Erste Schritte: Avast Small Office Protection

Weitere hilfreiche Informationen und Anleitungen zur Fehlerbehebung finden Sie in unserer Online-Dokumentation:

https://businesshelp.avast.com/

Inhalt

Einrichten des Geräts

Avast Small Office Protection ist erst seit Kurzem auf dem Markt und unterscheidet sich von Avast Business Antivirus wie folgt:

- Lizenz auf maximal 10 Geräte beschränkt, weil für Kleinunternehmen mit begrenzter Anzahl von Geräten vorgesehen
- kann *nicht* auf Server-Betriebssystemen installiert werden
- kann auf Android-/iOS-Geräten installiert werden
- enthält viele verschiedene Komponenten
- nur für *nicht verwaltete* Geräte verfügbar

Weitere Informationen über die verschiedenen Komponenten, die jeweils in Avast Business Antivirus und in Small Office Protection verfügbar sind, finden Sie unter Übersicht über die Komponenten.

Überprüfen der Systemanforderungen

Small Office Protection-Endgeräte

Windows:

- 7 SP1 oder höher, 8.x außer RT und Starter Edition, 10 außer Mobile und IoT Core Edition

Mac:

- MacOS 10.10 (Mavericks oder höher mit mindestens 500 MB freiem Festplattenspeicher)

Android:

- Android 4.1 (Jelly Bean) oder höher

iPhone/iPad:

- iOS 12.0 oder höher

Überprüfen der Firewall-Anforderungen

Sie müssen bestimmten Ports und URL-Adressen gestatten, Ihre Firewall oder Ihren Proxy-Server zu passieren, damit die Gesamtfunktionalität gewährleistet ist und Small Office Protection-Clients authentifiziert/aktualisiert werden können.

Ports

TCP und UDP:

- 53 – Secure DNS-Dienste (nur bei Verwendung der Real Site-Komponente)
- 80 – Überprüfung von Sicherheitsrisiken und Aktualisierung von Funktionen
- 443 – Aushandlung von FFL Verschlüsselungsschlüssel (nur bei Verwendung von Real Site-Komponente)

URLs

- *.avast.com
- *.avcdn.net
- *.mailshell.net (nur bei Verwendung von Anti-Spam)

Installieren von Small Office Protection auf Geräten

Windows Workstations

Für nicht verwaltete Small Office Protection können Sie das Installationsprogramm hier herunterladen. Nach dem Download können Sie das Installationsprogramm auf dem Windows-Gerät ausführen, auf dem Sie Antivirus installieren möchten.

Anpassung der Installation

1. Kopieren Sie die Installationsdatei an einen Speicherort, auf die das Endgerät Zugriff hat.
2. Doppelklicken Sie auf die Installationsdatei, um sie auszuführen.
3. Wenn die Frage angezeigt wird, ob die Anwendung auf Ihrem Gerät Änderungen vornehmen darf, klicken Sie auf **Ja**.
4. Klicken Sie auf **Anpassen**. Führen Sie dann eine der folgenden Aktionen aus:
    - Wählen Sie **Empfohlener Schutz**, um alle Komponenten zu installieren.
    - Wählen Sie **Minimaler Schutz**, um nur Dateisystem-, Web- und E-Mail-Schutz zu installieren.
    - Wählen Sie **Benutzerdefinierter Schutz**, um die zu installierenden Komponenten selbst auszuwählen.

5. Klicken Sie auf **Installieren** und warten Sie, bis Small Office Protection auf Ihrem Gerät installiert ist.
6. Starten Sie das Gerät neu, wenn Sie hierzu aufgefordert werden.

Empfohlene Komponenten für Server und Arbeitsstationen

In einer Business-Umgebung gelten andere Anforderungen als in Verbraucherumgebungen. Daher wird der Einsatz bestimmter Komponenten in derartigen Netzwerken nicht empfohlen, obwohl sie in Small Office Protection verfügbar sind.

Empfohlen für Business-Umgebungen

Die folgenden Komponenten sollten vollkommen deinstalliert oder durch Ziehen des Schiebereglers in die Position **Aus** deaktiviert werden:

- Real Site
- WLAN-Inspektor

Wenn diese Komponenten nicht entfernt werden, wird womöglich die Stabilität des Netzwerks oder die Leistung der Computer beeinträchtigt oder es treten Fehler auf.

MacOS X-Geräte

Für nicht verwaltete Small Office Protection können Sie das Installationsprogramm hier herunterladen. Nach dem Download können Sie das Installationsprogramm auf dem MacOS X-Gerät ausführen, auf dem Sie Antivirus installieren möchten.

