AVIRA

Whitepaper
Avira Cloud-Sicherheit

1. Einleitung

Viele Anwender sind mit dem Konzept des Cloud-Computings bereits vertraut – die Avira Cloud-Sicherheit bietet Ihnen auf dieser Grundlage ein neues Niveau an Internetsicherheit. Im Folgenden erfahren Sie alles über die nächste Generation der Internetsicherheit – die Avira Cloud-Sicherheit.

Wir beginnen mit einer kurzen Einführung in die Avira Cloud-Sicherheit und wenden uns dann den grundlegenden Elementen zu. Im Anschluss stellen wir die Vorteile dieser neuen Plattform vor und beantworten abschließend einige häufig gestellte Fragen.

1.1 Weshalb benötigt man die Cloud-Sicherheit?

Die Entwicklung der Avira Cloud-Sicherheit begann mit einer Frage: Wie können Nutzer sich vor Malware schützen, wenn die Hacker und Malware-Autoren in beängstigend hohem Tempo neue Bedrohungen produzieren?

Täglich werden Abertausende neue Malware-Bedrohungen entwickelt und in die freie Wildbahn entlassen. Trojaner lauern versteckt in Email-Anhängen. Rootkits sabotieren die Programme, die zu deren Entfernung gedacht sind. Adware blendet störende und potenziell unsichere Popup-Fenster ein. Keylogger spionieren die Passwörter der Nutzer aus.

In der Vergangenheit war die PC-Sicherheit ein überschaubarer Bereich. Die Entwickler von Virenschutz-Software programmierten Gegenmaßnahmen und hatten genug Zeit, auf neue Viren zu reagieren. Allerdings haben Hacker und Malware-Autoren daraufhin ihre Fertigkeiten verbessert, und es kam schon bald zu einer Art Wettbewerb zwischen Hackern und Virenschutzprogrammen. Wie bei einem Rüstungswettbewerb entstand ein Teufelskreis. Jede Seite versuchte, den Gegner zu übertrumpfen.

Hacker starteten Virenangriffe, und Sicherheitsexperten entwarfen massive virtuelle Schutzmauern, um die Angriffe zu kontern. In der Folge attackierten die Hacker die Programme so lange, bis sie einen Weg durch die Mauer gefunden hatten. Die Sicherheitsexperten begannen daraufhin, die virtuellen Mauern auszubauen und robuster zu machen. Die Malware-Autoren gaben sich jedoch nicht geschlagen und attackierten die neuen Virenschutzmaßnahmen erneut, bis sie weitere Schwachstellen entdeckten.

Die Sicherheitsexperten mussten wieder neue Schutzmauern entwerfen, die letztendlich erneut von Hackern überwunden wurden. Tagein, tagaus waren beide Seiten in einen Kampf verwickelt, um sich jeweils einen Schritt voraus zu sein.

Viele Jahre lang war dieses Modell der reaktiven Abwehr die Grundlage erfolgreicher Internetsicherheit. Allerdings war dieser Ansatz nicht nachhaltig. Ständig verschärfte Sicherheitsmaßnahmen verlangsamten die PCs und verbrauchten wertvolle Ressourcen, die für die eigentliche Arbeit am Rechner benötigt wurden. Die Anwender benötigten einen intelligenteren Schutz.

Vor Kurzem entstand in diesem Cyberkampf ein neues Feld – die Akteure sind in diesem Fall erfahrene Profis. Heutzutage ist Hacking nicht mehr das Werk von einsamen Einzeltätern, die Malware für ihre eigene zweifelhafte Unterhaltung entwerfen. Es gibt Organisationen, die sich auf die Ausspionierung privater Daten von Konsumenten spezialisiert haben. Datendiebstahl, Identitätsdiebstahl, Geldwäsche sowie viele weitere Bereiche des Internetbetrugs und der Erpressung gehören zu deren Metier – und sie sind gut darin.

Die neue Hackergeneration verfügt über einen maßgeblichen Unterschied: Sie besitzt Zugriff auf dieselben Virenschutzprogramme wie die Anwender. Sobald man den jeweiligen Virenschutz selbst besitzt, lässt sich bösartiger Code viel einfacher schreiben. Die Hacker nutzen einfach automatisierte Verfahren zum Testen ihrer Codes, bis sie durch eine bestimmte Abänderung ein Loch in der Mauer entdecken.

