Bitte deinstallieren Sie vor der Installation von IKARUS anti.virus andere auf Ihrem PC befindlichen Anti-Viren-Programme und führen Sie danach einen Neustart des Computers durch.

Nach der Installation von IKARUS anti.virus wird eine schnelle Systemprüfung empfohlen. Bitte führen Sie diese zum Schutz Ihrer Geräte durch.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

2.2 Installation von IKARUS anti.virus

Wir empfehlen vor der Installation von IKARUS anti.virus alle anderen Programme zu beenden.
Durch Doppelklicken der Datei „Setup-IKARUS antivirus.exe" starten Sie das Programm.
Es folgen nun Screenshots zu den einzelnen Installationsschritten:

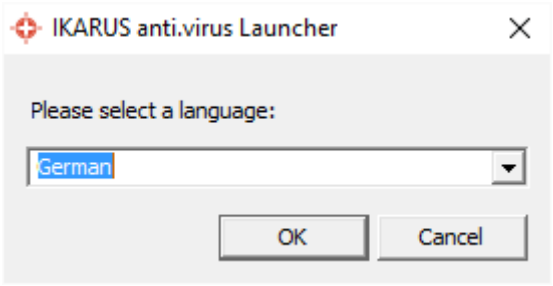


Abbildung 1: Installationsschritt 1
Wählen Sie die gewünschte Sprache

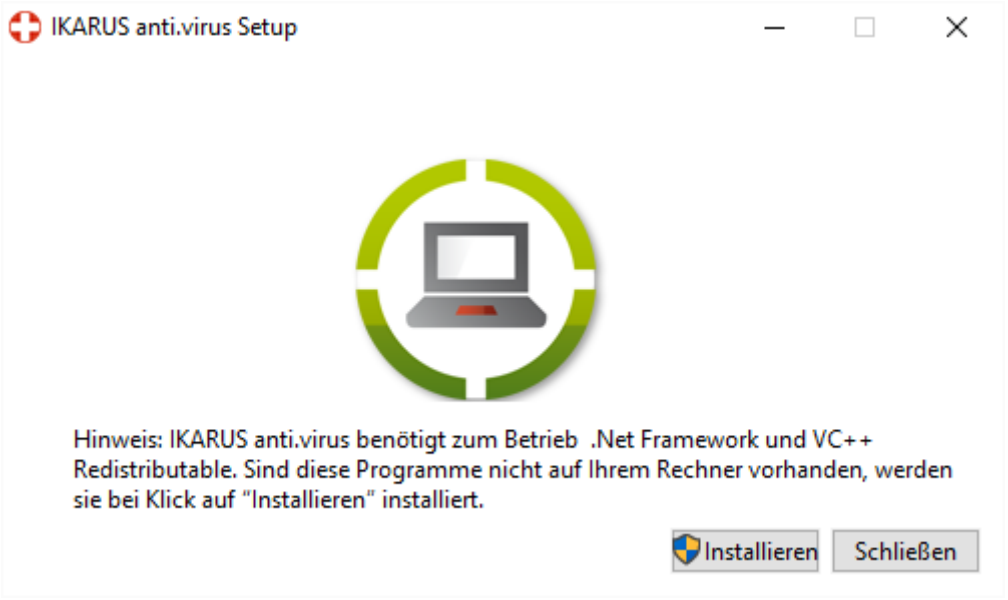


Abbildung 2: Installationsschritt 2
Um die Installation zu starten, benötigt Ihr PC das Microsoft-Programm .NET Framework. Haben Sie .NET Framework von Microsoft noch nicht installiert, wird dies automatisch nachgeholt. Eine bestehende Internetverbindung ist dafür Voraussetzung.

IKARUS anti.virus überprüft, ob eine ältere Version von IKARUS anti.virus installiert ist.
Wenn dies der Fall ist, muss die ältere IKARUS anti.virus Version zuvor manuell deinstalliert werden. Sie werden nach der Deinstallation vermutlich aufgefordert, den Rechner neu zu starten. Bitte führen Sie diesen Neustart durch, die Installation von IKARUS anti.virus kann danach sofort gestartet werden.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Abbildung 3: Installationsschritt 3

Folgen Sie für die Installation von IKARUS anti.virus bitte den Anweisungen des Installationsassistenten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

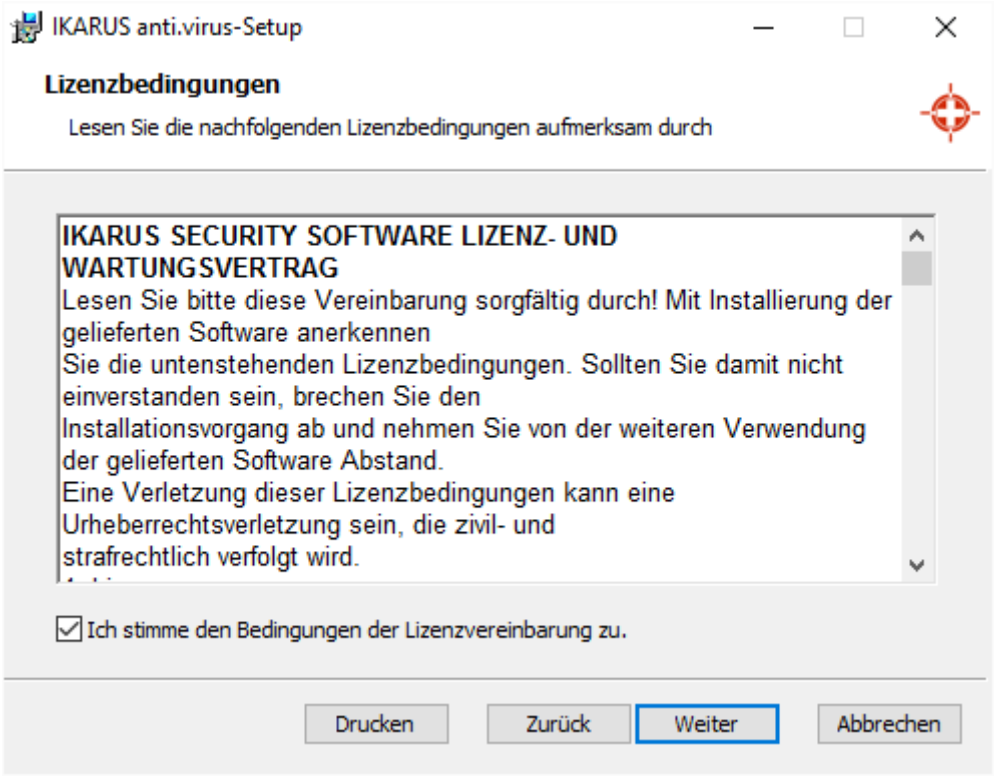


Abbildung 4: Installationsschritt 4

Akzeptieren Sie bitte die Lizenzbestimmungen von IKARUS, um mit der Installation fortzufahren.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

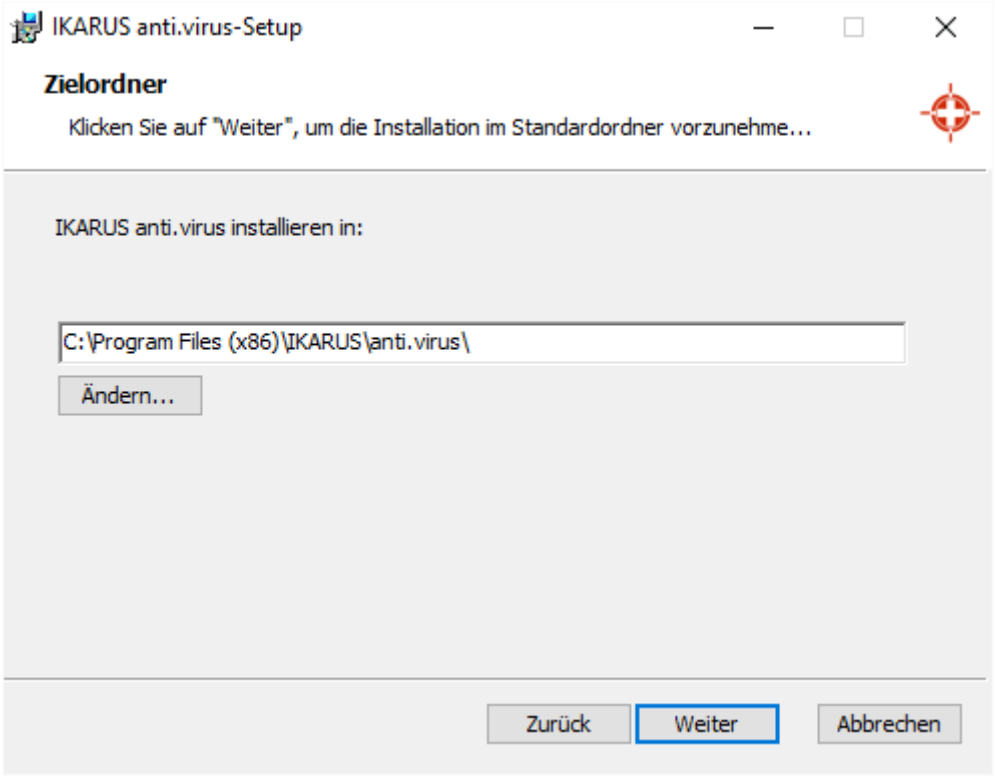


Abbildung 5: Installationsschritt 5

Wählen Sie das Zielverzeichnis für die Installation von IKARUS anti.virus aus. Wir empfehlen, den vorgeschlagenen Standardordner beizubehalten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

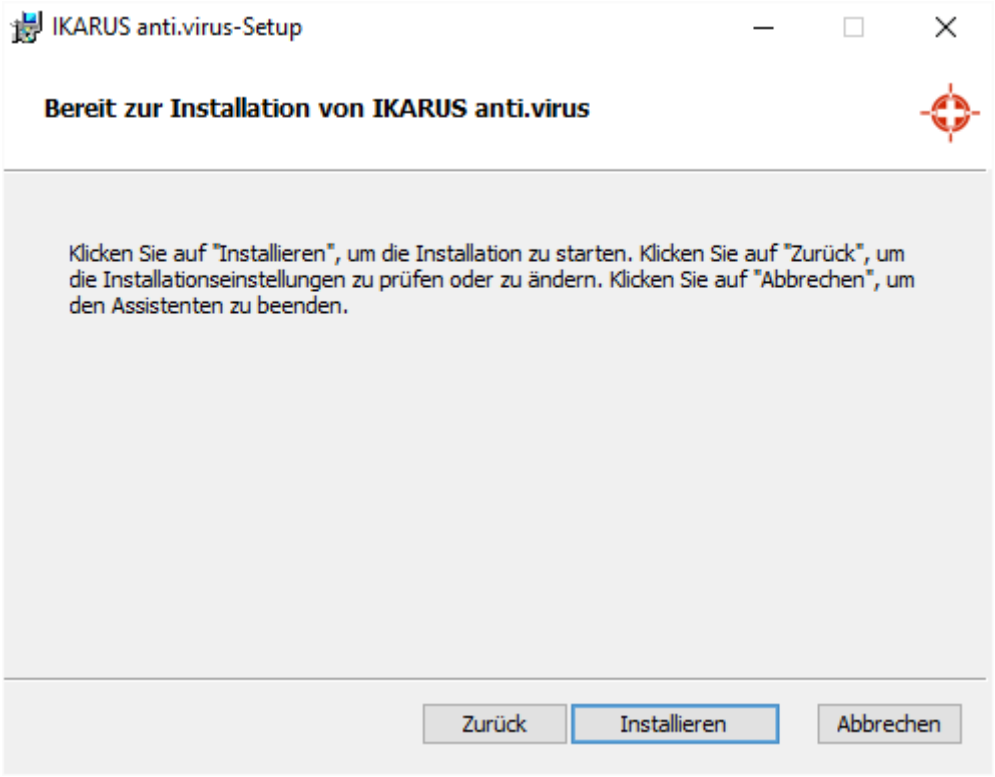


Abbildung 6: Installationsschritt 6

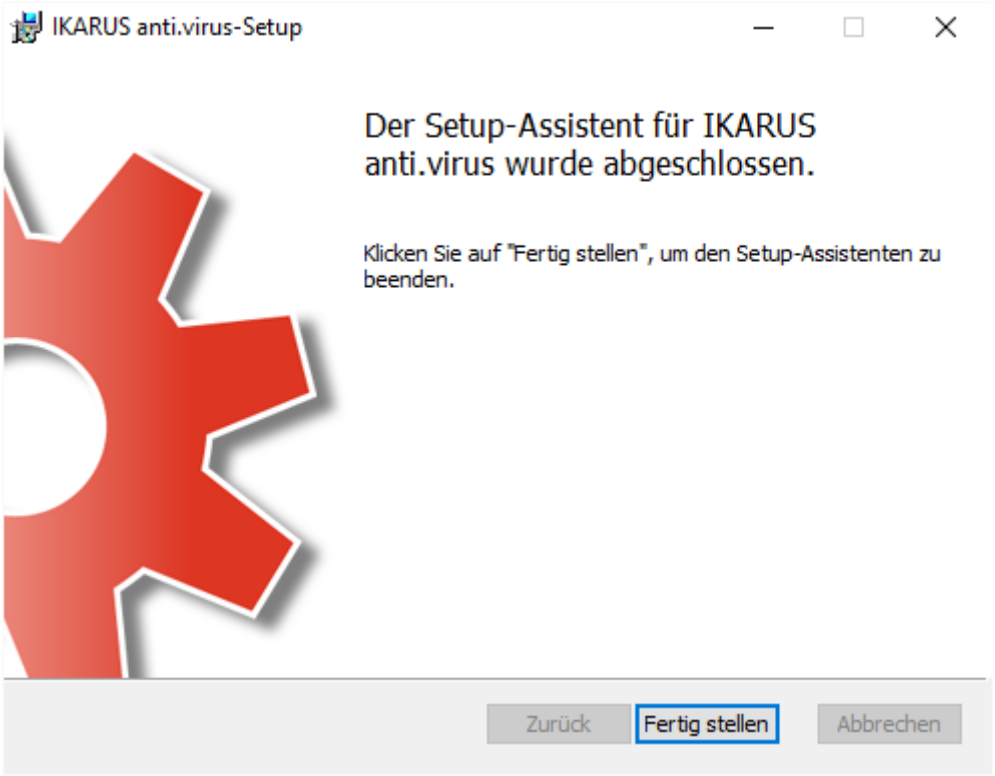


Abbildung 7: Installationsschritt 7

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

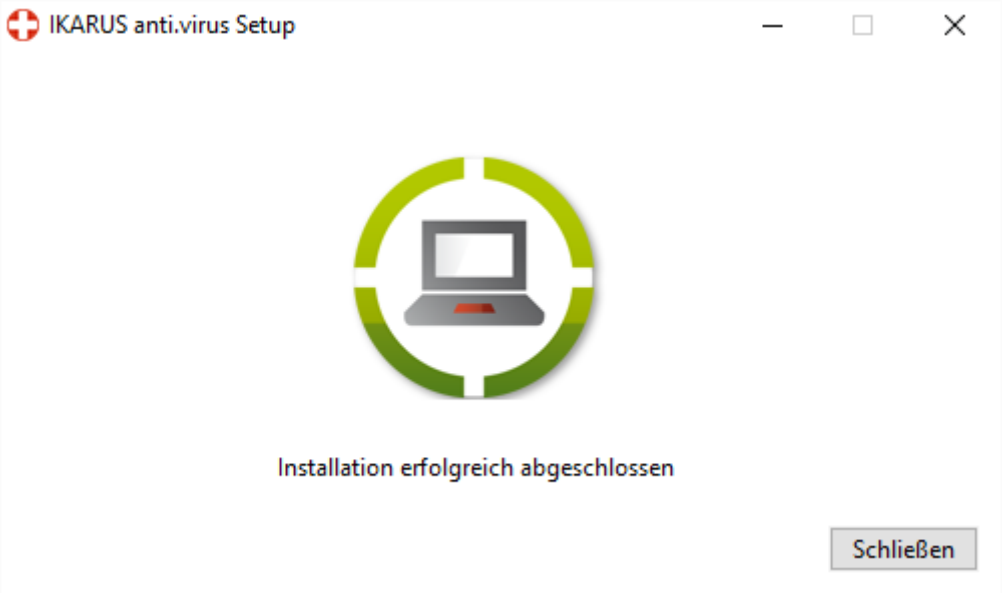


Abbildung 8: Installationsschritt 8

Nun ist die Installation von IKARUS anti.virus abgeschlossen. Wir empfehlen eine schnelle Systemprüfung durchzuführen!

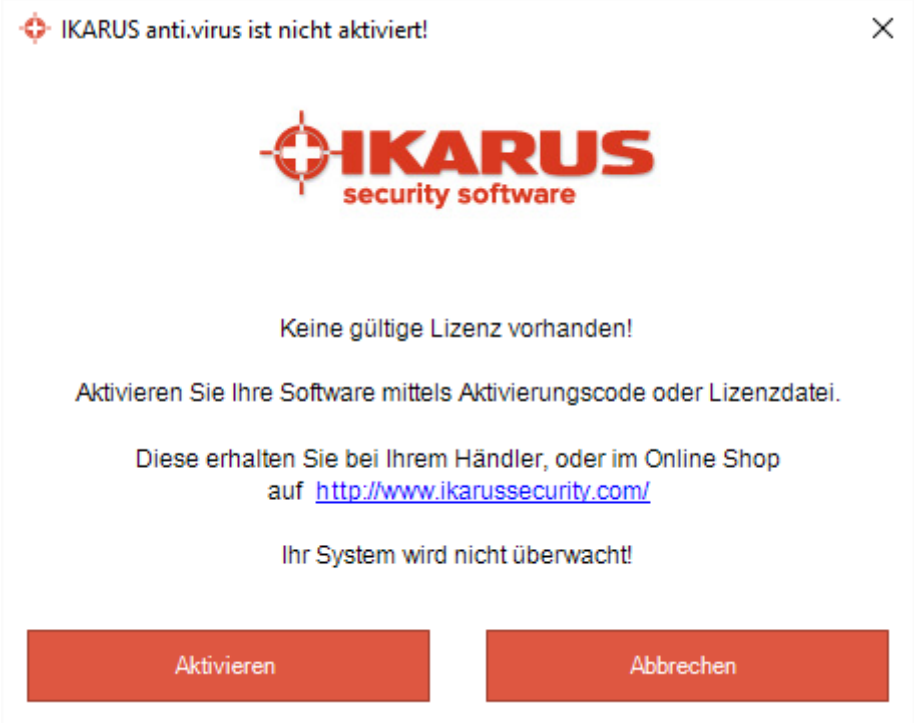


Abbildung 9

Bitte aktivieren Sie IKARUS anti.virus mittels Aktivierungscode oder Lizenzdatei.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