1. Kopieren Sie die Installationsdatei (.dmg) an einen Speicherort, auf den Ihr Gerät Zugriff hat. Achten Sie darauf, dass keine andere Anwendung oder Antivirus-Software ausgeführt wird.
2. Doppelklicken Sie auf die heruntergeladene Setup-Datei.
3. Doppelklicken Sie auf das Symbol für Small Office Protection, und schließen Sie dann das Fenster.
4. Klicken Sie im Popup-Fenster auf **Fortsetzen**. Lesen Sie die Datenschutzrichtlinie, und klicken Sie dann auf **Fortsetzen**.
5. Klicken Sie auf **Fortsetzen**, um zu bestätigen, dass Sie die *Endbenutzer-Lizenzvereinbarung* gelesen haben. Klicken Sie dann auf **Zustimmen**, um zu bestätigen, dass Sie die Bedingungen akzeptieren.

6. Wenn Sie Änderungen am Standard-Setup vornehmen möchten, klicken Sie auf **Anpassen**. Klicken Sie andernfalls auf **Installieren**.
7. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Touch-ID oder das Administratorpasswort ein, um die Installation zu gestatten. Klicken Sie dann auf **Software installieren**.
8. Klicken Sie auf „OK", damit Small Office Protection auf Ihren Download-Ordner zugreifen kann.
9. Wenn die Benachrichtigung *Systemerweiterung blockiert* angezeigt wird, klicken Sie auf **Sicherheitseinstellungen öffnen**. Gehen Sie dann wie folgt vor:
    1. Klicken Sie auf das Schlosssymbol. Geben Sie Ihr Administratorpasswort ein. Klicken Sie auf **Entsperren** und dann auf **Zulassen**
    2. Wählen Sie **Datenschutz**, und aktivieren Sie den vollständigen *Festplattenzugriff* für Small Office Protection. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Jetzt beenden**, und schließen Sie das Fenster **Sicherheit und Datenschutz**
10. Deaktivieren Sie optional das Kontrollkästchen, wenn Google Chrome nicht als Standardbrowser installiert werden soll, und klicken Sie dann auf **Weiter**.
11. Klicken Sie nach Abschluss der Installation auf **Schließen** und dann auf **In Papierkorb verschieben**.
12. Klicken Sie auf **OK**, damit das Installationsprogramm für Small Office Protection auf Ihren Download-Ordner zugreifen kann.

Android-Geräte

Sie können Small Office Protection für Ihr Android-Smartphone direkt aus dem Google Play Store herunterladen.

1. Öffnen Sie die Play Store-App.
2. Suchen Sie nach „Avast".
3. Wählen Sie **Avast Antivirus - Mobile Security & Virus Cleaner** aus der Liste.
4. Klicken Sie auf **Installieren**.
5. Klicken Sie gegebenenfalls auf **Akzeptieren**, damit der Download beginnen kann.

iOS-Geräte

Sie können Small Office Protection für Ihr iOS-Smartphone direkt aus dem App Store herunterladen.

1. Öffnen Sie den App Store.
2. Suchen Sie nach „Avast Mobile Security".
3. Wählen Sie **Avast Sicherheit und Datenschutz** aus der Liste.
4. Tippen Sie auf das Download-Symbol.
5. Tippen Sie auf **Öffnen**, nachdem Sie die App heruntergeladen haben.
6. Wenn Sie dazu aufgefordert werden, tippen Sie auf **Zulassen**, um Avast Sicherheit und Datenschutz die Berechtigung für das Senden von Benachrichtigungen zu gewähren.

Aktivieren von Lizenzen auf Ihrem Gerät

Sie können Ihr Small Office Protection-Abonnement nach der Installation des Programms auf Ihren Geräten aktivieren. Beim Kauf von Small Office Protection müssten Sie einen Abonnementcode zur Aktivierung Ihrer Geräte erhalten. Dieser Code müsste außerdem mit Ihrem Avast-Konto verbunden sein. Die Anzahl der Geräte, die Sie aktivieren können, hängt von dem erworbenen Abonnement ab.

Windows Workstations

1. Öffnen Sie die Benutzeroberfläche von Small Office Protection auf dem Gerät.
2. Klicken Sie auf **Menü**.
3. Klicken Sie auf **Aktivierungscode eingeben**.
4. Geben Sie Ihren Aktivierungscode/Lizenzschlüssel ein, und klicken Sie auf **Eingeben**.
5. Bestätigen Sie gegebenenfalls die Details Ihres Abonnements und die jeweiligen Komponenten.

