Avira Professional Security

Konfiguration von Sicherheitsleveln

Kurzanleitung

AVIRA

Inhaltsverzeichnis

1. Allgemeine Informationen

Dieses Dokument beschreibt die Konfigurationsmöglichkeiten der Module:

- System-Scanner (Scanner)
- Echtzeit-Scanner (Guard)
- Email-Schutz (MailGuard)
- Browser-Schutz (WebGuard)

Dabei werden unterschiedliche Konfigurationen je nach Sicherheitslevel empfohlen sowie die Einstellungen des integrierten Planers erläutert. Die Frage, ob Sie die Module Email-Schutz und Browser-Schutz installieren sollten, spielt in diesem HowTo keine zentrale Rolle. Zahlreiche Informationen zum „sinnvollen“ Einsatz finden Sie im Handbuch und im HowTo AntiVir Professional.

Sie benötigen den Email-Schutz, falls Sie die Emails via POP oder IMAP bei Ihrem Provider abrufen und dieser keinen (ausreichenden) Virenschutz anbietet oder Sie auf Ihrem eigenen Mailserver keinen Virenschutz installiert haben.

Den Browser-Schutz sollten Sie verwenden, falls Sie direktüber einen Router bzw. per Einwahl mit dem Internet verbunden sind oder kein Virenschutz auf einem genutzten Proxyserver vorhanden ist.

Hinweis
Das Dokument ist als schnelle und eigenständige Hilfe gedacht, somit können nicht alle Optionen im Detail erklärt werden.

Wann immer Sie offene Fragen zu bestimmten Einstellungen haben, empfehlen wir Ihnen, mit der F1 Taste die Onlinehilfe aufzurufen.

Je nach Konfiguration einer Virenschutz Software gewinnen oder verlieren Sie Sicherheit und Performance.
Je höher das Sicherheitslevel, desto geringer die Performance und genau deshalb geben wir Ihnen in Kapitel 5 unsere Empfehlung zur Konfiguration, um sie effektiv einzusetzen, ohne Performance zu verlieren.

Um vorab eine Orientierung zu bekommen, folgt ein kurzer Testbericht.

Testergebnisse auf folgendem Basissystem

- Windows XP SP3 32bit inkl. aller sicherheitsrelevanten Patches
- Intel® Core ™2 Duo CPU E6750 2.66GHz
- Insgesamt 4 GB Arbeitsspeicher, 3.25 GB verfügbar
- 2 Festplatten mit 235 GB; Dateisystem NTFS

System-Scanner

Durchschnittliche Dauer eines Suchlaufs über die Systempartition mit einer Belegung von 10,7 GB und Dateien in verschiedenen Formaten (.txt, .doc, .xls, .ppt, .exe, .com, .jpg, .zip, .rar) ohne aktivierte Systemwiederherstellung:

- Sicherheitsniveau Hoch: 16:35 Minuten (325.396 Dateien)
- Sicherheitsniveau Mittel: 15:30 Minuten (325.388 Dateien)
- Sicherheitsniveau Niedrig: 09:20 Minuten (54.329 Dateien)

Hinweis
Je nach Sicherheitslevel werden unterschiedlich viele Dateien überprüft.

Echtzeit-Scanner

Durchschnittliche Dauer eines Kopiervorgangs von insgesamt 12.279 Dateien (1,92 GB) in unterschiedlichen Formaten (s. o.) ohne aktivierte Systemwiederherstellung:

- Ohne aktiven Echtzeit-Scanner: 60 Sekunden
- Sicherheitsniveau Hoch: 140 Sekunden
- Sicherheitsniveau Mittel: 90 Sekunden
- Sicherheitsniveau Niedrig: 80 Sekunden

Die Performance verändert sich je nach Konfiguration! Mit Hilfe dieser Zahlen und weiteren Faktoren wie Gefahrenpotential, Anwenderberechtigungen oder Firmenregulierung leiten Sie das Sicherheitslevel ab.

Konfigurationseinstellungen

Wir empfehlen Ihnen, stets den Expertenmodus zu aktivieren, um alle Optionen nutzen zu können. Sie finden die Checkbox unter *Avira Control Center* > *Extras* > *Konfiguration* > *Expertenmodus*.
Die Beschreibungen und Screenshots in diesem Dokument beziehen sich auf eine lokale Konfiguration direkt am PC.

Die unterschiedlichen Konfigurationseinstellungen werden stets in der zentralen Konfigurationsdatei *avwin.ini* gespeichert, die im Avira Datenverzeichnis im Unterverzeichnis CONFIG abgelegt ist.

Datenverzeichnis unter Windows 2000 und XP:
C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir Desktop

Datenverzeichnis unter Windows Vista und Windows 7:
C:\ProgramData\Avira\AntiVir Desktop

Konfigurationsprofile

In der Avira Professional Security besteht die Möglichkeit, mehrere Konfigurationen in so genannten Konfigurationsprofilen vorzuhalten und je nach Anforderungen und Einsatzgebiet zu verwenden.

Hierfür müssen Sie lediglich ein neues Profil anlegen, die Konfiguration anpassen und den Wechsel (Automatisch oder Manuell) regulieren. Weitere Informationen finden Sie im Handbuch und in der programminternen Hilfe, die Sie mit der F1 Taste aufrufen können.

Es könnte beispielsweise sinnvoll sein, bei einem mobilen Anwender außer Haus eine andere Konfiguration anzuwenden als im Firmennetzwerk.
Denken Sie an die Module Email-Schutz und Browser-Schutz oder an den konfigurierten Updateserver, der außerhalb des Firmennetzwerks nicht erreichbar ist.

Die verschiedenen Konfigurationen werden in unterschiedlichen INI Dateien im Datenverzeichnis gespeichert. Dabei werden die Dateiennamen durchnummeriert, die aktuelle Konfiguration wird stets in der Datei *avwin.ini* vorgehalten und in der Konfigurationsoberfläche mit einem (*)markiert.

Verwendung einer bereits vorhandenen INI Datei

Zusätzlich zu diesem Dokument gibt es für jedes empfohlene Sicherheitslevel eine dazugehörige INI Datei, die Sie wie folgt verwenden können.

Übernahme bei der Installation

Sie können beim Silent Setup mit Hilfe der Datei *setup.inf* eine Konfigurationsdatei *avwin.ini* übergeben, die bei der Installation berücksichtigt wird.

- Aufruf des Silent Setups: *presetup.exe /inf=“C:\setup.inf“*
- Parameter in der setup.inf Datei: *AVWinIni=C:\avwin.ini*

Weitere Informationen finden Sie im Handbuch und in der Onlinehillfe.

Nachträgliches Einspielen nach der Installation

Falls der Antivirus bereits installiert ist und Sie die Konfigurationsdatei manuell einspielen möchten, gehen Sie bitte wie folgt vor:

- *Avira Control Center > Expertenmodus > Allgemeines > Sicherheit > Produktschutz komplett deaktivieren*; mit *OK* bestätigen und anschließend Programm schließen

- Dienste Verwaltung (*Start* > *Ausführen* > *services.msc*) aufrufen und alle Avira Dienste beenden
- Datei in das Verzeichnis *CONFIG* im Avira Datenverzeichnis kopieren und in *av-win.ini* umbenennen
- Alle Avira Dienste starten und kontrollieren, ob die Einstellungen akzeptiert wurden
- System bei nächster Gelegenheit neu starten, umden Produktschutz Treiber zu initialisieren
- Falls Sie die von uns bereitgestellten Konfigurationsdateien verwenden, achten Sie bitte darauf, dass im Sicherheitslevel Hoch und Mittel das Passwort avira lautet.

Aufträge und Profile

Da im letzten Abschnitt der folgenden Kapitel jeweils kurz auf den Avira Planer eingegangen wird, erhalten Sie nun einen kurzen Überblick über die Funktionsweise des Planers im Zusammenspiel mit Aufträgen und Profilen.

Der Avira Planer arbeitet mit so genannten Aufträgen, die Sie zentral über das SMC/AMC oder lokal am System anlegen und konfigurieren können.
Ein lokaler Auftrag wiederum verwendet immer ein Profil in dem die dazugehörigen Informationen gespeichert sind. Die Avira Auftrag Dateien (**.avj*) befinden sich im Verzeichnis JOBS unterhalb des Avira Datenverzeichnisses.

Eigene Profil Dateien (**.avp*) finden Sie im Verzeichnis *PROFILES*, die mitgelieferten Avira Profil Dateien (*sysdir.avp, alldiscs.avp, etc*.) liegen im Avira Installationsverzeichnis.

Da ein Scanprofil immer systemabhängig ist, können wir Ihnen „nur“ Standardaufträge mit entsprechenden Einstellungen je nach Sicherheitslevel geben. Zudem finden Sie einen Updateauftrag mit einer Intervall Einstellung je nach Sicherheitslevel. Hierbei handelt es sich um die AVJ-Dateien.

Um diesen Auftrag einzuspielen, gehen Sie bitte wie bei der INI Einspielung vor. Dabei achten Sie lediglich darauf, dass das Avira Control Center geschlossen ist und Sie nur den Planer Dienst beenden und neu starten müssen.

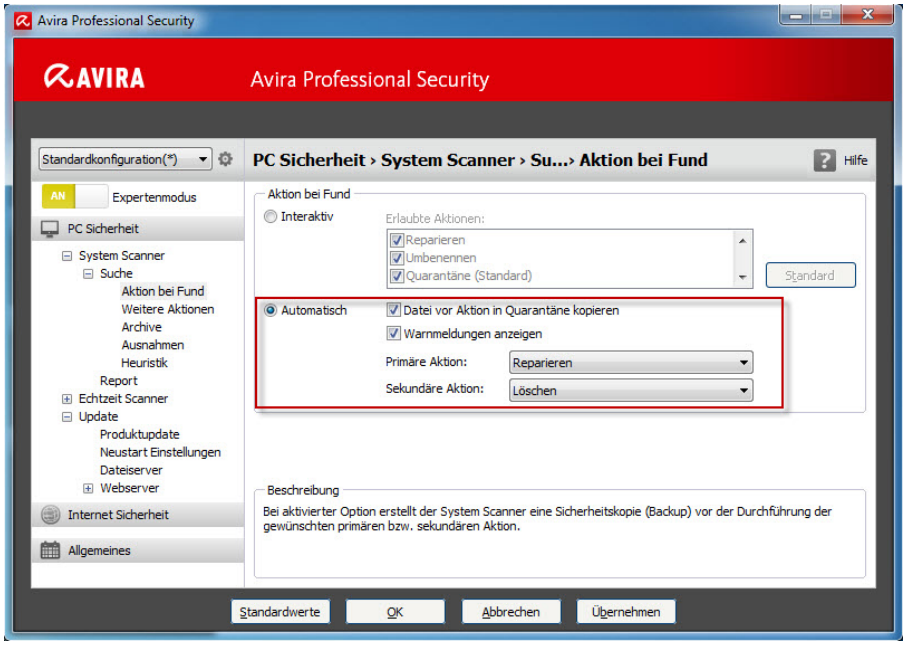
Hinweis
Falls Sie die Auftrag- oder Konfigurationsdateien verwenden möchten, achten Sie bitte darauf, dass diese für das Standardverzeichnis *C:\Alle Programme\Avira\Avira Desktop* angelegt wurden.

2. Sicherheitslevel Hoch

2.1 Modul übergreifend

Aktion bei Fund

- Aktion bei Fund: Automatisch
- Datei vor Aktion in Quarantäne kopieren
- Warnmeldungen anzeigen
- Primäre Aktion: reparieren
- Sekundäre Aktion: löschen



Durch die Konfiguration einer bzw. mehrerer automatischer Aktionen bei einem möglichen Fund können Sie sicherstellen, dass der Suchlauf ohne Unterbrechung durchgeführt wird und alle Aktionen in den jeweiligen Modulen gleich ausgewählt sind.

Wir empfehlen Ihnen, die Datei vor jeglicher Aktion in Quarantäne zu kopieren, damit Sie stets auf die Originaldatei zurückgreifen können.

Eine Reparatur funktioniert „nur“ bei Dateien, die infiziert wurden. Eine an sich virulente Datei wie ein Trojaner oder Wurm kann nicht repariert werden, diese Dateien werden aufgrund der Konfiguration gelöscht.

Hinweise zum Echtzeit-Scanner

Eine Reparatur durch den Echtzeit-Scanner ist nur bedingt möglich. Deshalb empfehlen wir Ihnen, immer einen Suchlauf nach einer mehrfachen Virenmeldung durch den Echtzeit-Scanner durchzuführen, um ein mögliches infiziertes System zu bereinigen.

Bitte führen Sie zudem bei einer Makroviren Meldung des Echtzeit-Scanners anschließend einen Suchlauf über die gemeldete Datei aus, um ebenfalls sicherzustellen, dass die Datei repariert wird.

Hinweise zum Email-Schutz

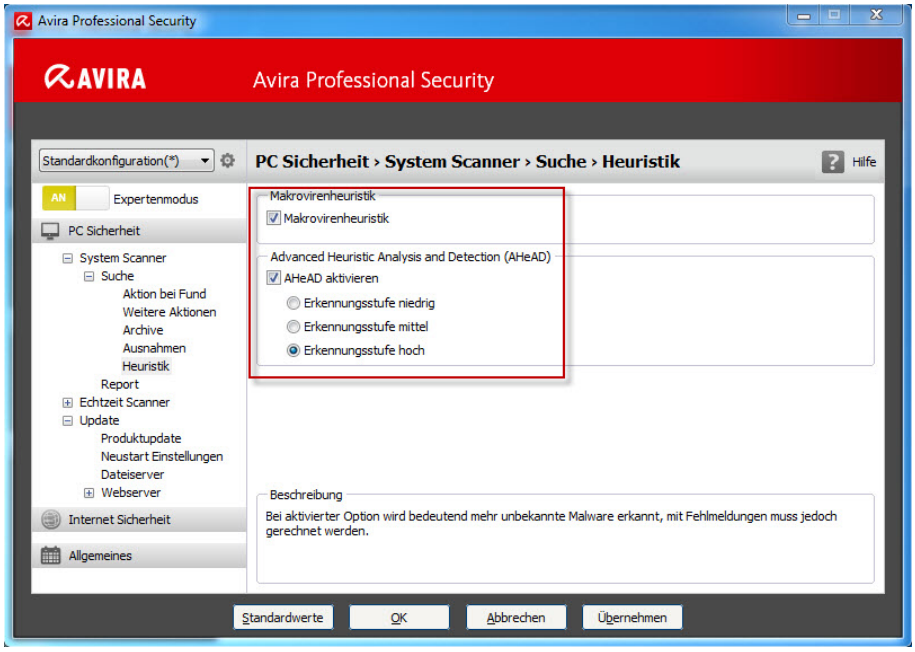
Bei einem Malwarefund durch den Email-Schutz können Emails und Dateien nicht repariert werden, deshalb empfehlen wir Ihnen, stets die Emails komplett in Quarantäne zu verschieben.

Hinweise zum Browser-Schutz

Wie beim Email-Schutz kann auch der Browser-Schutz keine Dateien reparieren, folglich empfehlen wir Ihnen ebenfalls, die Datei in Quarantäne zu verschieben. Wählen Sie hierfür die Primäre Aktion isolieren aus.

Heuristik

- Makrovirenheuristik aktiviert
- Advanced Heuristic (AHeAD) aktiviert: Erkennungsstufe hoch



Durch die Aktivierung der Makrovirenheuristik werden entsprechende Dokumente mit Makros nach möglichen Makroviren untersucht und ggf. repariert.

Durch die aktivierte Heuristik in der Erkennungsstufe hoch erkennt Avira bedeutend mehr unbekannte Malwaretypen, allerdings müssen Sie auch mit so genannten Fehlmeldungen rechnen.

Bitte aktivieren Sie die Heuristik in allen Modulen (System-Scanner, Echtzeit-Schutz, Email-Schutz und Browser-Schutz) und stellen Sie überall die AHeAD Erkennungs-stufe hoch ein.

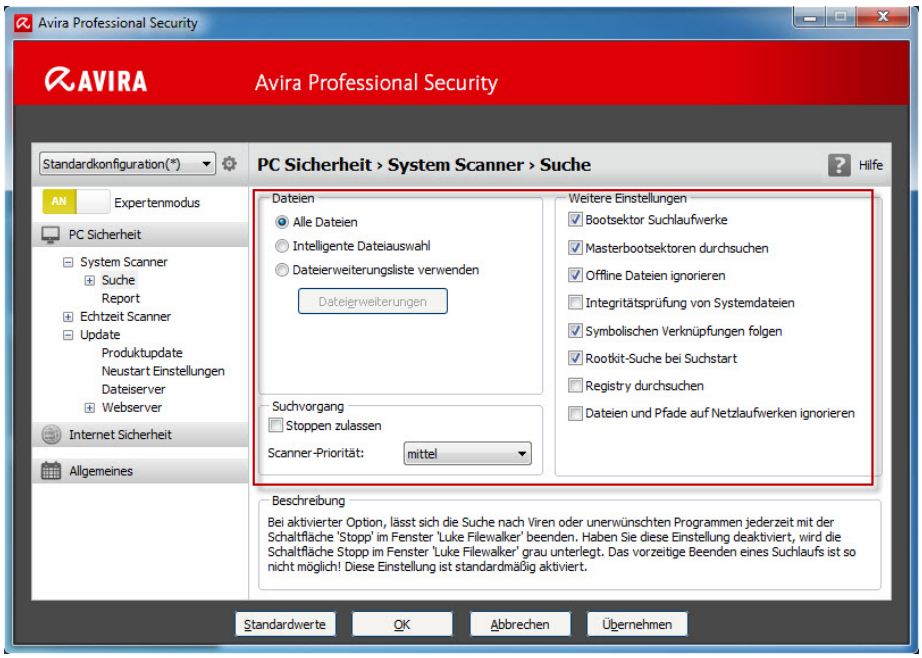
Hinweis
Sie finden die Konfiguration der Heuristik in allen Modulen unterhalb von Suche.

2.2 Modul System-Scanner

Suche

- Dateien: Alle Dateien
- Weitere Einstellungen:
  - Bootsektor Suchlaufwerke;
  - Masterbootsektoren durchsuchen;
  - Offline Dateien ignorieren;
  - Symbolischen Verknüpfungen folgen;
  - Rootkit-Suche bei Suchstart;

- Suchvorgang: Kein Stoppen zulassen
- Scanner Priorität: mittel



Es werden wirklich alle Dateien vom Scanner überprüft, was wichtig ist, da es immer wieder neue Malwaretypen und Exploits in verschiedenen Dateitypen gibt.

Zudem werden Bootsektoren überprüft, Offline Dateien nicht ignoriert (Stichwort: HSMS – siehe Programmhilfe), der Suchlauf optimiert ausgeführt (Multi-Prozessor) und eine Rootkit Suche beim Start durchgeführt.

Eine Rootkit Suche bei jedem Start eines Suchlaufs empfehlen wir Ihnen im Sicherheitslevel Hoch, da es derzeit kein Profil für die vollständige Rootkit Suche gibt.

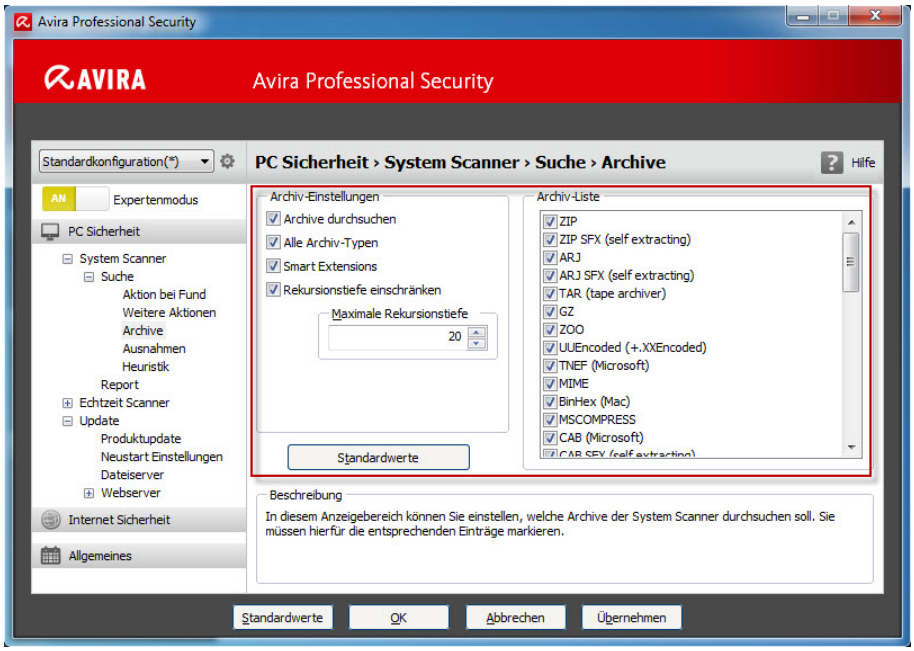
Durch das Deaktivieren eines möglichen Stoppvorgangs können Sie einen kompletten Suchlauf garantieren. Der Anwender hat also keine Möglichkeit, den Suchlauf abzubrechen.

Archive

- Archiv-Einstellungen:
  - Alle Archiv-Typen;
  - Smart Extensions aktiviert; Keine
  - Rekursionstiefe einschränken

- In der Archiv-Liste alle Formate aktivieren

(geschieht durch die Auswahl Alle Archiv-Typenautomatisch)



Durch die oben genannten Einstellungen stellen Sie sicher, dass alle uns bekannten Archivtypen entpacktund durchsucht werden.

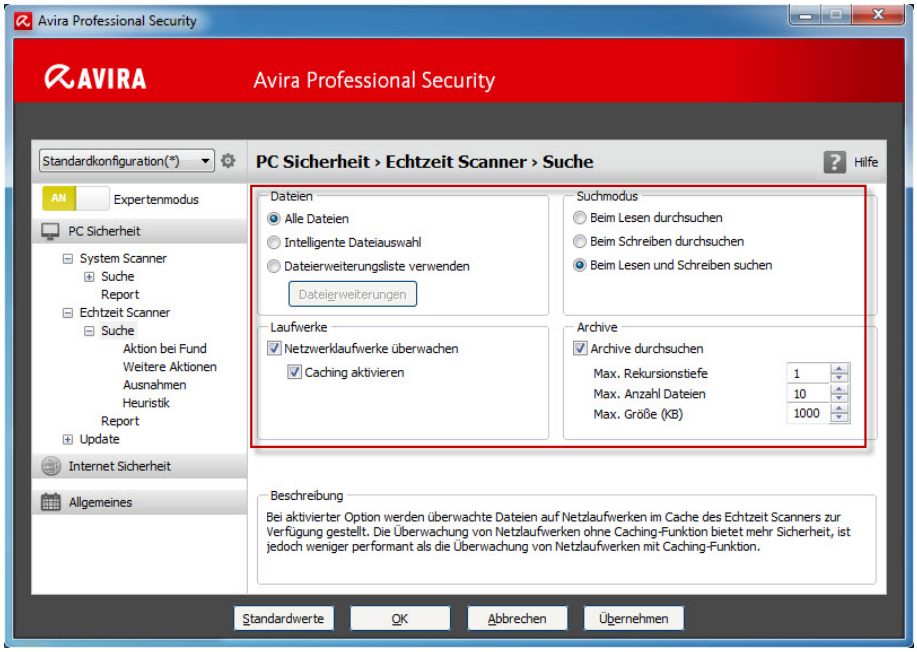
Die Option Smart Extensions sorgt dafür, dass Archive auch erkannt werden, falls die Dateiendung abweicht.