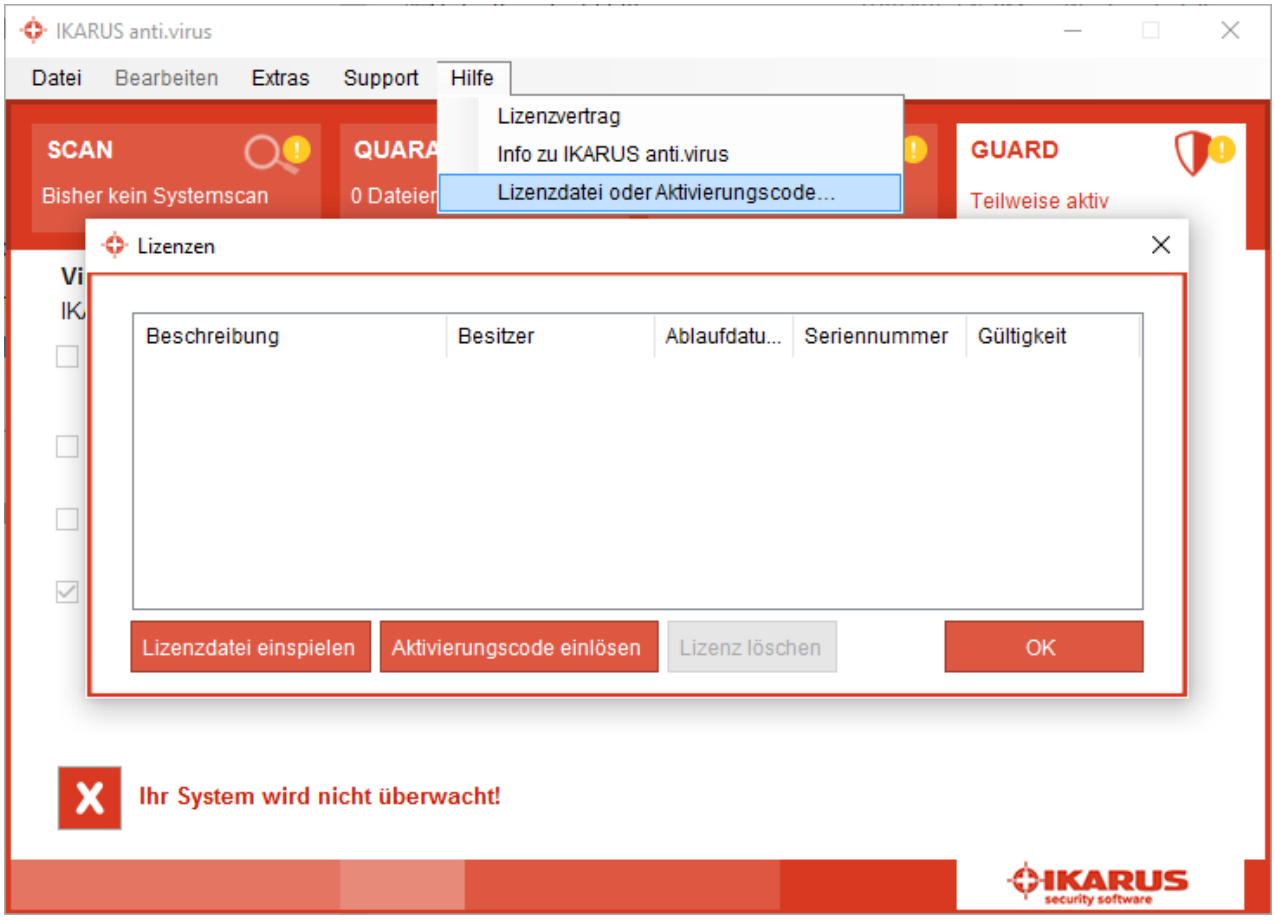


Abbildung 10

Wählen Sie im Menüpunkt „Hilfe“ „Lizenzdatei oder Aktivierungscode…“

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

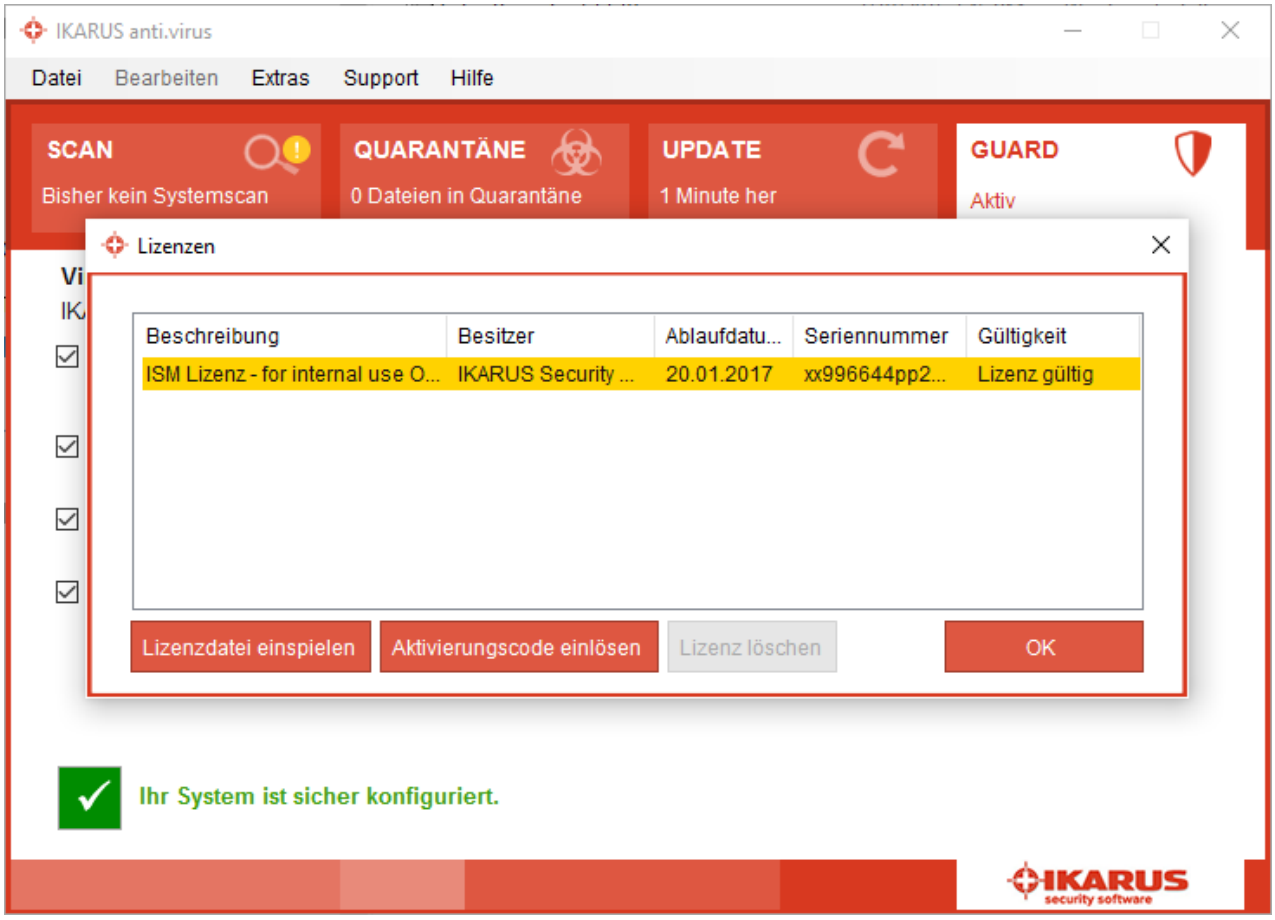


Abbildung 11

Lösen Sie den Aktivierungscode ein oder spielen Sie die Lizenzdatei ein.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

2.3 Unbeaufsichtigte Installation von der Kommandozeile

Mit der unbeaufsichtigten Installation von der Kommandozeile (im Folgenden „Silent Installation“ genannt) bestehen weitere Möglichkeiten zur Konfiguration von IKARUS anti.virus.

WICHTIG: Diese Form der Installation ist nur mit den MSI Installern der IKARUS anti.virus Software möglich und ausschließlich für fortgeschrittene Benutzer und Systemadministratoren gedacht. Downloads finden Sie unter:
https://www.ikarussecurity.com/at/downloads/produkte/download-ikarus-antivirus/

Öffnen Sie ein CMD Fenster. Admin-Rechte sind Voraussetzung.

Die korrekte Syntax für die Silent Installation ist:
`msiexec /q /l* SetupLog.txt /i SetupProject.msi PROPERTY=VALUE`

Der Parameter `/l* SetupLog.txt` für das Logfile des Setup ist nicht zwingend notwendig. Anstelle von `SetupProject.msi` kann auch ein absoluter Pfad verwendet werden (z.B. `C:\setup\setup.msi`). Wird kein absoluter Pfad zur Verfügung gestellt, muss der aktuelle Ordner im CMD-Fenster derjenige sein, der die Setup-Datei enthält. Die Syntax `PROPERTY=VALUE` ist besonders wichtig. PROPERTY muss unbedingt in Großbuchstaben geschrieben werden, außerdem sind keine Leerzeichen erlaubt (z.B. `PROPERTY=VALUE`). Die Reihenfolge der PROPERTIES ist unwichtig.

Ein Beispiel für eine gültige und korrekte Syntax wäre:
`msiexec.exe /q /l* setuplog.txt /i SetupProject.msi ACCEPTLICENSEAGREEMENT="yes"USEPROXY="yes" PROXY="127.0.0.1:8080"`

Folgende PROPERTIES werden derzeit für die Silent Installation unterstützt
(Standardwerte, wenn die Eigenschaft nicht gesetzt ist, werden fett geschrieben):

Zwingend notwendig:
Die einzige zwingende PROPERTY für die Silent Installation ist das Akzeptieren der Lizenzvereinbarungen.
`ACCEPTLICENSEAGREEMENT (yes -` Muss akzeptiert werden.

Anti.virus-Settings:
Proxy:
`USEPROXY (yes/`**`no`**`)` - Definierter Proxy-Server wird verwendet
`PROXY (Host:Port)` - Definierter Proxy-Server

Abhängigkeiten:

- `Port= 1 … 65535`
- `USEPROXY=yes -> PROXY must be set`

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

- PROXY is set, USEPROXY not set -> USEPROXY=yes

Schutz:
WSYSTEM (**yes**/no) - Systemüberwachung aktivieren
WEMAIL (**yes**/no) - E-Mail-Schutz aktivieren
WSPAM (**yes**/no) - SPAM-Schutz aktivieren
UPDATE (**yes**/no) - Automatische Updates aktivieren

Scan Planung:
Anmerkung: Die Standardwerte (fettgedruckt) sind nur gültig, wenn mindestens eine der folgenden Eigenschaften bereitsteht. Sind keine Eigenschaften definiert, werden keine geplanten Scan-Profile erstellt.

AUTOSCAN (yes/**no**) - Automatisch geplante Scans aktivieren
SCANTYPE (**quick**/standard/full) - Scanprofil für geplanten Scan
DAILY (yes) - Intervall für geplanten Scan
WEEKLY (0-6) - Intervall für geplanten Scan (0 = Sunday, 5 = default)
MONTHLY (1-31) - Intervall für geplanten Scan
SCANHOUR (xx:xx) - Zeitpunkt für geplanten Scan (17:00 = default)

Abhängigkeiten:
- Wählen Sie einen Scan-Intervall aus (DAILY, WEEKLY, MONTHLY)
- DAILY akzeptiert ausschließlich "yes", andere Parameter führen zu einer Fehlermeldung
- Ist nur eine der Eigenschaften definiert, werden den anderen Standardwerte zugewiesen, z.B.:
  - ➔ SCANTYPE="standard"
    - AUTOSCAN="yes"
    - WEEKLY="5"
    - SCANHOUR="17:00"

Existierende Dateien:
Für die Silent Installation können eigene Pfade zu existierenden Dateien definiert werden. Werden diese nicht definiert, verwendet das Setup die Default-Einstellungen.
Die Dateipfade können unabhängig voneinander definiert werden.

CONFIG (path)	Pfad zu einer bestehenden guardx-conf, z.B.: CONFIG="C:\mydir". Falls vorhanden, werden die anderen Eigenschaften von "*Anti.virus-Settings"* ignoriert.
VDB (path)	Pfad zu einer bestehenden t3sigs.vdb, z.B.: VDB="C:\mydir"
T3 (path)	Pfad zu einer bestehenden t3.dll, z.B.: T3="C:\mydir"
T3_W64 (path)	Pfad zu einer bestehenden t3_w64.dll, z.B.: T3_W64="C:\mydir"
SDB (path)	Pfad zu einer bestehenden antispam.sdb, z.B.: SDB="C:\mydir"

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Verhalten bei der Installation:
Mit den folgenden Eigenschaften (PROPERTIES) kann das Verhalten während und nach der Installation beeinflusst werden:

`INSTALLFOLDER (path)`	Installationspfad - wenn nicht anders angegeben, wird die Default-Einstellung verwendet. Der Installationspfad endet automatisch auf “anti.virus“. Aus "C:\myfolder" wird für die Installation z.B. automatisch "C:\myfolder\anti.virus".
`UPDATENOW (yes/no)`	Update ausführen, wenn das Setup beendet wurde.
`LICENSE (path)`	Absoluter Pfad zum Lizenzfile, z.B.: LICENSE="C:\mydir\license.ikkey"
`CLOSEOUTLOOK (yes/no)`	Legt fest, ob Outlook automatisch beendet werden soll, falls es während der Installation geöffnet wurde. Hinweis: keine User-Interaktion vorgesehen.

Fehlermeldungen:
Wenn die Installation fehlschlägt, kann die Ursache dafür in der erstellten Protokolldatei (log file) eingesehen werden.

Um festzustellen, ob die Installation aufgrund einer falschen PROPERTY Syntax fehlgeschlagen ist, sollten Sie im log file nach dem "Error 0x80004005" suchen. Dies ist der Fehlercode, wenn die Lizenzbestimmungen nicht akzeptiert wurden.

"Error 0x80004005: In order to install IKARUS anti.virus you must accept the license agreement. Please provide the property `ACCEPTLICENSEAGREEMENT="yes"` in order to install the product."

Weitere Informationen finden Sie unter:
https://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

2.4 Deinstallation von IKARUS anti.virus

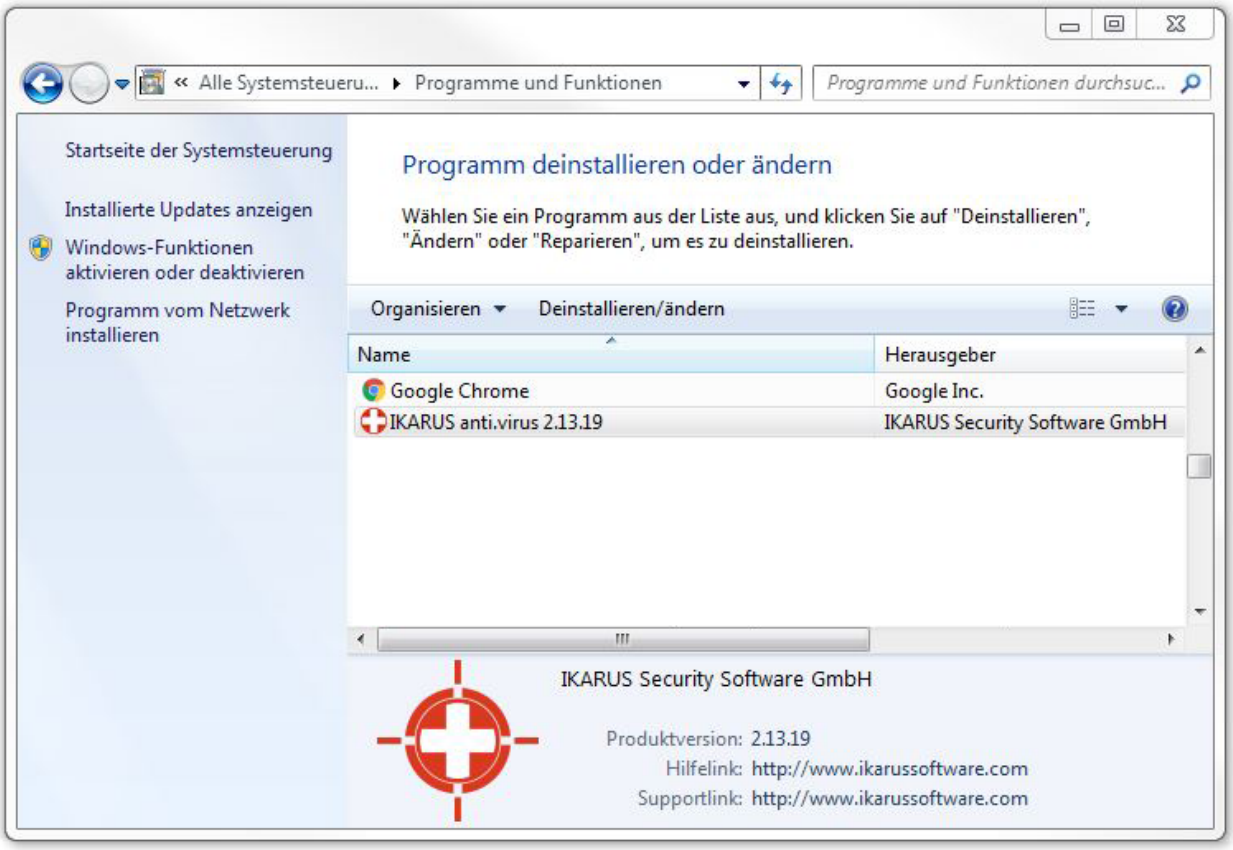


Abbildung 12: IKARUS Deinstallation starten

Um IKARUS anti.virus zu deinstallieren, öffnen Sie in der Systemsteuerung „Programme und Features“ und suchen Sie nach „IKARUS“.

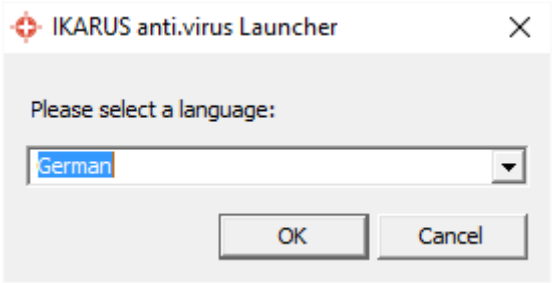


Abbildung 13: Deinstallation Schritt 2

Wählen Sie die Sprache des Assistenten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

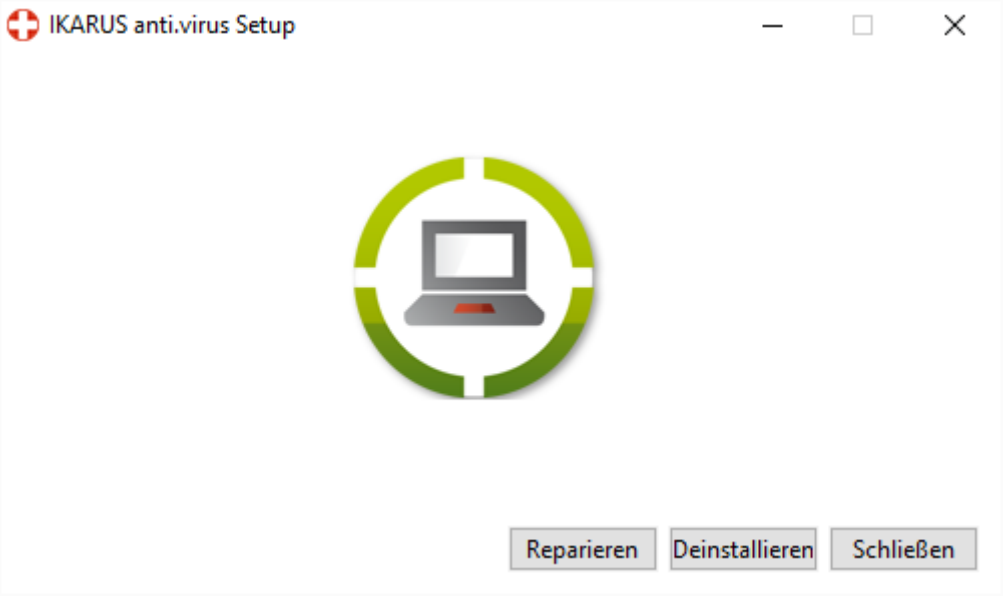


Abbildung 14: Deinstallation Schritt 3

Wählen Sie die Option „Deinstallieren“.

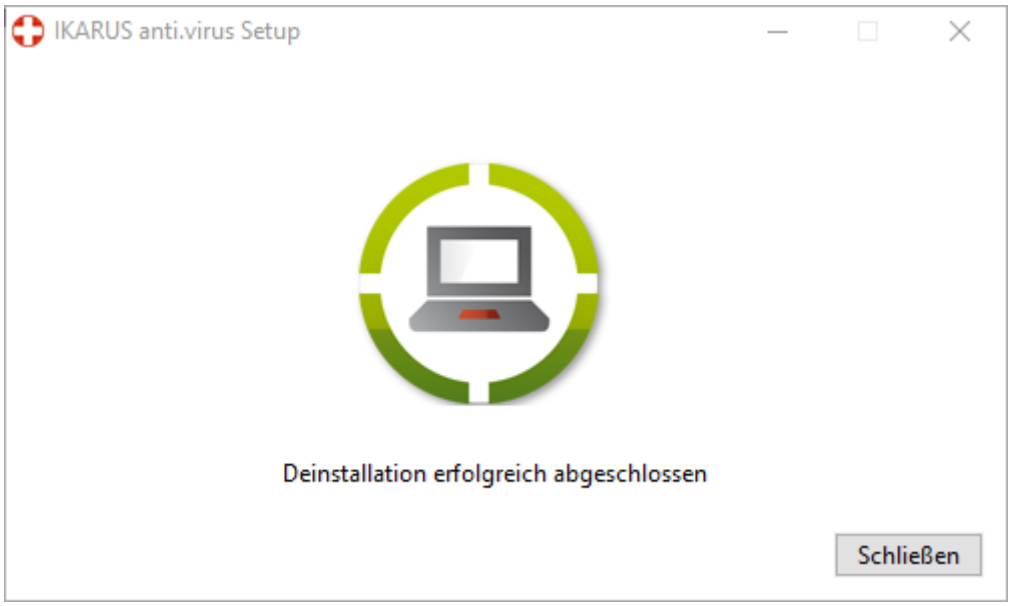


Abbildung 15: Deinstallation Schritt 4

Wenn die Deinstallation abgeschlossen ist, erscheint ein entsprechender Hinweis im Fenster. Gleichzeitig werden Sie gefragt, ob Sie Ihren Computer neu starten möchten. Es wird empfohlen, diesen Neustart sobald wie möglich durchzuführen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

3

Features von IKARUS anti.virus

IKARUS anti.virus bietet Ihnen:

- Zuverlässige Malware-Erkennung dank IKARUS scan.engine
- Regelmäßige Updates inkl. Programmupdates
- Umfassende Virenscans
- Microsoft SharePoint Überwachung
- E-Mail Überwachung (Outlook) sowie Anti-SPAM-Feature
- Verfügbare Sprachen: Deutsch, Englisch, Russisch, Italienisch, Kroatisch
- Kompatibel mit IKARUS security.manager – der zentralen Managementkonsole für Firmennetzwerke
- Geplante On-Demand-Scan-Profile
- Schneller On-Access Scan
- Senden von verdächtigen Dateien an das IKARUS Labor für weitere Analysen
- Quarantäne Feature mit verschiedenen Aufräummöglichkeiten
- „Guard“-Option für proaktiven Viren- und SPAM Schutz
- Passwortschutz für Einstellungen
- Ressourcenschonender Betrieb
- Flexible Lizenzierung – 1/2/3/5 Jahre

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

3.1 Symbole und Anzeigen

Machen Sie sich nun mit den Symbolen der IKARUS anti.virus vertraut. Symbole, deren Beschreibung mit * markiert sind, entfallen ab Windows 10.

Symbol	Beschreibung
	Das Standardsymbol von IKARUS anti.virus finden Sie rechts unten in der Taskleiste Ihres PCs.
	Wenn Sie mit dem Mauszeiger über das Symbol in der Taskleiste fahren, erscheint für einige Sekunden das hier gezeigte Fenster. Klicken in eines der anzeigten Felder (Scan, Update oder Guard) öffnet die Konfigurationsmaske von IKARUS anti.virus. Sie sehen hier auf einen Blick, ob IKARUS anti.virus einwandfrei läuft, wann es zuletzt aktualisiert wurde, wann die letzte Prüfung stattgefunden hat und ob alle Komponenten des Virenschutzes aktiviert sind. Auch mit Doppelklick auf das Standardsymbol in der Taskleiste können Sie Konfigurationsmaske von IKARUS anti.virus öffnen.
	In diesem Beispiel wurde ein Teil des Guards, d.h. ein Teil der Überprüfung, deaktiviert. *
Die Darstellung des Symbols in der Taskleiste kann sich verändern, die unterschiedlichen Symbole haben jeweils eine andere Bedeutung:	
	Das weiß-rote Kreuz zeigt Ihnen, dass alles in Ordnung ist sowie der Virenschutz optimal eingestellt und aktualisiert ist. IKARUS anti.virus ist aktiv und überwacht Ihren PC.
	Dieses Symbol zeigt Ihnen an, dass einer der Bereiche Scan, Update oder Guard nicht den hohen Sicherheitsrichtlinien von IKARUS anti.virus entspricht. Wenn Sie das Informationsfenster öffnen, sehen Sie, welcher Bereich betroffen ist.
	Ein größer und kleiner werdendes Symbol (ähnlich einem Herzschlag) zeigt an, dass IKARUS anti.virus gerade aktualisiert wird.
	Ein sich drehendes Symbol ist das Zeichen für einen aktuell laufenden Scan.
	Sieht Ihr IKARUS anti.virus-Symbol in der Taskleiste so aus, wissen Sie, dass ein Virus gefunden wurde. Was dann zu tun ist, erfahren Sie im Kapitel *4.4 Quarantäne*.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

4

Die vier Hauptfunktionen

4.1 Der Guard – Ihr Sicherheitswächter

Der Guard ist das Wächter-Programm von IKARUS anti.virus. Eine Aktivierung aller Checkboxen bietet Ihnen den größtmöglichen Schutz vor Schadprogrammen. Nach Bedarf können Sie die Virenschutzeinstellungen „lockern" und eine oder mehrere der Checkboxen deaktivieren.