Android-Geräte

Aktivieren mit Aktivierungscode

1. Tippen Sie auf Ihrem Gerät auf das Symbol für *Avast Mobile Security*, um die App zu öffnen.
2. Tippen Sie auf **Menü** ▸ **Werbung entfernen**.
3. Tippen Sie oben rechts auf die **drei Punkte**, und wählen Sie die Option **Bereits gekauft?**

4. Tippen Sie auf **Aktivierungscode einlösen**.
5. Geben oder fügen Sie Ihren Aktivierungscode in das Textfeld ein, einschließlich der Bindestriche.
6. Tippen Sie auf **Diesen Code verwenden**, um die Aktivierung abzuschließen.

Aktivieren über das Avast-Konto

1. Tippen Sie auf Ihrem Gerät auf das Symbol für *Avast Mobile Security*, um die App zu öffnen.
2. Tippen Sie auf **Menü** ▸ **Werbung entfernen**.
3. Tippen Sie oben rechts auf die **drei Punkte**, und wählen Sie die Option **Bereits gekauft?**
4. Wählen Sie **Von Avast-Konto wiederherstellen**.
5. Wählen Sie **E-Mail**.
6. Geben Sie die Anmeldedaten für Ihr Avast-Konto ein.
7. Tippen Sie auf **Beim Avast-Konto anmelden.**

iOS-Geräte

1. Tippen Sie auf Ihrem Gerät auf das Symbol für *Avast Sicherheit und Datenschutz*, um die App zu öffnen.
2. Tippen Sie auf „Upgrade".
3. Tippen Sie auf **Bereits gekauft?**
4. Wählen Sie **Avast-Abonnementcode eingeben** aus.
5. Geben oder fügen Sie Ihren Aktivierungscode in das Textfeld ein, einschließlich der Bindestriche.
6. Tippen Sie auf **OK**, um die Aktivierung abzuschließen.

Einstellungskonfiguration und Komponenten

Für Small Office Protection gibt es zahlreiche Komponenten, sowohl für Workstations als auch für Mobilgeräte.

Komponenten nach Betriebssystem

Komponente	Windows Workstations	MacOS X	Android	iOS
Dateisystem-Schutz	X	X		
Web-Schutz	X	X	X	
E-Mail-Schutz	X	X		
Verhaltensschutz	X			
Ransomware-Schutz	X	X		
Schutz gegen Fernzugriff	X			
WLAN-Inspektor	X	X		
Real Site	X			
Firewall	X			
Sandbox	X			
Anti-Spam				
Exchange				
Sharepoint				
Webcam-Schutz	X			
Schutz für sensible Daten	X			
SecureLine VPN				
Daten-Schredder	X			
Passwords	X			
Passwortschutz	X			
Software Updater	X			
Browser Cleanup	X			
Nicht-Stören-Modus	X			
Rettungsmedium	X			
Dateiscanner			X	
Foto-Tresor			X	X
Identitätsschutz				X
App-Sperre			X	

Komponente	Windows Workstations	MacOS X	Android	iOS
Anti-Theft			X	
Kamerafalle			X	
Letzter bekannter Standort			X	
SIM-Sicherheit			X	
Anrufblocker			X	
Energie sparen			X	
RAM-Boost			X	
Datenmüllbereinigung			X	
WLAN-Geschwindigkeitstest			X	
WLAN-Sicherheit			X	X
App Insights			X	
Eigenständige VPN-App			X	X

Aktivieren und Deaktivieren von Komponenten

Viele der in Small Office Protection verfügbaren Schutzmodule und Tools können auf dem Gerät aktiviert oder deaktiviert werden. Dies ist insbesondere nützlich, wenn Sie lediglich ein paar der Komponenten auf einem Server installieren oder die Anzahl der Tools möglichst gering halten möchten. Einige Tools können aber nur vollständig installiert oder deinstalliert werden, darunter Sandbox und Rettungsmedium.

1. Öffnen Sie die Client-Benutzeroberfläche von Small Office Protection.
2. Klicken Sie auf die Registerkarte für die Komponente, die Sie aktivieren oder deaktivieren möchten:
   - **Schutz:** Dateisystem-Schutz, Web-Schutz, E-Mail-Schutz, Verhaltensschutz, Sandbox, WLAN-Inspektor, Real Site, Firewall
   - **Privatsphäre:** Passwörter, Anti-Spam, Daten-Schredder, Webcam-Schutz
   - **Leistung:** Software-Updater
3. Klicken Sie auf die Schaltfläche für die Komponente.
4. Führen Sie neben der zu ändernden Komponente einen der folgenden Schritte aus:
   - Ziehen Sie den Schieberegler in die Position **Ein**, um die Komponente zu aktivieren.

- Ziehen Sie den Schieberegler in die Position **Aus**, um die Komponente zu deaktivieren.