Hinweis
Falls eine virulente Datei in einem Archiv gefunden wird, wird das gesamte Archiv aufgrund der Einstellung in Quarantäne gestellt und anschließend gelöscht. Eine Reparatur eines Archivs (Entfernung der virulenten Datei aus dem Archiv) ist aus technischen Gründen leider nicht möglich.

2.3 Modul Echtzeit-Scanner

Suche

- Beim Lesen und Schreiben suchen
- Alle Dateien
- Archive durchsuchen mit entsprechender Konfiguration
- Netzlaufwerke überwachen und Caching aktivieren



Durch diese Einstellungen werden alle Dateioperationen wie Öffnen, Ausführen und Schreiben bei allen Dateien durch den Echtzeit-Scanner überwacht.

Zudem werden Archive in Echtzeit überprüft und Netzlaufwerke überwacht. Ein Caching sorgt dabei für bessere Performance.

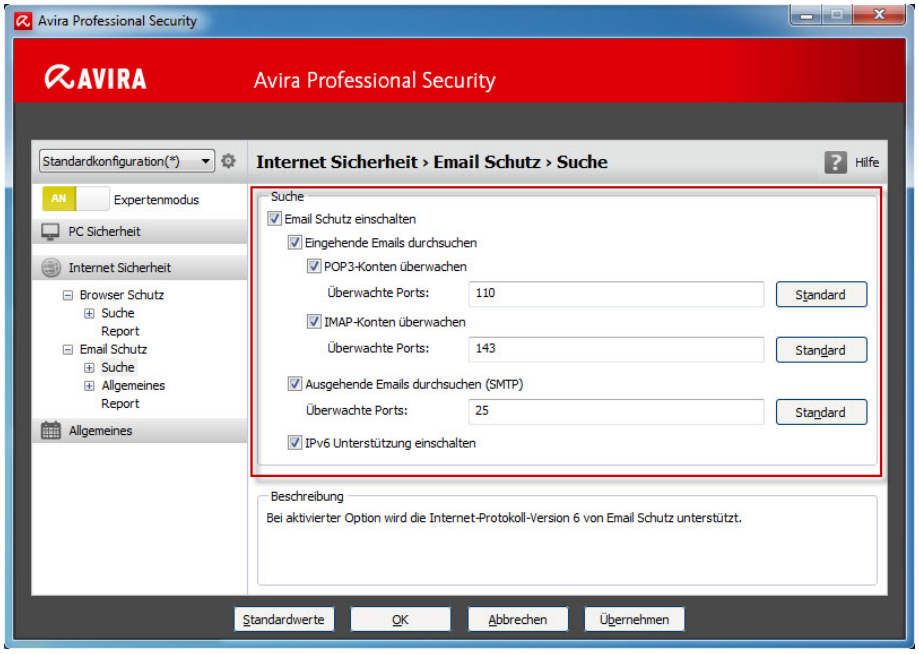
Hinweis
Eine aktivierte Archivsuche im Echtzeit-Scanner wirkt sich stark auf die Performance des Systems aus. Falls die Performance zu sehr leidet, empfehlen wir Ihnen, Rekursionstiefe, Anzahl an Dateien und Größe der Archivdatei einzuschränken.

2.4 Module Email-Schutz und Browser-Schutz

Diese Module werden wie bereits erwähnt ja nach Unternehmensumgebung und Anforderungen installiert. Falls Sie sich für eine Installation entschieden haben, empfehlen wir Ihnen bei einem hohen Sicherheitslevel die folgenden Einstellungen.

Email-Schutz-Suche

- Eingehenden Emails durchsuchen
- Ausgehende Emails durchsuchen
- IPv6 Unterstützung einschalten



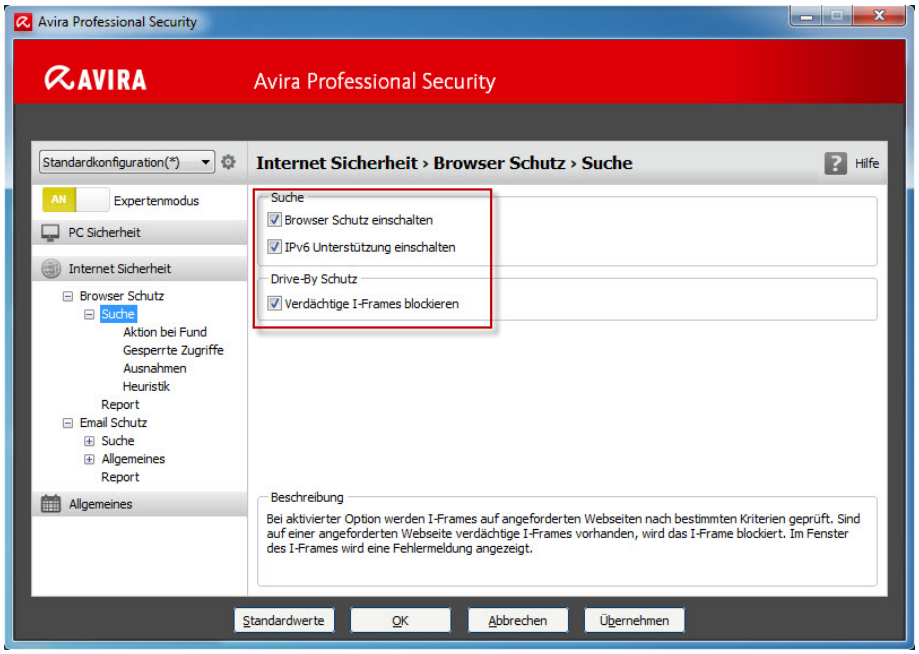
So können Sie sicherstellen, dass alle ein- und ausgehenden Emails überwacht werden. Auf Emails kann dabei entweder via POP oder via IMAP zugegriffen werden, beide Protokolle werden berücksichtigt.

Die Überwachung von ausgehenden Emails dient dazu, mögliche Malwaretypen ausfindig zu machen, die den Rechner übernommen haben (Stichwort: Bot Netze), um Malware oder Spam mit eigener SMTP Engine zu versenden.

Browser-Schutz-Suche

- Browser Schutz einschalten
- IPv6 Unterstützung einschalten
- Verdächtige I-Frames blockieren

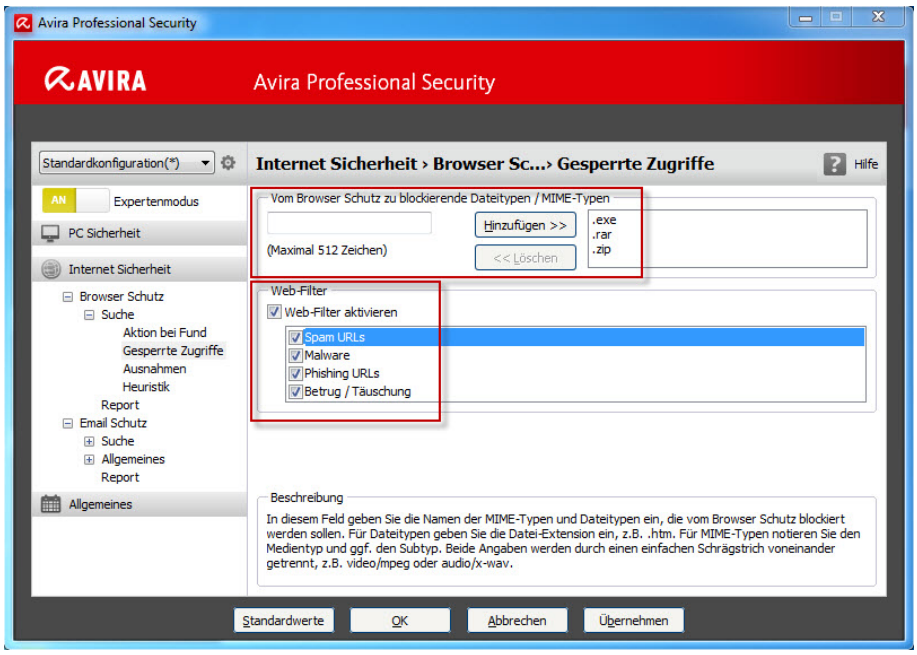
I-Frames sind HTML-Elemente, die einen Bereich einer Webseite abgrenzen. Mit diesen so genannten Inlineframes können andere Webinhalte (meist anderer URLs) als selbständige Dokumente in einem Unterfenster des Browsers geladen werden.



In der Regel werden I-Frames für Banner-Werbung genutzt, allerdings dienen sie auch zur Verbreitung verschiedener Malware Typen. Eine verdächtige Verwendung von I-Frames besteht, wenn das I-Frame sehr klein ist und so im Browser nicht sichtbar ist.

Browser-Schutz – Gesperrte Zugriffe

- Vom Browser Schutz zu blockierende Dateitypen / MIME-Typen: Nach Bedarf
- Web-Filter aktivieren: Alle Kategorien ausgewählt



Die zu blockierenden Datei- und MIME-Typen können Sie je nach Policy selbst hinzufügen, hier können bestimmte Downloads unterbunden werden.

Im Level Hoch empfehlen wir Ihnen, ausführbare Dateien (EXE) sowie Archivdateien wie ZIP und RAR zu blockieren, um den Download solcher Dateien zu unterbinden.

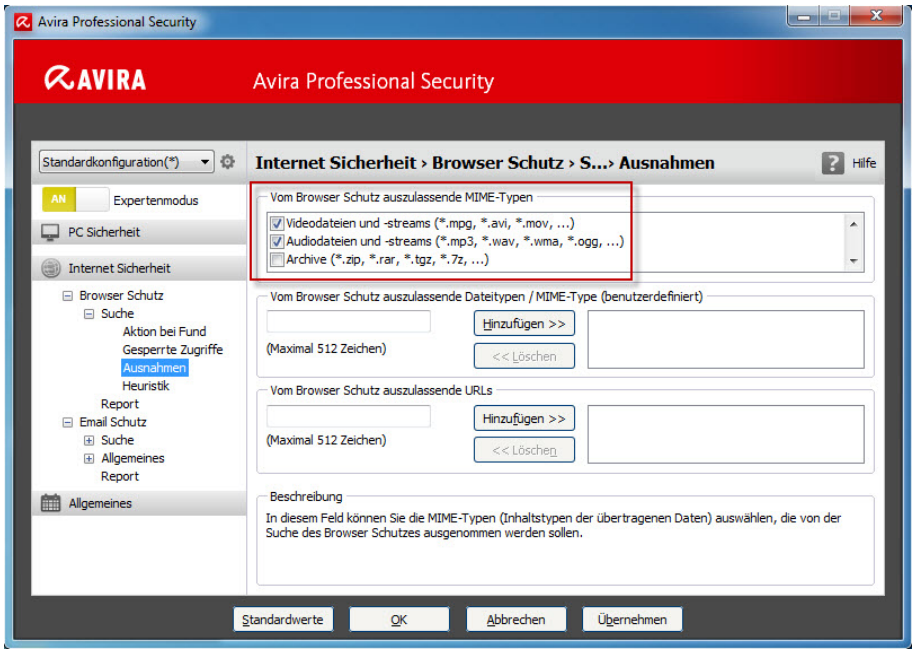
Hinweis
Bitte kontrollieren Sie anhand der Policy, ob diese Dateien blockiert und noch weitere Datei- und/oder MIME-Typen hinzugefügt werden sollen.

Im Webfilter selbst aktivieren Sie alle Kategorien. Malware- und Phishing URLs sind selbsterklärend, Betrug/Täuschung liegt vor, falls ein Anbieter eines unseriösen Angebots versucht, Ihnen einen Vertrag ohne konkrete Angaben zu verkaufen (Stichwort Abo Falle).

Browser-Schutz – Ausnahmen

Vom Browser Schutz auszulassende MIME-Typen

- Videodateien und -streams (*.mpg, *.avi, *.mov, ...)
- Audiodateien und -streams (*.mp3, *. wav, *.wma, *.ogg, ...)



Diese Dateien sollten aufgrund der Performance und der allgemeinen Verarbeitung im Webbrowser oder in anderen Applikationen stets ausgenommen werden, damit sie funktionieren.

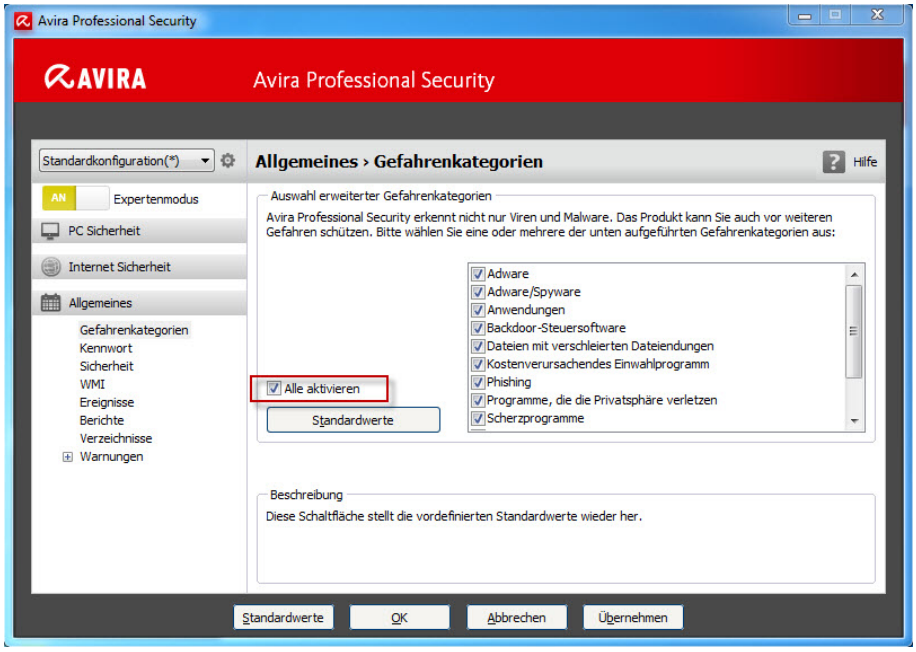
Ansonsten kann es vorkommen, dass Streams überhaupt nicht funktionieren, da es bei dieser Art von Dateien kein so genanntes End of File gibt und Avira somit keine Möglichkeit hat, die Datei zu prüfen.

Alle anderen Arten wie Archivdateien oder ausführbare Dateien sollten im Sicherheitslevel Hoch natürlich geprüft werden, folglich sind diese Ausnahmen deaktiviert.

2.5 Allgemeine Einstellungen

Erweiterte - Gefahrenkategorien

- Alle aktivieren



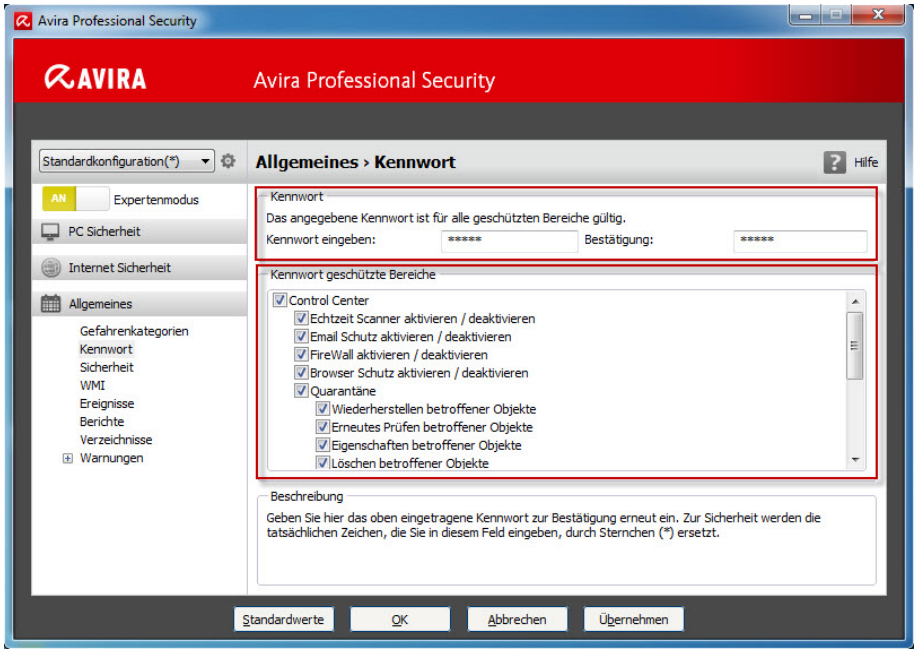
Neben der üblichen Viren und Malware Erkennung können Sie mit dieser Einstellung dafür sorgen, dass zusätzliche Gefahrenquellen wie Dialer, SPR Programme oder Witzprogramme blockiert werden.

Weitere Informationen zu den verschiedenen Kategorien finden Sie in der im Programm integrierten Online Hilfe, die Sie mit der F1 Taste aufrufen können.

Kennwort

Bitte hinterlegen Sie unbedingt einen Kennwortschutz für alleBereiche

Durch einen Kennwortschutz für alle Bereiche stellen Sie sicher, dass die vorgegebene Konfiguration nur mit Hilfe des entsprechenden Kennworts geändert oder Module wie Echtzeit-Scanner, Email-Schutz und Browser-Schutz deaktiviert werden können.



Außerdem können Sie das Quarantänemanagement absichern und verhindern, dass einzelne Module (Stichwort: Änderungsinstallation) oder gar das komplette Avira Programm deinstalliert werden.

Diese Einstellung empfehlen wir generell und im Speziellen bei Anwendern, die aufgrund bestimmter Voraussetzungen mit administrativen Rechten arbeiten.

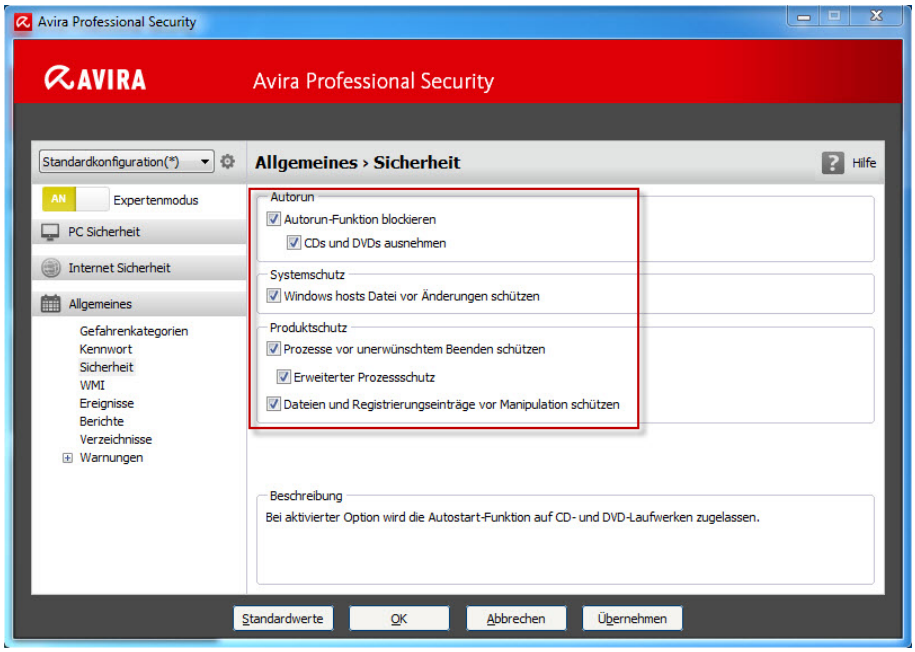
Hinweis
Im Sicherheitslevel Hoch wird das Passwort aviraverwendet, bitte ändern Sie dieses Passwort nach Einspielen der mitgelieferten INI Datei!

Sicherheit

- Autorun-Funktion blockieren
- CDs und DVDs ausnehmen
- Windows hosts Datei vor Änderungen schützen
- Prozesse vor unerwünschtem Beenden schützen
- Erweiterter Prozessschutz
- Dateien und Registrierungseinträge vor Manipulation schützen

Bei aktiviertem Autorun wird die Ausführung der Windows Autostart-Funktion auf allen eingebundenen Laufwerken wie USB-Sticks, CD- und DVD-Laufwerken, Netzlaufwerken blockiert.

Bei der aktivierter Option „ CDs und DVDs ausnehmen“ wird die Autostart-Funktion auf CD- und DVD-Laufwerken zugelassen.



In der Option Systemschutz sind die Windows hosts-Dateien schreibgeschützt. Eine Manipulation der Dateien ist dann nicht länger möglich. Malware ist dann beispielweise nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten.

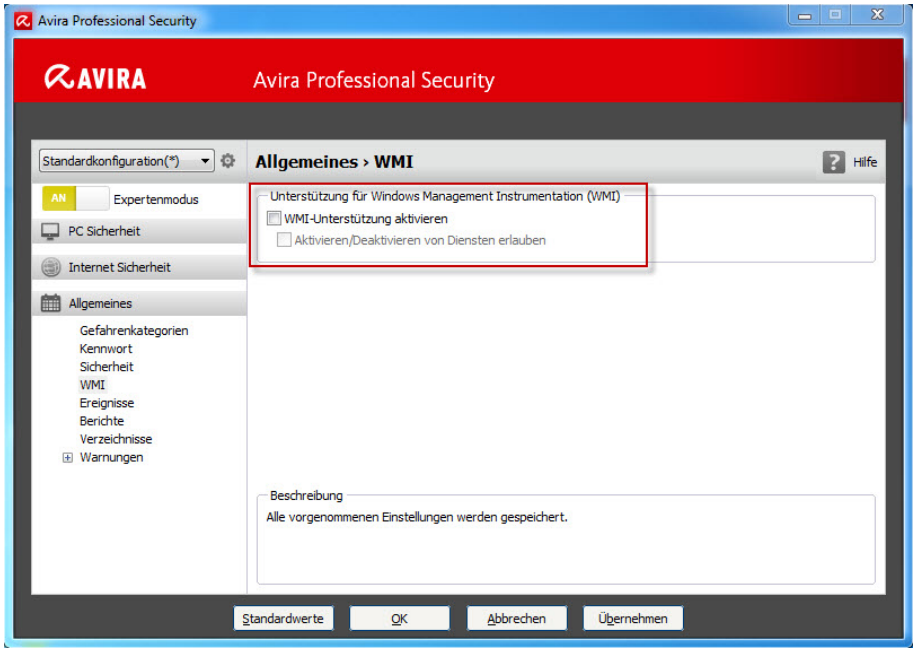
Bei den aktivierten Optionen im Produktschutz werden alle Prozesse des Programms sowie alle Dateien des Programms vor unerwünschter Manipulation oder Beenden durch Viren und Malware geschützt

WMI

- Option bitte vollständig deaktivieren

Bitte deaktivieren Sie die WMI Schnittstelle komplett, sodass weder Daten und Informationen über Avira (Aktive Module, Updatestand, etc.) abgefragt noch Manipulationen wie das Beenden eines Dienstes durchgeführt werden können.