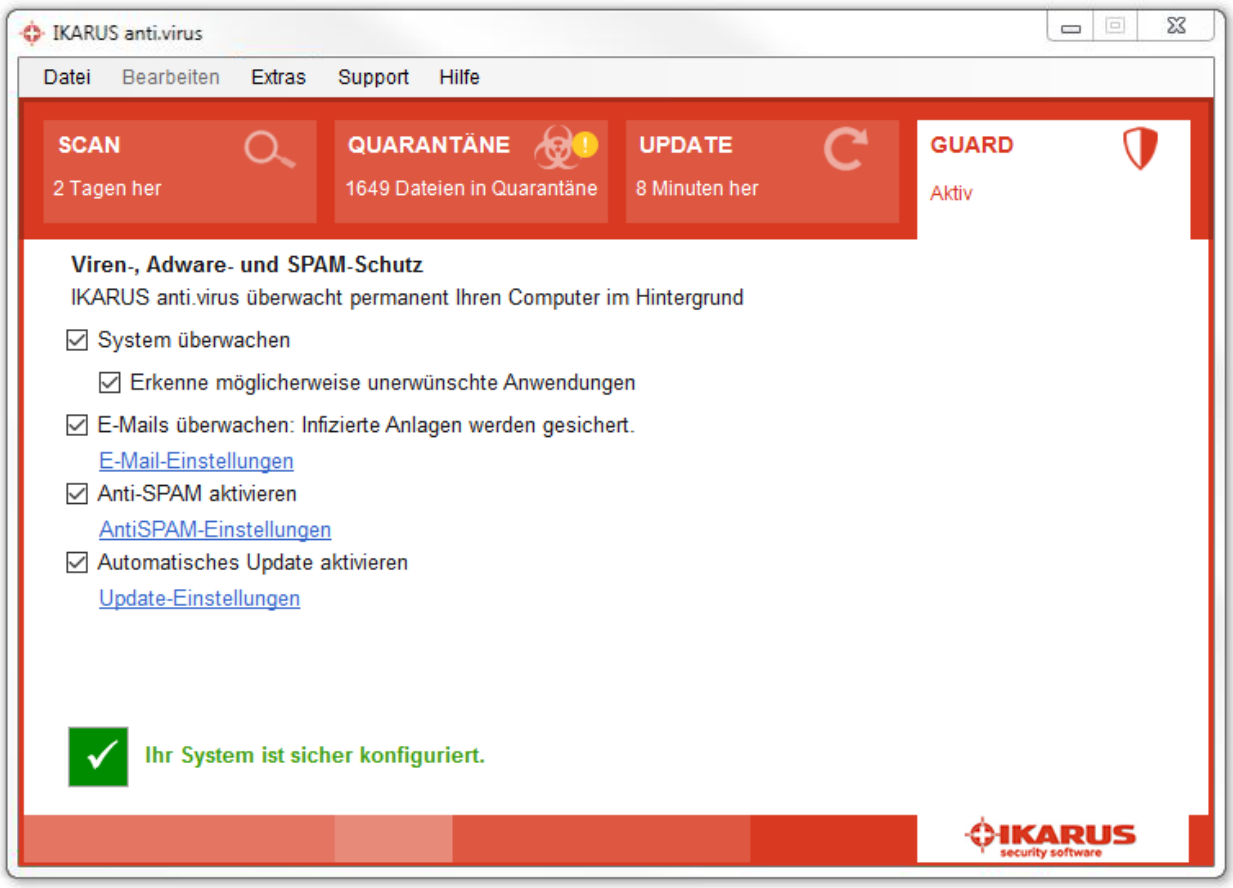


Abbildung 16: Guard

Nur wenn alle Optionen ausgewählt und aktiviert sind, bietet Ihnen IKARUS anti.virus den bestmöglichen Schutz.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

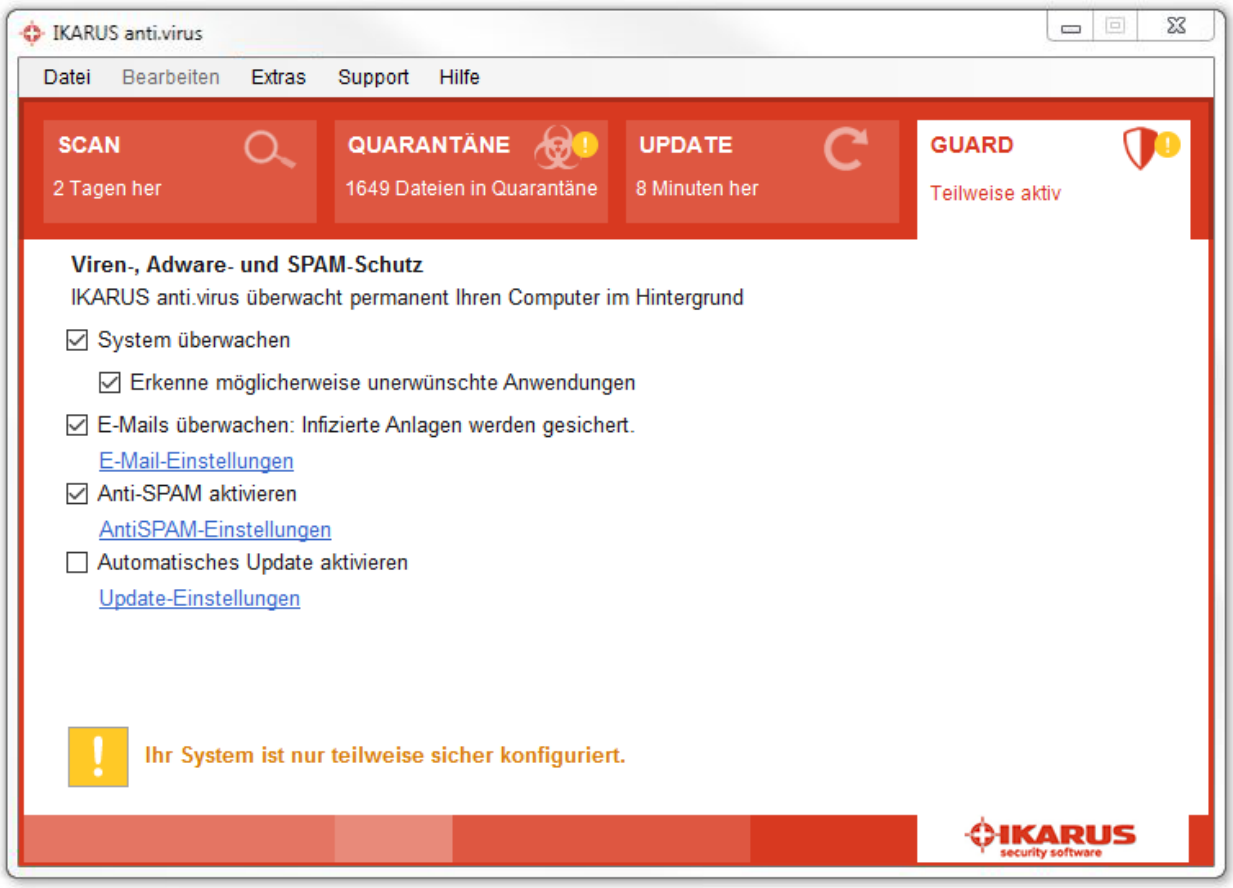


Abbildung 17: Guard - teilweise aktiv

Wenn eine oder mehrere Sicherheitseinstellungen inaktiv sind, erkennen Sie das am gelben Symbol und dem Text „Ihr System ist nur teilweise sicher konfiguriert“.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

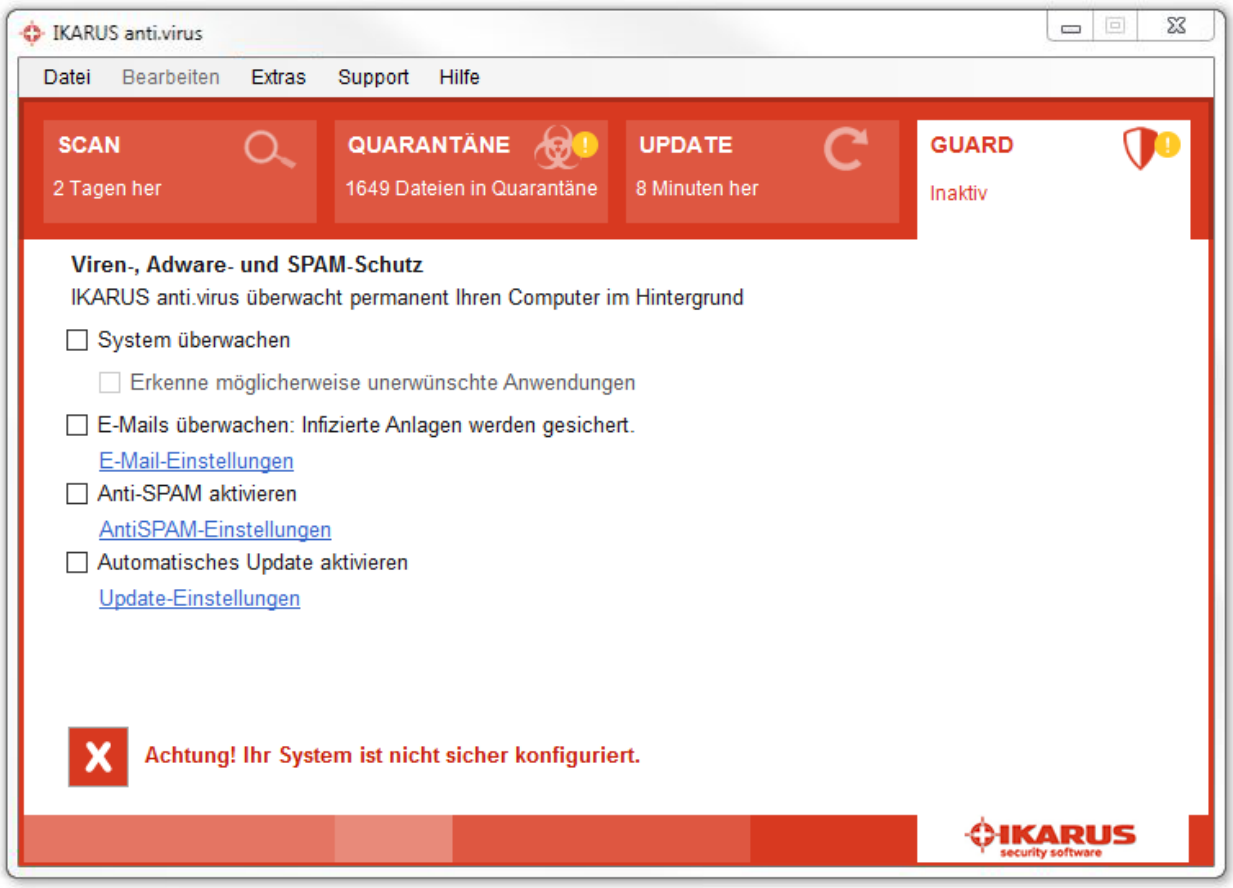


Abbildung 18: Guard inaktiv

Sollten Sie ein rotes Symbol erkennen können, so ist der IKARUS Guard außer Kraft und die Meldung „Achtung! Ihr System ist nicht sicher konfiguriert" erscheint.

Wurden ein oder mehrere Bereiche von der Prüfung ausgenommen, sehen Sie dies auch am veränderten IKARUS anti.virus-Symbol in der Taskleiste. IKARUS anti.virus bietet Ihnen dann nicht mehr den optimalen Schutz!

4.2 Update von IKARUS anti.virus

Nur ein aktueller Virenschutz ist auch ein zuverlässiger Schutz vor Viren, Würmern, Spyware und Trojanern!

IKARUS anti.virus verfügt über eine automatische Aktualisierung. Das Programm überprüft regelmäßig (alle 20 Minuten), ob ein neues Update zur Verfügung steht. Neue Updates werden automatisch installiert. Bei Bedarf wird dazu eine Internet-Verbindung aufgebaut.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Haben Sie Ihren PC längere Zeit nicht in Betrieb gehabt, so aktualisieret sich IKARUS anti.virus automatisch nach dem Starten des PCs.

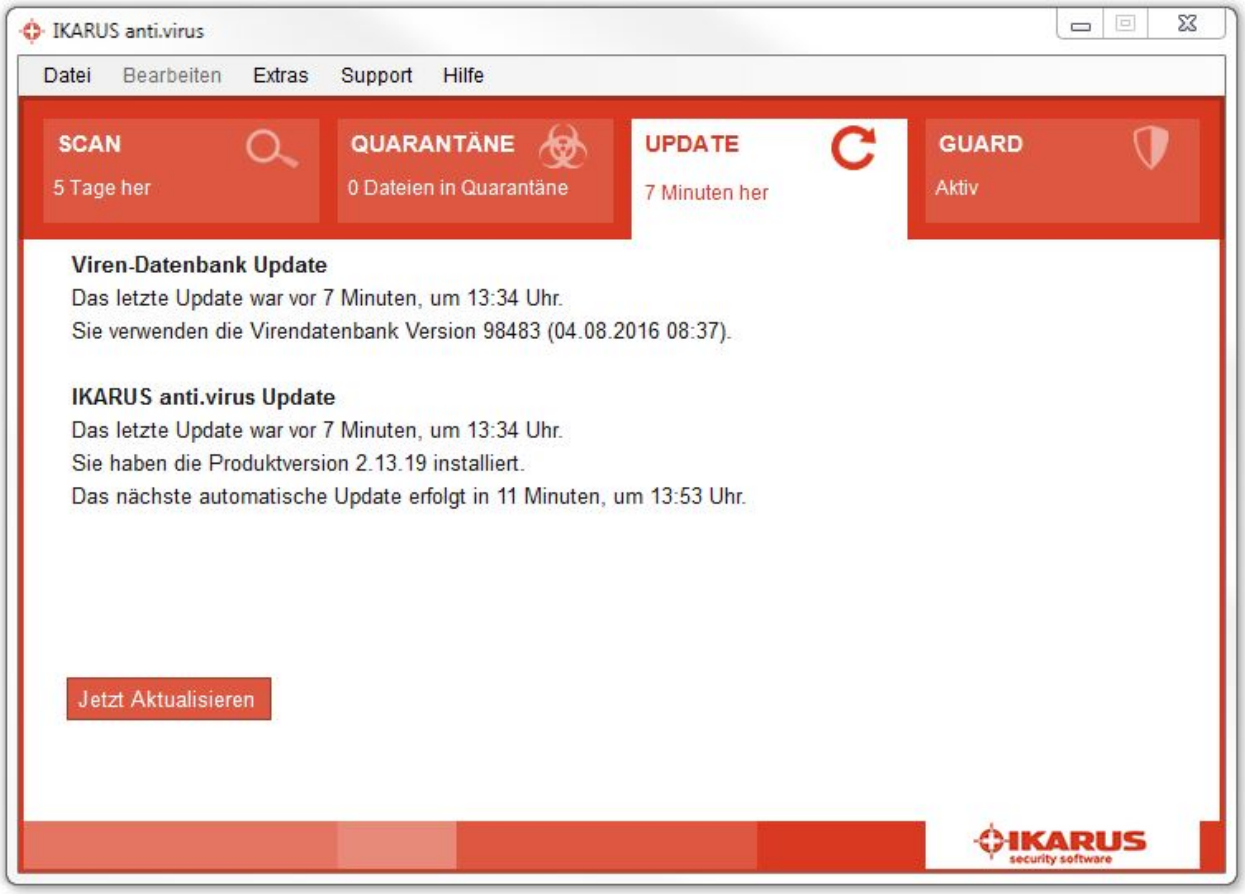


Abbildung 19: Update

Das Update von IKARUS anti.virus unterscheidet zwischen dem Viren-Datenbank-Update und jenem von IKARUS anti.virus selbst.

Updates der Virendatenbank (VDB) garantieren Ihnen, dass auch neue Schadprogramme erkannt werden. Bei den Updates von IKARUS anti.virus handelt es sich um Programmupdates, um Ihnen z.B. Programmneuheiten oder neue Features zugänglich zu machen.

Über den Button „Jetzt Aktualisieren" können Sie jederzeit eine Aktualisierung durchführen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

4.3 Scan - Virenüberprüfung von IKARUS anti.virus

Der Scanvorgang von IKARUS anti.virus kann sowohl automatisch als auch händisch angestoßen werden. Sie können beliebig viele Scans anlegen und verwalten.

Voreingestellte Scans sind:

- **Schnelle Systemprüfung:** Mit dieser Auswahl prüfen Sie unter anderem das Windows Installations-Verzeichnis. Die meisten Computerschädlinge befinden sich in diesem Verzeichnis und können so zuverlässig und rasch erkannt werden.
- **Systempartition:** IKARUS anti.virus scannt mit dieser Auswahl jenes Laufwerk, auf dem Ihr Betriebssystem installiert ist. Sämtliche Archive, Verzeichnisse, Ordner und Dateien, die auf diesem Laufwerk liegen, werden von IKARUS anti.virus überprüft.
- **Gesamter Computer:** Alle Laufwerke des PCs werden von IKARUS anti.virus gescannt.
- **Wechseldatenträger:** Hier werden alle externen Datenträger wie USB-Sticks oder optische Laufwerke überprüft.

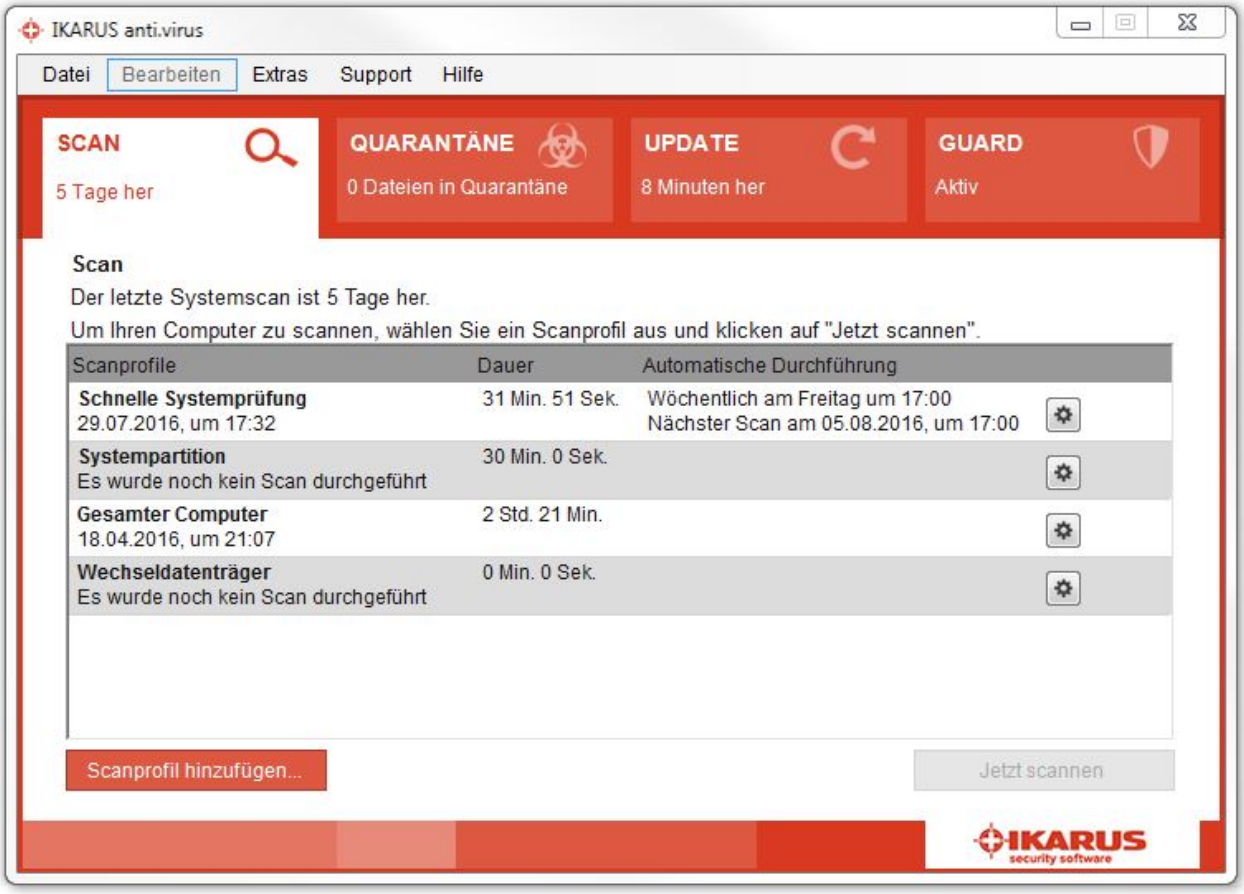


Abbildung 20: Scan

Individuelle Scans werden durch den Button „Scanprofil hinzufügen" angelegt.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

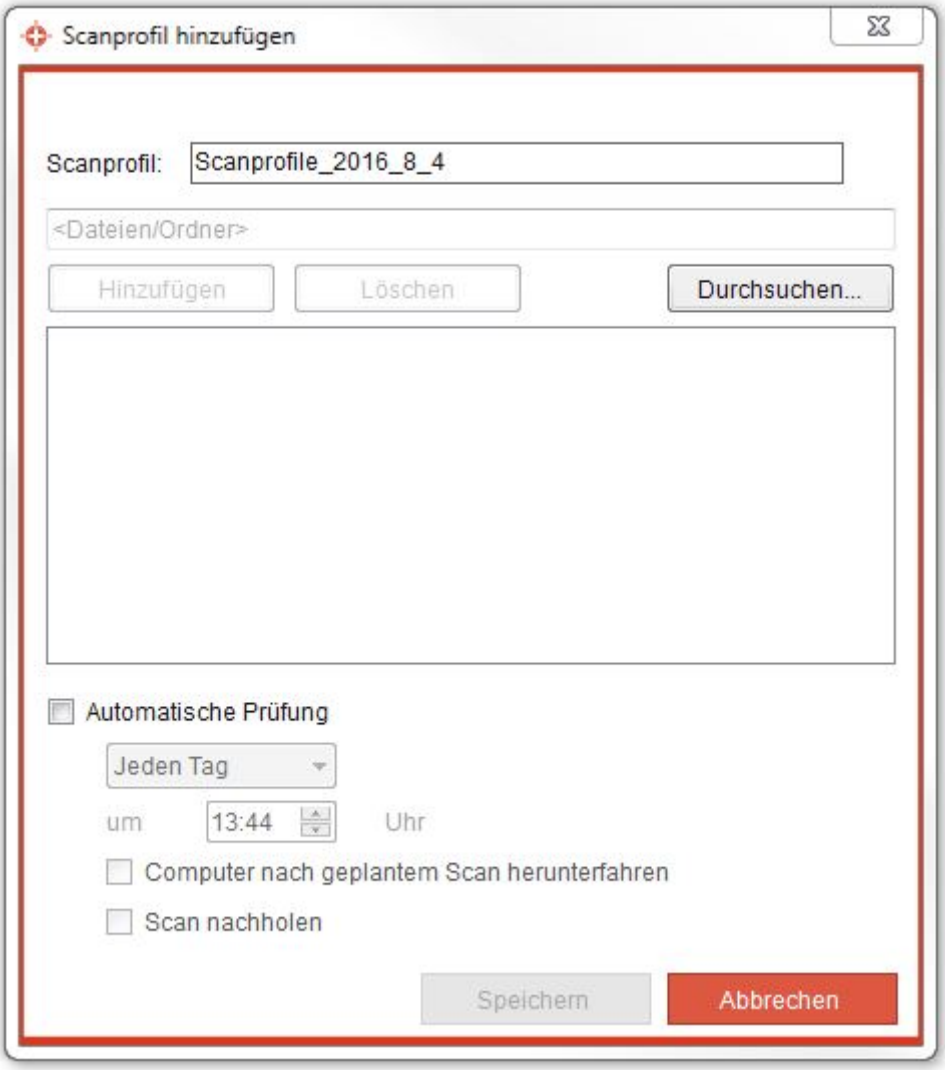


Abbildung 21: Scanprofil hinzufügen

Sie können dem Scanprofil einen beliebigen Namen geben. Mit dem Button „Durchsuchen…" wählen Sie die zu scannenden Ordner, Dateien etc. aus. Außerdem können Sie festlegen, ob Sie eine automatische Prüfung einstellen wollen.