5. Bestätigen Sie gegebenenfalls Ihre Wahl.

Installieren und Deinstallieren von Komponenten

Die meisten Funktionen von „Aktiver Schutz" werden mit Small Office Protection installiert. Diese Komponenten können aber nach Bedarf über das Menü „Fehlerbehebung" deinstalliert und erneut installiert werden. MacOS X-Schutzkomponenten können nicht installiert oder deinstalliert werden. Es ist aber möglich, sie auszuschalten.

1. Öffnen Sie die Client-Benutzeroberfläche von Small Office Protection.
2. Gehen Sie zu**Menü ▸ Einstellungen ▸ Allgemein ▸ Fehlerbehebung**.
3. Klicken Sie auf **Komponenten hinzufügen und ändern**.
4. Führen Sie neben den zu ändernden Komponenten einen der folgenden Schritte aus:
   - Wenn die Komponente noch nicht installiert ist, aktivieren Sie das Kästchen daneben.
   - Wenn die Komponente bereits installiert ist, deaktivieren Sie das Kästchen daneben.
5. Klicken Sie zum Schluss auf **Ändern**, um Ihre Änderungen zu bestätigen.

Weitere Einzelheiten zum Konfigurieren der in den Einstellungen von Small Office Protection verfügbaren Komponenten finden Sie unter Konfigurieren von Einstellungen in Small Office Protection (auf Englisch).

Konfigurieren von Ausnahmen

Platzhalter

Viele der Schutzmodule und andere Komponenten von Small Office Protection sowie Antivirus selbst ermöglichen es Ihnen, Ausnahmen zu konfigurieren oder bestimmte Pfade zu blockieren. Platzhalter sind hilfreich, wenn Sie den genauen Dateipfad oder Dateinamen von Dateien, die Sie ein- oder ausschließen möchten, nicht kennen oder wenn Sie mehrere Dateien in einem Pfad angeben möchten. Die Verwendung von Platzhaltern ist nicht in allen Dateipfaden möglich.

Zeichen	Bedeutung
?	Ersetzt einen einzelnen Buchstaben **Zum Beispiel:** `ab?.html` entspricht den Dateien `abc.html`, `abd.html`, `abe.html` etc. Es entspricht **nicht** der Datei`abc.htm`.
*	Ersetzt null oder mehr Zeichen **Zum Beispiel:** `*mtl` entspricht den Dateien `abc.html` und `d.html`. `*txt` entspricht den Dateien `abc.txt`, `x.txt` und `xyztxt`.

Ausnahmen

Auf der Seite **Einstellungen** ▸ **Allgemein** können Sie auf der Registerkarte *Ausnahmen* Ausnahmen konfigurieren, die über alle Schutzmodule und Komponenten von Small Office Protection verteilt werden.

Hinzufügen von Ausnahmen

1. Öffnen Sie die Client-Benutzeroberfläche von Small Office Protection.
2. Klicken Sie oben rechts auf das **Menü**, und wählen Sie **Einstellungen**.
3. Klicken Sie im Abschnitt **Allgemein** ▸ **Ausnahmen** auf **Ausnahme hinzufügen**. Führen Sie anschließend eine der folgenden Aktionen aus:
   - Geben Sie den auszuschließenden Dateipfad ein oder suchen Sie ihn.
   - Geben Sie den auszuschließenden Ordnerpfad ein oder suchen Sie ihn.
   - Geben Sie eine URL ein, die Sie ausschließen möchten.
4. Klicken Sie zum Abschluss auf **Ausnahme hinzufügen**.

Konfigurieren automatischer Updates

Sie können die Virendefinitionen und die Programmversion von Small Office Protection auf Ihren Geräten automatisch aktualisieren, wenn neue Updates verfügbar sind. Alternativ können Sie Ihre Geräte auf manuelle Updates einstellen. Weitere Informationen finden Sie unterAktualisieren von Small Office Protection (auf Englisch).

Konfigurieren automatischer Updates

1. Klicken Sie in der Benutzeroberfläche oben rechts auf **Menü**.

2. Klicken Sie auf **Einstellungen**.
3. Gehen Sie im Abschnitt *Allgemein* zur Registerkarte **Aktualisieren**.
4. Klicken Sie neben den beiden Schaltflächen **Auf Updates prüfen** auf **Weitere Optionen**.
5. Wählen Sie **Automatische Aktualisierung**.

Erstellen und Konfigurieren von Scans

Windows Workstations

In den Virenscan-Einstellungen können Sie die Dateitypen und Programme konfigurieren, die von Small Office Protection gescannt werden. Die wesentlichen Details für die Scanziele werden daher in den Scan-Einstellungen konfiguriert, Ausnahmen aber im Abschnitt „Allgemein".