Dadurch stellen Sie sicher, dass ein Angreifer keine Informationen auslesen kann, um einen Angriff zu planen und die WMI Schnittstelle auch nicht zu einer geplanten Sabotageaktion nutzen kann.



2.6 Avira Planer

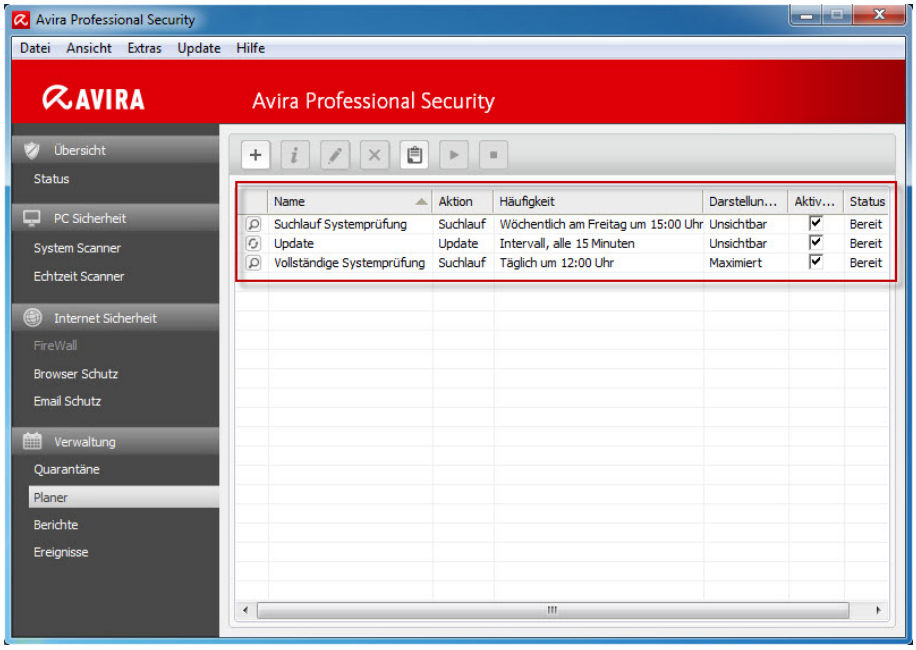
Im Avira Planer können Sie die Aufträge (so genannte Jobs) lokal anlegen, um die lokale Avira Instanz hinsichtlich Updates und Suchläufen zu steuern.
Diese Planung können Sie natürlich auch zentral über das AMC steuern und somit eine einheitliche Planung für alle Klienten anlegen.

- Update Intervall – Alle 15 Minuten
- Suchlauf Lokale Laufwerke – Täglich um 12:00 Uhr (Mittagspause)
- Suchlauf Vollständige Systemprüfung – Wöchentlich am Freitag um 15:00 Uhr
- Alle Aufträge im Darstellungsmodus unsichtbar

Durch die Einstellung Update alle 15 Minuten stellen Sie sicher, dass jedes Update (ca. 5 Updates täglich) spätestens 15 Minuten nach Veröffentlichung verwendet wird.

Bei der Konfiguration der Suchläufe müssen Sie natürlich darauf achten, dass das jeweilige System individuell zu schützen ist. Das bedeutet, dass Sie Profile für bestimmte Verzeichnisse wie Downloads oder temporäre Dateien anlegen müssen, um anschließend mit dem Avira Planer darauf zugreifen zu können.

Hierfür legen Sie bitte ein neues Profil an: *Avira Control Center* > *PC Sicherheit* > *System Scanner* > *Neues Profil anlegen* (Icon +) und wählen anschließend, welche Verzeichnisse einbezogen werden sollen.



Allerdings bringt Avira bei der Installation sogenannte Standardprofile mit, die weitestgehend alle Möglichkeiten abdecken und in diesem HowTo verwendet werden. Unsere Empfehlungen zur Planung der Suchläufe im Sicherheitslevel Hoch finden Sie oben. Dabei wird das Profil Lokale Laufwerkeverwendet, was dafür sorgt, dass wirklich alle Laufwerke (Wechseldatenträger und Festplatten) einmaltäglich zur Mittagspause überprüft werden.

Hinweis
Dabei werden nur die Datenträger geprüft, die zum Zeitpunkt des Auftrags verbunden sind!

Zusätzlich zum täglichen Suchlauf über alle lokalen Laufwerke legen Sie einen weiteren Auftrag an, der einmal wöchentlich eine vollständige Systemprüfung vornimmt. Hierbei handelt es sich um ein spezielles Profil für die Suche auf allen lokalen Festplatten mit erweiterten Sucheigenschaften und Synchronisation mit dem Avira Hauptprogramm.

Alle Aufträge wurden im Darstellungsmodus unsichtbar angelegt, damit der Anwender nicht abgelenkt wird und ggf. den Fokus aus seiner aktiven Applikation verliert.

Hinweis
Bitte ändern Sie aufgrund Ihrer individuellen Vorgaben die Uhrzeiten, sodass der Suchlauf zu einem Zeitpunkt stattfindet, an dem nicht aktiv am System gearbeitet wird. Hintergrund ist, dass Sie auch während eines Suchlaufs am System arbeiten können, dabei allerdings die Performance sinkt.

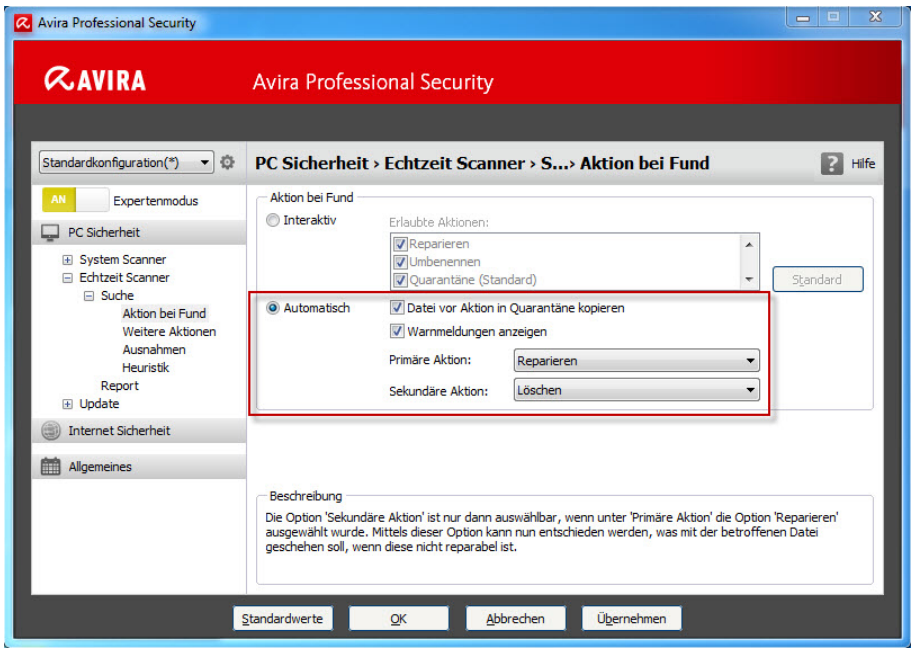
Tipp
Sie können den Suchlauf zu einer Uhrzeit nahe dem Feierabend planen und beim Anlegen des Auftrags im Planer die Option Computer herunterfahren, wenn „Auftrag ausgeführt wurde“ verwenden.

3. Sicherheitslevel Mittel

3.1 Modul übergreifend

Aktion bei Fund

- Aktion bei Fund: Automatisch
- Datei vor Aktion in Quarantäne kopieren
- Warnmeldungen anzeigen
- Primäre Aktion: reparieren
- Sekundäre Aktion: löschen



Durch die gleiche Konfiguration wie im Sicherheitslevel Hoch können Sie auch im Sicherheitslevel Mittel sicherstellen, dass der Suchlauf ohne Unterbrechung durchgeführt wird und alle Aktionen in den jeweiligen Modulen gleich konfiguriert sind. Dabei gelten die gleichen Regeln und Hinweise wie im Sicherheitslevel Hoch.

Wir empfehlen Ihnen, die Datei vor jeglicher Aktion in Quarantäne zu kopieren, damit Sie stets auf die Originaldatei zurückgreifen können.

Eine Reparatur funktioniert „nur“ bei Dateien, die infiziert wurden. Eine an sich virulente Datei wie ein Trojaner oder Wurm kann nicht repariert werden, diese Dateien werden aufgrund der Konfiguration gelöscht.

Echzeit-Scanner

Hinweis
Eine Reparatur durch den Echtzeit-Scanner ist nur bedingt möglich. Deshalb empfehlen wir Ihnen, immer einen Suchlauf nach einer mehrfachen Virenmeldung durch den Guard durchzuführen, um ein mögliches infiziertes System zu bereinigen.

Bitte führen Sie zudem bei einer Makroviren Meldung des Echtzeit-Scanners anschließend einen Suchlauf über die gemeldete Datei aus, um ebenfalls sicherzustellen, dass die Datei repariert wird.

Email-Schutz

Hinweis
Bei einem Malwarefund durch den Email-Schutz können Emails und Dateien nicht repariert werden, deshalb empfehlen wir Ihnen, die Emails komplett in Quarantäne zu verschieben.

Browser-Schutz

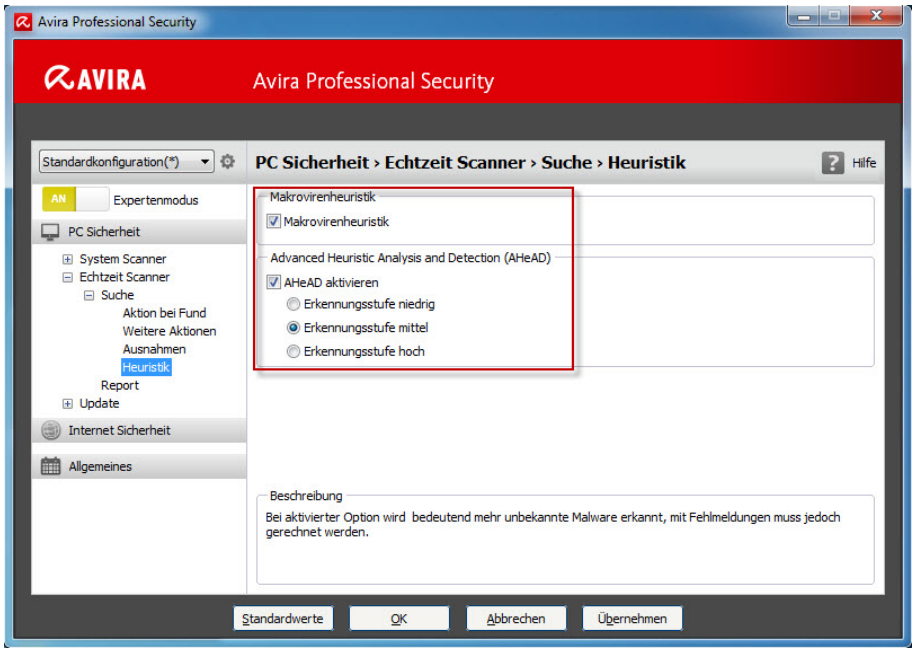
Hinweis
Wie beim Email-Schutz kann auch der Browser-Schutz keine Dateien reparieren, folglich empfehlen wir Ihnen ebenfalls, die Datei in Quarantäne zu verschieben. Wählen Sie hierfür die Primäre Aktion isolieren aus.

Heuristik

- Makrovirenheuristik aktiviert
- Advanced Heuristic (AHeAD) aktiviert: Erkennungsstufe mittel

Durch die Aktivierung der Makrovirenheuristik werden entsprechende Dokumente mit Makros nach möglichen Makroviren untersucht und ggf. repariert.

Durch die aktivierte Heuristik in der Erkennungsstufe mittel erkennt Avira auch unbekannte Malwaretypen, allerdings müssen Sie auch hier mit so genannten Fehlmeldungen rechnen.



Bitte aktivieren Sie die Heuristik in allen Modulen (System-Scanner, Echtzeit-Scanner, Email-Schutz und Browser-Schutz) und stellen Sie überall die Erkennungsstufe mittel bei AHeAD ein.

3.2 Modul System-Scanner

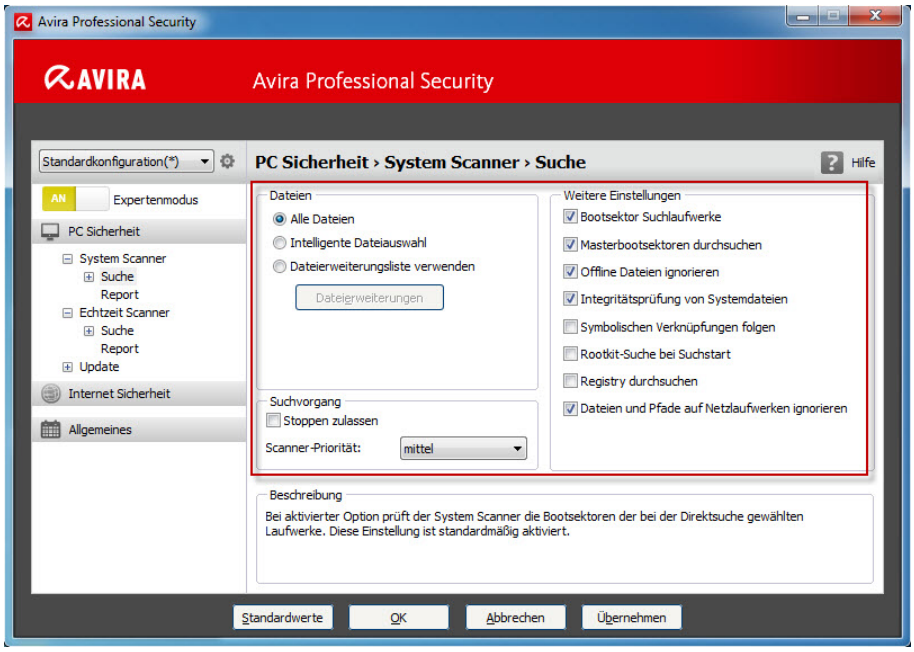
Suche

- Alle Dateien
- Bootsektor Suchlaufwerke
- Masterbootsektoren durchsuchen
- Offline Dateien ignorieren
- Integritätsprüfung von Systemdateien
- Dateien und Pfade auf Netzlaufwerke ignorieren
- Kein Stoppen zulassen
- Scanner Priorität: mittel

Dadurch werden auch im Sicherheitslevel Mittel alle Dateien vom Scanner überprüft, zudem werden Bootsektoren überprüft, der Suchlauf optimiert ausgeführt, sowie Offline Dateien und Netzlaufwerke ignoriert.

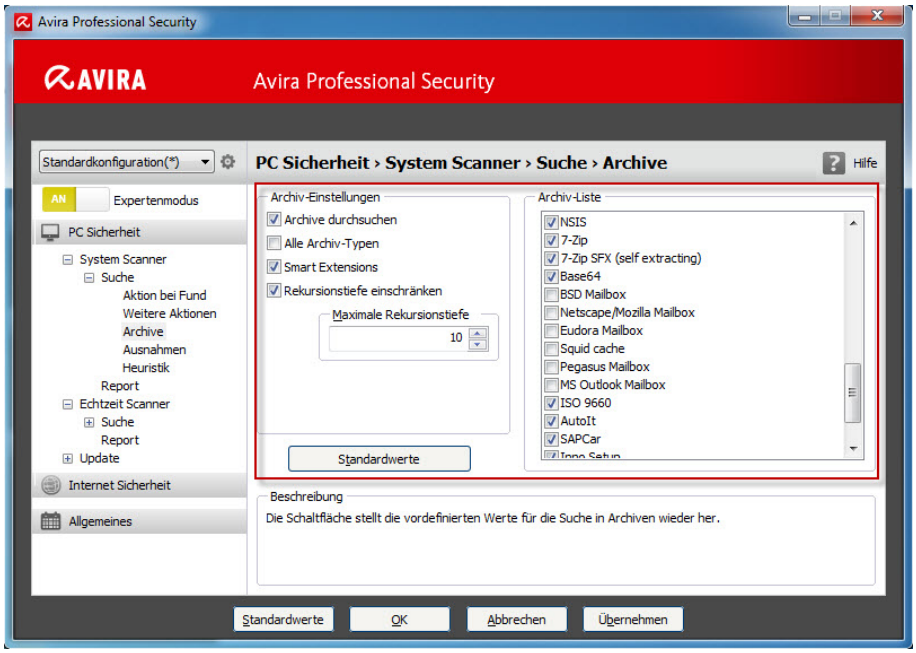
Es findet keine Rootkit-Suche bei jedem Suchlauf statt, diese Suche müssen Sie mit dem Suchprofil manuell durchführen.

Durch das Deaktivieren eines möglichen Stoppvorgangs können Sie auch hier einen kompletten Suchlauf garantieren. Der Anwender hat also keine Möglichkeit, den Suchlauf abzubrechen.



Archive

- Archive durchsuchen
- Smart Extensions
- Rekursionstiefe auf 10 eingeschränkt
- In der Archiv-Liste alle Formate außer Squid Cache und Mailboxen aktiviert



Durch die oben genannten Einstellungen stellen Sie sicher, dass die wichtigsten Archive entpackt und durchsucht werden.

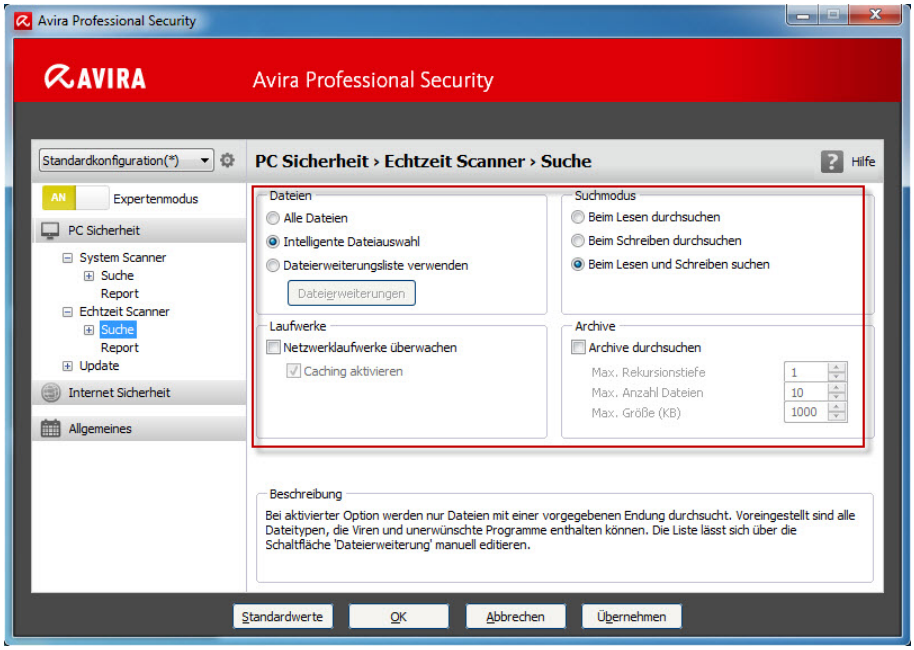
Die Option Smart Extensions sorgt dafür, dass Archive auch erkannt werden, falls die Dateiendung abweicht.

Hinweis
Falls eine virulente Datei in einem Archiv gefunden wird, wird das gesamte Archiv je nach Einstellung in Quarantäne gestellt und anschließend gelöscht. Eine Reparatur eines Archivs (Entfernung der virulenten Datei aus dem Archiv) ist aus technischen Gründen leider nicht möglich.

3.3 Modul Echzeit-Scanner

Suche

- Beim Lesen und Schreiben suchen
- Intelligente Dateiauswahl
- Keine Netzlaufwerke und Archive überwachen oder durchsuchen



Durch die Einstellungen werden alle Dateioperationen wie Öffnen, Ausführen und Schreiben durch den Echtzeit-Scanner überwacht.

Mit der Konfiguration Intelligente Dateiauswahl stellen Sie sicher, dass die Auswahl vollautomatisch von Avira Professional Security übernommen wird.

Das bedeutet, dass Avira Professional Security anhand des Inhalts einer Datei entscheidet, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht.

Dieses Verfahren ist langsamer als Dateierweiterungsliste, aber wesentlich sicherer. Außerdem werden keine Archive und Netzlaufwerke in Echtzeit überprüft. Diese Optionen werden im Sicherheitslevel Mittel nicht genutzt, da sie in der Regel durch andere Einstellungen und Mechanismen abgedeckt sind.

Archive

Hinweis
Falls sich eine Malware in einem Archiv befindet, kann man dies als eine Art Hülle um die virulente Datei an sich betrachten. Das bedeutet, dass keine unmittelbare Gefahr von der virulenten Datei ausgeht, solange sie nicht entpackt wird.

Beim Entpacken eines Archivs werden die enthaltenen Dateien schließlich im Originalformat hergestellt und dabei vom Echzeit-Scanner kontrolliert.

Sollte sich also eine virulente Datei in einem Archiv befinden und dieses Archiv entpackt werden, würde der Echtzeit-Scanner den Vorgang kontrollieren und dabei die Datei je nach Konfiguration in Quarantäne verschieben, reparieren oder löschen.

Netzlaufwerke

Hinweis
Falls diese Option aktiviert ist, werden verbundene Netzlaufwerke zusätzlich überwacht, siehe Sicherheitslevel Hoch.

Allerdings sollte man den Virenschutz direkt auf dem jeweiligen System installieren, um die Performance auszubalancieren und um auch das lokale System abzusichern.