Die automatische Prüfung kann zu einem beliebigen Zeitpunkt festgelegt werden (z.B.: jeden Freitag um 12 Uhr) und scannt dann die von Ihnen definierten Bereiche.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

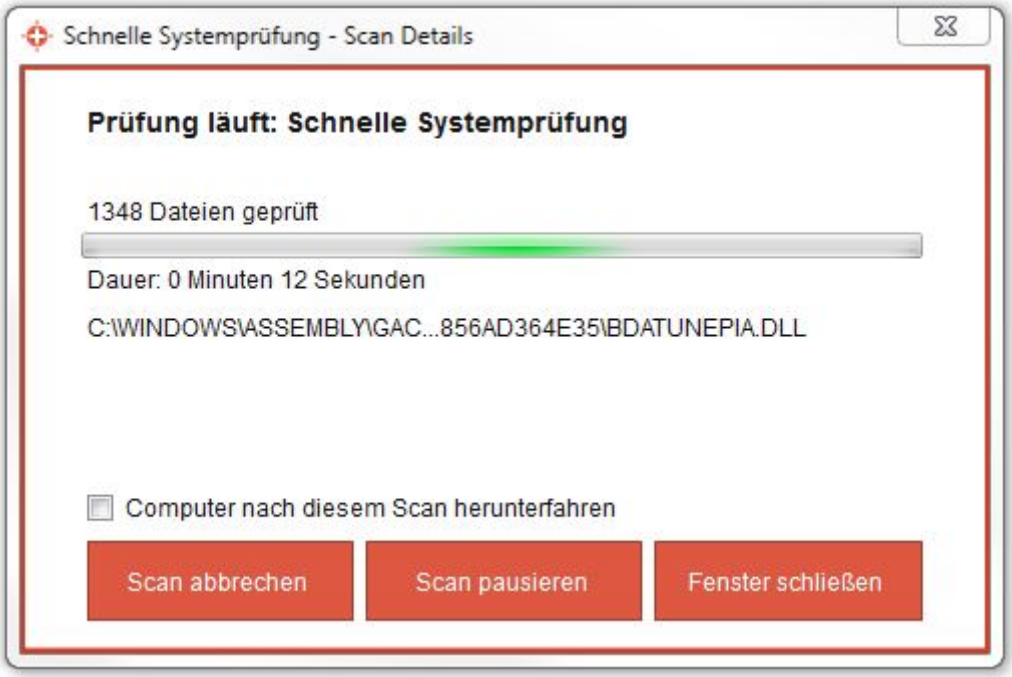


Abbildung 22: Prüfung läuft

Um einen Scan manuell zu aktivieren, klicken Sie einfach auf „Jetzt scannen".

Einen gestarteten Scan können Sie jederzeit pausieren bzw. abbrechen.

Am Fortschrittsbalken können Sie den Verlauf des Scan-Vorgangs beobachten.

Ist der Scan beendet und wurde kein Virus gefunden, kommen Sie mit Klick auf den Button „Fenster schließen" zum Hauptmenü zurück.

Was bei einem Virenfund zu tun ist, lesen Sie im Kapitel 4.4, „Quarantäne - Was tun bei Virenfund?"

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

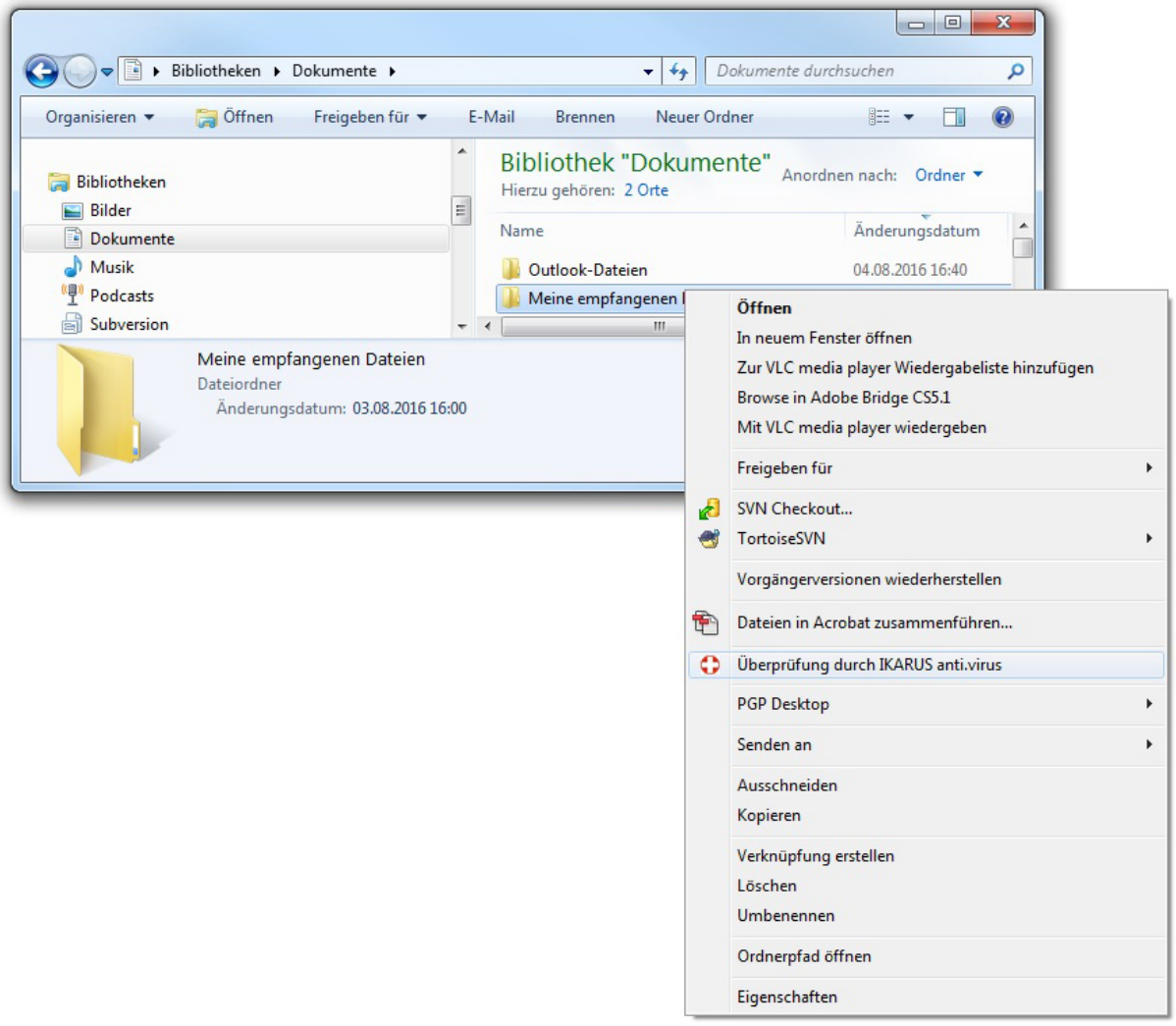


Abbildung 23: IKARUS anti.virus-Scan über Explorer starten

Eine weitere Möglichkeit, einen Scan zu starten, bietet der Windows Explorer: Wählen Sie ein Laufwerk, eine Datei oder einen Ordner aus und starten Sie über die rechte Maustaste die „Überprüfung durch IKARUS anti.virus“.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

4.3.1 Scan-Einstellungen

Über den Menüpunkt „Einstellungen” und den Reiter „Exklusionen” gelangen Sie zu den Einstellungen für den Scan.

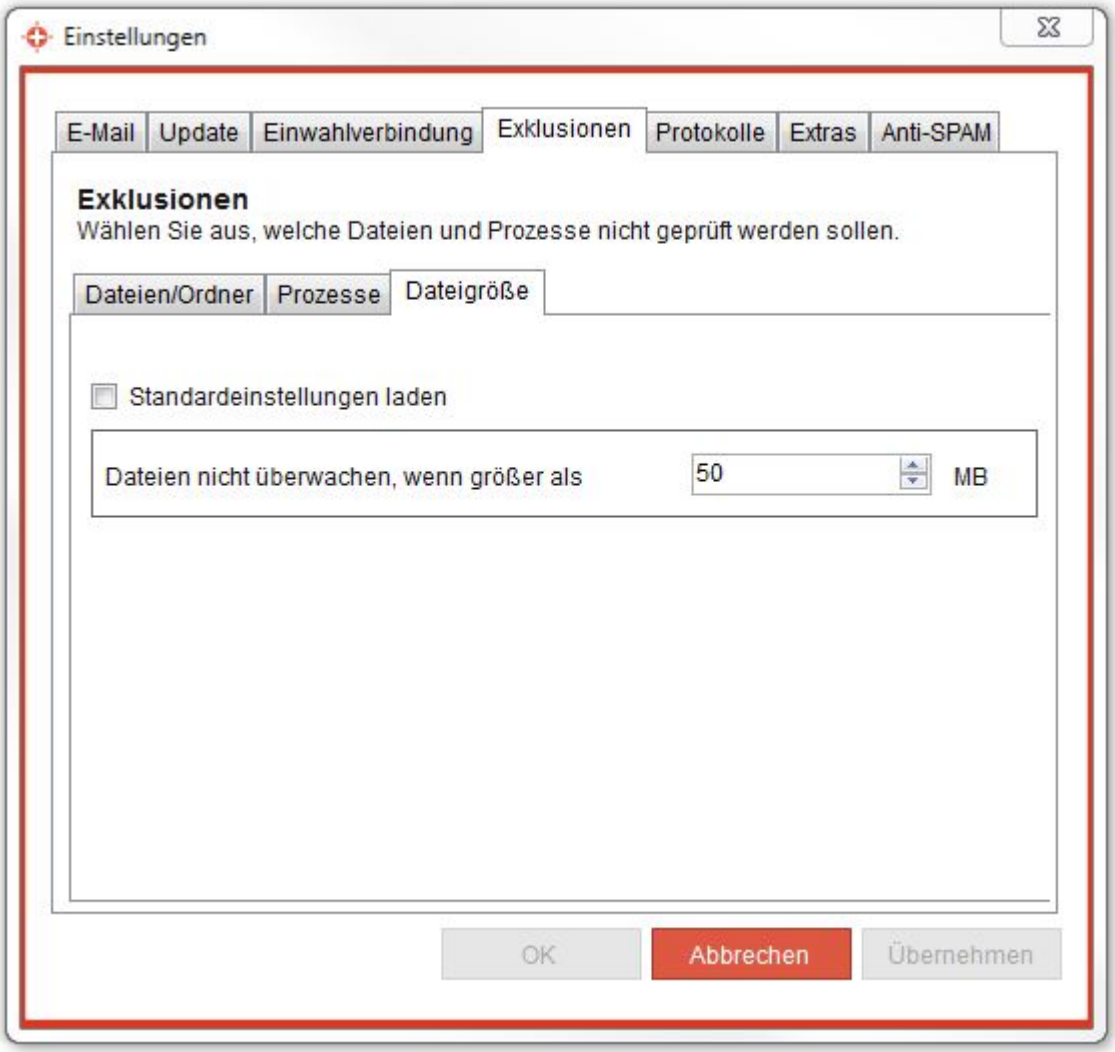


Abbildung 24: Exklusionen

Hier können Sie z.B. festlegen, welche Dateien und Prozesse von dem Scanvorgang durch IKARUS anti.virus ausgenommen werden sollen.

Ein weiteres Kriterium zur Exklusion ist die Größe einer Datei.

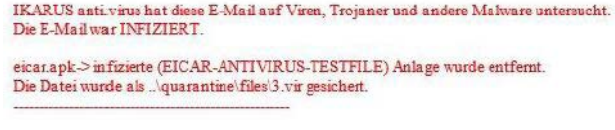
IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

4.4 Quarantäne - Was tun bei Virenfund?

Lesen Sie in diesem Kapitel, wo Sie alle gefundenen Viren einsehen und bearbeiten können. Die Quarantäne von IKARUS anti.virus bietet Ihnen verschiedene Möglichkeiten, um eine infizierte Datei sicher von Ihrem System zu entfernen.

4.4.1 Anzeigen eines Virenfundes

Einen Virenfund zeigt Ihnen IKARUS anti.virus mit folgenden Meldungen an:

Meldungen	
	Mit einem gelben Icon in der Taskleiste zeigt IKARUS anti.virus einen Virenfund an.
	Beim Empfang einer infizierten E-Mail erkennt IKARUS anti.virus das Schadprogramm. Es öffnet sich ein Fenster, in dem IKARUS anti.virusSie darüber informiert, dass ein Virus gefunden und dieser in das Quaratäneverzeichnis verschoben wurde.
	In der infizierten E-Mail selbst finden Sie bei einem Virenfund einen Text mit einem entsprechenden Hinweis auf den Virenfund.
	Im Ansichtsfenster von IKARUS anti.virus wird der Virenfund mit einem Warnsymbol im Scan-Fenster und dem Text "Ihr System ist möglicherweise infiziert! Quarantäne überprüfen!" angezeigt.

Anzeigen bei einem Virenfund

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

4.4.2 Virenfund beim Scanvorgang

Wenn Sie einen automatischen oder einen individuellen Scan gestartet haben und dabei ein Virus gefunden wird, sieht dies wie folgt aus:

- In der Taskleiste wird das gelbe Icon von IKARUS anti.virus angezeigt sowie ein Warnhinweis im Ansichtsfenster.
- Im Scanfenster erscheint während und nach der Virensuche die Meldung „1 mögliche Bedrohung gefunden".
- Nach Beendigung des Scan-Vorgangs von IKARUS anti.virus öffnet sich automatisch das Quarantäne-Fenster.

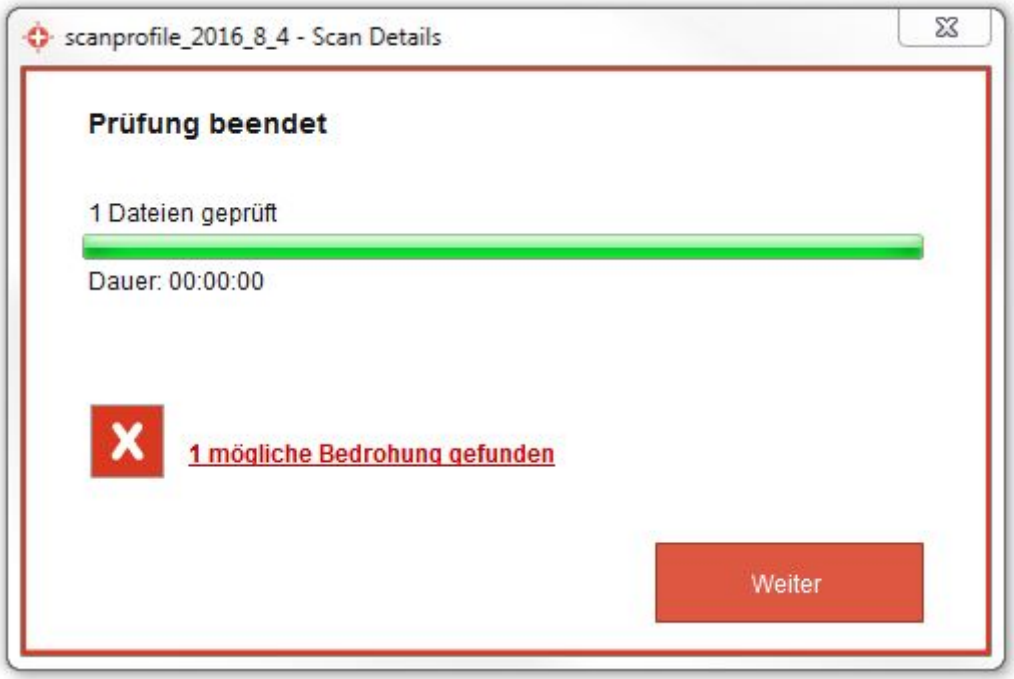


Abbildung 25: Prüfung beendet – Virus gefunden

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

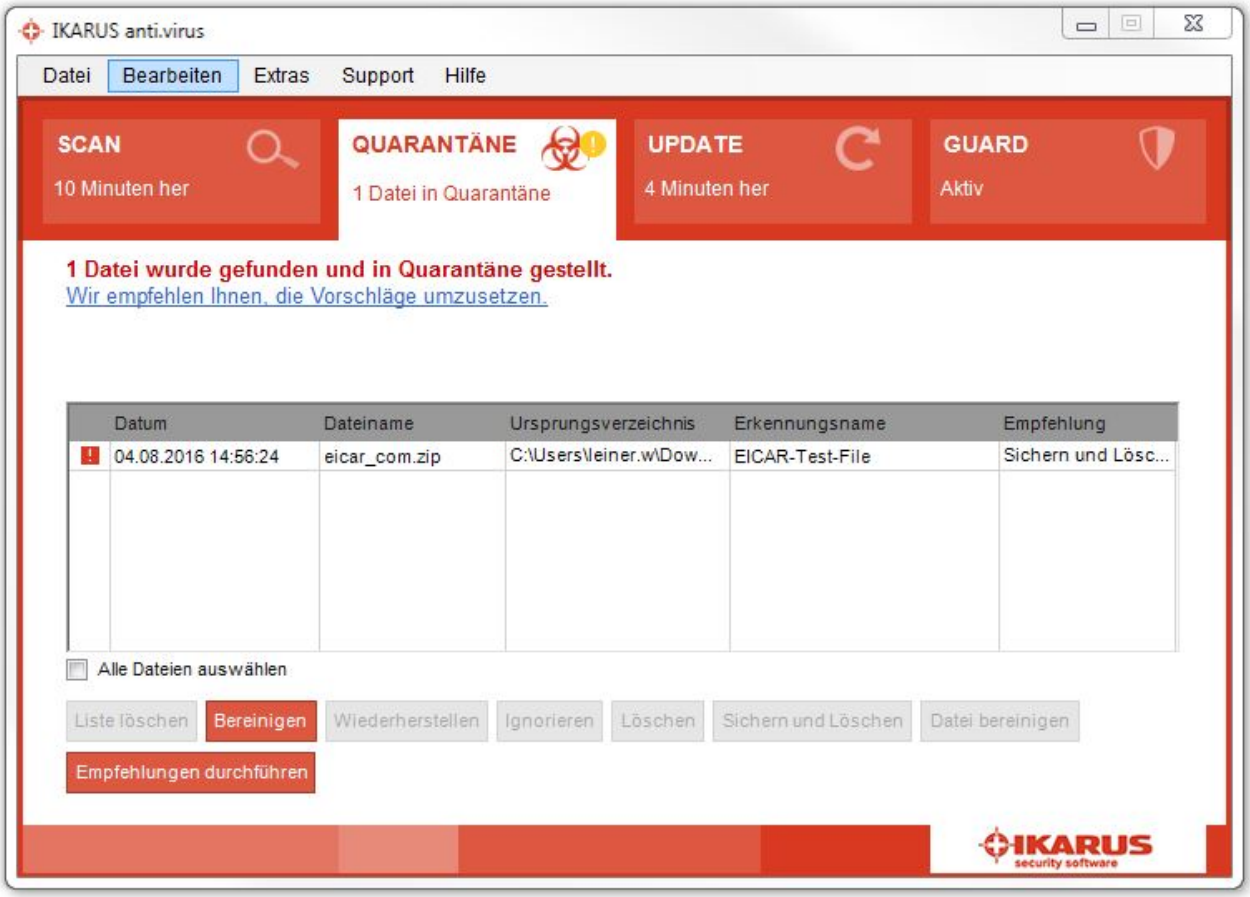


Abbildung 26: Quarantäne – Virus gefunden

4.4.3 Die Quarantäne

Ein von IKARUS anti.virus gefundenes Virus oder PUA (potentially unwanted application – potenziell unerwünschte Anwendung) wird automatisch in die Quarantäne verschoben. Viren werden in der Quarantäneliste mit einem roten Icon (Rufzeichen) ganz links in der Spalte angezeigt, während PUAs mit einem gelben Icon (Rufzeichen) gekennzeichnet werden.

Ist das Virus einmal in der Quarantäne „gefangen", geht für Ihr System keine Gefahr mehr davon aus. Sobald eine infizierte Datei in die Quarantäne verschoben wurde, wird der Zugriff darauf automatisch gesperrt. Sie kann daher ab diesem Zeitpunkt auf Ihrem PC keinen Schaden mehr verursachen.

Sie können alle Funktionen des Quarantäne-Fensters auch direkt über die Menüleiste und den Menüpunkt „Bearbeiten" durchführen.

Die Quarantäne von IKARUS anti.virus bietet Ihnen verschiedene Möglichkeiten an, wie mit dem Virus bzw. der infizierten Datei umgegangen werden soll.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Überdies gibt Ihnen IKARUS anti.virus eine Empfehlung, welche Aktion im jeweiligen Fall am sinnvollsten erscheint.

Mit Klick auf den Button „Empfehlungen durchführen" werden die von IKARUS anti.virus vorgeschlagenen Aktionen ausgeführt.