Arten von Scans

- **Vollständiger Virenscan**: führt einen intensiven System-Scan durch, bei dem alle Festplatten, Rootkits und Autostart-Programme überprüft werden
- **Gezielter Scan**: scannt nur die zu Beginn des Scans von Ihnen ausgewählten Ordner
- **Explorer-Scan**: scannt bestimmte, von Ihnen angegebene Dateien oder Ordner, ist aber nur über das Windows-Kontextmenü verfügbar, das mit einem Rechtsklick auf eine Datei, einen Ordner oder ein Laufwerk aufgerufen wird
- **Startzeit-Prüfung (nur MS Windows)**: führt beim Starten des Geräts einen Scan aus

Sie können auf die Einstellungen für die verschiedenen Scantypen zugreifen, indem Sie auf Menü ▸ Einstellungen klicken und dann zu Schutz ▸ Virenscans gehen.

Anpassen vollständiger Virenscans

Empfindlichkeit

Sie können den Wirkungsgrad des Scans bestimmen, indem Sie die entsprechenden Einstellungen anpassen. Je höher der Wirkungsgrad, desto höher der Schutz und das Potenzial für fehlerhafte Malware-Erkennungen. Die Verringerung des Wirkungsgrads senkt die Wahrscheinlichkeit von Fehlmeldungen, möglicherweise aber auch die

Wirksamkeit der Scans. Der Wirkungsgrad eines Scans kann durch Ziehen des Schiebereglers auf ein mittleres, hohes oder niedriges Niveau eingestellt werden.

Auf potenziell unerwünschte Programme (PUPs) prüfen: ermöglicht es Avast, nach Programmen zu suchen, die heimlich mit anderen Programmen heruntergeladen werden und unerwünschte Aktivitäten ausführen können

Links während der Überprüfung folgen: ermöglicht es Avast, andere Dateien, die von den zu scannenden Dateien verwendet werden, auf potenziell schädliche Inhalte zu prüfen

Komplette Datei prüfen (sehr langsam bei großen Dateien): ermöglicht es Avast, ganze Dateien zu scannen und nicht nur die Teile, die normalerweise von bösartigem Code betroffen sind

Priorität: bestimmt, wie viele Ressourcen von Avast während des Scans genutzt werden können. Je höher die Priorität, desto schneller der Scan, aber womöglich werden andere Prozesse auf dem Gerät verlangsamt.

Prüfbereiche

Aktivieren Sie die Kontrollkästchen neben den aufgelisteten Bereichen, um sie in den Scan miteinzubeziehen. Die wichtigsten Optionen für Bereiche sind:

- **Alle Laufwerke**: ermöglicht es Avast alle Festplatten auf Ihrem PC zu scannen
- **Systemlaufwerk**: Die Optionen in diesem Abschnitt gelten für Daten, die auf physischen Geräten wie Festplatten und USB-Sticks gespeichert sind.

Die folgenden Scanoptionen werden auf die oben angegebenen Bereiche angewendet.

Alle Wechseldatenträger: ermöglicht es Avast, Anwendungen zu scannen, die automatisch gestartet werden, wenn Sie einen USB-Stick oder andere Wechseldatenträger in den PC einstecken

Rootkits: ermöglicht es Avast, nach versteckten Bedrohungen im System zu suchen

UEFI BIOS: ermöglicht es Avast, beim Startvorgang die wichtigsten Firmware-Schnittstellen zu prüfen

CD-ROM- und DVD-Laufwerke: ermöglicht es Avast, CD- und DVD-Laufwerke auf schädliche Inhalte zu prüfen

Im Speicher geladene Module: ermöglicht es Avast, Anwendungen und Prozesse zu scannen, die nach dem Systemstart gestartet oder im Hintergrund ausgeführt werden

Pakete und Archive

Im Abschnitt „Packer und Archive" können Sie angeben, welche Arten von komprimierten Dateien von Avast während des Scans entpackt werden sollen.

- **Nur gewöhnliche Installationsprogramme scannen:** scannt den Inhalt von ausführbaren Dateien, die zur Installation von Anwendungen verwendet werden
- **Alle Archive scannen:** scannt alle Inhalte von Archivdateien; dies kann den Scanvorgang erheblich verlangsamen.
- **Archive nicht scannen**: deaktiviert Scans von Archivdateien

Dateitypen

Geben Sie die Dateitypen an, die beim Scannen Ihres PC auf Malware priorisiert werden sollen:

- **Inhaltsbasierte Typen (langsam)**: scannt Dateien, die normalerweise am anfälligsten für Malware-Angriffe sind
- **Auf Namenserweiterung basierte Typen (schnell)**: überprüft nur Dateien mit riskanten Erweiterungen wie „.exe", „.com", „.bat"
- **Alle Dateien scannen (sehr langsam)**: prüft alle Dateien auf Ihrem PC auf Malware

