

Erste Schritte: Avast Business Antivirus

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

<https://businesshelp.avast.com/>

Inhalt

Erste Schritte: Avast Business Antivirus	1
Inhalt	2
Einrichten des Geräts	4
Überprüfen der Systemanforderungen	4
Avast Business Antivirus-Endgeräte.....	4
Überprüfen der Firewall-Anforderungen	4
Ports.....	4
URLs.....	5
Installation von Avast Business Antivirus auf Geräten	5
Anpassung der Installation	5
Empfohlene Komponenten für Server und Arbeitsstationen	6
Empfohlen für Business-Umgebungen.....	6
Empfohlen für Server.....	6
Aktivieren von Lizenzen auf Ihrem Gerät	6
Einstellungskonfiguration und Komponenten	8
Antivirus-Komponenten nach Produktlizenz	8
Aktivieren und Deaktivieren von Komponenten.....	8
Installieren und Deinstallieren von Komponenten.....	9
Konfigurieren von Ausnahmen	10
Platzhalter.....	10
Ausnahmen.....	10
Hinzufügen von Ausnahmen.....	10
Konfigurieren automatischer Updates	11
Konfigurieren automatischer Updates	11
Erstellen und Konfigurieren von Scans	11

Arten von Scans	11
Anpassen vollständiger Virens cans.....	12
Empfindlichkeit	12
Prüfbereiche	12
Pakete und Archive	13
Dateitypen.....	13
Ausnahmen	14
Anpassen von gezielten Scans	14
Empfindlichkeit	14
Pakete und Archive	15
Dateitypen.....	15
Anpassen von Explorer-Scans	16
Empfindlichkeit	16
Pakete und Archive	16
Dateitypen.....	17
Konfigurieren von Startzeit-Prüfungen.....	18
Empfindlichkeit	18
Prüfbereiche	18

Einrichten des Geräts

Überprüfen der Systemanforderungen

Avast Business Antivirus-Endgeräte

Windows:

- 7 SP1 oder höher, 8.x außer RT und Starter Edition, 10 außer Mobile und IoT Core Edition
- Server 2008 R2, 2012 R2, 2016, 2019, beliebige Edition mit aktuellem Service Pack außer Server Core
- Microsoft Exchange Server 2010 SP2, 2013, 2016, 2019
- Microsoft SharePoint Services 3.0 und SharePoint Server 2010 und höher

Mac:

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

Linux:

- CentOS ab Version 7
- Debian ab Version 8
- Red Hat Enterprise Linux 7.4
- Ab Ubuntu LTS 16.04

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 Avast Business Antivirus-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)

Installation von Avast Business Antivirus auf Geräten

Für nicht verwaltetes Avast Business Antivirus können Sie das Installationsprogramm unter <https://www.avast.com/installation-files> herunterladen. Klicken Sie auf die Registerkarte „Business“, und wählen Sie entweder das Online- oder das Offline-Installationsprogramm für Ihre Antivirus-Version aus. Nach dem Download können Sie das Installationsprogramm auf dem Gerät ausführen, auf dem Sie Antivirus installieren möchten.

Bei Auswahl des Online-Installationsprogramms werden die anderen Dienste nach der Installation des Antivirus-Agenten heruntergeladen. Diese Option wird nicht empfohlen, wenn Sie Antivirus auf mehreren Geräten gleichzeitig installieren. Der Grund ist, dass von jedem einzelnen Gerät eine Verbindung mit den Avast-Servern hergestellt wird, um die anderen Dienste herunterzuladen.

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 Avast Business Antivirus 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 Avast Business Antivirus 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.

Empfohlen für Server

Die folgenden Komponenten sollten vollkommen deinstalliert, durch Ziehen des Schiebereglers in die Position **Aus** deaktiviert oder erst gar nicht auf dem Gerät installiert werden:

- Web-Schutz
- E-Mail-Schutz

Aktivieren von Lizenzen auf Ihrem Gerät

Sie können Ihr Avast Business Antivirus-Abonnement nach der Installation des Programms auf Ihren Geräten aktivieren.

1. Öffnen Sie die Benutzeroberfläche von Avast Business Antivirus 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.

Einstellungskonfiguration und Komponenten

Für Avast Business Antivirus gibt es zahlreiche Komponenten, sowohl für die Grundversion als auch für die Versionen Pro und Plus von Antivirus.

Antivirus-Komponenten nach Produktlizenz

Komponente	Avast Business Antivirus	Avast Business Antivirus Pro	Avast Business Antivirus Pro Plus
Dateisystem-Schutz	X	X	X
Web-Schutz	X	X	X
E-Mail-Schutz	X	X	X
Verhaltensschutz	X	X	X
Schutz gegen Fernzugriff			X
WLAN-Inspektor	X	X	X
Real Site	X	X	X
Firewall	X	X	X
Sandbox	X	X	X
Anti-Spam	X	X	X
Exchange		X	X
Sharepoint		X	X
Webcam-Schutz			X
SecureLine VPN			X
Daten-Schredder		X	X
Passwords			X
Passwortschutz			X
Software Updater	X	X	X
Browser Cleanup			X
Rettungsmedium	X	X	X

Aktivieren und Deaktivieren von Komponenten

Viele der in Avast Business Antivirus 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 Avast Business Antivirus.
2. Klicken Sie auf die Registerkarte für die Komponente, die Sie aktivieren oder deaktivieren möchten:
 - **Schutz:** Dateisystem-Schutz, Web-Schutz, E-Mail-Schutz, Verhaltenschutz, 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 Avast Business Antivirus 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 Avast Business Antivirus.
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 Avast Business Antivirus verfügbaren Komponenten finden Sie unter [Konfigurieren von Einstellungen in Avast Business Antivirus](#) (auf Englisch).

Konfigurieren von Ausnahmen

Platzhalter

Viele der Schutzmodule und andere Komponenten von Avast Business Antivirus 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 Dateiabc.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 Avast Business Antivirus verteilt werden.

Hinzufügen von Ausnahmen

1. Öffnen Sie die Client-Benutzeroberfläche von Avast Business Antivirus.
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 Avast Business Antivirus auf Ihren Geräten automatisch aktualisieren, wenn neue Updates verfügbar sind. Alternativ können Sie Ihre Geräte auf manuelle Updates einstellen. Weitere Informationen finden Sie unter [Aktualisieren von Avast Business Antivirus](#) (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

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

Arten von Scans

- **Vollständiger Virensan**: 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 > Virens cans gehen.

Anpassen vollständiger Virens cans

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 Fehlern, 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-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.

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 Fehlalarmen, 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-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.

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 Fehlalarmen, 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 ausgeführt 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.

In Avast Business Antivirus sind viele weitere Funktionen und Optionen verfügbar. Weitere Informationen finden Sie in unserer Knowledge Base unter <https://businesshelp.avast.com/>.