Wollen Sie den Empfehlungen von IKARUS anti.virus nicht folgen, können Sie auch andere Aktionen wählen. Mögliche Aktionen sind:

- **Bereinigen:** Die infizierte Datei wird gelöscht.
- **Ignorieren:** Die als infiziert erkannte Datei wird temporär freigegeben. Das bedeutet, dass diese Datei bis zum Neustart des Services (d.h. normalerweise bis zum Neustart des PCs) nicht mehr gemeldet wird. Dies ermöglicht Ihnen wieder den Zugriff auf diese Datei. Nach einem Neustart Ihres PCs finden Sie die Datei jedoch wieder in der Quarantäne. Nach Betätigen des Buttons werden Sie außerdem gefragt, ob Sie die infizierte Datei an IKARUS zur Analyse schicken möchten (anonym oder mit E-Mail-Adresse zur Rückmeldung)
- **Löschen:** Die markierte Datei wird gelöscht.
- **Sichern und löschen:** Die markierte Datei wird gelöscht. Gleichzeitig wird eine Sicherungskopie der Datei in Ihrem IKARUS anti.virus-Verzeichnis belassen. Der Eintrag in der Quarantäne wird danach hellgrau. Wenn gewünscht, können Sie die Datei durch Klick auf den Button „Zurück verschieben" wiederherstellen.
- **Datei bereinigen:** Wenn möglich, wird nur das Virus selbst aus der infizierten Datei entfernt. Die Datei selbst bleibt dabei bestehen und wird nicht gelöscht. Dateien, die im Grunde nur aus einem Virus bestehen, werden zur Gänze gelöscht.
- **Liste löschen:** Entfernt die Einträge aus der Quarantäneliste. Mehr als 7 Tage alte Einträge werden automatisch aus der Liste entfernt.

In der Quarantäneliste von IKARUS anti.virus können Sie jederzeit überprüfen, welche Viren bereits gefunden wurden, ob Viren gelöscht bzw. welche Aktionen durchgeführt worden sind.

Schwarze Einträge bedeuten, dass ein Virus in Quarantäne ist und noch keine Aktionen gesetzt wurden. Entscheiden Sie, welche Aktion Sie durchführen wollen, oder führen Sie die Empfehlungen von IKARUS anti.virus durch.

Graue Einträge bedeuten, dass ein Virus gelöscht oder gesichert wurde. Sie können diese Einträge mit einem Klick auf „Liste säubern" jederzeit entfernen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

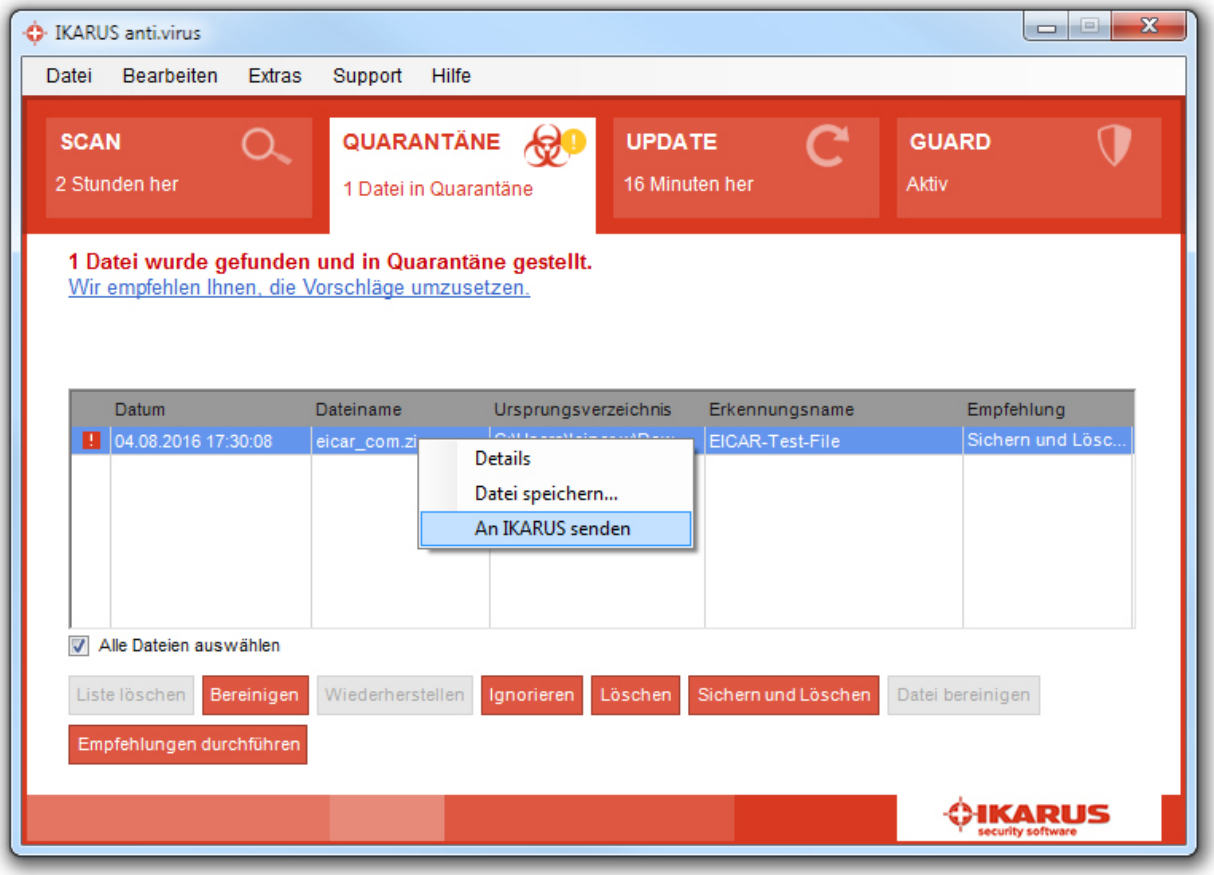


Abbildung 27: Rechtsklick auf Virus

Mit einem Klick der rechten Maustaste auf einen Vireneintrag in der Quarantäne können Sie ein Kontextmenü öffnen, in dem Sie individuelle Aktionen festlegen können.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

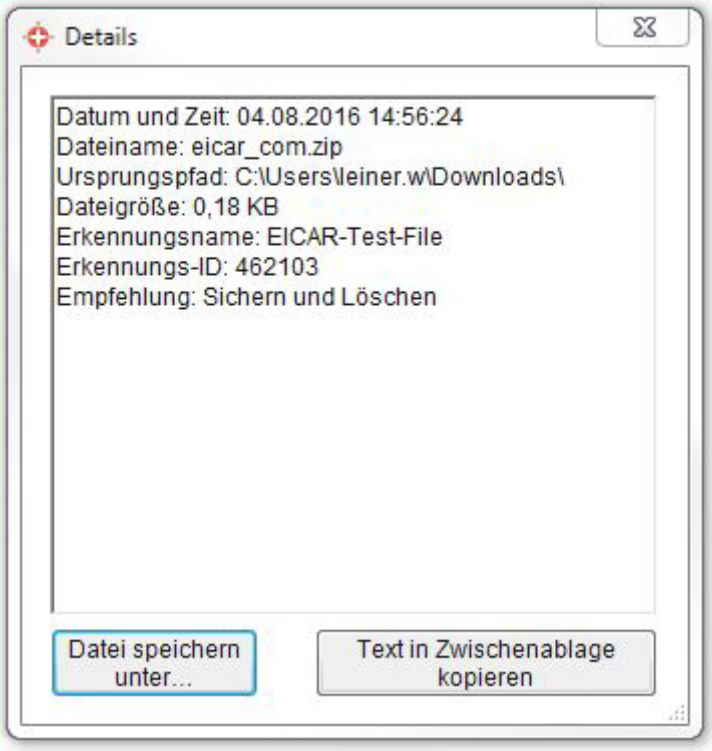


Abbildung 28: Virusinformation

Wollen Sie mehr zu einem Virus erfahren, das sich in Ihrer Quarantäne befindet, können Sie durch Doppelklick auf den Dateinamen bzw. das Ursprungsverzeichnis weitere Informationen abrufen.

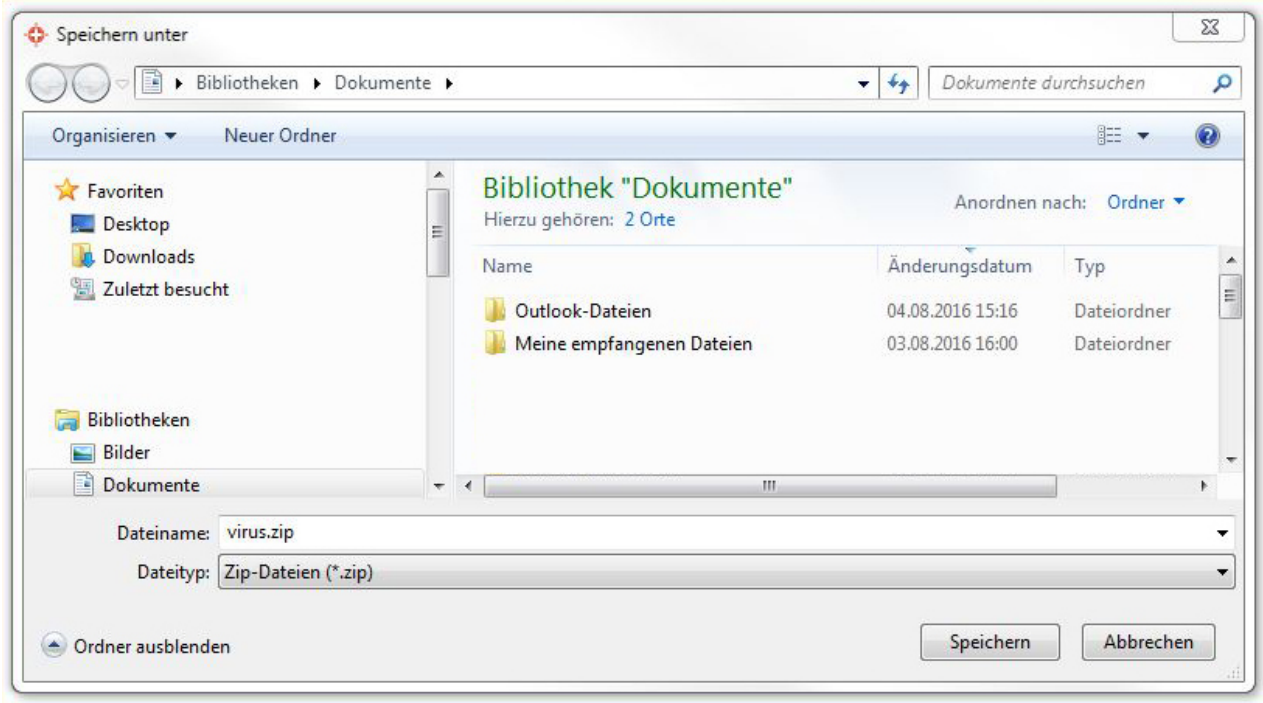


Abbildung 29: Virus speichern

Wenn Sie auf „Datei speichern” klicken, wird automatisch eine Datei „virus.zip” generiert, die Sie per E-Mail an IKARUS zur weiteren Analyse schicken können.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

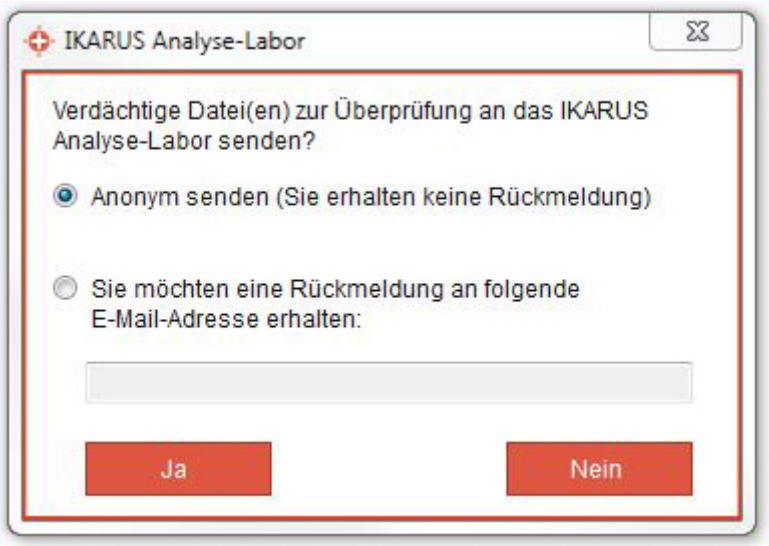


Abbildung 30: Virus zu IKARUS senden

Um die infizierte Datei automatisch an IKARUS zu senden, benützen Sie bitte die Funktion „An IKARUS senden". Sie haben die Möglichkeit, dies anonym zu tun oder eine E-Mail-Adresse anzugeben, um eine Rückmeldung zu erhalten.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

5

Zusätzliche Funktionen

5.1 Anti-SPAM

Das IKARUS Anti-SPAM-Modul ermöglicht das Filtern von E-Mails, die mittels Microsoft Outlook abgerufen werden. Um den SPAM-Schutz zu aktivieren, klicken Sie bitte in den Virenschutz-Einstellungen von IKARUS anti.virus auf die Option „Anti-SPAM".

Beim nächsten IKARUS anti.virus-Update wird die Anti-SPAM Funktion aktiviert.

Mit den beiden Reglern (gelb bzw. rot) wird festgelegt, ab welcher Bewertung eingehende E-Mails als „SPAM" bzw. „Possible SPAM" erkannt werden.

Zum Ändern der Standardeinstellung (3/7) klicken Sie in der jeweiligen Zeile (oben „Possible SPAM", unten „SPAM") auf die entsprechende farbige Markierung.

Als Aktion für E-Mails, die als SPAM bewertet wurden, lassen sich die Optionen „Mail markieren" (hier wird der Betreff mit dem Wort „SPAM" ergänzt) und „Mail verschieben" (hier wird die E-Mail in den Junk-Ordner des Mailclients verschoben) auswählen.

E-Mails, die als „POSSIBLE SPAM " erkannt wurden, werden im Betreff immer mit „POSSIBLE SPAM" gekennzeichnet und bleiben im Posteingang des Mailclients.

Unter dem Punkt „Erweiterter SPAM-Schutz" finden Sie die Möglichkeit weitere Einstellungen zu setzen, u.a. spezielle Filter zum Black- und Whitelisten von eingehenden E-Mails anhand von Sender, Empfänger, Inhalt oder Betreff.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

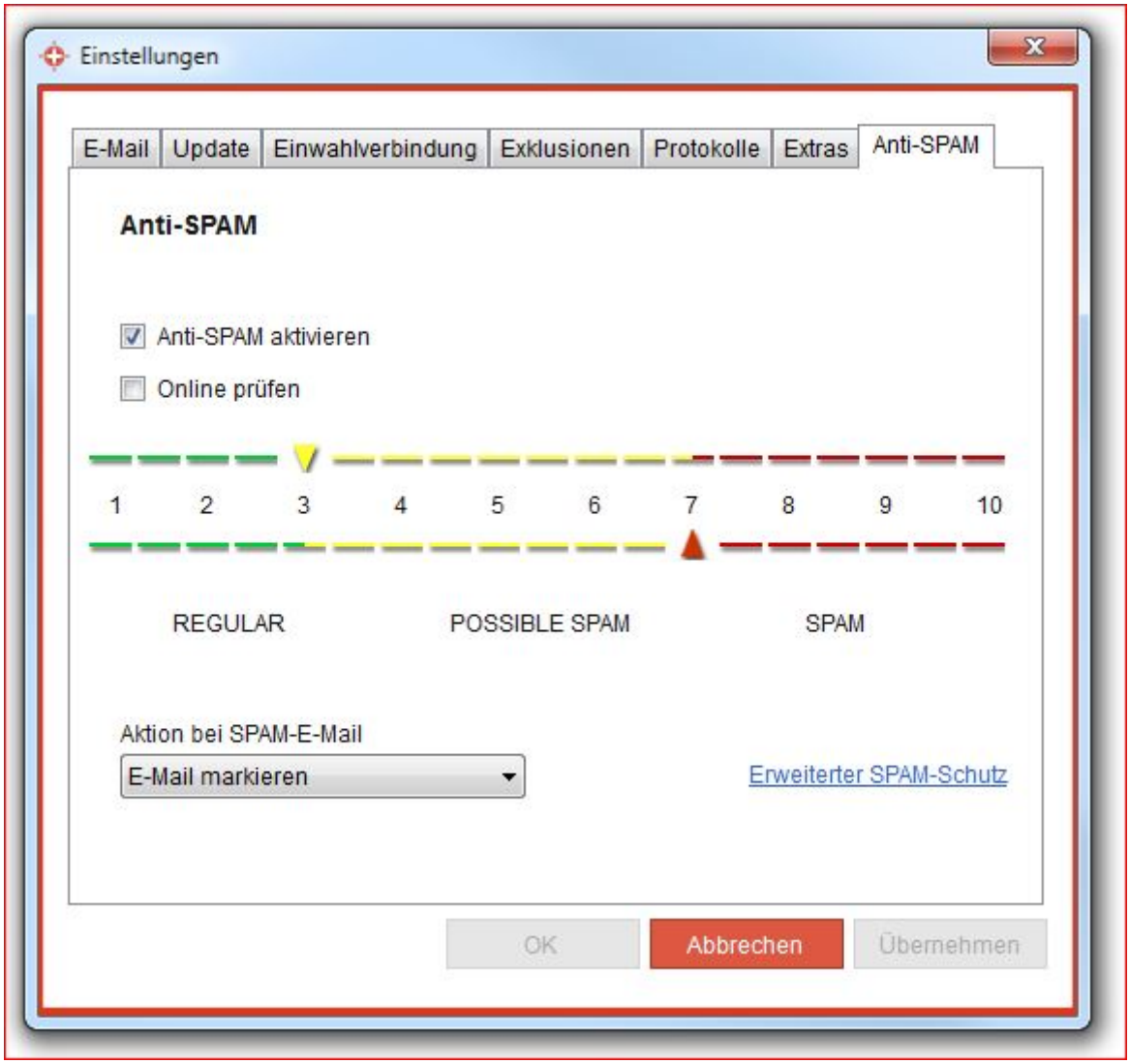


Abbildung 31: Anti-SPAM Einstellungen

Durch Bewegen der Regler nach links oder rechts können Sie die Einstellungen verändern und festlegen, ab welcher Bewertung eingehende E-Mails als *SPAM* bzw. *Possible SPAM* erkannt werden.

5.2 Microsoft-SharePoint Überwachung

Der folgende Abschnitt beschreibt die Verwendung von IKARUS anti.virus als AntiViren-Plugin für Microsoft SharePoint und wendet sich an fortgeschrittene Benutzer und Systemadministratoren.

Wenn SharePoint nicht auf Ihrem Computer installiert ist, ist dieser Abschnitt des Handbuches für Sie nicht von Bedeutung.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

5.2.1 Leistungsumfang

IKARUS anti.virus kann als AntiViren-Plugin für Microsoft SharePoint verwendet werden.
Der Schutz deckt zwei Bereiche ab:

- Dateien werden während des Uploads auf den Server gescannt, und der Upload wird unterbunden, wenn ein Virus gefunden wurde.
- Dateien werden während des Downloads vom Server gescannt, und der Download wird unterbunden, wenn ein Virus gefunden wurde.

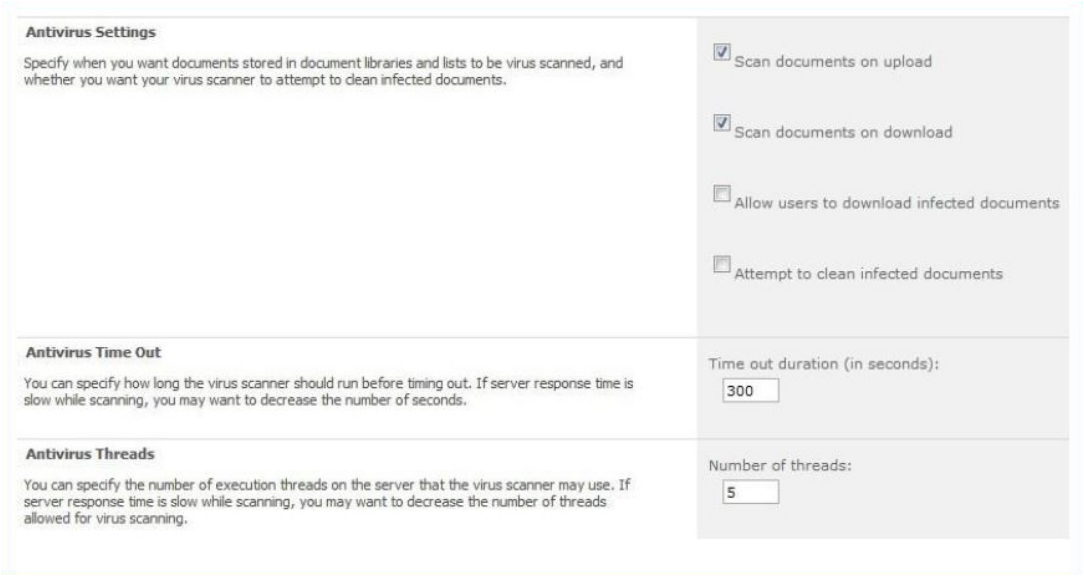


Abbildung 32: AntiVirus Settings für Microsoft SharePoint

In der Oberfläche von IKARUS anti.virus besteht nur die Möglichkeit, die SharePoint-Überwachung global zu aktivieren oder zu deaktivieren. Gesteuert wird das Plugin über die Administrationsoberfläche von Microsoft SharePoint. Zu beachten ist hier, dass die Option „Attempt to clean infected documents" von IKARUS anti.virus nicht unterstützt wird und daher in jedem Fall wirkungslos bleibt.

WICHTIG: Das IKARUS anti.virus-Plugin erfordert SharePoint Server Version 2007 oder höher und setzt ein 64-bit Betriebssystem voraus.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

5.2.2 Installation

Führen Sie die Installation von IKARUS anti.virus durch, wie in Kapitel 2 beschrieben. IKARUS anti.virus erkennt einen bereits installierten Microsoft SharePoint automatisch, aber Sie müssen nach erfolgter Installation dennoch den Microsoft IIS neu starten, um die Registrierung des Plugins abzuschließen. Ebenso müssen Sie den Microsoft IIS neu starten, um nach einer eventuellen Deinstallation von IKARUS anti.virus die Reregistrierung des Plugins abzuschließen.

Beachten Sie außerdem, dass die Installation nur dann erfolgreich ist, wenn nicht bereits eine andere AntiViren-Software mit SharePoint-Unterstützung auf Ihrem Rechner installiert wurde.