Automatische Aktionen während dieser Prüfung durchführen: Aktivieren Sie diese Option und definieren Sie dann die automatische Aktion, die ausführt werden soll, wenn eine infizierte Datei gefunden wird:

- **Automatisch beheben**: ermöglicht es Avast, die infizierte Datei zu reparieren. Wenn keine Reparatur möglich ist, wird die Datei in den Virus-Containerverschoben. Schlägt dies fehl, wird die Datei gelöscht.
- **Datei in Virus-Container verschieben**: Die infizierte Datei wird nicht automatisch repariert, sondern in den Virus-Container verschoben.
- **Datei löschen:** Avast versucht nicht, die infizierte Datei zu reparieren oder in den Virus-Container zu verschieben. Die Datei wird stattdessen automatisch gelöscht.

Computer nach Abschluss des Scans herunterfahren: ermöglicht es Avast, Ihren PC nach Abschluss des Scans herunterzufahren

Protokolldatei erstellen: ermöglicht es Avast, automatisch eine Protokolldatei zu erstellen und zu speichern. Der Speicherort der Protokolldatei wird unterhalb dieser Option genannt.

Ausnahmen

Generell wird nicht empfohlen, Dateien oder Ordner von einem Scan auszuschließen. Sie können aber Ausnahmen definieren, um bestimmte Dateien oder Ordner vorübergehend zwecks Fehlerbehebung von einem Scan auszuschließen. Klicken Sie unten auf der Seite mit den Scan-Einstellungen auf **Ausnahmen anzeigen**. Von dort können Sie die Schritte in **Konfigurieren von Ausnahmen** befolgen.

Anpassen von gezielten Scans

Empfindlichkeit

Sie können den Wirkungsgrad des Scans bestimmen, indem Sie die entsprechenden Einstellungen anpassen. Je höher der Wirkungsgrad, desto höher der Schutz und das Potenzial für fehlerhafte Malware-Erkennungen. Die Verringerung des Wirkungsgrads senkt die Wahrscheinlichkeit von Fehlmeldungen, möglicherweise aber auch die Wirksamkeit der Scans. Der Wirkungsgrad eines Scans kann durch Ziehen des Schiebereglers auf ein mittleres, hohes oder niedriges Niveau eingestellt werden.

Auf potenziell unerwünschte Programme (PUPs) prüfen: ermöglicht es Avast, nach Programmen zu suchen, die heimlich mit anderen Programmen heruntergeladen werden und unerwünschte Aktivitäten ausführen können

Links während der Überprüfung folgen: ermöglicht es Avast, andere Dateien, die von den zu scannenden Dateien verwendet werden, auf potenziell schädliche Inhalte zu prüfen

Komplette Datei prüfen (sehr langsam bei großen Dateien): ermöglicht es Avast, ganze Dateien zu scannen und nicht nur die Teile, die normalerweise von bösartigem Code betroffen sind

Priorität: bestimmt, wie viele Ressourcen von Avast während des Scans genutzt werden können. Je höher die Priorität, desto schneller der Scan, aber womöglich werden andere Prozesse auf dem Gerät verlangsamt.

Pakete und Archive

Im Abschnitt „Packer und Archive" können Sie angeben, welche Arten von komprimierten Dateien von Avast während des Scans entpackt werden sollen.

- **Nur gewöhnliche Installationsprogramme scannen:** scannt den Inhalt von ausführbaren Dateien, die zur Installation von Anwendungen verwendet werden

- **Alle Archive scannen:** scannt alle Inhalte von Archivdateien; dies kann den Scanvorgang erheblich verlangsamen.
- **Archive nicht scannen**: deaktiviert Scans von Archivdateien

Dateitypen

Geben Sie die Dateitypen an, die beim Scannen Ihres PC auf Malware priorisiert werden sollen:

- **Inhaltsbasierte Typen (langsam)**: scannt Dateien, die normalerweise am anfälligsten für Malware-Angriffe sind
- **Auf Namenserweiterung basierte Typen (schnell)**: überprüft nur Dateien mit riskanten Erweiterungen wie „.exe", „.com", „.bat"
- **Alle Dateien scannen (sehr langsam)**: prüft alle Dateien auf Ihrem PC auf Malware

Automatische Aktionen während dieser Prüfung durchführen: Aktivieren Sie diese Option und definieren Sie dann die automatische Aktion, die ausführt werden soll, wenn eine infizierte Datei gefunden wird:

- **Automatisch beheben**: ermöglicht es Avast, die infizierte Datei zu reparieren. Wenn keine Reparatur möglich ist, wird die Datei in den Virus-Containerverschoben. Schlägt dies fehl, wird die Datei gelöscht.
- **Datei in Virus-Container verschieben**: Die infizierte Datei wird nicht automatisch repariert, sondern in den Virus-Container verschoben.
- **Datei löschen:** Avast versucht nicht, die infizierte Datei zu reparieren oder in den Virus-Container zu verschieben. Die Datei wird stattdessen automatisch gelöscht.