Auch hier geht keine unmittelbare Gefahr aus, fallsdie Option deaktiviert wurde, da ein direktes Ausführen von einem Programm auf einem Netzlaufwerktrotzdem überwacht wird (feste Einstellung im Programm). Sobald also ein Tool oder eine Anwendung direkt vom Netzlaufwerk gestartet wird, findet eine Kontrolle durch den Guard statt.

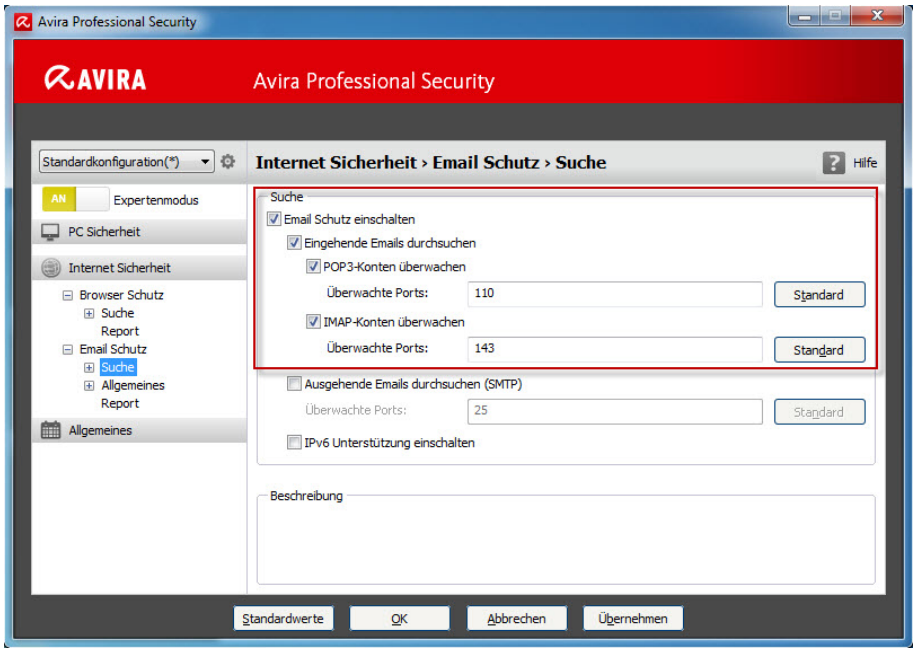
Zudem wird eine Datei bei einem Kopiervorgang trotzdem überprüft, da sie ja auf die lokale Festplatte geschrieben wird und dies in der Konfiguration Beim Lesen und Schreiben durchsuchenberücksichtigt wird.

3.4 Module Email-Schutz und Browser-Schutz

Diese Module werden wie bereits erwähnt ja nach Unternehmensumgebung und Anforderungen installiert. Falls Sie sich für eine Installation entschieden haben, empfehlen wir Ihnen bei einem hohen Sicherheitslevel die folgenden Einstellungen.

Email-Schutz - Suche

- Alle eingehenden Emails überwachen



Mit dieser Konfiguration können Sie sicherstellen, dass alle eingehenden Emails überwacht werden. Dabei werden sowohl POP als auch IMAP unterstützt und entsprechend berücksichtigt.

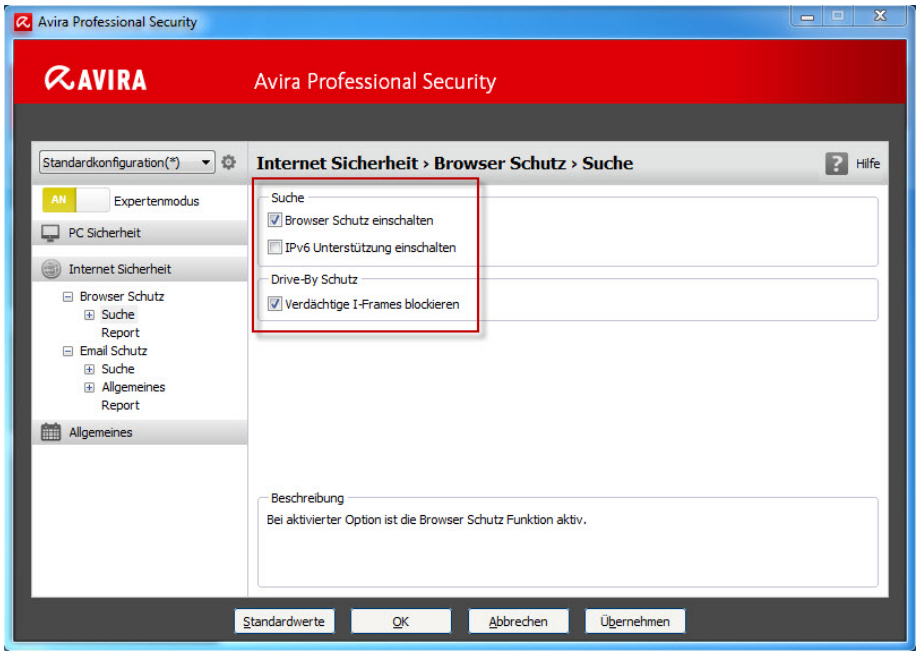
Browser-Schutz - Suche

- Browser-Schutz einschalten
- Verdächtige I-Frames blockieren

Wir empfehlen Ihnen die gleichen Einstellungen wie im Sicherheitslevel Hoch, damit auch hier verdächtige I-Frames entdeckt und gemeldet werden.

Informationen zum Thema I-Frames (Inlineframes) finden Sie im Kapitel Sicherheits-level Hoch sowie in der Onlinehilfe in unserem Programm.

Da die Malware Verbreitung immer häufiger durch infizierte Webseiten erfolgt und die verschiedenen Typen und Varianten jeden Tag neu entstehen, empfehlen wir Ihnen, alle verdächtigen I-Frames auch im Sicherheitslevel Mittel zu blockieren.



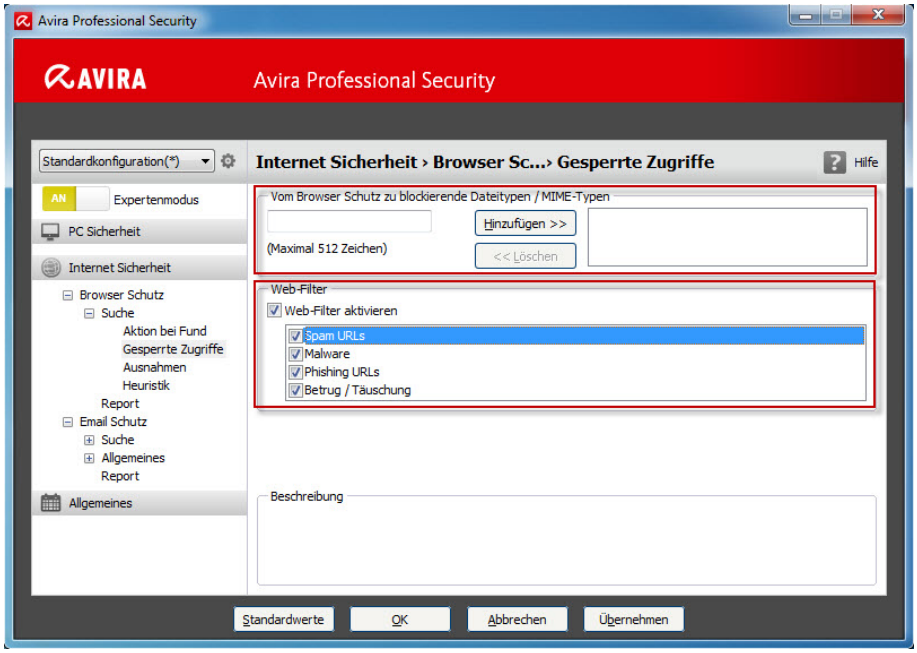
Browser-Schutz - Gesperte Zugriffe

- Vom Browser-Schutz zu blockierende Dateitypen / MIME-Typen: Nach Bedarf
- Web-Filter aktivieren: Alle Kategorien ausgewählt

Wie bereits im Kapitel Sicherheitslevel Hoch beschrieben, können Sie die zu blockierenden Datei- und MIME-Typen je nach Policy selbst bestimmen.

In der empfohlenen Konfiguration im Sicherheitslevel Mittel fehlen diese Einstellungen komplett, da keine unmittelbare Gefahr von diesen Dateien ausgeht.

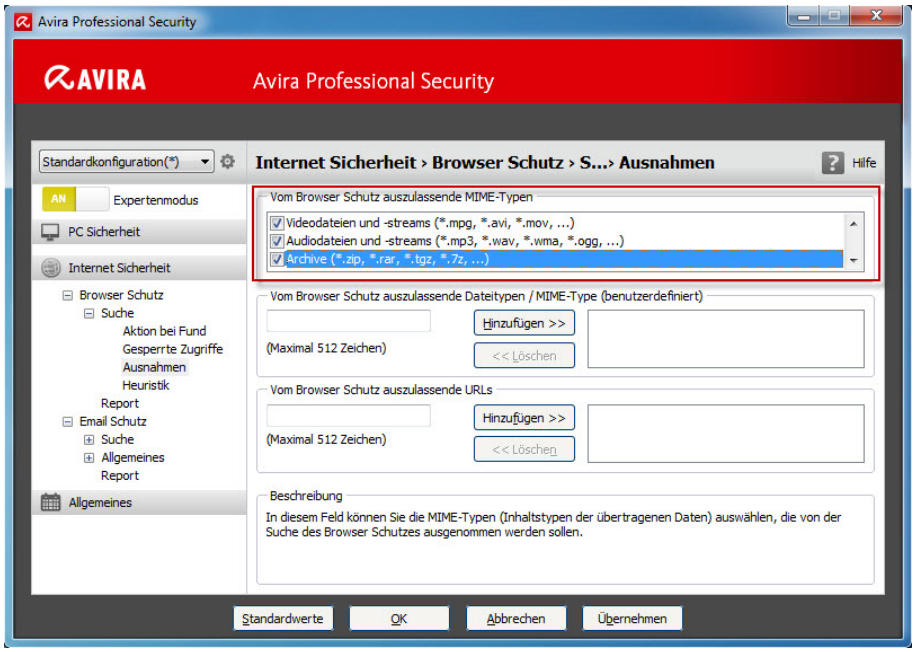
Im Webfilter selbst aktivieren Sie wie gehabt alle Kategorien. Malware- und Phishing URLs sind selbsterklärend, Betrug/Täuschung liegt vor, falls ein Anbieter eines unseriösen Angebots versucht, Ihnen einen Vertrag ohne konkrete Angaben zu verkaufen (Stichwort Abo Falle).



Browser-Schutz - Ausnahmen

- Auszulassende MIME-Typen: Video- und Audiodateien und –streams, sowie Archive werden ausgelassen und somit nicht geprüft

Die Video- und Audio-Dateien sollten aufgrund der Performance und der allgemeinen Verarbeitung im Webbrowser oder in anderen Applikationen stets ausgenommen werden, damit sie funktionieren.
Zudem empfehlen wir Ihnen, im Sicherheitslevel Mittel auch Archivdateien von der Suche auszunehmen, da von diesen Dateien keine unmittelbare Gefahr ausgeht.



Alles andere wie elektronische Dokumente oder ausführbare Dateien werden geprüft, folglich sind diese Ausnahmen deaktiviert.

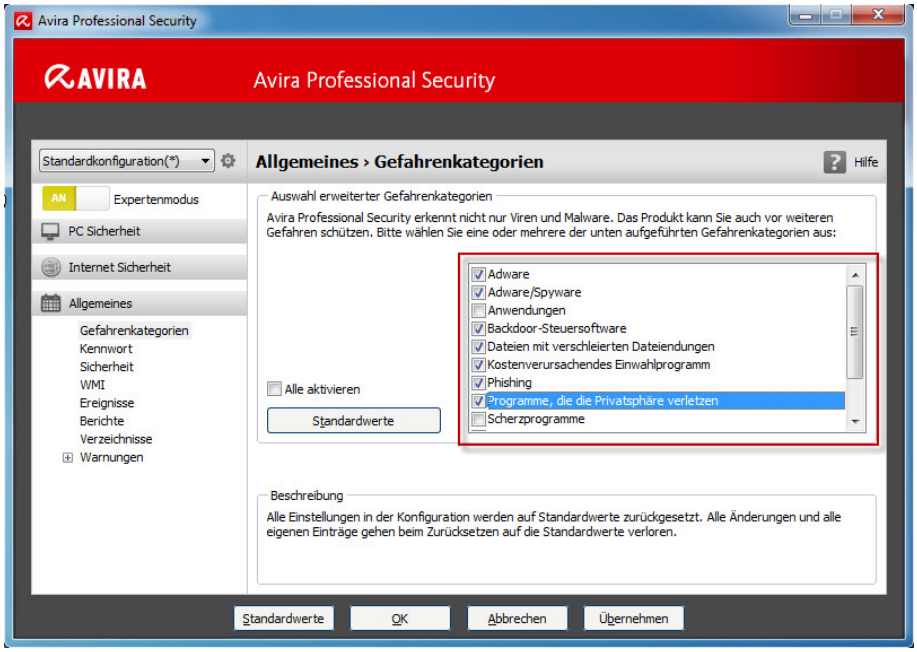
3.5 Allgemeine Einstellungen

Erweiterte Gefahrenkategorien

- Folgende Kategorien sind aktiviert: Adware/Spyware, Backdoor-Steuersoftware, Dateien mit verschleierten Dateiendungen, Kostenverursachendes Einwahlprogramm, Phishing und Programme, die die Privatsphäre verletzen

Neben der üblichen Viren und Malware Erkennung können Sie mit den zusätzlichen Optionen dafür sorgen, dass zusätzliche Gefahrenquellen wie Backdoor-Steuersoftware, Dialer oder SPR Programme überprüft und ggf. blockiert werden.

Da von sonstigen Applikationen (APPL) oder Spielen und Witzprogrammen keine Gefahr ausgeht, wird auf die Erkennung solcher Dateien im Sicherheitslevel Mittel verzichtet.



Weitere Informationen zu den unterschiedlichen Kategorien finden Sie im Programm integrierten Hilfe, die Sie mit der F1 Taste aufrufen können.

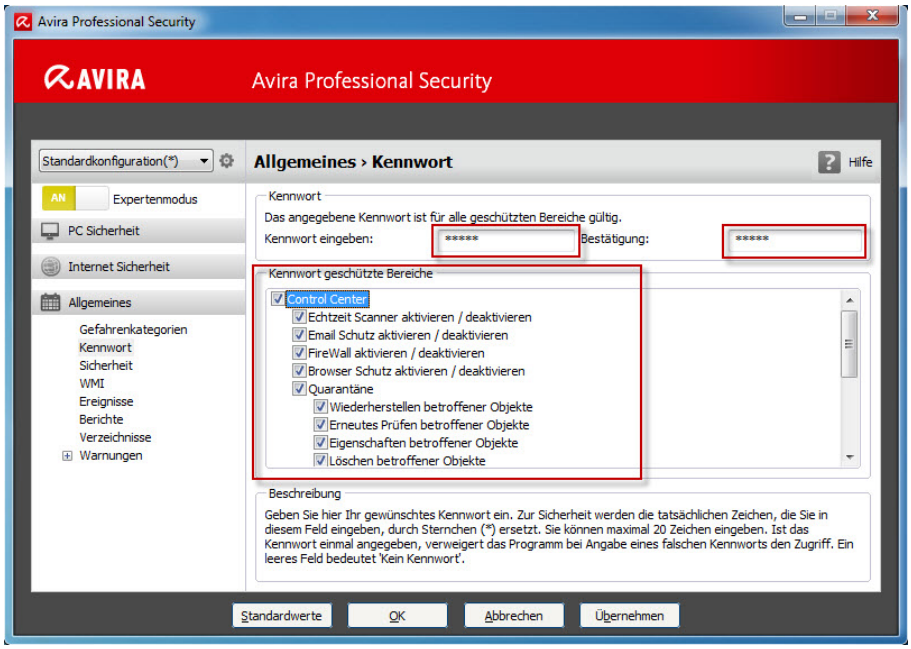
Kennwort

- Bitte hinterlegen Sie einen Kennwortschutz für alleBereiche

Im Sicherheitslevel Mittel empfehlen wir Ihnen, ebenfalls einen Kennwortschutz für alle Bereiche zu hinterlegen.

Dadurch können ohne Kennwort überhaupt keine Änderungen vorgenommen werden.

Außerdem können Sie das Quarantäne-management absichern und verhindern, dass einzelne Module (Stichwort: Änderungsinstallation) oder gar das komplette Anti-Vir Programm deinstalliert werden.



Diese Einstellung empfehlen wir generell und im Speziellen bei Anwendern, die aufgrund bestimmter Voraussetzungen mit administrativen Rechten arbeiten.

Hinweis
Im Sicherheitslevel Hoch wird das Passwort aviraverwendet, bitte ändern Sie dieses Passwort nach Einspielen der mitgelieferten INI Datei!

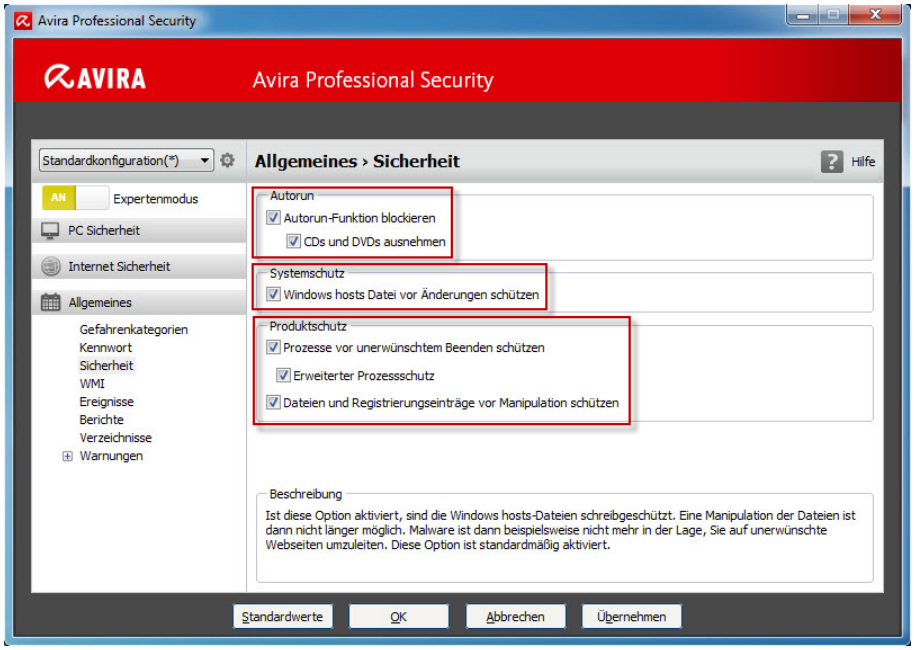
Sicherheit

- Autorun: Autorun-Funktion blockieren - CDs und DVDs ausnehmen
- Systemschutz: Windows hosts Datei vor Änderungen schützen
- Produktschutz: Prozesse vor unerwünschtem Beenden schützen, Erweiterter Prozessschutz und Dateien und Registryeinträge schützen

Erhöhen Sie die Sicherheit, in dem Sie dafür sorgen, dass Sie die Autorun-Funktion blockieren.

Ist die Systemschutz Option aktiviert, dann ist eine Manipulation der hosts-Dateien nicht länger möglich. Malware ist dann nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten.

Zudem sorgen Sie mit dem Produktschutz auch im Sicherheitslevel Mittel für eine zusätzliche Absicherung von Avira, in dem Sie sicherstellen,dass keine Prozesse beendet oder Dateien (z.B. Konfigurationsdatei) bzw. Registry Einträge (z.B. Dienst-einstellungen) manipuliert werden können.

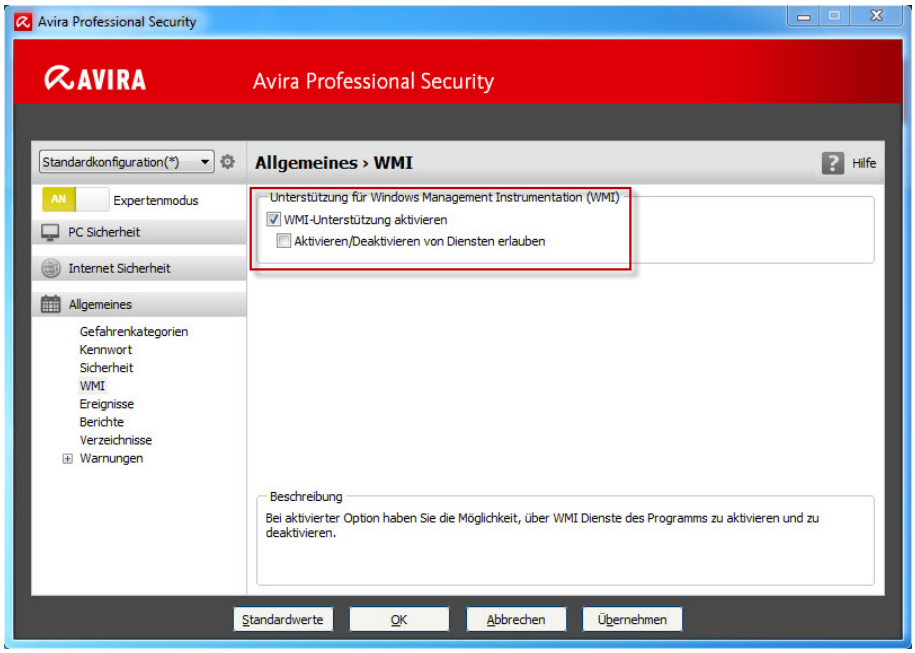


WMI

- Option kann je nach Anforderung aktiviert werden
- Das Aktivieren und Deaktivieren sollte aber auch im Sicherheitslevel Mittel unterbunden und somit nicht möglich sein

Avira bietet die Möglichkeit, verschiedene Daten wie Updatestand, Status des Browser-Schutz‘s oder das Ergebnis des letzten Suchlaufs per WMI abzufragen.

Eine vollständige Referenz der WMI-Schnittstelle können Sie bei uns anfordern.



Falls Sie diese Schnittstelle nutzen möchten, aktivieren Sie bitte die Option, unterbinden Sie aber die Möglichkeit, Module deaktivieren zu können. Falls Sie aber WMI nicht verwenden möchten, empfehlen wir Ihnen, auch im Sicherheitslevel Mittel die Option zu deaktivieren, damit ein Angreifer keine Informationen abfragen kann.