Für die Client-Rechner, die sich mit Ihrem SharePoint-Server verbinden, ist keinerlei weitere Konfiguration nötig!

5.2.3 Arbeitsweise

In den Standardeinstellungen von SharePoint und IKARUS anti.virus wird jede hochgeladene oder heruntergeladene Datei einer Virenprüfung unterzogen. Wenn das Untersuchungsergebnis negativ ist, die Datei also nicht infiziert ist, bemerkt der Endbenutzer auf seinem Clientrechner nichts von diesem Vorgang und kann seine Arbeit ungestört fortsetzen.

Wird von IKARUS anti.virus jedoch ein Virus gefunden, wird die laufende Aktion unterbunden, und der Benutzer wird über ein Dialogfenster im Webbrowser informiert.

Abbildung 33: Meldung über Virusfund beim Upload

Die Abbildung zeigt das Dialogfenster, das dem SharePoint-Endbenutzer angezeigt wird, wenn IKARUS anti.virus in der hochzuladenden Datei einen Virus gefunden hat.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Abbildung 34: Meldung über Virusfund beim Download

Hier hingegen das Dialogfenster, das beim Download einer infizierten Datei erscheint, wenn am SharePoint die Option „Scan documents on download" aktiviert und die Option „Allow users to download infected documents" deaktiviert ist.

SharePoint stellt es dem Server-Administrator frei, das Scannen von Uploads und Downloads separat zu aktivieren oder zu deaktivieren. Wenn eine dieser beiden Optionen deaktiviert ist, führt also auch IKARUS anti.virus keine entsprechende Virenprüfung mehr durch. In der IKARUS anti.virus-Benutzeroberfläche wird der Status der beiden Optionen als Zusatzinformation angezeigt; geändert werden können sie jedoch nur direkt in der Administrationsoberfläche von SharePoint.

IKARUS anti.virus bietet die Möglichkeit, den SharePoint-Schutz komplett auszuschalten. In diesem Fall werden weder Uploads noch Downloads gescannt.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

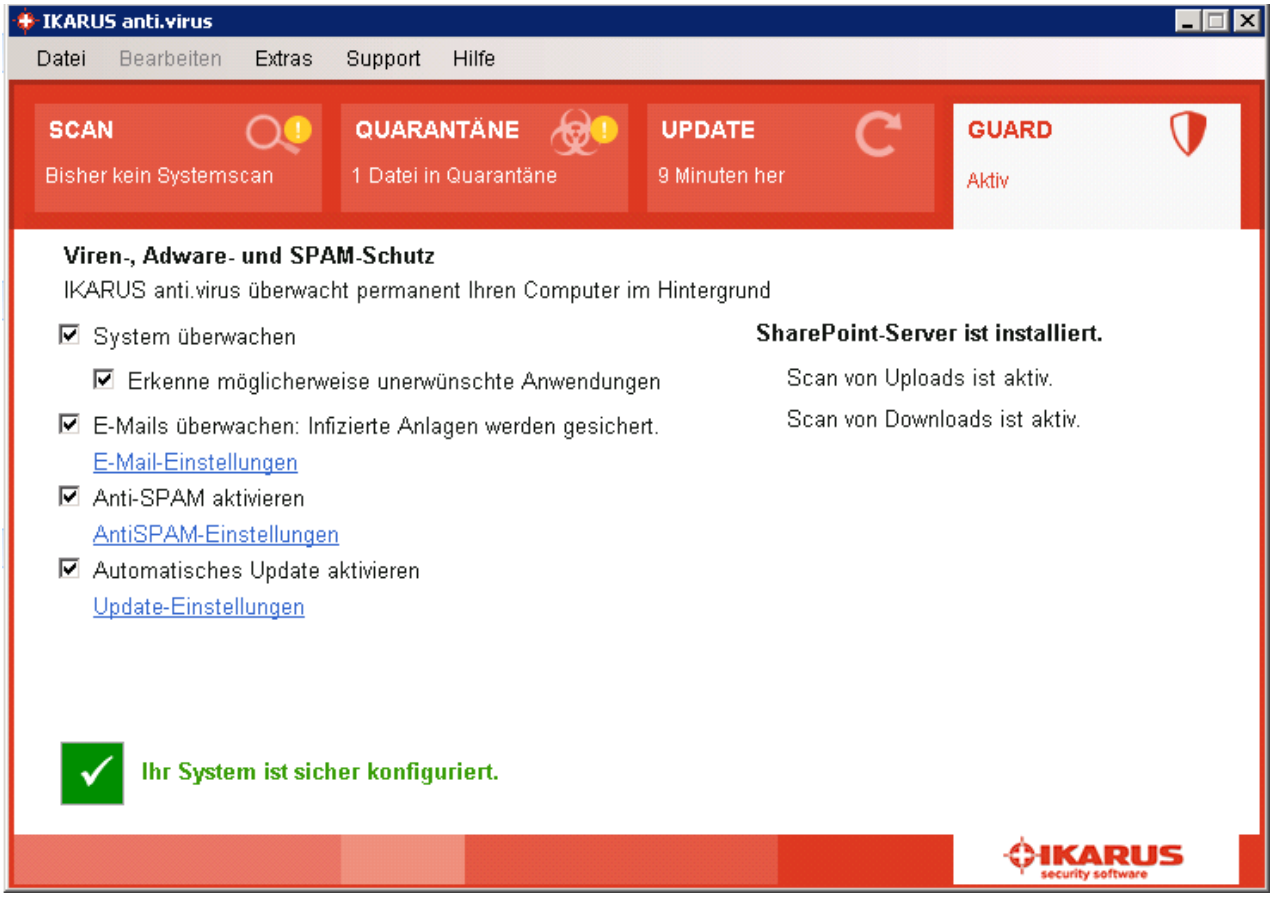


Abbildung 35: SharePoint-Einstellungen IKARUS anti.virus

Die Abbildung zeigt die Statusinfo „SharePoint-Server ist installiert“. Es wird der aktuelle Status von Upload- und Download-Scanning dargestellt.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

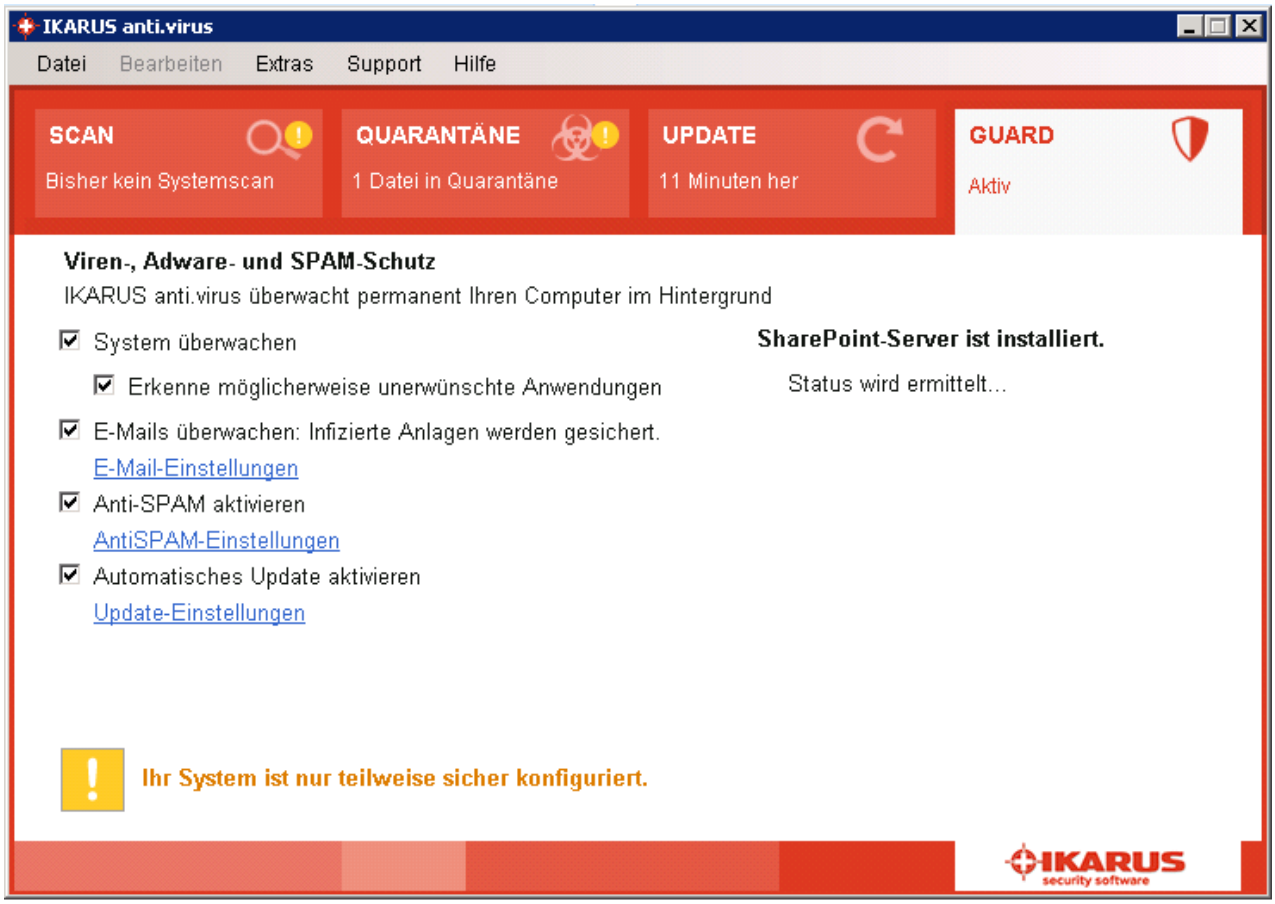


Abbildung 36: SharePoint-Einstellungen – Status wird ermittelt

Es kann unter Umständen einige Augenblicke dauern, bis diese Einstellungen überprüft sind. In diesem Fall wird vorübergehend „Status wird ermittelt...“ angezeigt.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

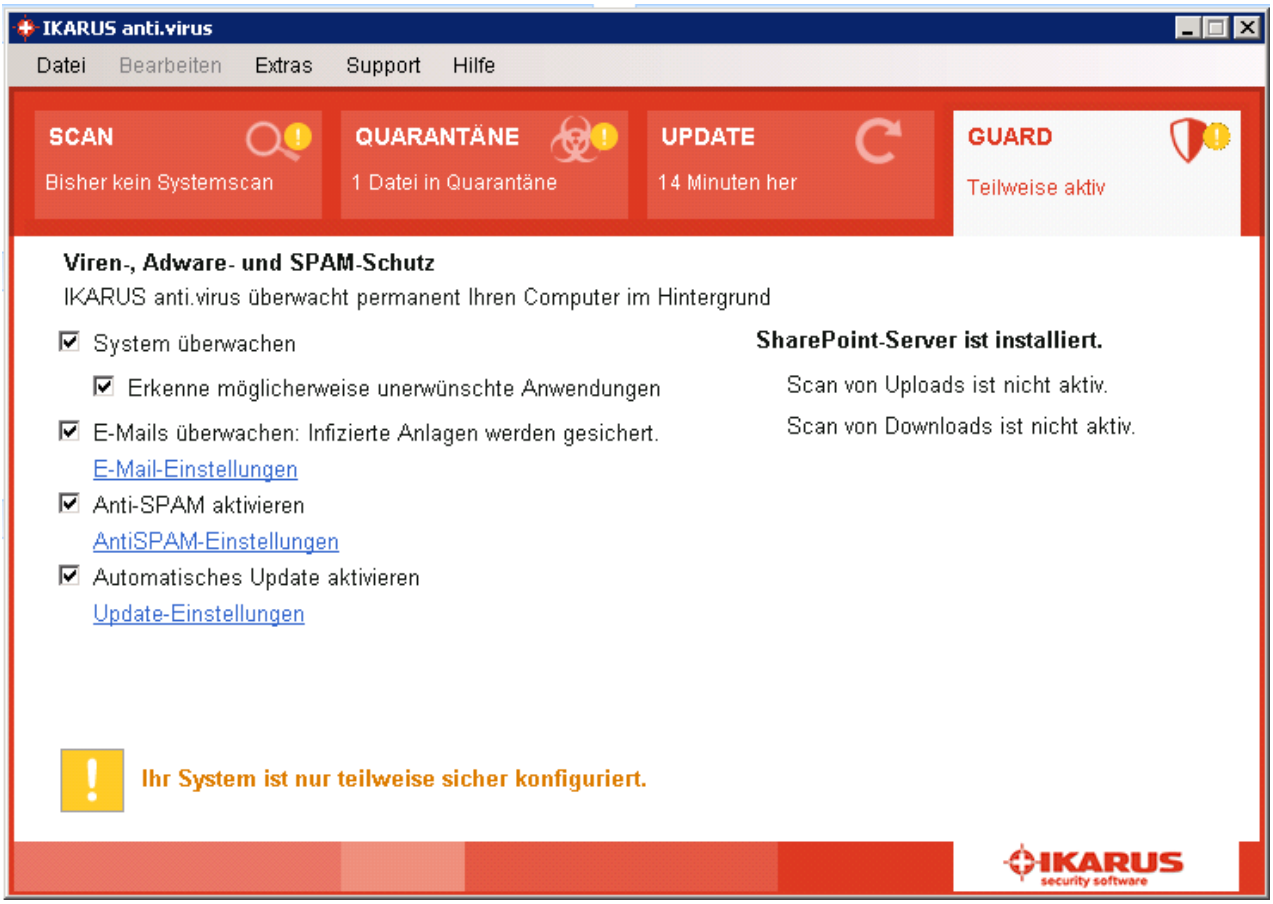


Abbildung 37: SharePoint-Schutz ausgeschaltet

Diese Abbildung zeigt, dass bei deaktivierter SharePoint-Überwachung die Anzeigen von Upload- und Download-Status auf „nicht aktiv“ wechseln. Damit ist der Systemschutz nicht mehr vollständig gegeben, was sich in der Anzeige des orangen Warnsymbols und dem Hinweis „Ihr System ist nur teilweise sicher konfiguriert“ äußert.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

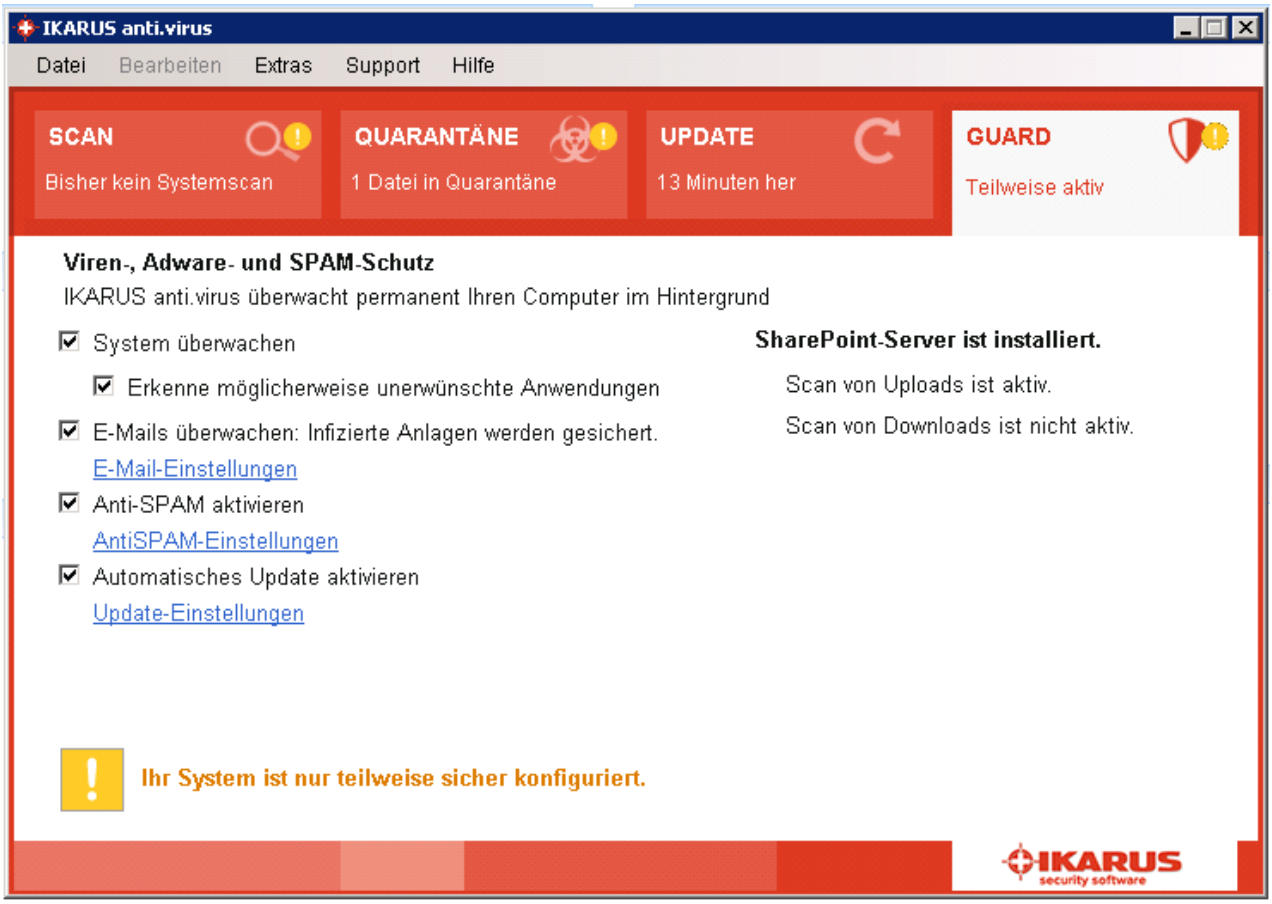


Abbildung 38: SharePoint-Schutz nicht komplett

Derselbe Gesamtsystemstatus ist auch dann gegeben, wenn in der Administrationsoberfläche von SharePoint zumindest eine der beiden Optionen für Upload- oder Download-Scanning deaktiviert ist.

Sollten mit IKARUS anti.virus unerwartete Probleme auftreten, können keine SharePoint-Dateien gescannt werden. In diesem Fall werden aus Sicherheitsgründen der Upload und Download komplett unterbunden, so fern die jeweilige Scan-Option am SharePoint aktiviert ist. Für den SharePoint-Endbenutzer am Clientrechner äußert sich dieses Problem in folgender Fehlermeldung: „installed virus scanner is currently unavailable. If the problem persists, contact your administrator."

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

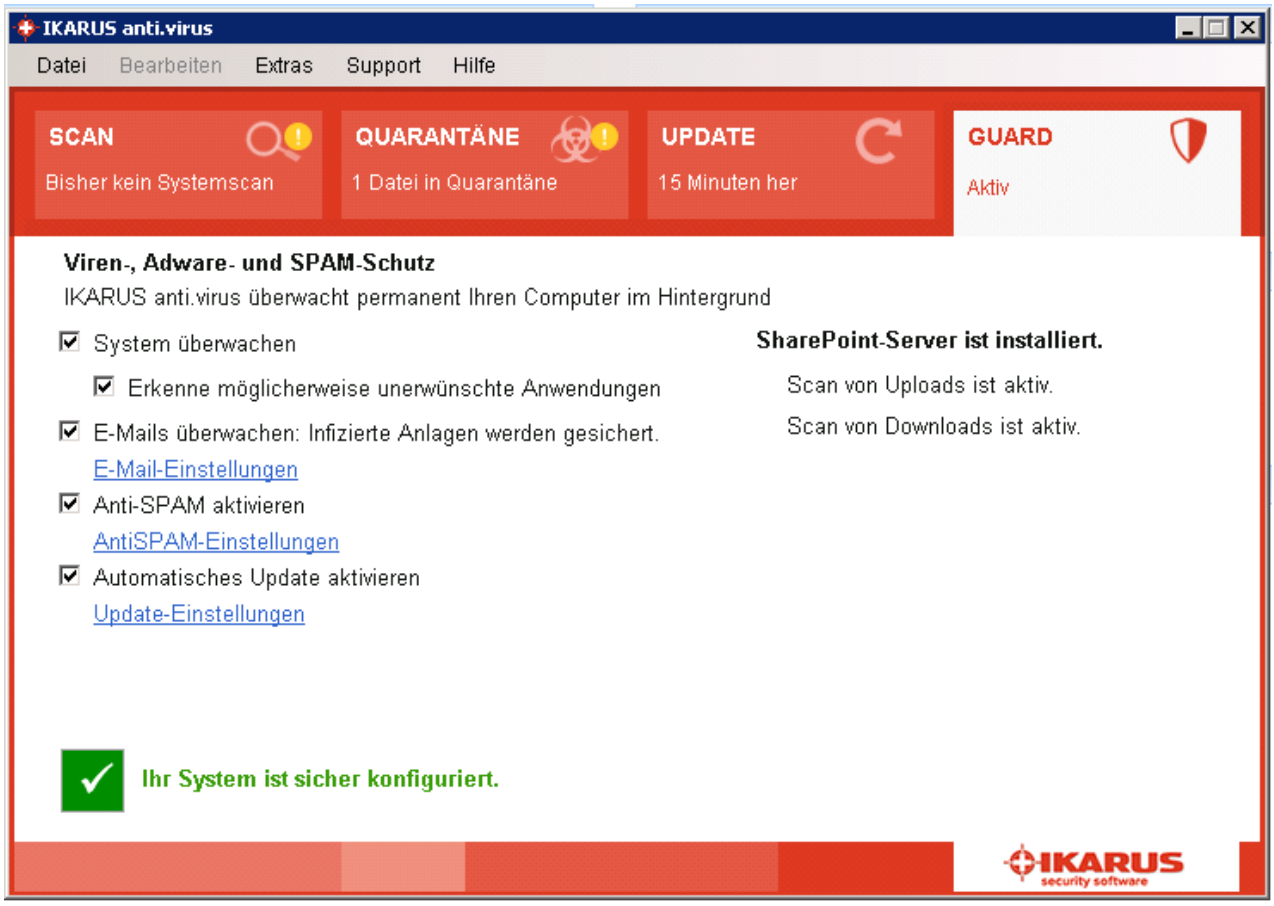


Abbildung 39: SharePoint-Schutz ist komplett

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6

Einstellungen

6.1 Spracheinstellungen

IKARUS anti.virus kann in unterschiedlichen Sprachen verwendet werden. Bei der Installation wird die Sprache anhand der Einstellungen des PCs ermittelt.