Computer nach Abschluss des Scans herunterfahren: ermöglicht es Avast, Ihren PC nach Abschluss des Scans herunterzufahren

Protokolldatei erstellen: ermöglicht es Avast, automatisch eine Protokolldatei zu erstellen und zu speichern. Der Speicherort der Protokolldatei wird unterhalb dieser Option genannt.

Anpassen von Explorer-Scans

Empfindlichkeit

Sie können den Wirkungsgrad des Scans bestimmen, indem Sie die entsprechenden Einstellungen anpassen. Je höher der Wirkungsgrad, desto höher der Schutz und das

Potenzial für fehlerhafte Malware-Erkennungen. Die Verringerung des Wirkungsgrads senkt die Wahrscheinlichkeit von Fehlmeldungen, möglicherweise aber auch die Wirksamkeit der Scans. Der Wirkungsgrad eines Scans kann durch Ziehen des Schiebereglers auf ein mittleres, hohes oder niedriges Niveau eingestellt werden.

Auf potenziell unerwünschte Programme (PUPs) prüfen: ermöglicht es Avast, nach Programmen zu suchen, die heimlich mit anderen Programmen heruntergeladen werden und unerwünschte Aktivitäten ausführen können

Links während der Überprüfung folgen: ermöglicht es Avast, andere Dateien, die von den zu scannenden Dateien verwendet werden, auf potenziell schädliche Inhalte zu prüfen

Komplette Datei prüfen (sehr langsam bei großen Dateien): ermöglicht es Avast, ganze Dateien zu scannen und nicht nur die Teile, die normalerweise von bösartigem Code betroffen sind

Priorität: bestimmt, wie viele Ressourcen von Avast während des Scans genutzt werden können. Je höher die Priorität, desto schneller der Scan, aber womöglich werden andere Prozesse auf dem Gerät verlangsamt.

Pakete und Archive

Im Abschnitt „Packer und Archive" können Sie angeben, welche Arten von komprimierten Dateien von Avast während des Scans entpackt werden sollen.

- **Nur gewöhnliche Installationsprogramme scannen:** scannt den Inhalt von ausführbaren Dateien, die zur Installation von Anwendungen verwendet werden
- **Alle Archive scannen:** scannt alle Inhalte von Archivdateien; dies kann den Scanvorgang erheblich verlangsamen.
- **Archive nicht scannen**: deaktiviert Scans von Archivdateien

Dateitypen

Geben Sie die Dateitypen an, die beim Scannen Ihres PC auf Malware priorisiert werden sollen:

- **Inhaltsbasierte Typen (langsam)**: scannt Dateien, die normalerweise am anfälligsten für Malware-Angriffe sind
- **Auf Namenserweiterung basierte Typen (schnell)**: überprüft nur Dateien mit riskanten Erweiterungen wie „.exe", „.com", „.bat"

- **Alle Dateien scannen (sehr langsam)**: prüft alle Dateien auf Ihrem PC auf Malware

Automatische Aktionen während dieser Prüfung durchführen: Aktivieren Sie diese Option und definieren Sie dann die automatische Aktion, die ausführt werden soll, wenn eine infizierte Datei gefunden wird:

- **Automatisch beheben**: ermöglicht es Avast, die infizierte Datei zu reparieren. Wenn keine Reparatur möglich ist, wird die Datei in den Virus-Containerverschoben. Schlägt dies fehl, wird die Datei gelöscht.
- **Datei in Virus-Container verschieben**: Die infizierte Datei wird nicht automatisch repariert, sondern in den Virus-Container verschoben.
- **Datei löschen:** Avast versucht nicht, die infizierte Datei zu reparieren oder in den Virus-Container zu verschieben. Die Datei wird stattdessen automatisch gelöscht.

Computer nach Abschluss des Scans herunterfahren: ermöglicht es Avast, Ihren PC nach Abschluss des Scans herunterzufahren

Protokolldatei erstellen: ermöglicht es Avast, automatisch eine Protokolldatei zu erstellen und zu speichern. Der Speicherort der Protokolldatei wird unterhalb dieser Option genannt.

Konfigurieren von Startzeit-Prüfungen

Empfindlichkeit

Sie können den Wirkungsgrad des Scans bestimmen, indem Sie die entsprechenden Einstellungen anpassen. Je höher der Wirkungsgrad, desto höher der Schutz und das Potenzial für fehlerhafte Malware-Erkennungen. Die Verringerung des Wirkungsgrads senkt die Wahrscheinlichkeit von Fehlmeldungen, möglicherweise aber auch die Wirksamkeit der Scans. Der Wirkungsgrad eines Scans kann durch Ziehen des Schiebereglers auf ein mittleres, hohes oder niedriges Niveau eingestellt werden.