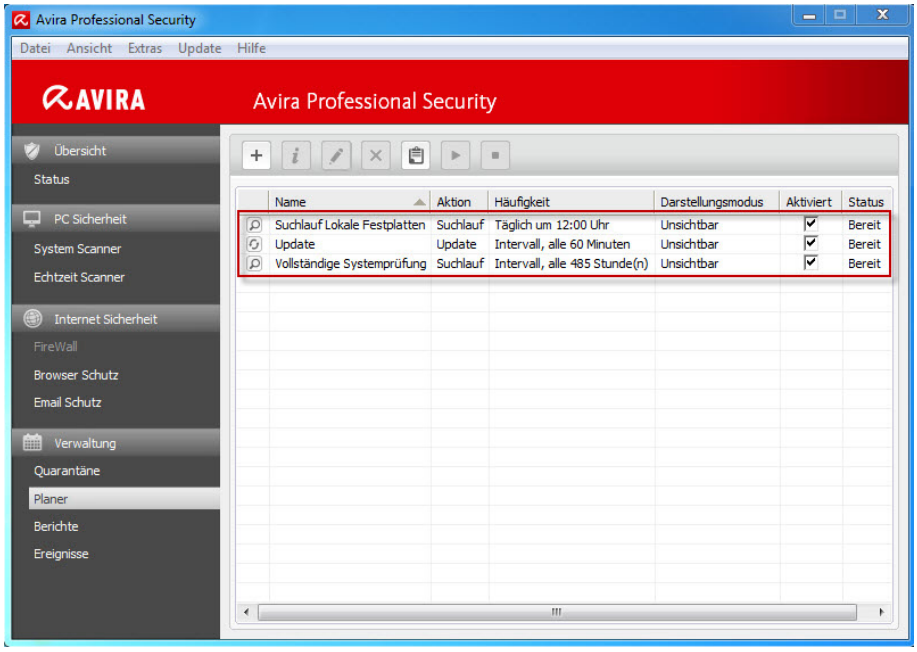
3.6 Avira Planer

Im Planer können Sie die Aufträge (so genannte Jobs) lokal anlegen, um die lokale Avira Instanz hinsichtlich Updates und Suchläufen zu steuern. Diese Planung können Sie natürlich wie bereits im Kapitel Sicherheitslevel Hoch zentral über das AMC steuern und somit eine einheitliche Planung für alle Klienten anlegen. Weitere Informationen finden Sie im Handbuch und HowTo der Professional und AMC.

- Update
  - Intervall – Alle 60 Minuten

- Suchlauf
  - Lokale Festplatten – Täglich um 12:00 Uhr (Mittagspause)
  - Vollständige Systemprüfung – Alle 20 Tage

- Alle Aufträge im Darstellungsmodus unsichtbar



Durch die Einstellung Update alle 60 Minuten stellen Sie sicher, dass nahezu jedes Update (ca. 5 Updates täglich) verwendet wird und Avira Professional Security jede Stunde aktualisiert wird.

Bei der Konfiguration der Suchläufe müssen Sie wie bereits im Kapitel Sicherheitslevel Hoch erwähnt darauf achten, dass das jeweilige System individuell zu schützen ist. Das bedeutet, dass Sie Profile für bestimmte Verzeichnisse wie Downloads oder temporäre Dateien anlegen müssen, um anschließend mit dem Avira Planer darauf zugreifen zu können.

Avira bringt bei der Installation so genannte Standardprofile mit, die nahezu alle Möglichkeiten abdecken und in diesem HowTo verwendet werden.

Unsere Empfehlungen zur Planung eines Suchlaufs im Sicherheitslevel Mittel finden Sie oben. Dabei wird das Profil Lokale Festplatten verwendet, was dafür sorgt, dass alle lokalen Festplatten einmal täglich zur Mittagspause überprüft werden.
Falls Sie an einem System verstärkt mit Wechseldatenträger arbeiten, verwenden Sie bitte das Profil Lokale Laufwerke, das im Kapitel Sicherheitslevel Hoch beschrieben wird.

Die vollständige Systemprüfung können Sie aufgrund der Einstellungen im Sicherheitslevel Mittel alle 20 bis 30 Tage durchführen lassen. Planen Sie hierfür einfach einen Auftrag mit einer Intervalleinstellung von 20 Tagen.

Alle Aufträge wurden im Darstellungsmodus unsichtbar angelegt, damit der Anwender nicht abgelenkt wird und ggf. den Fokus aus seiner aktiven Applikation verliert.

Hinweis
Bitte ändern Sie aufgrund Ihrer individuellen Vorgaben die Uhrzeiten, sodass der Suchlauf zu einem Zeitpunkt stattfindet, an dem nicht aktiv am System gearbeitet wird. Hintergrund ist, dass Sie auch während eines Suchlaufs am System arbeiten können, dabei allerdings die Performance sinkt.

Tipp
Sie können den Suchlauf zu einer Uhrzeit nahe dem Feierabend planen und beim Anlegen des Auftrags im Planer die Option Computer herunterfahren, wenn Auftrag ausgeführt wurde, verwenden.

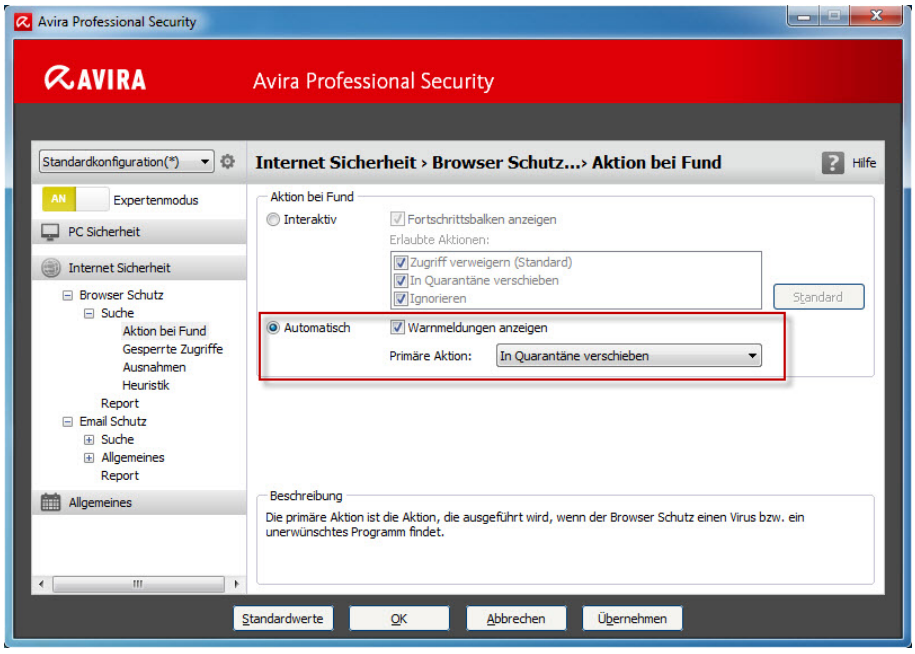
4. Sicherheitslevel Niedrig

4.1 Modul übergreifend

Aktion bei Fund

- Aktion bei Fund: Automatisch
- Warnmeldungen anzeigen
- Primäre Aktion: In Quarantäne verschieben

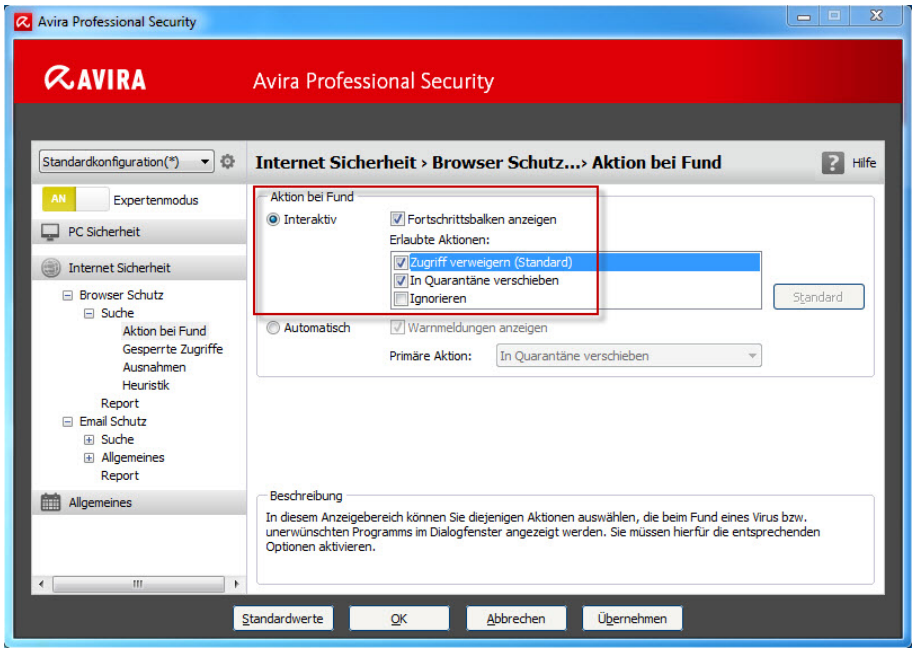
Durch die gleiche Konfiguration wie im Sicherheitslevel Mittel und Hoch können Sie auch im Sicherheitslevel Niedrig sicherstellen, dass der Suchlauf ohne Unterbrechung durchgeführt wird. Wir empfehlen Ihnen, auch hier die Datei vor jeglicher Aktion in Quarantäne zu kopieren.



Hinweise zum Browser-Schutz

- Interaktiver Modus
- Erlaubte Aktionen reduzieren auf folgende Optionen: Zugriff verweigern (Standard) in Quarantäne verschieben

Durch die Reduzierung der erlaubten Aktionen können Sie sicherstellen, dass ein Anwender zwar interaktiv reagieren darf, aber die Datei nicht löschen oder die Meldung, sprich den Virenfund ignorieren kann.
Wir empfehlen Ihnen, nach einer Virenmeldung immer einen Suchlauf durchzuführen.



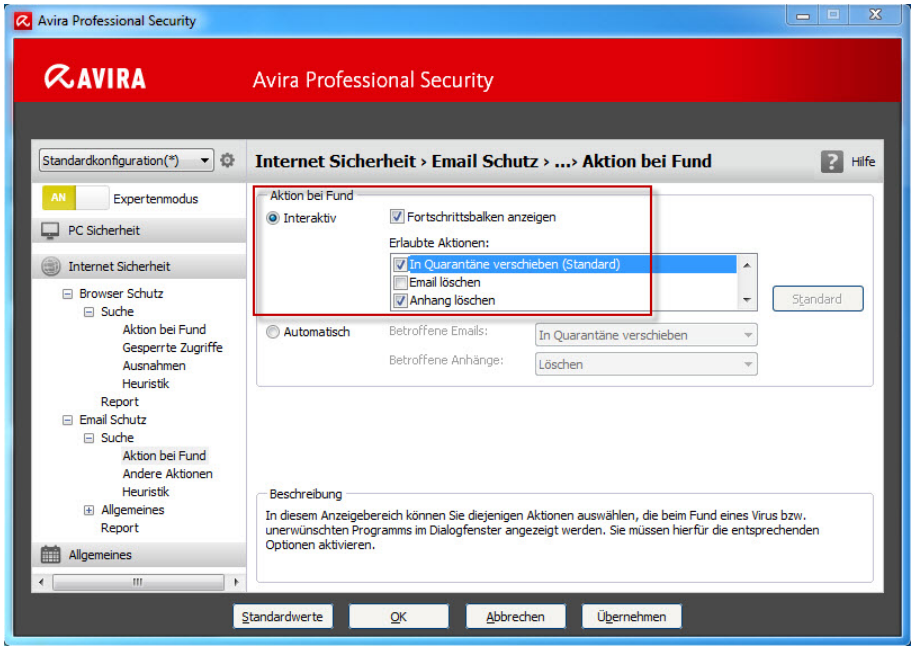
Hinweise zum Email-Schutz

- Interaktiver Modus
- Fortschrittsbalken anzeigen
- Erlaubte Aktionen reduzieren auf folgende Optionen: In Quarantäne verschieben (Standard) und Anhänge in Quarantäne verschieben

Auch hier können Sie durch die Verringerung der erlaubten Aktionen gewährleisten, dass ein Anwender zwar interaktiv reagieren darf, aber die Email nicht löschen oder die Meldung, sprich den Virenfund ignorieren kann.

Achtung
Bei einem Fund durch den Avira Email-Schutz können Emails und Dateianhänge nicht repariert werden.

Bitte betrachten Sie den Fortschrittsbalken lediglich als Möglichkeit zur Anzeige für einen Anwender, dies spielt hinsichtlich der Sicherheit natürlich keine Rolle.

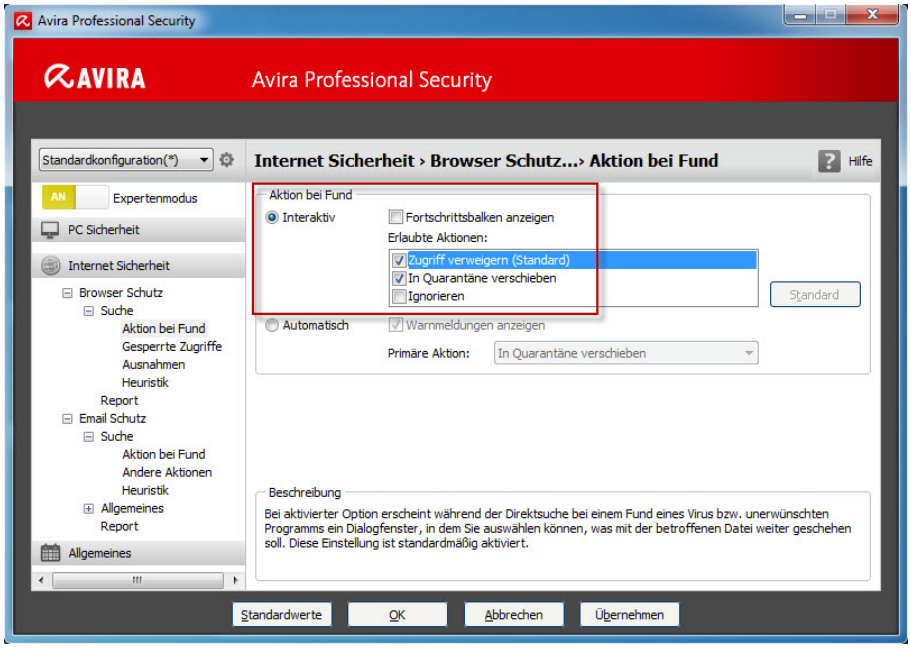


Hinweise zum Browser-Schutz

- Interaktiver Modus
- Kein Fortschrittsbalken anzeigen
- Erlaubte Aktionen reduzieren auf folgende Optionen: „Zugriff verweigern (Standard)“ und „In Quarantäne verschieben“

Falls Webseiten oder Downloads aufgrund der Internetanbindung länger dauern, empfehlen wir Ihnen, die Fortschrittsanzeige zu aktivieren.

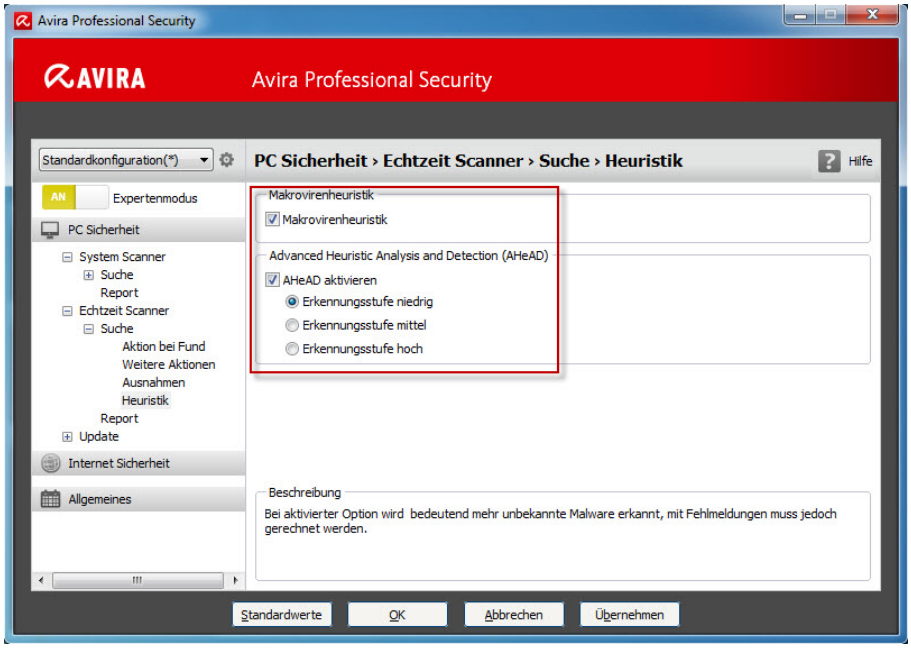
Auch hier können Sie durch die Verringerung der erlaubten Aktionen gewährleisten, dass ein Anwender zwar interaktiv reagieren darf, aber die Meldung, sprich den Virenfund nicht ignorieren kann.



Heuristik

- Makrovirenheuristik aktiviert
- Advanced Heuristic (AHeAD) aktiviert: Erkennungsstufe niedrig

Durch die Aktivierung der Makrovirenheuristik werden auch im Sicherheitslevel Niedrig entsprechende Dokumente mit Makros nach möglichen Makroviren untersucht und ggf. repariert.



Falls im Unternehmen keine Makros eingesetzt werden bzw. die Funktionalität aufgrund der Policy deaktiviert wurde, können Sie die Makrovirenheuristik in allen Modulen deaktivieren.

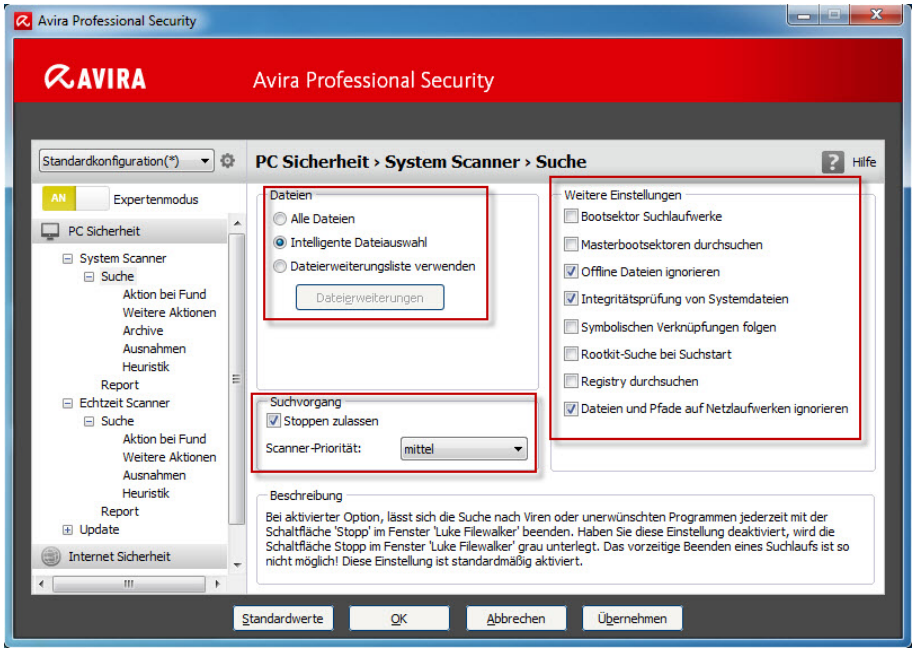
Bitte aktivieren Sie die Heuristik in allen Modulen und stellen Sie ggf. überall die Erkennungsstufe niedrig bei AHeAD ein. Durch die niedrige Einstellung ist das Risiko so genannter Fehlmeldungen gering.
Sie finden die Konfiguration der Heuristik in allen Modulen unterhalb von Suche.

4.2 Modul System-Scanner

Suche

- Dateien: Intelligente Dateiauswahl
- Weitere Einstellungen: Offline Dateien ignorieren; Integritätsprüfung von Systemdateien; Dateien und Pfade auf Netzlaufwerke ignorieren;
- Suchvorgang: Stoppen zulassen
- Scanner Priorität: mittel

Durch die Konfiguration werden im Sicherheitslevel Niedrig nur die relevanten und potentiell gefährlichen Dateien vom Scanner überprüft.

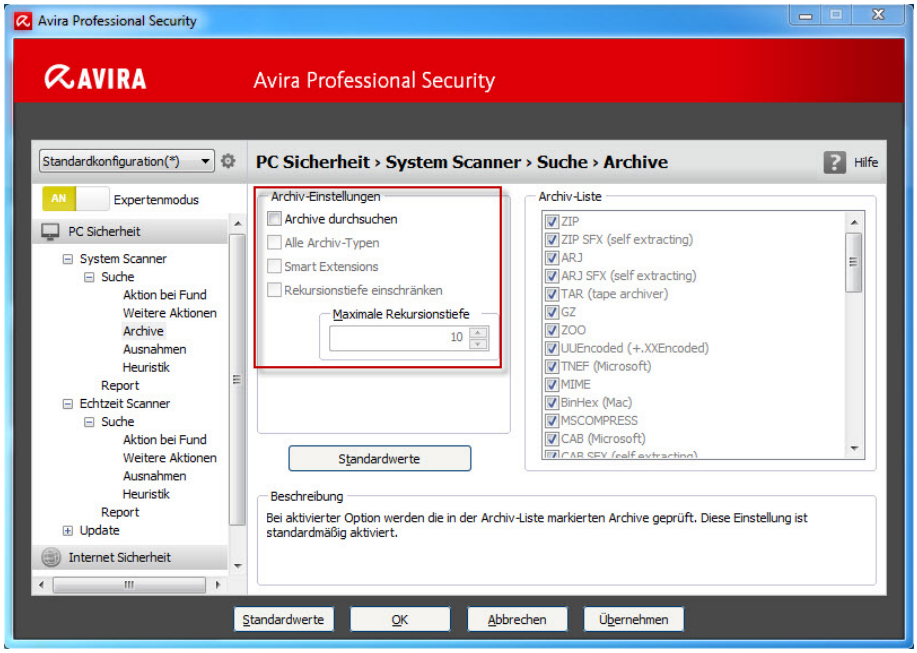


Es werden keine Bootsektoren überprüft, da diese Art der Infektion in der letzten Zeit sehr stark nachgelassen hat. Es wird keine Rootkit-Suche beim Start durchgeführt, zudem werden Offline Dateien und Netzlaufwerke wie im Sicherheitslevel Mittel ignoriert. Außerdem wird dem Anwender die Möglichkeit gegeben, den Suchlauf zu stoppen.