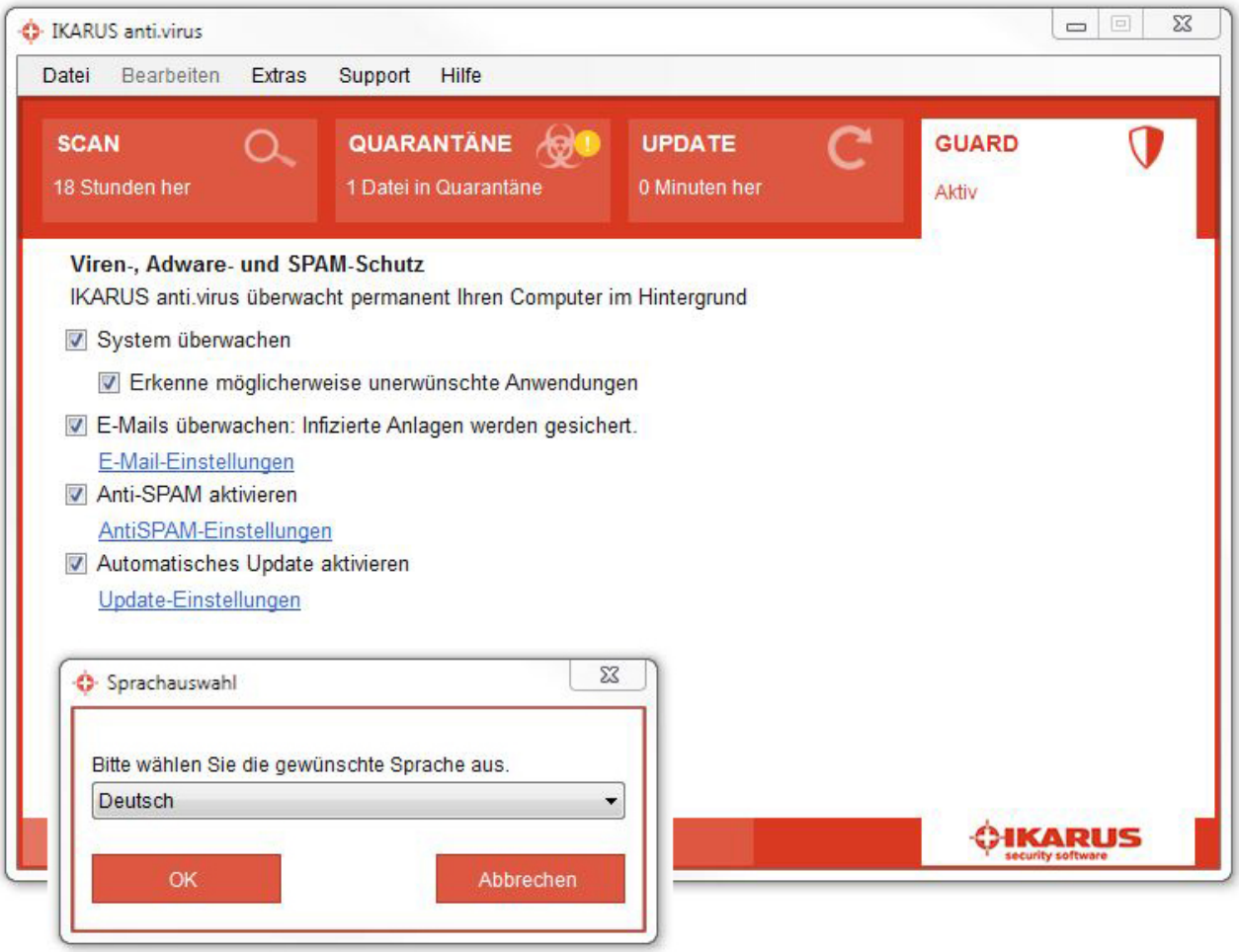


Abbildung 40: Spracheinstellungen

Während des Betriebes können Sie die verwendete Sprache über den Menüpunkt „Extras/Sprache" ändern.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Nach einem Neustart von IKARUS anti.virus steht die Anzeige in dieser Sprache zur Verfügung. Derzeit werden folgenden Sprachen unterstützt:

- Deutsch
- Englisch
- Kroatisch
- Italienisch
- Russisch

6.2 Protokolle

Im Menüpunkt „Extras/Protokoll" können Sie auswählen, welche Protokolle von durchgeführten Aktionen Sie anzeigen wollen. Im Protokollfenster werden die letzten Aktionen von IKARUS anti.virus angezeigt.

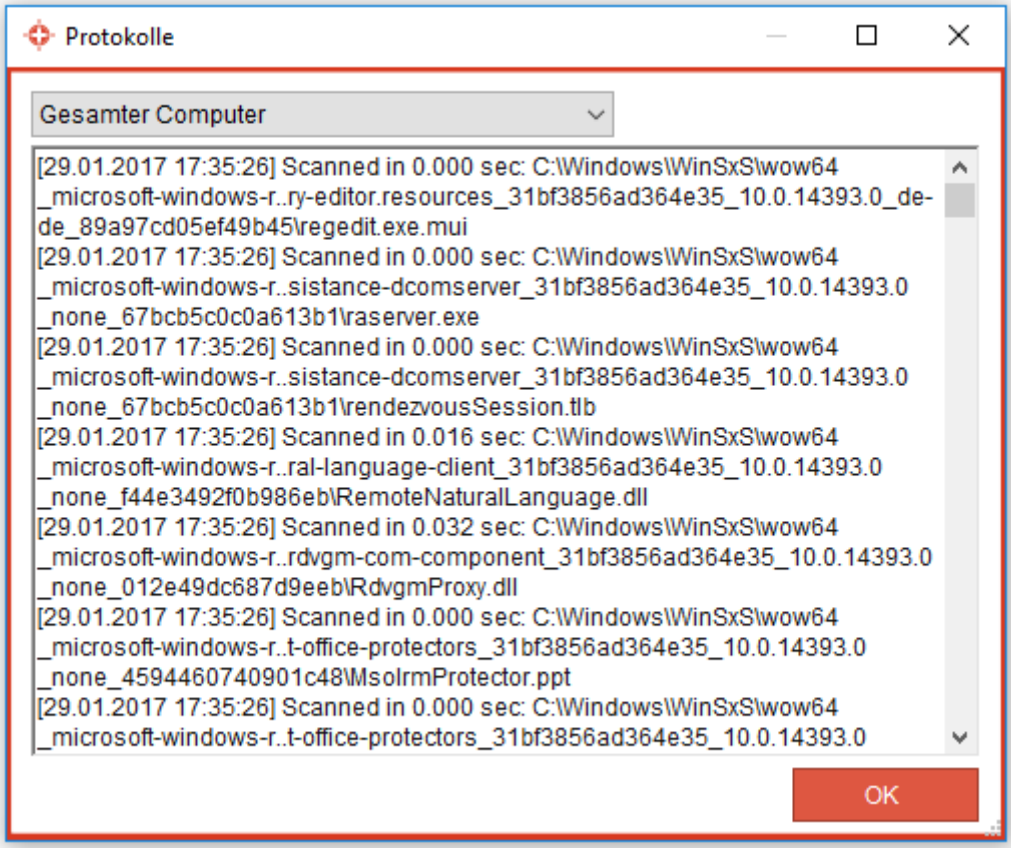


Abbildung 41: Protokolle durchgeführter Aktionen

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Diese Aufzeichnungen sind für Sie eine wesentliche Hilfestellung beim Kontakt mit der IKARUS Support-Hotline (siehe Kapitel 7). Sie können auch selbst in den Protokollen nachsehen und überprüfen, welche Aktionen von IKARUS anti.virus durchgeführt wurden.

6.3 Weitere Einstellungen

IKARUS anti.virus bietet Ihnen im Menü „Extras/Einstellungen" einen Dialog zur Konfiguration an. In dem Dialog sind die Einstellungsmöglichkeiten über Registerkarten nach Themenbereichen gegliedert.

6.3.1 E-Mail

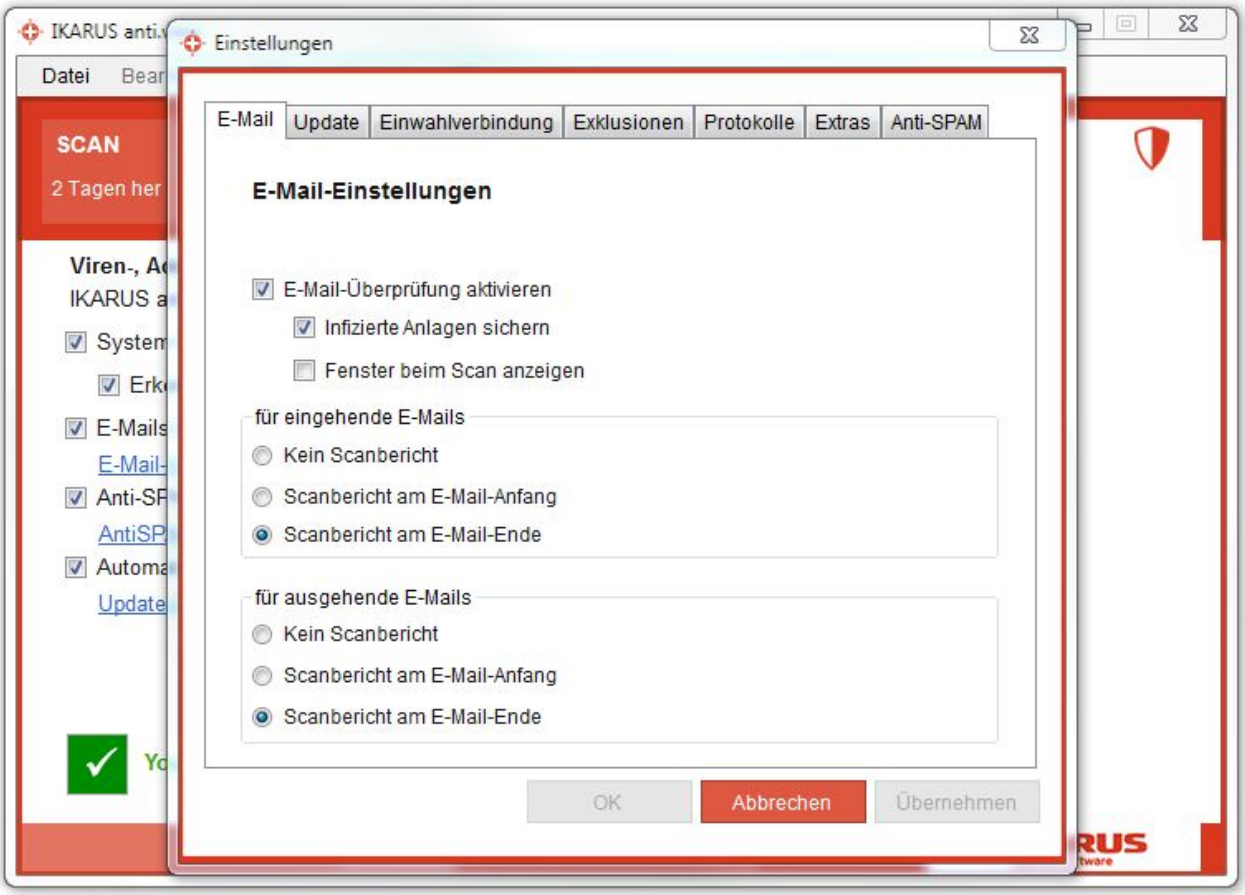


Abbildung 42: E-Mail Einstellungen

Auf der Registerkarte „E-Mail" können Sie die E-Mail-Überprüfung aktivieren und einstellen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6.3.2 Update

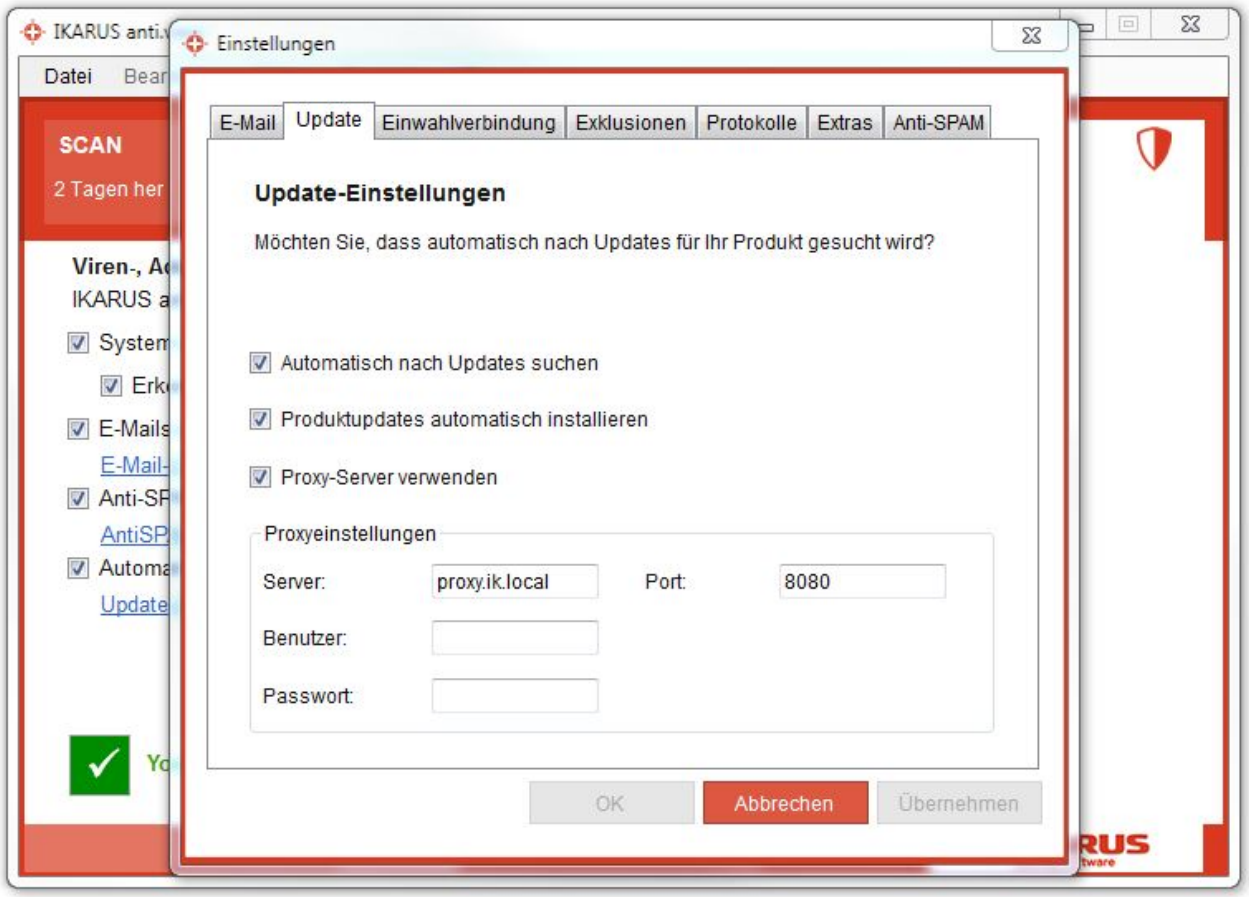


Abbildung 43: Update-Einstellungen

Die Registerkarte „Update" zeigt Ihnen die verschiedenen Auswahlmöglichkeiten zum IKARUS anti.virus-Update.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6.3.3 Internetverbindung

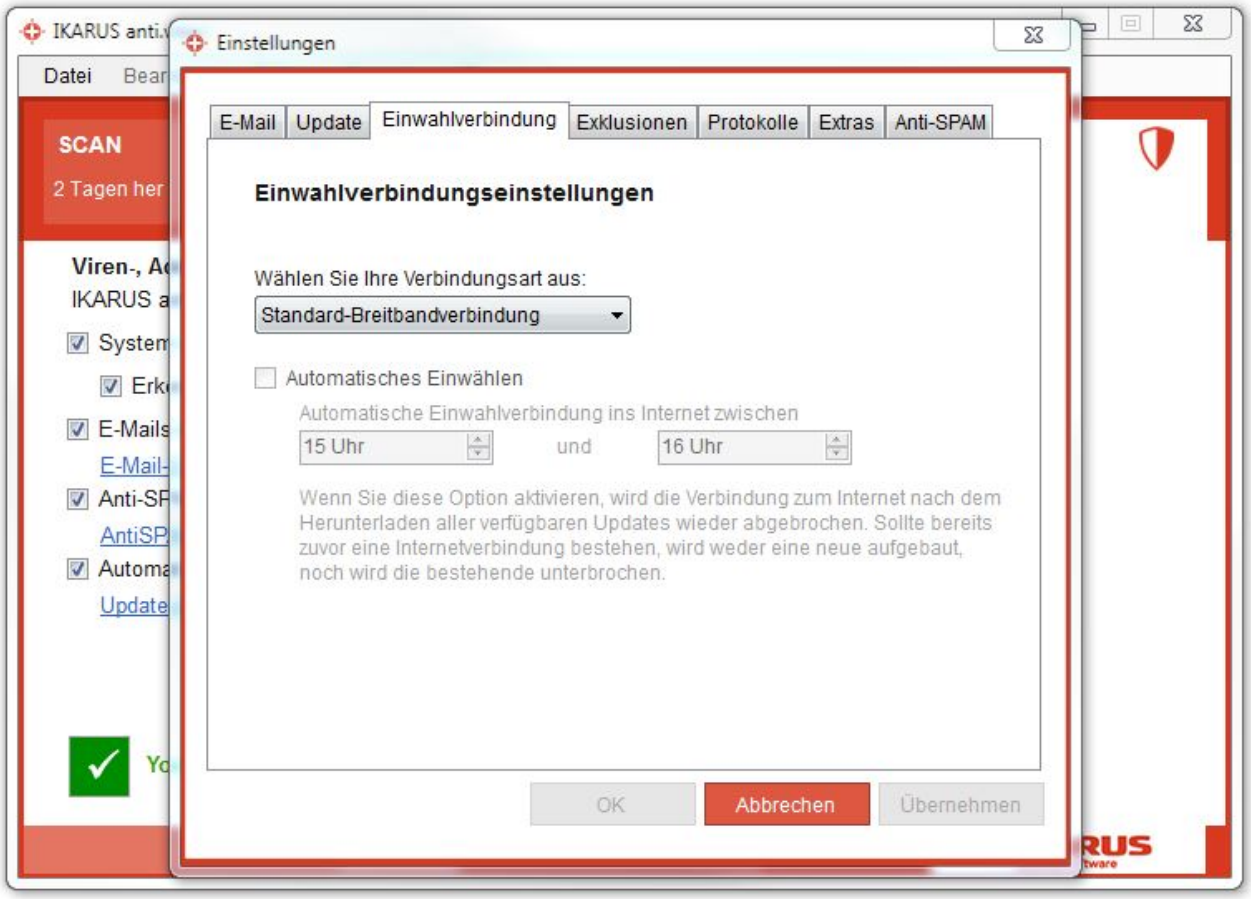


Abbildung 44: Internetverbindung-Einstellungen

Auf dem Registerblatt „Einwahlverbindung" stellen Sie die automatische Einwahl beim Update von IKARUS anti.virus ein. Hier können Sie einen Zeitraum auswählen, in welchem sich das AutoUpdate (bei Auswahl einer DFÜ-Verbindung) auch selbständig einwählen darf.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6.3.4 Exklusionen

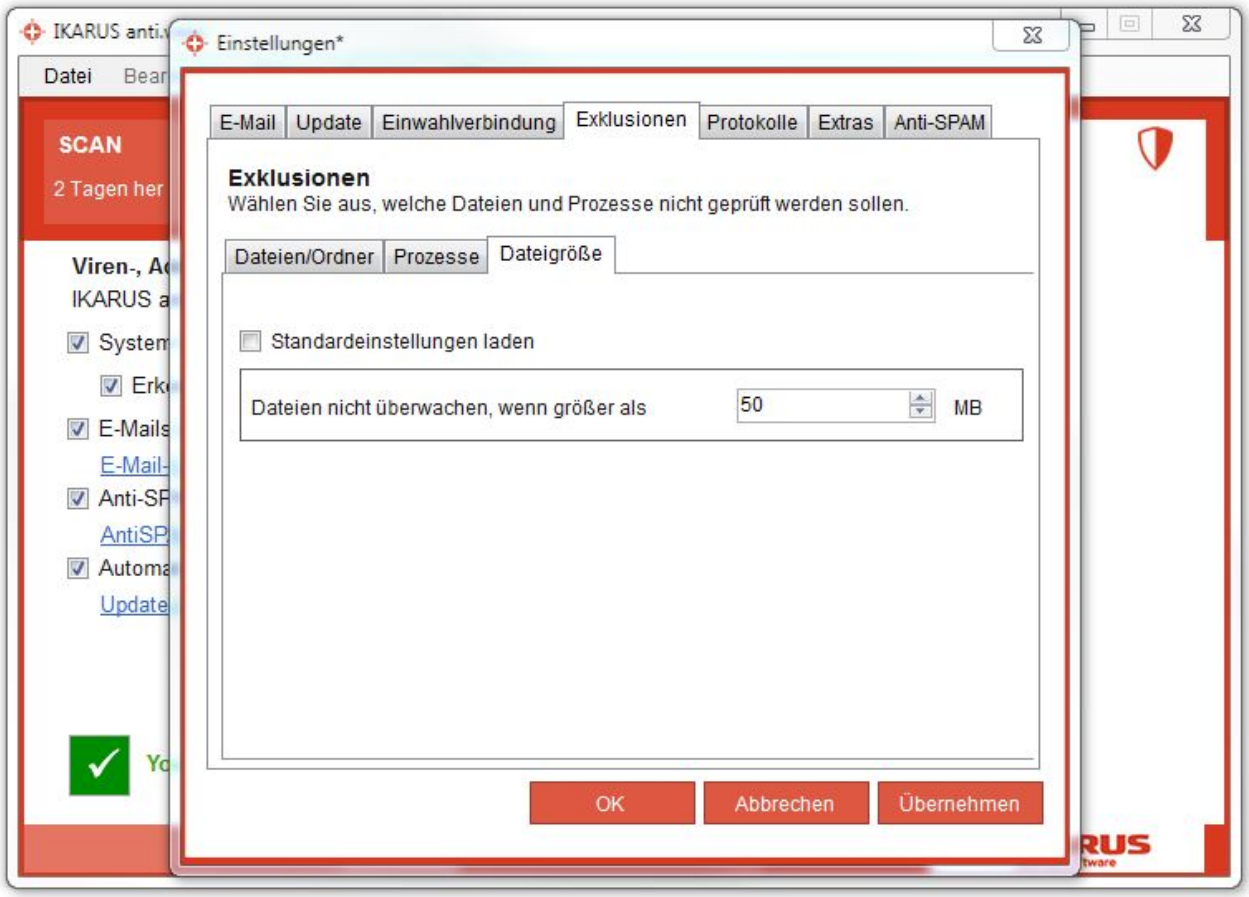


Abbildung 45: Exklusionen-Einstellungen

Auf der Registerkarte „Exklusionen" können Sie auswählen, welche Dateien und Prozesse von der Prüfung durch IKARUS anti.virus ausgenommen sind. Diese Option kann für Sie von Vorteil sein, wenn Sie einen Dienst von der Prüfung ausnehmen wollen, der ohnedies schon genug Leistung Ihres PCs in Anspruch nimmt oder wenn ein Verzeichnis keinesfalls gescannt werden soll (MP3, Urlaubsfotos etc.).