Auf potenziell unerwünschte Programme (PUPs) prüfen: ermöglicht es Avast, nach Programmen zu suchen, die heimlich mit anderen Programmen heruntergeladen werden und unerwünschte Aktivitäten ausführen können

Archivdateien entpacken: ermöglicht es Avast, Dateien und Ordner aus Archiven zum Scannen zu extrahieren („entpacken")

Prüfbereiche

Aktivieren Sie die Kontrollkästchen neben den aufgelisteten Bereichen, um sie in den Scan miteinzubeziehen. Die wichtigsten Optionen für Bereiche sind:

- **Alle Laufwerke**: ermöglicht es Avast alle Festplatten auf Ihrem PC zu scannen
- **Systemlaufwerk**: Die Optionen in diesem Abschnitt gelten für Daten, die auf physischen Geräten wie Festplatten und USB-Sticks gespeichert sind.

Die folgenden Scanoptionen werden auf die oben angegebenen Bereiche angewendet.

Autostart-Programme: ermöglicht es Avast, alle Autostart-Programme zu prüfen

Automatische Aktionen während dieser Prüfung durchführen: Aktivieren Sie diese Option und definieren Sie dann die automatische Aktion, die ausführt werden soll, wenn eine infizierte Datei gefunden wird:

- **Automatisch beheben**: ermöglicht es Avast, die infizierte Datei zu reparieren. Wenn keine Reparatur möglich ist, wird die Datei in den Virus-Container verschoben. Schlägt dies fehl, wird die Datei gelöscht.
- **Datei in Virus-Container verschieben**: Die infizierte Datei wird nicht automatisch repariert, sondern in den Virus-Container verschoben.
- **Datei löschen:** Avast versucht nicht, die infizierte Datei zu reparieren oder in den Virus-Container zu verschieben. Die Datei wird stattdessen automatisch gelöscht.

Android-Geräte

Mit der Option „Scannen" können Sie alle auf dem Gerät installierten Anwendungen scannen. Sie werden dabei über Sicherheitsrisiken informiert, die durch Änderungen von Android-Standardeinstellungen verursacht werden. Die vom Scan verwendeten Virendefinitionen werden automatisch aktualisiert.

1. Tippen Sie auf Ihrem Gerät auf das Symbol für *Avast Mobile Security*, um die App zu öffnen.
2. Tippen Sie im Hauptbildschirm auf **Scannen**.

Wenn der Scan abgeschlossen ist, wird von der App eine Meldung angezeigt. Entweder wird gemeldet, dass keine Probleme gefunden wurden, oder aber es wird eine Liste der gefundenen Probleme zusammen mit Lösungsmöglichkeiten aufgelistet. Sie können auf **Beheben** oder **Aktivieren** tippen, sofern verfügbar.

Scannen des internen Speichers

Der Scan des internen Speichers ist standardmäßig deaktiviert. Wenn Sie den internen Speicher in die Scans miteinbeziehen möchten, können Sie dies in den Einstellungen angeben.

1. Tippen Sie auf Ihrem Gerät auf das Symbol für *Avast Mobile Security*, um die App zu öffnen.
2. Tippen Sie auf **Menü** ▸ **Einstellungen**.
3. Tippen Sie auf **Schutz**.
4. Klicken Sie auf den Schieberegler, um *Internen Speicher überprüfen* zu aktivieren.

iOS-Geräte

Mit der Option „Scannen" können Sie alle auf dem Gerät installierten Anwendungen scannen. Sie werden dabei über Sicherheitsrisiken informiert, die durch Änderungen von iOS-Standardeinstellungen verursacht werden. Die vom Scan verwendeten Virendefinitionen werden automatisch aktualisiert.

1. Tippen Sie auf Ihrem Gerät auf das Symbol für *Avast Sicherheit und Datenschutz*, um die App zu öffnen.
2. Tippen Sie im Hauptbildschirm auf **Scannen**.

Wenn der Scan abgeschlossen ist, wird von der App eine Meldung angezeigt. Entweder wird gemeldet, dass keine Probleme gefunden wurden, oder aber es wird eine Liste der gefundenen Probleme zusammen mit Lösungsmöglichkeiten aufgelistet. Sie können auf **Beheben** oder **Aktivieren** tippen, sofern verfügbar.

In Small Office Protection sind viele weitere Funktionen und Optionen verfügbar. Weitere Informationen finden Sie in unserer Knowledge Base unter https://businesshelp.avast.com/.