Archive

- Archiv-Einstellungen: Es werden keine Archive durchsuch

Durch die oben genannten Einstellungen werden keinerlei Archive durchsucht.
Wie bereits erwähnt, stellt eine Malware in einem Archiv keine unmittelbare Gefahr dar. Beim Entpacken eines Archivs werden die enthaltenen Dateien im Originalformat hergestellt und dabei vom Echtzeit-Scanner kontrolliert.



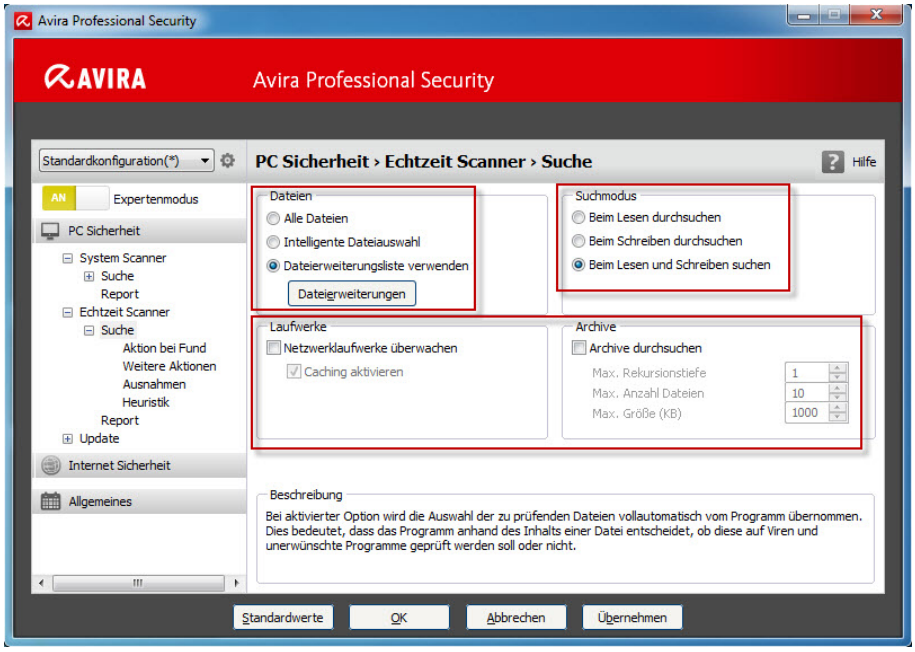
Sollte sich also eine virulente Datei in einem Archiv befinden und dieses Archiv entpackt werden, würde der System Scanner den Vorgang kontrollieren und dabei die Datei je nach Konfiguration in Quarantäne verschieben, reparieren oder löschen.

4.3 Modul Echtzeit-Scanner

Suche

- Dateien: Dateierweiterungsliste verwenden
- Suchmodus: Beim Lesen und Schreiben suchen
- Keine Netzlaufwerke und Archive durchsuchen

Durch die Einstellungen werden auch im Sicherheitslevel Niedrig alle Operationen wie Öffnen, Ausführen und Schreiben durch den Guard überwacht.



Allerdings werden dabei „nur“ die Dateien mit der jeweiligen Endung berücksichtigt, die in der Dateierweiterungsliste enthalten sind.

Dies bedeutet, ein mögliches Vortäuschen einer ausführbaren Datei durch eine harmlose Dateiendung wird nicht erkannt.

Dieses „Manko“ können Sie durch Pflege der Dateierweiterungsliste beseitigen, in der bereits die gängigsten Endungen enthalten sind.

4.4 Module Email-Schutz und Browser-Schutz

In diesem Falle unterscheidet sichdie Konfiguration im Level Niedrig nur noch marginal vom Level Mittel.

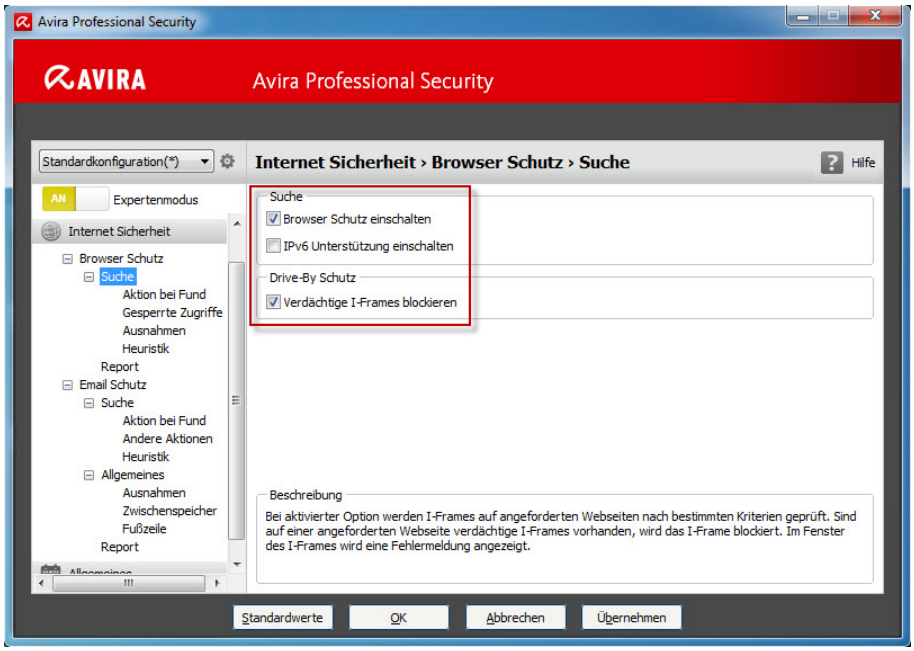
Email-Schutz – Suche

- Alle eingehenden Emails überwachen(siehe Sicherheitslevel Mittel

Browser-Schutz – Suche

- Browser-Schutz aktivieren
- Verdächtige I-Frames blockieren

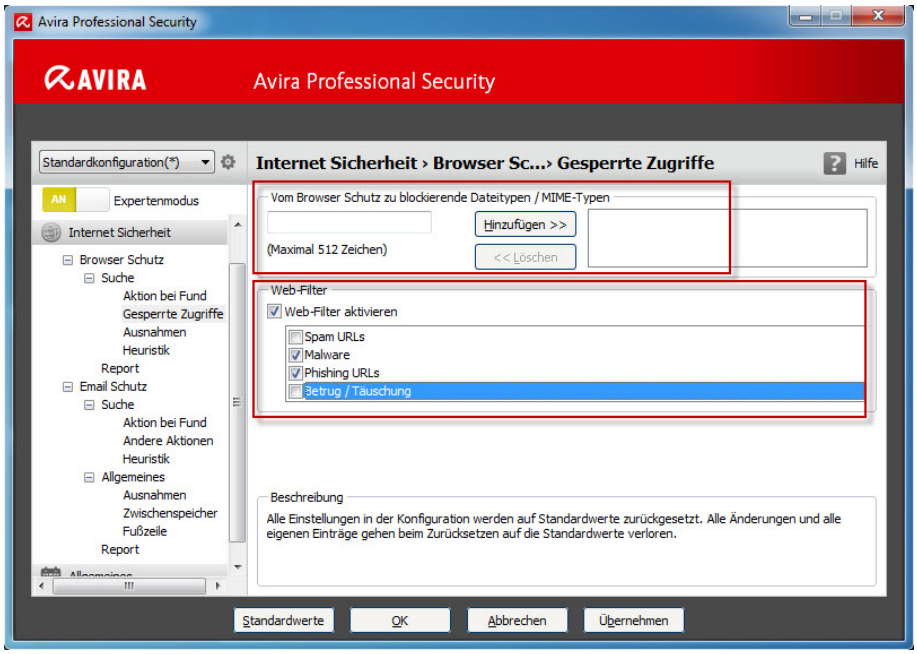
Der Browser-Schutz ist aktiv und überprüft verdächtige I-Frames im Standardmodus.



Browser-Schutz – Gesperrte Zugriffe

- Keine vom Browser-Schutz zu blockierende Dateitypen / MIME-Typen
- Web-Filter aktivieren: Kategorien Malware und Phishing aktiviert

Wie bereits erwähnt, bestimmen Sie die zu blockierenden MIME-Typen je nach Policy.

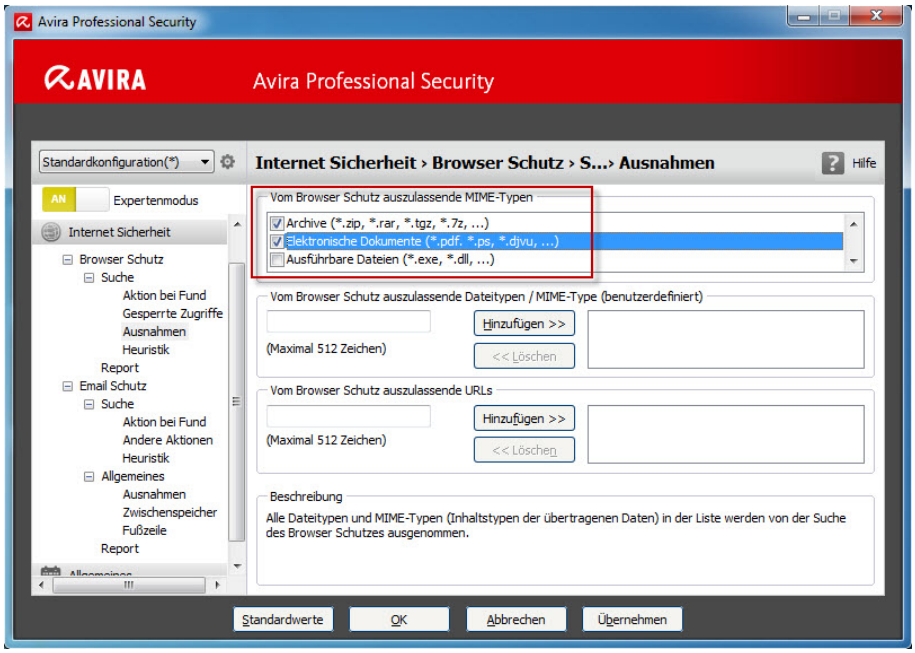


Im Web-Filter selbst aktivieren Sie die Kategorien Malware- und Phishing URLs, da von hier ein entsprechendes Riskio ausgeht.
Die Kategorien Spam URLs und Betrug / Täuschung sind nicht aktiv, da es sich hierbei um keine potentiell gefährlichen URLs handelt.

Browser-Schutz – Ausnahmen

- Alle MIME-Typen bis auf ausführbare Dateien als Ausnahme definiert

Durch diese Konfiguration bestimmen Sie, dass Video-, Audio- und Archivdateien sowie elektronische Dokumente wie z. B. PDF-Dateien nicht kontrolliert werden.



Allerdings werden trotzdem alle ausführbaren Dateien auch im Sicherheitslevel Niedrig überwacht, da von diesen Dateien die größte Gefahr ausgeht.

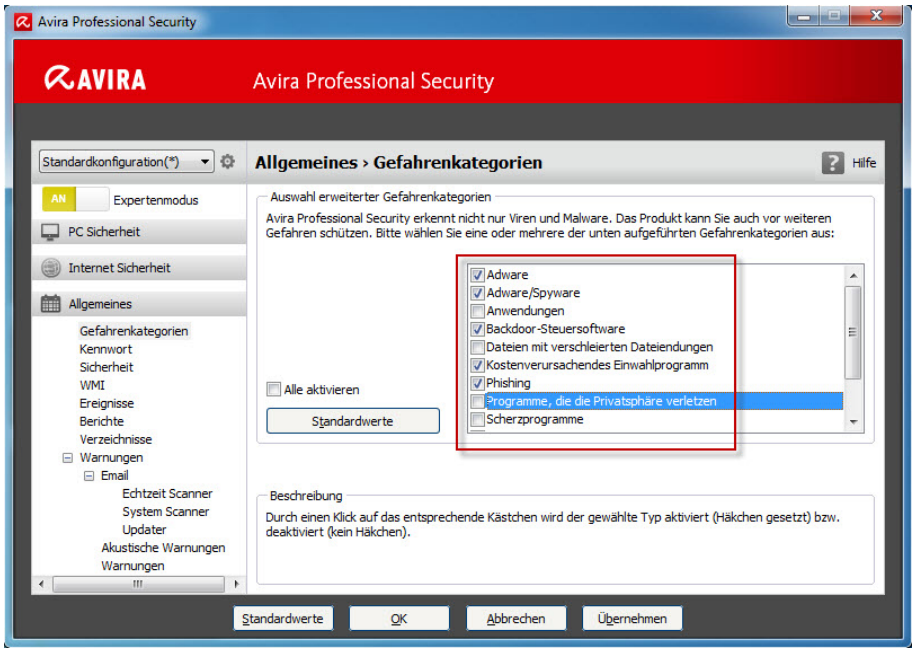
4.5 Allgemeine Einstellungen

Erweiterte Gefahrenkategorien

- Folgende Kategorien sind aktiv: Adware/Spyware, Backdoor-Steuersoftware, Dialer und Phishing

Neben der üblichen Viren und Malware Erkennung können Sie mit den zusätzlichen Optionen dafür sorgen, dass zusätzliche Gefahrenquellen wie Backdoor-Steuersoftware oder Dialer überprüft und ggf. blockiert werden.

Weitere Informationen zu den unterschiedlichen Kategorien finden Sie in der im Programm integrierten Online Hilfe, die Sie mit der Taste F1 aufrufen können.



Kennwort

- Im Sicherheitslevel Niedrig können Sie je nach Anforderung auf einen Kennwortschutz verzichten

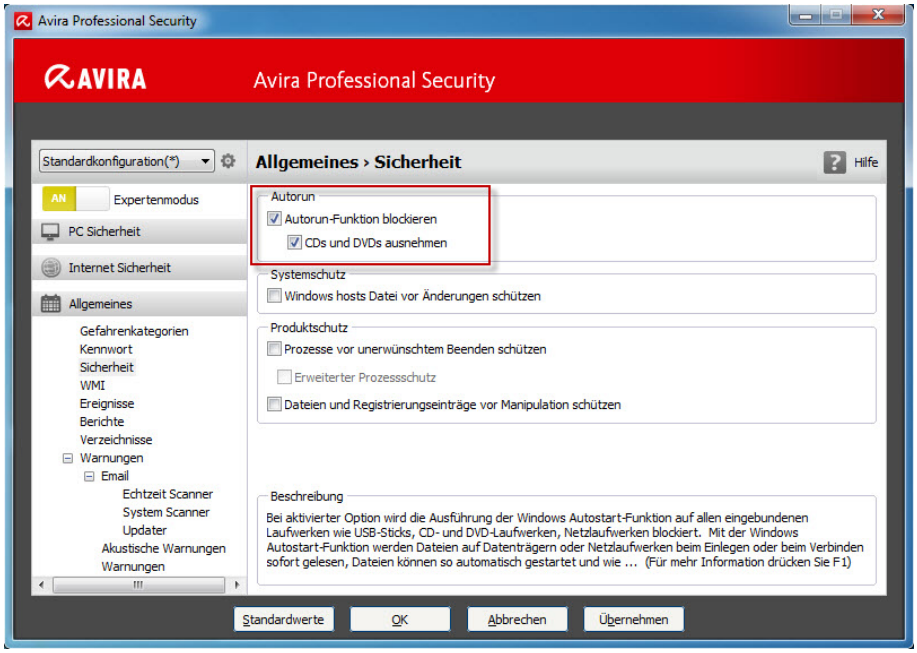
Sicherheit

- Warnung, falls letztes Update älter als drei Tage mit Hinweis
- Vollständige Systemprüfung mit Status gelb nach 300 und rot nach 350 Tagen
- Kein Produktschutz aktiviert

Die Ausführung der Windows Autostart-Funktion wie USB-Sticks wird auf Netzlaufwerken blockiert.

Auf die Systemprüfung wird quasi durch Konfiguration von sehr hohen Werten verzichtet.

Zudem wird kein Produktschutz eingesetzt, was wiederum die Möglichkeit bietet, den Avira Antivirus durch selbst geschriebene Batchdateien o. ä. zu steuern.



Hinweis
Falls Sie Avira Antivirus nicht selbst über Batchdateien oder andere Mechanismen steuern möchten, empfehlen wir Ihnen, den Produktschutz auch im Sicherheitslevel Niedrig zu aktivieren!

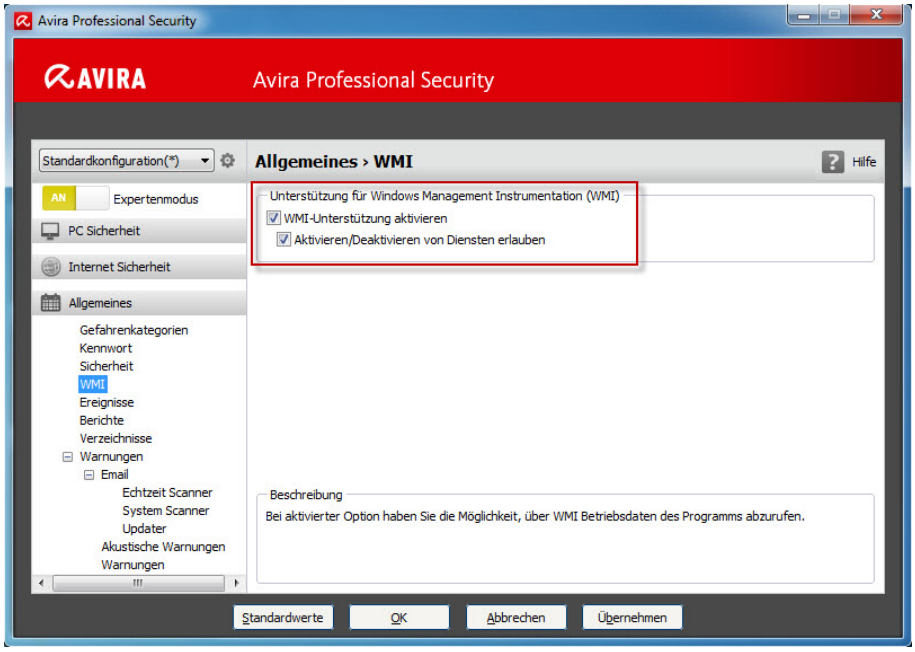
WMI

- Option inkl. Aktivieren und Deaktivieren kann je nach Anforderung verwendet werden

Im Sicherheitslevel Niedrig können Sie die volle Funktionalität der Avira WMI Schnittstelle verwenden. Sie haben dadurch die Möglichkeit, Betriebsdaten von Avira Professional (Updatestand, Status des Guards, etc.) oder Module wie Echtzeit-Scanner, Email-Schutz oder Browser-Schutz anzusteuern.

Eine vollständige Referenz der WMI-Schnittstelle können Sie bei uns anfordern.

Hinweis
Falls Sie jedoch WMI nicht verwenden möchten, empfehlen wir Ihnen, auch im Sicherheitslevel Niedrig die Option zu deaktivieren, damit ein Angreifer keine Informationen abfragen oder gar Module manipulieren kann.



4.6 Avira Planer

Im Avira Planer können Sie die Aufträge (so genannte Jobs) lokal anlegen, um die lokale Avira Instanz hinsichtlich Updates und Suchläufen zu steuern. Diese Planung können Sie natürlich wie bereits im Kapitel Sicherheitslevel Hoch zentral über die AMC steuern und somit eine einheitliche Planung für alle Klienten anzulegen. Weitere Informationen finden Sie im Handbuch und HowTo der Professional und AMC.

Update
- Intervall – Alle 2 Stunden

Suchlauf
- Lokale Festplatten – Wöchentlich am Freitag um 12:00 Uhr

- Alle Aufträge im Darstellungsmodus unsichtbar

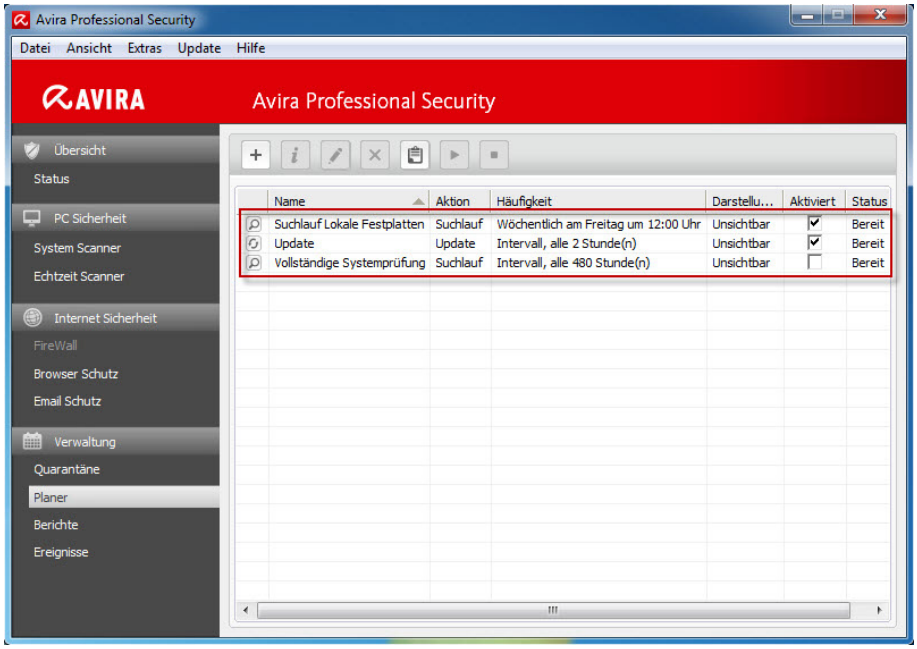
Durch die Einstellung Update alle 2 Stunden stellen Sie sicher, dass nahezu jedes Update (ca. 5 Updates täglich) verwendet wird.

Im Sicherheitslevel Niedrig wird aufgrund der hohen Werte in der Konfiguration auf einen Auftrag zur vollständigen Systemprüfung im Planer verzichtet.

Bei der Konfiguration der Suchläufe müssen Sie wie bereits im Kapitel Sicherheitslevel Hoch und Mittel erwähnt darauf achten, dass das jeweilige System individuell zu schützen ist.

Das bedeutet, dass Sie Profile für bestimmte Verzeichnisse wie Downloads oder temporäre Dateien anlegen müssen, um anschließend mit dem Avira Planer darauf zugreifen zu können.

Eine Anleitung finden Sie im Abschnitt Avira Planer im Kapitel Sicherheitslevel Hoch und Mittel.



Avira bringt bei der Installation so genannte Standardprofile mit, die nahezu alle Möglichkeiten abdecken und in diesem HowTo verwendet werden.