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6.3.5 Protokolle

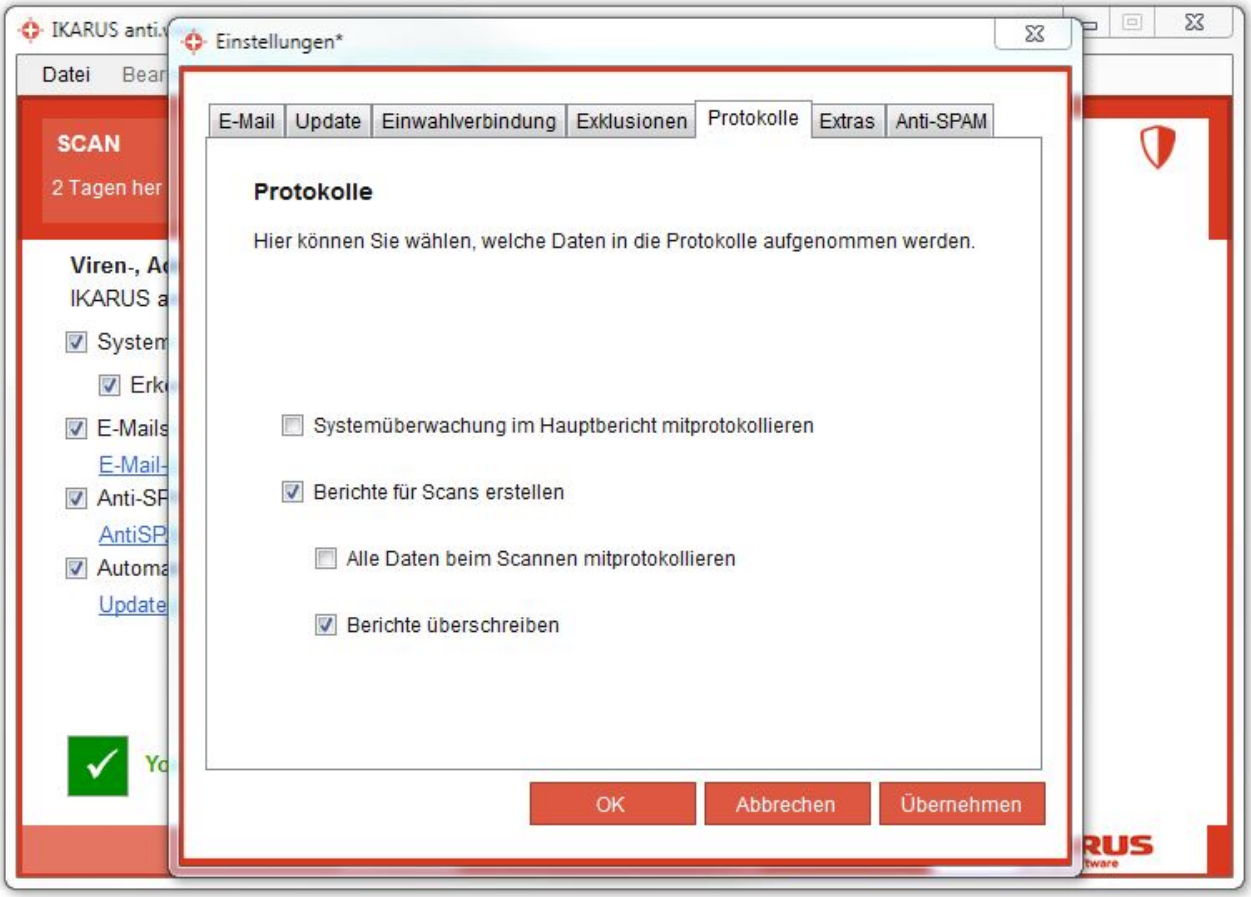


Abbildung 46: Protokolle-Einstellungen

Auf der Registerkarte „Protokolle" wählen Sie aus, welche Aktionen IKARUS anti.virus mitprotokollieren soll.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6.3.6 Extras

Auf der Registerkarte „Extras” können Sie einige zusätzliche Einstellungen vornehmen.

- Es kann festgelegt werden, dass nach einem Neustart Ihres PCs die Systemüberwachung automatisch wieder aktiviert wird.
- Sie können an dem Programm zur Signatur-Qualitätssicherung teilnehmen. Dabei werden an IKARUS statistische Informationen zur Verbesserung der Virenerkennung auf Ihrem System übermittelt. Beachten Sie diesbezüglich die Lizenzbestimmungen im Kapitel 8.3.
- Es besteht die Möglichkeit, einen Passwortschutz zu aktivieren. Ist dieser Schutz aktiviert, so können die Einstellungen von IKARUS anti.virus nur nach Eingabe des Passwortes geändert werden. Diese Option ist vor allem dann hilfreich, wenn Sie als Administrator eines Computers verhindern wollen, dass nichtberechtigte Benutzer Änderungen an den Einstellungen vornehmen. Dieser Passwortschutz gilt auch für das Aktivieren bzw. Deaktivieren der Systemüberwachung.

Mit dem Button „Auf Standardeinstellungen zurücksetzen” werden alle Ihre Änderungen rückgängig gemacht und IKARUS anti.virus wird auf den Zustand nach der Installation zurückgesetzt.

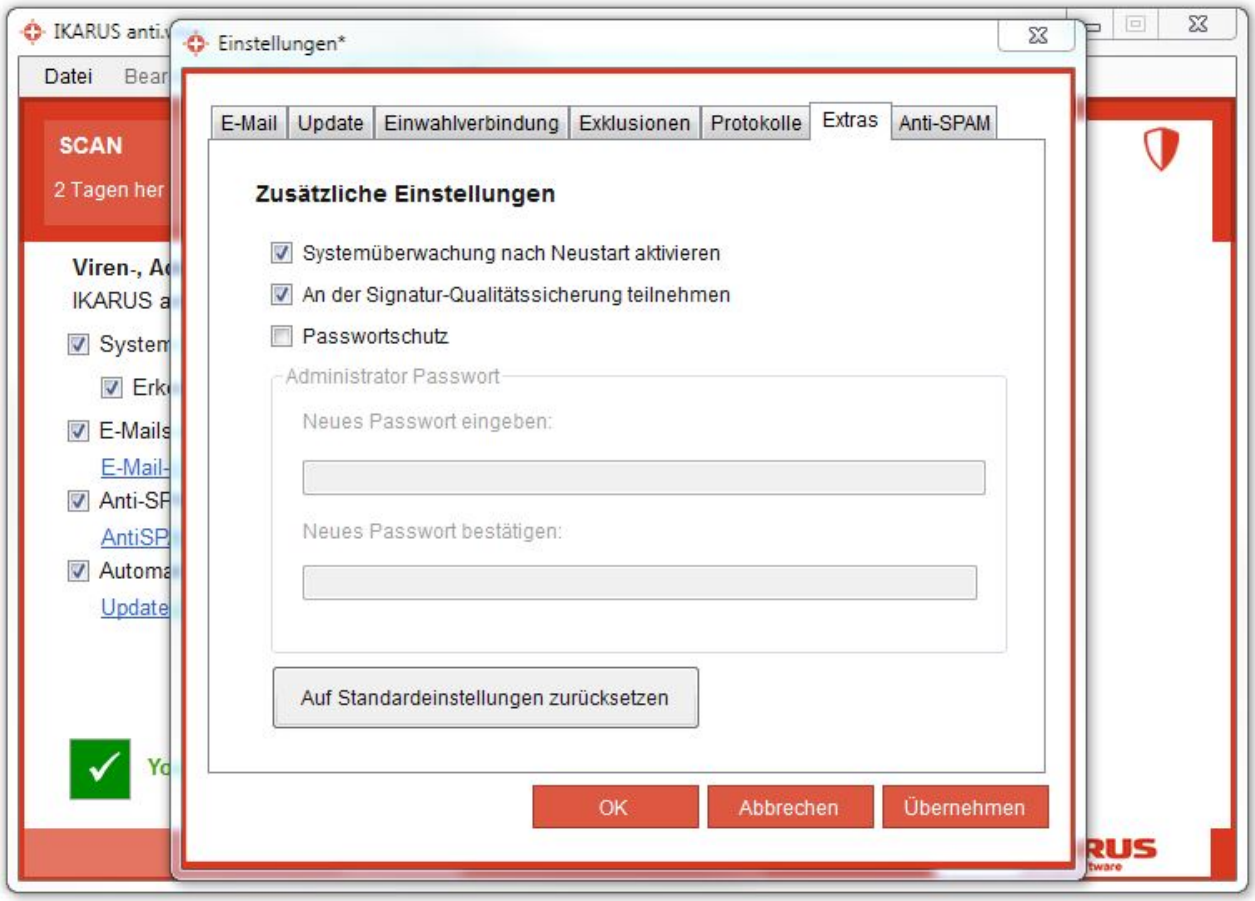


Abbildung 47: Extras-Einstellungen

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

6.3.7 Anti-SPAM

Auf der Registerkarte „Anti-SPAM” finden Sie die Einstellungen für das IKARUS anti.virus Anti-SPAM-Modul. Weitere Informationen hierzu finden Sie im Kapitel 5.1, Anti-SPAM.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

7

Support

Für Anfragen und Rücksprache mit IKARUS ist es hilfreich, detaillierte Informationen über die installierte Version von IKARUS anti.virus zu erhalten.

Um die Kontaktaufnahme so effizient wie möglich anzubieten, haben wir eine Kontaktmöglichkeit und mehrere Wege der Informationsübermittlungen in IKARUS anti.virus eingebaut.

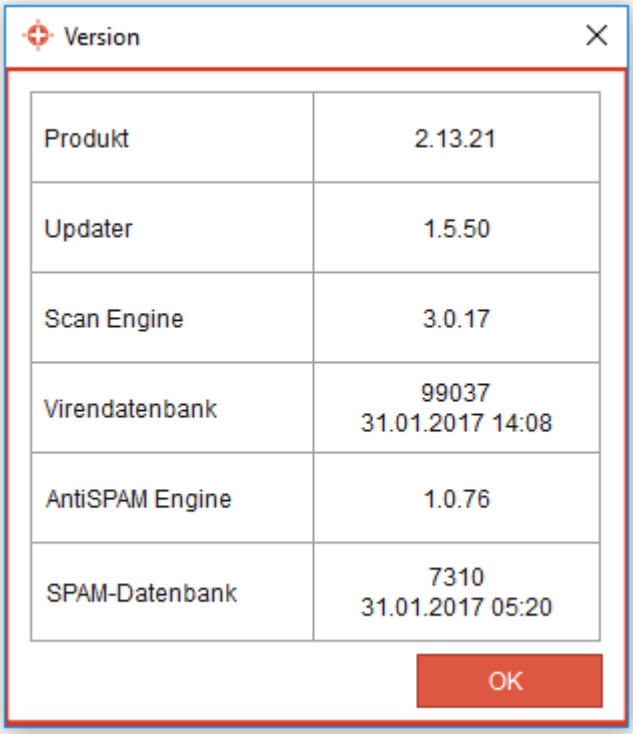


Abbildung 48: Support – Versionsinformation

Über die Menüleiste „Support“ können Sie ganz einfach die aktuellen Versionsnummern von IKARUS anti.virus eruieren. Diese Angaben sind bei einem Kontakt mit unserem Supportteam wichtig!

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

Abbildung 49: Support – Kontakt

Die Kontaktdaten selbst können Sie ebenfalls einfach über IKARUS anti.virus aufrufen. Wenn Sie uns über diesen Link eine E-Mail schicken, wird diese automatisch mit den wichtigsten Versionsinformationen ergänzt.

Unter dem Menüpunkt „Support" – „Support Info speichern" können Sie auf einen Klick die wichtigsten Supportinfos zusammenfassen und uns in Form eines ZIP-Files übermitteln.

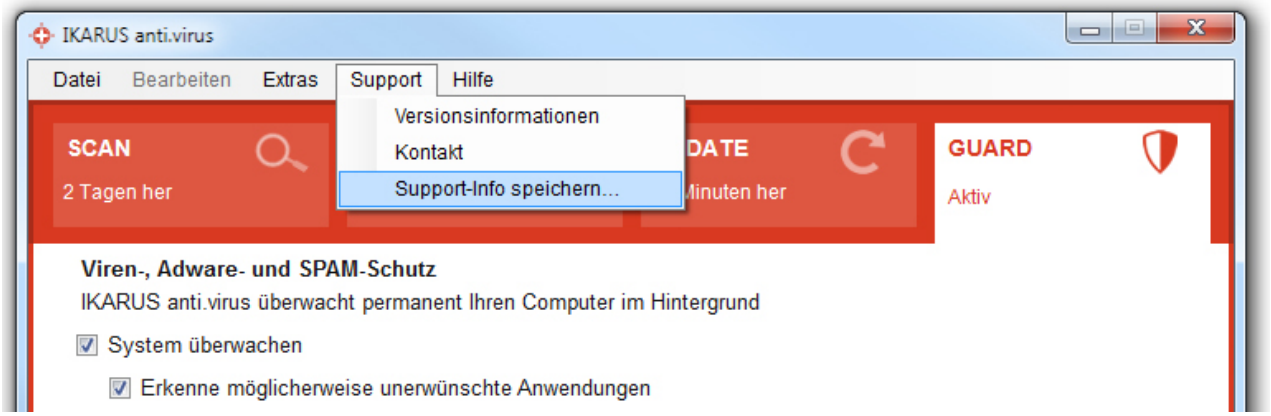


Abbildung 50: Support-Info

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

7.1 Lizenzschlüssel

Die Verwendung von IKARUS anti.virus wird über den Lizenzschlüssel aktiviert. Dieser Schlüssel regelt die Dauer der Verwendung sowie die Anzahl der Benutzer.

Sie erhalten diesen Schlüssel beim Kauf bzw. bei der Registrierung mittels Aktivierungscode in Form einer Lizenzdatei.

Über den Menüpunkt „Hilfe/Lizenzdatei oder Aktivierungscode" können Sie Ihre Lizenzschlüssel überprüfen, löschen, hinzufügen und archivieren.

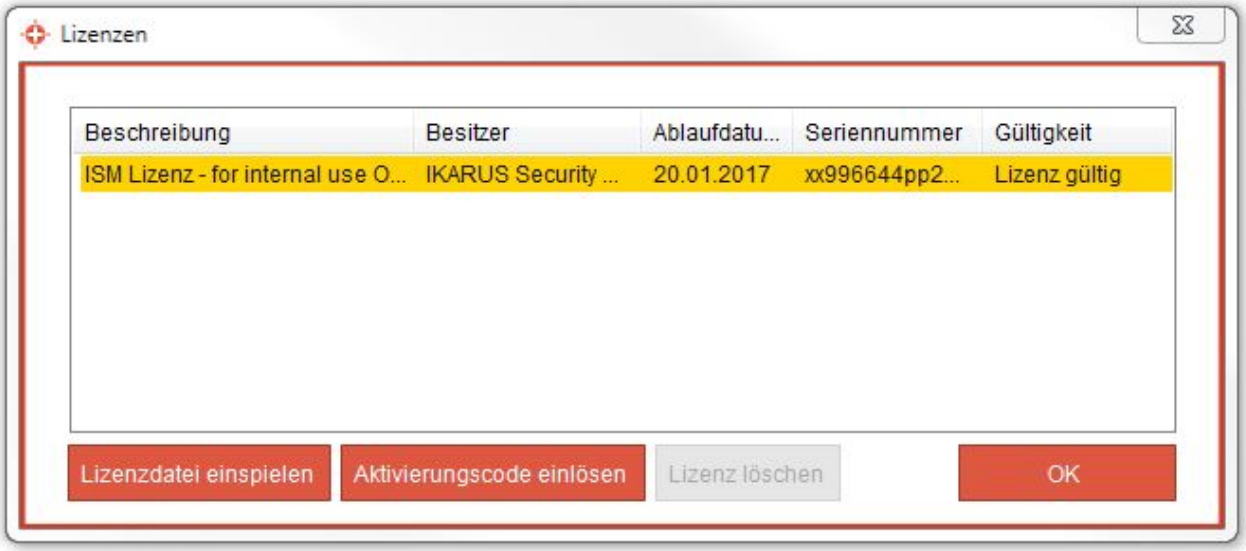


Abbildung 51: IKARUS anti.virus Lizenzen

Es können auch mehrere Lizenzschlüssel gleichzeitig verwaltet werden, z.B. wenn ein Lizenzschlüssel in Kürze ausläuft und Sie bereits einen neuen erhalten haben.

IKARUS anti.virus wählt automatisch den richtigen Schlüssel aus.

Bitte kontaktieren Sie unseren Support, wenn Sie Ihren Lizenzschlüssel nicht mehr finden oder keinen erhalten haben.

Wenn Sie einen Aktivierungscode besitzen, haben Sie hier die Möglichkeit, sich damit zu registrieren und einen Lizenzschlüssel vollautomatisch in das Programm integrieren zu lassen.

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

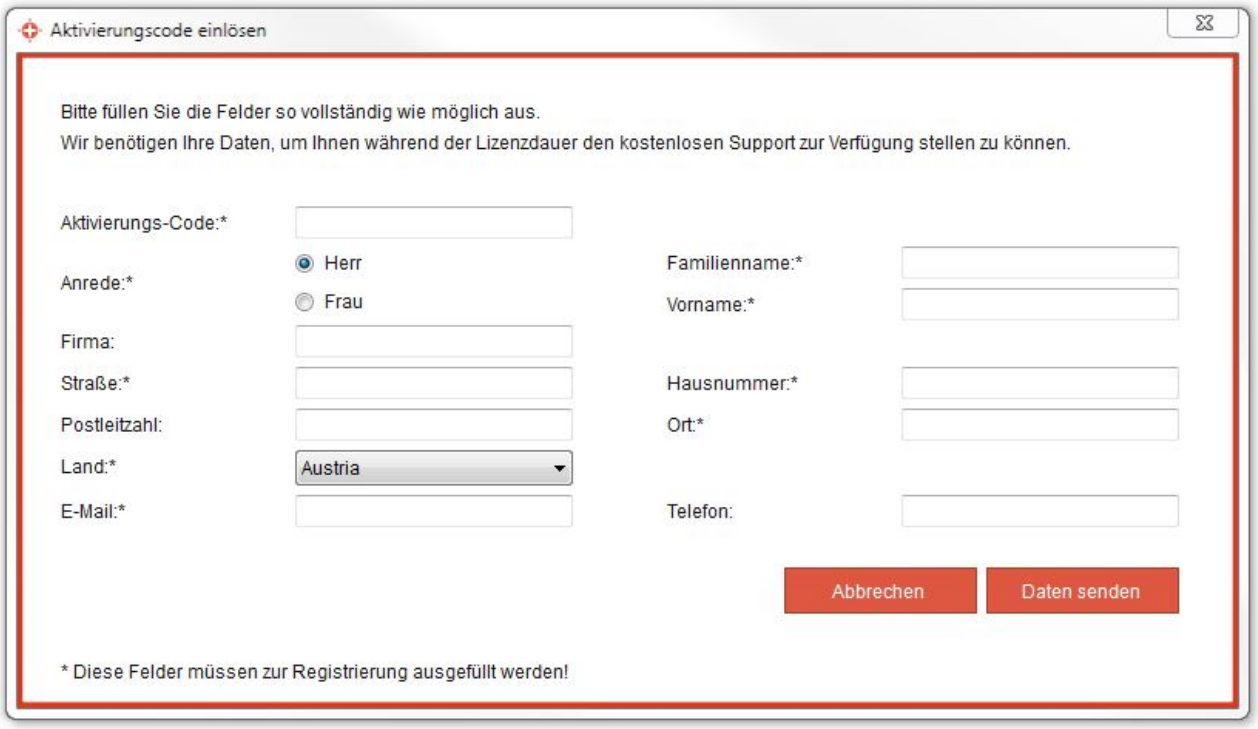


Abbildung 52: Aktivierung der Software mittels Aktivierungscode

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

8

Weitere Informationen

Hier erhalten sie Informationen über die Installation des Microsoft NET Framework, die Konfiguration von Firewalls und die lizenzrechtlichen Bestimmungen der IKARUS Security Software GmbH.

8.1 .NET Framework

.NET Framework wird benötigt, um die grafische Oberfläche von IKARUS anti.virus darstellen zu können. Wenn Sie .NET Framework bereits auf Ihrem Computer installiert haben, wird die Installation von IKARUS anti.virus ohne Unterbrechung abgeschlossen und gegebenenfalls .NET Framework aktualisiert. Existiert auf Ihrem PC noch kein .NET Framework, wird dieses automatisch im Rahmen der IKARUS anti.virus Installation nachinstalliert. Dazu muss eine bestehende Internetverbindung vorhanden sein.

.NET Framework ist eine Freeware-Version von Microsoft. Sie müssen dafür also keinerlei Lizenzkosten bezahlen und keine Registrierung durchführen.

8.2 Lizenzrechtliche Bestimmungen

Die aktuelle EULA finden Sie auch unter https://www.ikarussecurity.com/eula/

IKARUS Security Software GmbH | Blechturmgasse 11 | A-1050 Wien/Österreich | Tel.: +43 1 589 95-0 | Fax: +43 1 589 95-100 | office@ikarus.at
www.ikarussecurity.com | Erste Bank Österreich | BIC: GIBAATWWXXX | IBAN: AT14 2011 1821 2208 2100 | Firmenbuch: FN 64708i | Gerichtsstand: Wien
UID-Nr.: ATU15191405

9

Kontakt

IKARUS Security Software GmbH

Blechturmgasse 11
1050 Wien
Österreich

Telefon: +43 (0) 1 58995-0
Fax: +43 (0) 1 58995-100
office@ikarus.at
https://www.ikarussecurity.com

IKARUS Security Software Support Kontakt

Telefon: +43 (0) 1 58995-400
Support-Zeiten: Mo bis Do: 8.00 – 18.00 Uhr
Fr: 8.00 – 15.00 Uhr

E-Mail: support@ikarus.at

IKARUS Security Software Sales Kontakt

Telefon: +43 (0) 1 58995-500
E-Mail: sales@ikarus.at