Unsere Empfehlungen zur Planung eines Suchlaufs im Sicherheitslevel Niedrig finden Sie oben. Dabei wird das Profil „Lokale Festplatten“ verwendet, was dafür sorgt, dass alle lokalen Festplatten einmal wöchentlich am Freitag zur Mittagspause überprüft werden.

Falls Sie an einem System verstärkt mit Wechseldatenträger arbeiten, verwenden Sie bitte das Profil Lokale Laufwerke, das im Kapitel Sicherheitslevel Hoch beschrieben wird.

Alle Aufträge wurden im Darstellungsmodus unsichtbar angelegt, damit der Anwender nicht abgelenkt wird und ggf. den Fokus aus seiner aktiven Applikation verliert.

Hinweis
Bitte ändern Sie aufgrund Ihrer individuellen Vorgaben die Uhrzeiten, sodass der Suchlauf zu einem Zeitpunkt stattfindet, an dem nicht aktiv am System gearbeitet wird. Hintergrund ist, dass Sie auch während eines Suchlaufs am System arbeiten können, dabei allerdings die Performance sinkt.

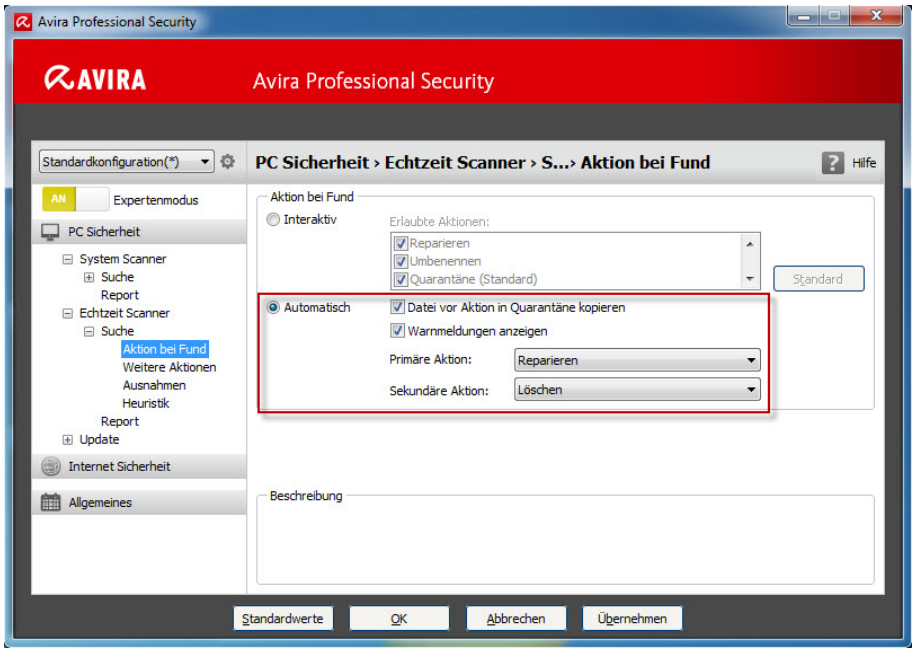
Tipp
Sie können den Suchlauf zu einer Uhrzeit nahe dem Feierabend planen und beim Anlegen des Auftrags im Planer die Option Computer herunterfahren, wenn Auftrag ausgeführt wurde verwenden.

5. Empfehlungen des Avira Supports

5.1 Modul übergreifend

Aktion bei Fund

- Aktion bei Fund: Automatisch
- Datei vor Aktion in Quarantäne kopieren
- Warnmeldungen anzeigen
- Primäre Aktion: reparieren
- Sekundäre Aktion: löschen



Durch die Konfiguration einer bzw. mehrerer automatischer Aktionen bei einem möglichen Fund können Sie sicherstellen, dass der Suchlauf ohne Unterbrechung durchgeführt wird und alle Aktionen in den jeweiligen Modulen gleich ausgewählt sind.

Wir empfehlen Ihnen, die Datei vor jeglicher Aktion in Quarantäne zu kopieren, damit Sie stets auf die Originaldatei zurückgreifen können.

Eine Reparatur funktioniert „nur“ bei Dateien, die infiziert wurden. Eine an sich virulente Datei wie ein Trojaner oder Wurm kann nicht repariert werden, diese Dateien werden aufgrund der Konfiguration gelöscht.

Hinweise zum Echtzeit-Scanner

Eine Reparatur durch den Echtzeit-Scanner ist nur bedingt möglich. Deshalb empfehlen wir Ihnen, immer einen Suchlauf nach einer mehrfachen Virenmeldung durch den Echtzeit-Scanner durchzuführen, um ein mögliches infiziertes System zu bereinigen.

Bitte führen Sie zudem bei einer Makroviren Meldung des Echtzeit-Scanners, anschließend einen Suchlauf über die gemeldete Datei aus, um ebenfalls sicherzustellen, dass die Datei repariert wird.

Wir empfehlen Ihnen beim Echtzeit-Scanner die gleichen Einstellungen wie beim System-Scanner vorzunehmen, also automatische Aktion bei Fund mit den Zusatzoptionen Datei vor Aktion in Quarantäne kopieren (Stichwort: Sicherungskopie) und Warnmeldungen anzeigen, damit der Anwender informiert wird. Ansonsten verwenden Sie wie beim System-Scanner als primäre Aktion reparierenund als Sekundäre Aktion löschen aus.

Hinweise zum Email-Schutz

Bei einem Malwarefund durch den Email-Schutz können Emails und Dateien nicht repariert werden, deshalb empfehlen wir Ihnen, stets die Emails komplett in Quarantäne zu verschieben.

Hinweise zum Browser-Schutz

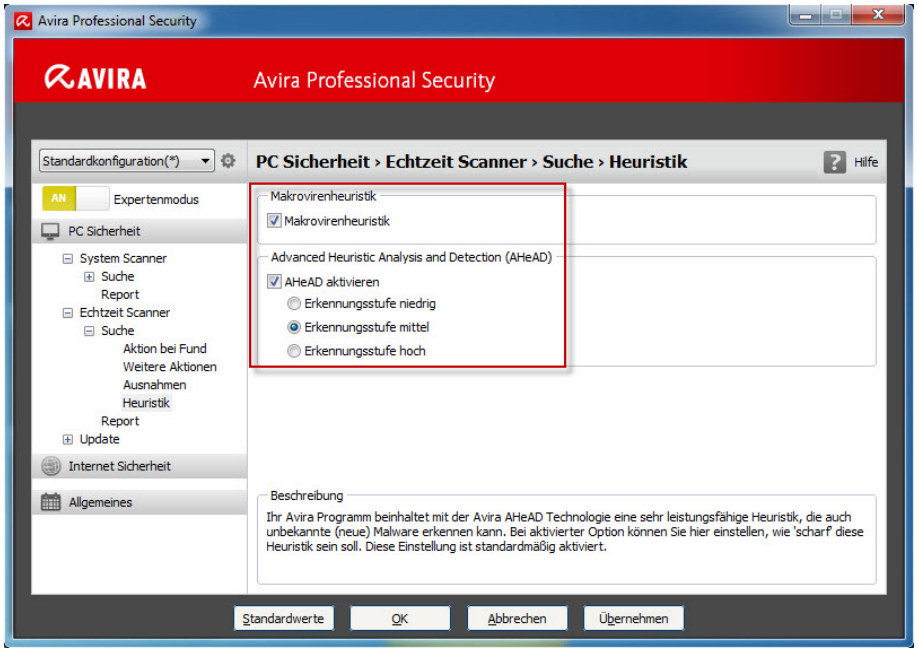
Wie beim Email-Schutz kann auch der Browser-Schutz keine Dateien reparieren, folglich empfehlen wir Ihnen ebenfalls, die Datei in Quarantäne zu verschieben. Wählen Sie hierfür die Primäre Aktion isolieren aus.

Heuristik

- Makrovirenheuristik aktiviert
- Advanced Heuristic (AHeAD) aktiviert: Erkennungsstufe mittel

Durch die Aktivierung der Makrovirenheuristik werden entsprechende Dokumente mit Makros nach möglichen Makroviren untersucht und ggf. repariert.
Durch die aktivierte Heuristik in der Erkennungsstufe hoch erkennt Avira bedeutend mehr unbekannte Malwaretypen, allerdings müssen Sie auch mit so genannten Fehlmeldungen rechnen.

Bitte aktivieren Sie die Heuristik in allen Modulen (System-Scanner, Echtzeit-Scanner, Email-Schutz und Browser-Schutz) und stellen Sie überall die AHeAD Erkennungsstufe hoch ein.



Hinweis
Sie finden die Konfiguration der Heuristik in allen Modulen unterhalb von Suche.

5.2 Modul Scanner

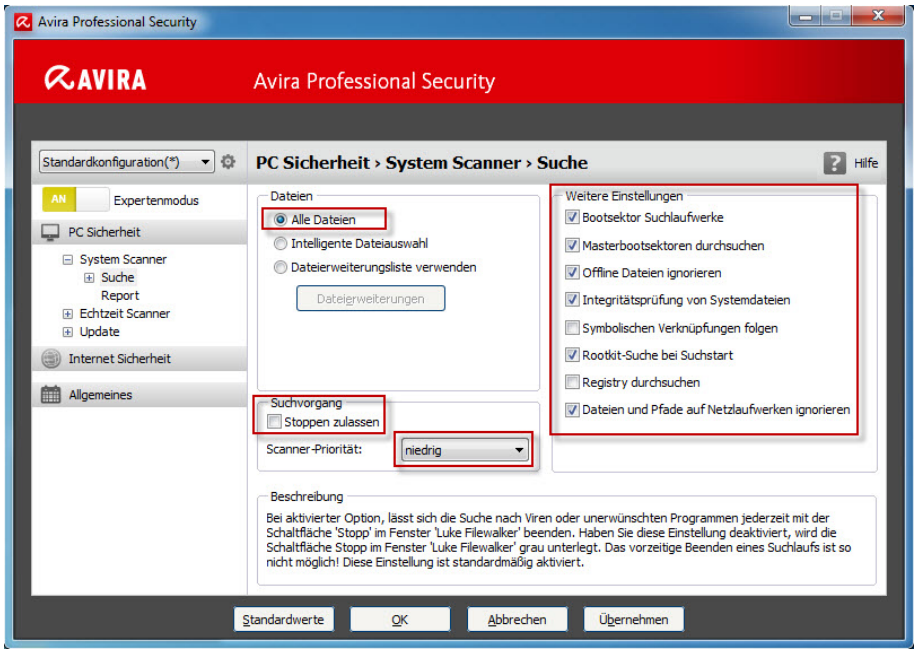
Suche

- Dateien: Alle Dateien
- Weitere Einstellungen: Bootsektor

Suchlaufwerke; Masterbootsektoren; Offline Dateien ignorieren; Optimierter Suchlauf; Rootkit-Suche; Netzlaufwerke ignorieren; Suchvorgang: Kein Stoppen zulassen; Scanner Priorität: niedrig

Es werden wirklich alle Dateien vom Scanner überprüft, was wichtig ist, da es immer wieder neue Malwaretypen und Exploits in verschiedenen Dateitypen gibt.

Zudem werden Bootsektoren überprüft, Offline Dateien nicht ignoriert, der Suchlauf optimiert ausgeführt (Multi-Prozessor) und eine Rootkit Suche beim Start durchgeführt.



Eine Rootkit Suche bei jedem Start eines Suchlaufs empfehlen wir Ihnen, da es derzeit kein Profil für die vollständige Rootkit Suche gibt. Durch das Deaktivieren eines möglichen Stoppvorgangs können Sie einen kompletten Suchlauf garantieren.
Der Anwender hat also keine Möglichkeit, den Suchlauf abzubrechen.

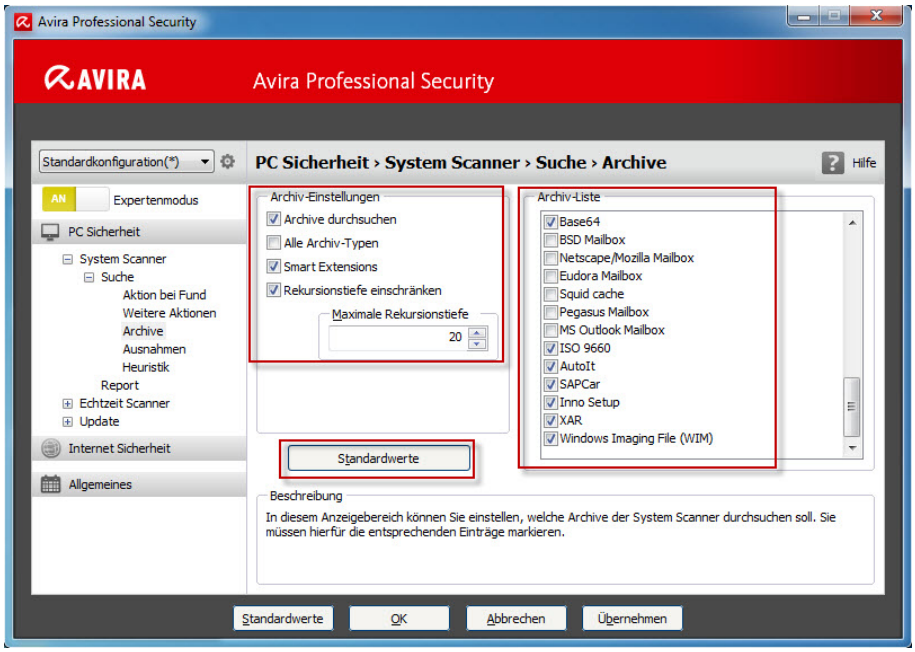
Archive

- Archiv- Einstellungen: Archive durchsuchen; Smart Extensions aktiviert; Rekursionstiefe auf 20 eingeschränkt
- In der Archiv-Liste alle Formate außer Squid Cache und Mailboxen aktiviert (Standwerte)

Durch die oben genannten Einstellungen stellen Sie sicher, dass die wichtigsten Archive entpackt und durchsucht werden.

Die Option Smart Extensions sorgt dafür, dass Archive auch erkannt werden, falls die Dateiendung abweicht.

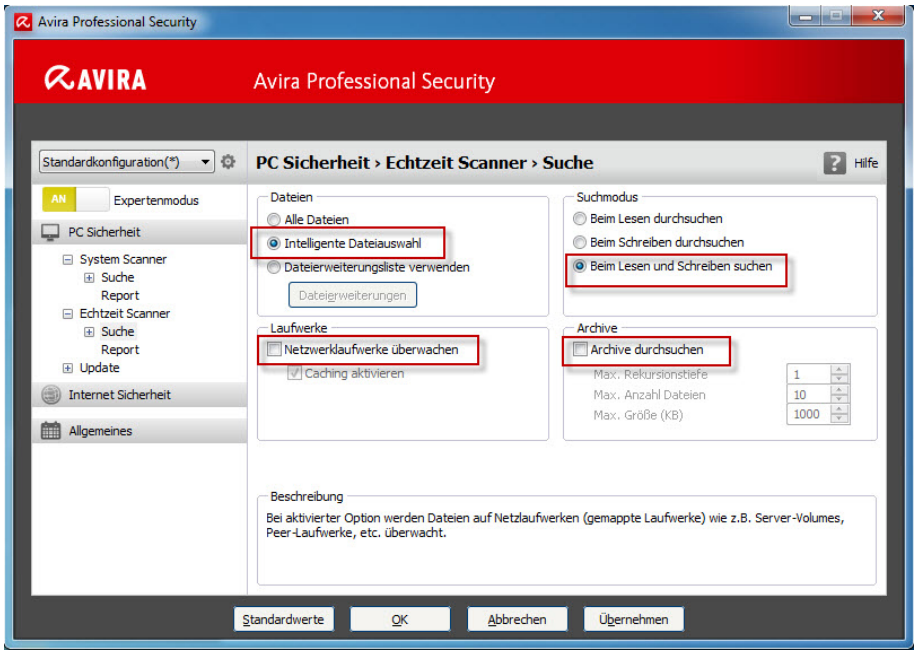
Hinweis
Falls eine virulente Datei in einem Archiv gefunden wird, wird das gesamte Archiv je nach Einstellung in Quarantäne gestellt und anschließend gelöscht. Eine Reparatur eines Archivs (Entfernung der virulenten Datei aus dem Archiv) ist aus technischen Gründen leider nicht möglich.



5.3 Modul Echtzeit-Scanner

Suche

- Suchmodus: Beim Lesen und Schreiben suchen
- Dateien: Intelligente Dateiauswahl
- Keine Archive durchsuchen
- Keine Netzlaufwerke überwachen



Durch diese Einstellungen werden alle Dateioperationen wie Öffnen, Ausführen und Schreiben bei allen wichtigen Dateien durch den Echtzeit-Scanner überwacht.

Mit der Konfiguration Intelligente Dateiauswahlstellen Sie sicher, dass die Auswahl vollautomatisch von Avira Professional übernommen wird.

Das bedeutet, dass Avira Professional anhand des Inhalts einer Datei entscheidet, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist zwar etwas langsamer als die Dateierweiterungsliste, aber wesentlich sicherer.

Außerdem werden keine Archive und Netzlaufwerke in Echtzeit überprüft. Diese Optionen werden laut unseren Empfehlungen nicht im Echtzeitschutz genutzt, da sie in der Regel durch andere Einstellungen und Mechanismen im Scanner abgedeckt sind.

Hinweise zu Archiven

Falls sich eine Malware in einem Archiv befindet, kann man dies als eine Art Hülle um die virulente Datei an sich betrachten. Das bedeutet, dass keine unmittelbare Gefahr von der virulenten Datei ausgeht, solange sie nicht entpackt wird.

Beim Entpacken eines Archivs werden die enthaltenen Dateien schließlich im Originalformat hergestellt und dabei vom Guard kontrolliert.

Sollte sich also eine virulente Datei in einem Archiv befinden und dieses Archiv entpackt werden, würde der Guard den Vorgang kontrollieren und dabei die Datei je nach Konfiguration in Quarantäne verschieben, reparieren oder löschen.

Hinweise zu Netzlaufwerken

Falls diese Option aktiviert ist, werden verbundene Netzlaufwerke zusätzlich überwacht, siehe Sicherheitslevel Hoch.

Allerdings sollte man den Virenschutz direkt auf dem jeweiligen System installieren, um die Performance auszubalancieren und um auch das lokale System abzusichern.

Auch hier geht keine unmittelbare Gefahr aus, fallsdie Option deaktiviert wurde, da ein direktes Ausführen von einem Programm auf einem Netzlaufwerktrotzdem überwacht wird (feste Einstellung im Programm). Sobald also ein Tool oder eine Anwendung direkt vom Netzlaufwerk gestartet wird, findet eine Kontrolle durch den Echtzeit-Scanner statt.

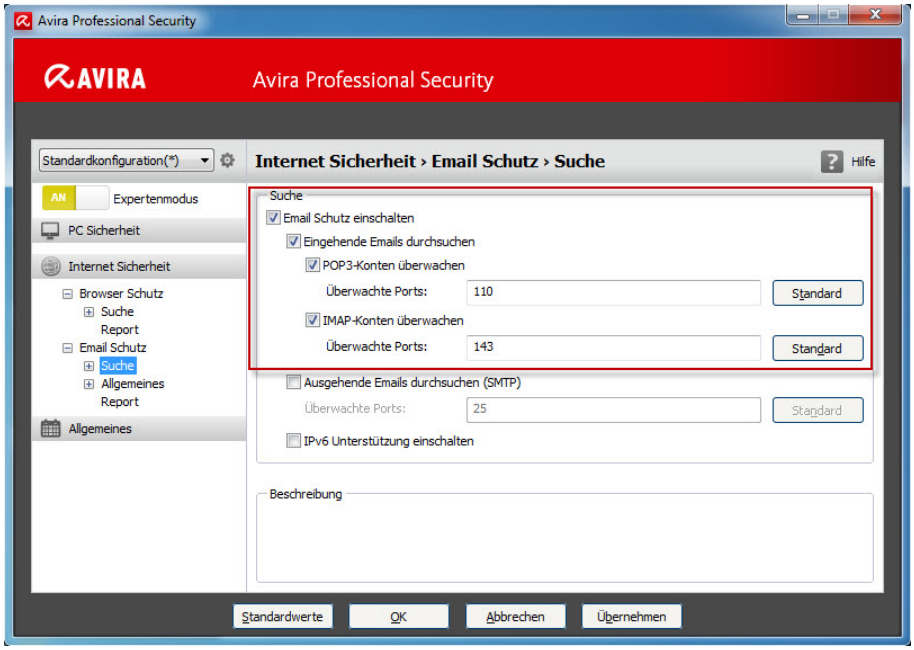
Zudem wird eine Datei bei einem Kopiervorgang trotzdem überprüft, da sie ja auf die lokale Festplatte geschrieben wird und dies in der Konfiguration Beim Lesen und Schreiben durchsuchenberücksichtigt wird

5.4 Module Email-Schutz und Browser-Schutz

Diese Module werden wie bereits erwähnt ja nach Unternehmensumgebung und Anforderungen installiert. Falls Sie sich für eine Installation entschieden haben, empfehlen wir Ihnen die folgenden Einstellungen.

Email-Schutz – Suche

- Alle eingehenden Emails überwachen



So können Sie sicherstellen, dass alle eingehenden Emails überwacht werden. Auf Emails kann dabei entweder via POP oder via IMAP zugegriffen werden, beide Protokolle werden berücksichtigt.

Auf die Überwachung von ausgehenden Emails können Sie verzichten, da in der Regel Ihr eigener Mailserver oder Ihr ISP diese Aufgabe übernimmt.

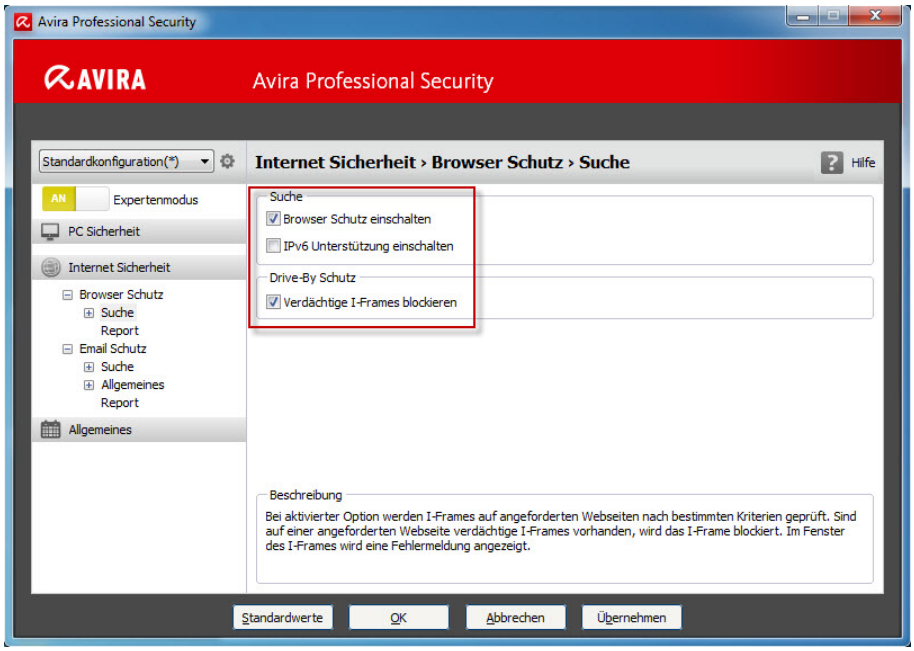
Falls Sicherheit aber an erster Stelle steht, dann lassen Sie auch ausgehende Emails prüfen, da Sie so bereits im Vorfeld einen möglicherweise noch unbekannten Wurm entdecken können.

Browser-Schutz – Suche

- Browser Schutz einschalten
- Verdächtige I-Frames blockieren

Mit der Option „Verdächtige I-Frames blockieren“ werden I-Frames auf angeforderten Webseiten nach bestimmten Kriterien geprüft. Falls verdächtige I-Frames vorhanden sind, wird das I-Frame blockiert.

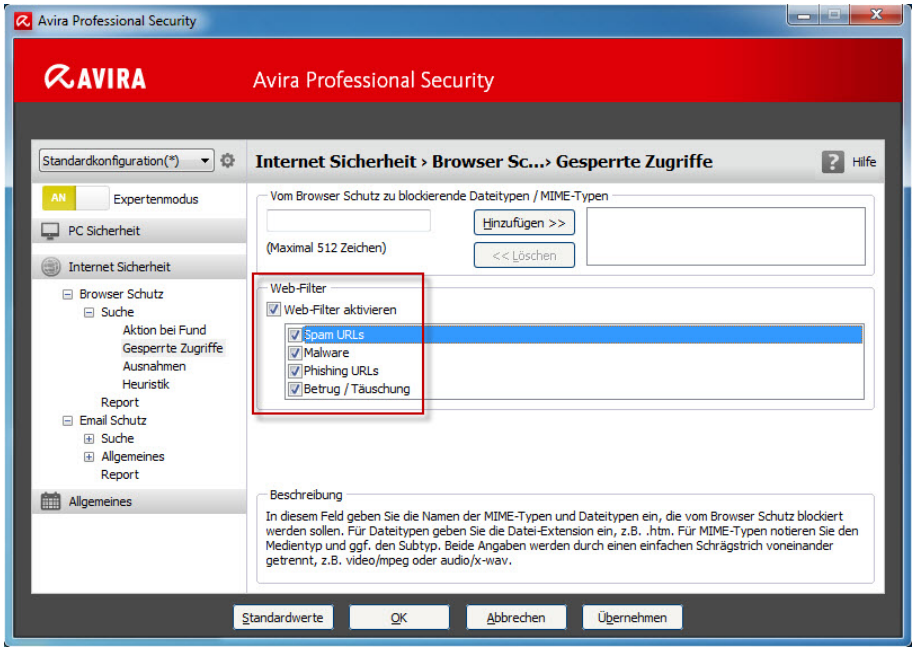
Weitere Informationen finden Sie in den Beschreibungen im Sicherheitslevel Hoch und Mittel.



Gesperrte Zugriffe

- Vom Browser-Schutz zu blockierende Dateitypen / MIME-Typen: Nach Bedarf
- Web-Filter aktivieren: Alle Kategorien ausgewählt

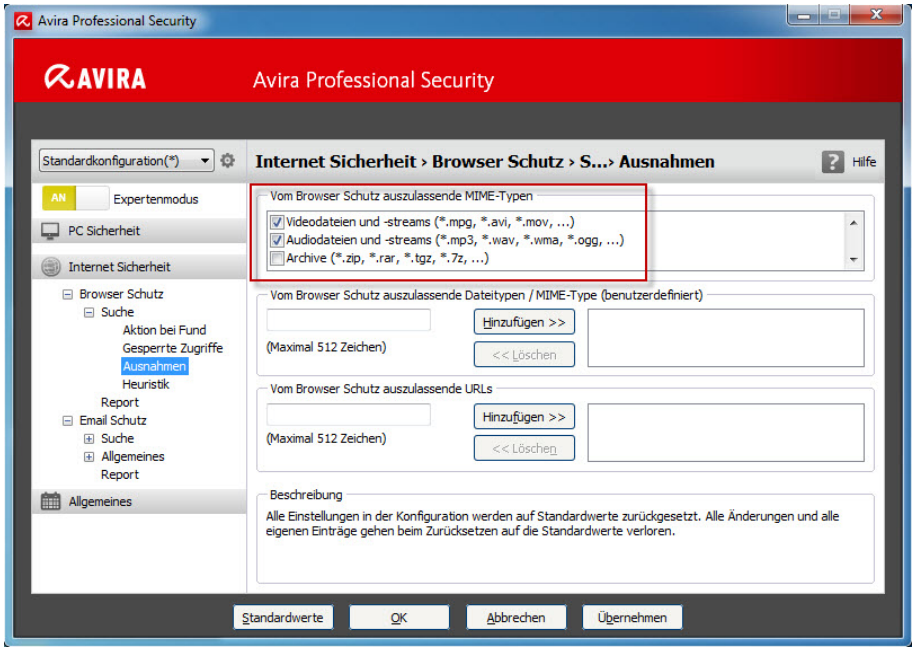
Die zu blockierenden Datei- und MIME-Typen können Sie je nach Policy selbst hinzufügen, hier können bestimmte Downloads unterbunden werden.



Im Webfilter selbst aktivieren Sie alle Kategorien. Malware- und Phishing URLs sind selbsterklärend, Betrug/Täuschung liegt vor, falls ein Anbieter eines unseriösen Angebots versucht, Ihnen einen Vertrag ohne konkrete Angaben zu verkaufen (Stichwort Abo Falle).

Browser-Schutz – Ausnahmen

- Auszulassende MIME-Typen: Nur Video- und Audiodateien und –streams werden ausgelassen und somit nicht geprüft



Diese Dateien sollten aufgrund der Performance und der allgemeinen Verarbeitung im Webbrowser oder in anderen Applikationen stets ausgenommen werden, damit sie funktionieren.

Ansonsten kann es vorkommen, dass Streams überhaupt nicht funktionieren, da es bei dieser Art von Dateien kein so genanntes End of File gibt und Avira somit keine Möglichkeit hat, die Datei zu prüfen.

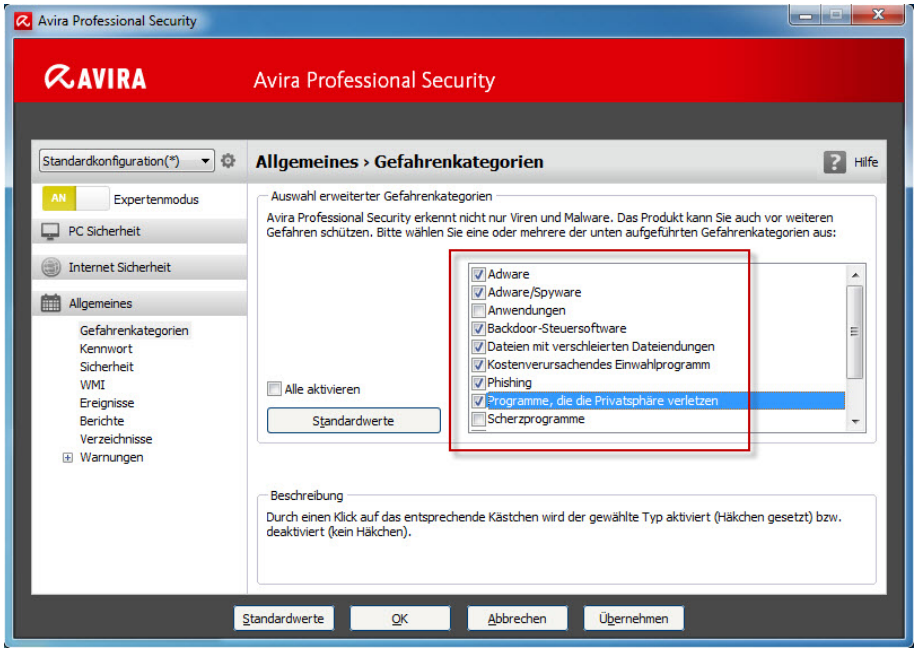
Alle anderen Arten wie Archivdateien oder ausführbare Dateien sollten überprüft werden, folglich sind diese Ausnahmen deaktiviert.

5.5 Allgemeine Einstellungen

Erweiterte Gefahrenkategorien

Folgende Kategorien sind aktiviert:

- Adware/Spyware, BDC, Dateien mit verschleierten Dateiendungen, Dialer, Phishing und Security Privacy Risk



Neben der üblichen Viren und Malware Erkennung können Sie mit den zusätzlichen Optionen dafür sorgen, dass zusätzliche Gefahrenquellen wie Backdoor-Steuersoftware, Dialer oder SPR Programme überprüft und ggf. blockiert werden.

Da von sonstigen Applikationen (APPL) oder Spielen und Witzprogrammen keine Gefahr ausgeht, wird auf die Erkennung solcher Dateien im Sicherheitslevel Mittel verzichtet.

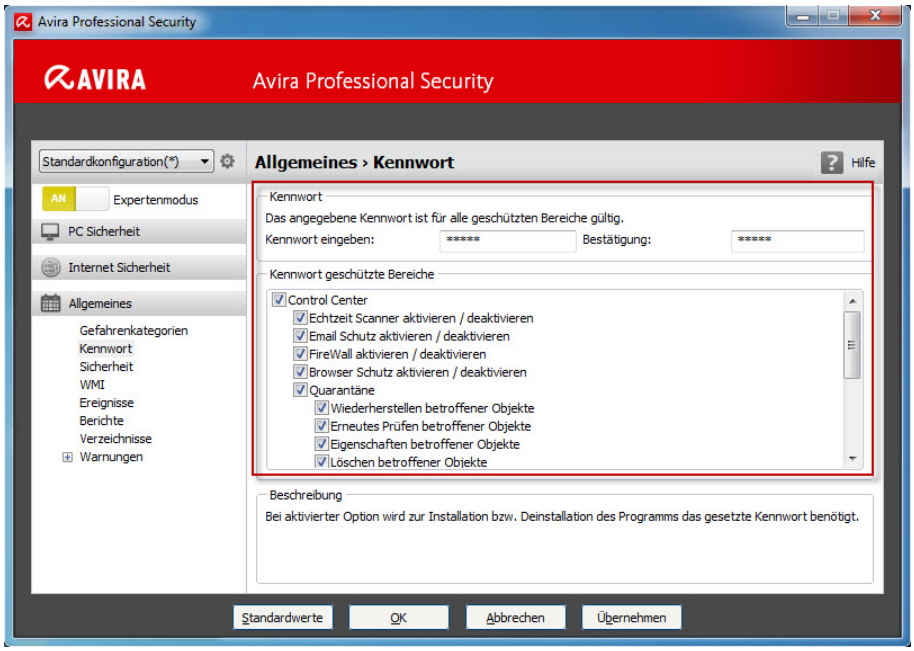
Weitere Informationen zu den unterschiedlichen Kategorien finden Sie in der im Programm integrierten Hilfe, die Sie mit der F1 Taste aufrufen können.

Kennwort

- Bitte hinterlegen Sie unbedingt einen Kennwortschutz für alle Bereiche

Durch einen Kennwortschutz für alle Bereiche stellen Sie sicher, dass die vorgegebene Konfiguration nur mit Hilfe des entsprechenden Kennworts geändert oder Module wie Echtzeit-Scanner, Email-Schutz und Browser-Schutz deaktiviert werden können.

Außerdem können Sie das Quarantänemanagement absichern und verhindern, dass einzelne Module oder gar das komplette Avira Programm deinstalliert werden.



Diese Einstellung empfehlen wir generell und im Speziellen bei Anwendern, die aufgrund bestimmter Voraussetzungen mit administrativen Rechten arbeiten.

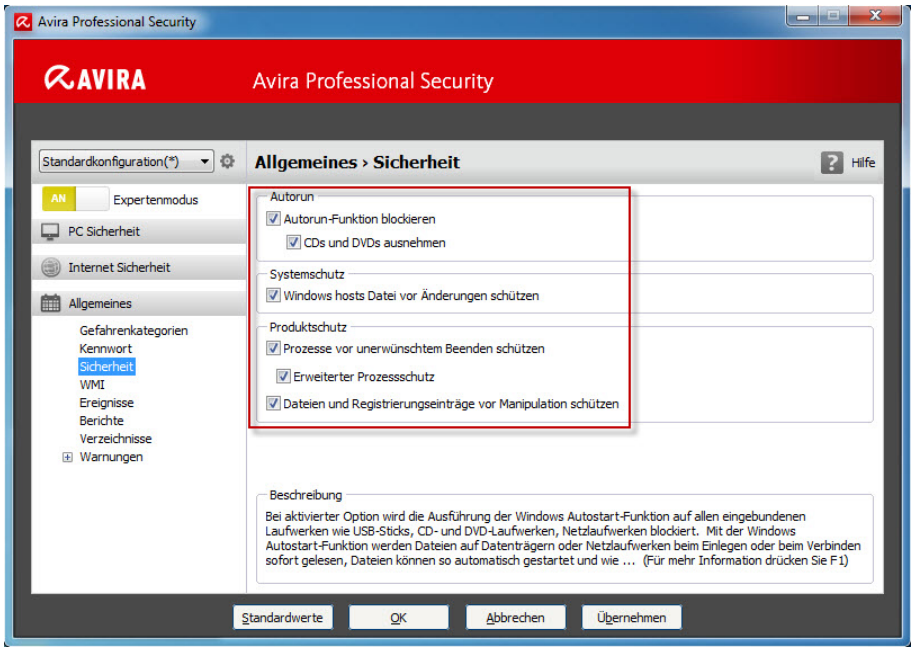
Hinweis
In den mitgelieferten Konfigurationsdateien wird stets das Passwort *avira* verwendet, bitte ändern Sie dieses Passwort nach Einspielen der mitgelieferten INI Datei.

Sicherheit

- Autorun-Funktion blockieren / CDs und DVDs ausnehmen
- Windows hosts Datei vor Änderungen schützen
- Produktschutz: AntiVir-Prozesse, -Dateien und -Registryeinträge schütze

Bei aktiviertem Autorun wird die Ausführung der Windows Autostart-Funktion auf allen eingebundenen Laufwerke, USB-Sticks und Netzlaufwerke blockiert.

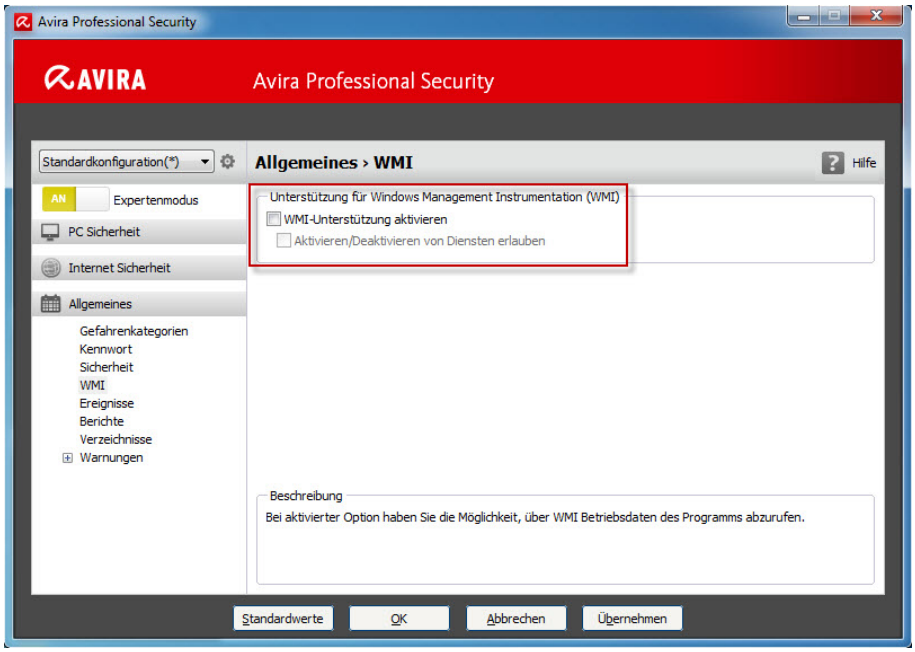
Ist die Option Systemschutz aktiviert, sind die Windows hosts-Dateien schreibgeschützt. Eine Manipulation der Dateien ist dann nicht länger möglich.
Malware ist dann nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten.



Bei aktivierter Option „Prozesse vor unerwünschtem Beenden schützen“ werden alle Prozesse des Programms vor unerwünschtem Beenden durch Viren und Malware oder vor einem ‚unkontrollierten‘ Beenden durch einen Benutzer geschützt.

WMI

- Option bitte vollständig deaktivieren



Falls Sie keinerlei Abfragen oder Aktionen via WMI (VB-Script o. ä.) ausführen möchten, was die Regel ist, dann deaktivieren Sie bitte die WMI Schnittstelle komplett.

Dadurch kann eine potentielle Malware keine Informationen über Avira abfragen und auch keine Manipulationen wie das Beenden eines Dienstes durchgeführen!

Zudem stellen Sie sicher, dass auch ein Angreifer keine Informationen auslesen kann, um einen Angriff zu planen.

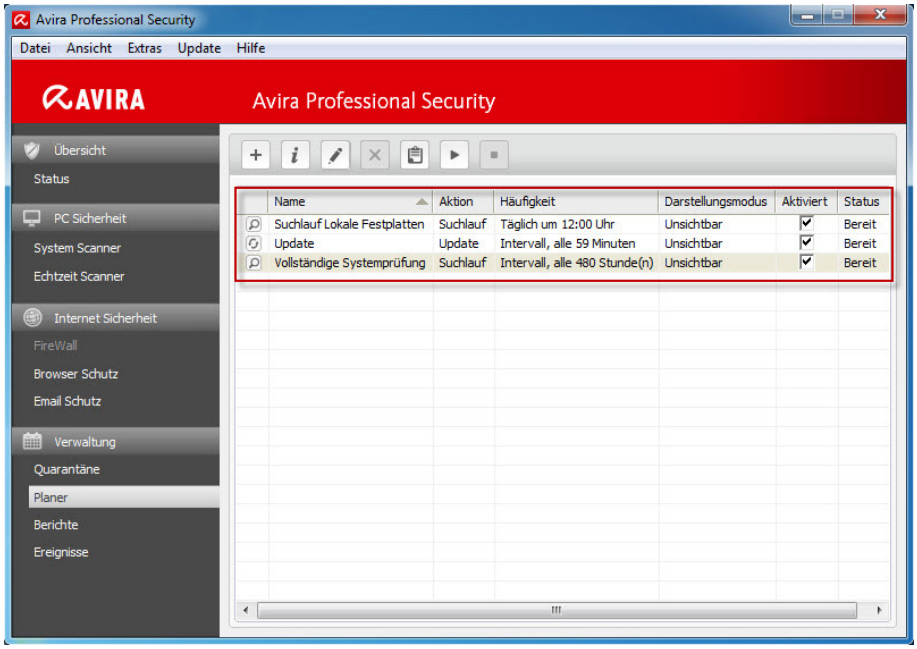
Avira Planer

Im Avira Planer können Sie die Aufträge (so genannte Jobs) lokal anlegen, um die lokale Avira Instanz hinsichtlich Updates und Suchläufen zu steuern.

Diese Planung können Sie natürlich auch zentral über das AMC steuern und somit eine einheitliche Planung für alle Klienten anlegen.

Wir empfehlen Ihnen, die Planer Einstellungen wie im Sicherheitslevel Mittel beschrieben zu übernehmen:

- Update
  - Intervall – Alle 60 Minuten
- Suchlauf
  - Lokale Festplatten – Täglich um 12:00 Uhr (Mittagspause)
  - Vollständige Systemprüfung – Alle 20 Tage
- Alle Aufträge im Darstellungsmodus unsichtbar



Durch die Einstellung Update alle 60 Minuten stellen Sie sicher, dass nahezu jedes Update (ca. 5 Updates täglich) verwendet wird und Avira jede Stunde aktualisiert wird.

Bei der Konfiguration der Suchläufe müssen Sie natürlich darauf achten, dass das jeweilige System individuell zu schützen ist. Das bedeutet, dass Sie Profile für bestimmte Verzeichnisse wie Downloads oder temporäre Dateien anlegen müssen, um anschließend mit dem Avira Planer darauf zugreifen zu können.

Hierfür legen Sie bitte ein neues Profil an: Avira starten – Lokaler Schutz – Prüfen – Neues Profil anlegen und wählen anschließend, welche Verzeichnisse einbezogen werden sollen.

Allerdings bringt Avira bei der Installation so genannte Standardprofile mit, die weitestgehend alle Möglichkeiten abdecken und in diesem HowTo verwendet werden.

Unsere Empfehlungen zur Planung der Suchläufe finden Sie oben. Dabei wird das Profil Lokale Laufwerke verwendet, was dafür sorgt, dass wirklich alle Laufwerke (Wechseldatenträger und Festplatten) einmal täglich zur Mittagspause überprüft werden.

Achtung
Dabei werden nur die Datenträger geprüft, die zum Zeitpunkt des Auftrags verbunden sind!

Zusätzlich zum täglichen Suchlauf über alle lokalen Laufwerke legen Sie einen weiteren Auftrag an, der alle 20 Tage eine vollständige Systemprüfung vornimmt.

Alle Aufträge wurden im Darstellungsmodus unsichtbar angelegt, damit der Anwender nicht abgelenkt wird und ggf. den Fokus aus seiner aktiven Applikation verliert.

Hinweis
Bitte ändern Sie aufgrund Ihrer individuellen Vorgaben die Uhrzeiten, sodass der Suchlauf zu einem Zeitpunkt stattfindet, an dem nicht aktiv am System gearbeitet wird. Hintergrund ist, dass Sie auch während eines Suchlaufs am System arbeiten können, dabei allerdings die Performance sinkt.

Tipp
Sie können den Suchlauf zu einer Uhrzeit nahe dem Feierabend planen und beim Anlegen des Auftrags im Planer die Option Computer herunterfahren, wenn Auftrag ausgeführt wurde verwenden.

Ausgabe Q3-2012

AVIRA

live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de