Aus diesem Grund sind dickere Mauern nicht mehr sinnvoll. PCs hinter gigantischen Firewalls mit modernsten Algorithmen zur Malware-Erkennung schützen den Nutzer nur vor bekannten Bedrohungen. Daher benötigte man einen neuen Ansatz zum Virenschutz. Und genau unter diesen Bedingungen wurde die Avira Cloud-Sicherheit entwickelt.

1.2 Was ist die Avira Cloud-Sicherheit?

Die Avira Cloud-Sicherheit ist ein globales, cloudbasiertes Online-System, das ressourcenschonende und innovative Dateiklassifizierung in Echtzeit ermöglicht. Das intelligente Internet-Sicherheitssystem ist rund um die Uhr aktiv und auf mehrere Standorte verteilt.

Oder einfacher gesagt: es ist ein weltweites PC-Netzwerk mit einer gemeinsamen Onlinedatenbank zur Dateidefinition. Diese Dateien werden mit innovativen Algorithmen und Systemen klassifiziert und den Nutzern dann in Echtzeit bereitgestellt. Das Ergebnis: Sie erhalten eine schnelle, ultraleichte und äußerst zuverlässige Plattform zum Virenschutz mit sehr kurzer Reaktionszeit.

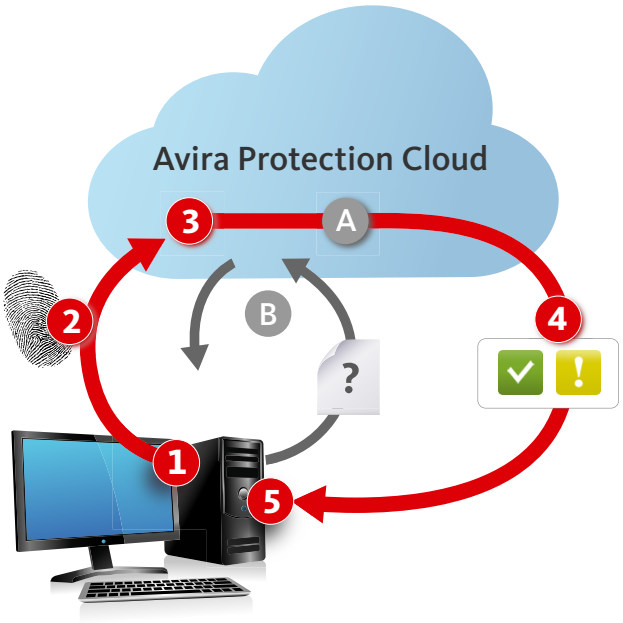
1.3 Wie funktioniert die Avira Cloud-Sicherheit?

Der Avira Cloud-Sicherheit-Prozess wird aktiv, wenn ein einzelner, durch die Cloud geschützter PC an einem beliebigen Standort auf der Welt eine unbekannte Datei aufruft. In diesem Fall erhält der Nutzer eine Benachrichtigung, und der Avira Cloud-Sicherheit-Prozess wird automatisch gestartet.

Augenblicklich, nachdem die unbekannte (nicht verdächtige, aber noch nicht klassifizierte) Datei aufgerufen wird, wird ein „Fingerabdruck“ dieser Datei in die Avira Cloud-Sicherheit hochgeladen. Nach dem Hochladen wird der Fingerabdruck mit Millionen Definitionen sicherer und unsicherer Dateien, die bereits in der Avira Cloud-Sicherheit gespeichert sind, abgeglichen. Wenn die Datei einer bereits bekannten, sicheren Datei entspricht, wird der Aufruf genehmigt, und der Nutzer erhält Zugriff – alles geht dann seinen normalen Gang weiter.

Wenn die Datei jedoch nicht identifiziert werden kann, fordert Avira Cloud-Sicherheit den Nutzer auf, die komplette Datei für eine umfassende Analyse hochzuladen. Nach dem Scannen wird die Cloud bei erkannter Malware eine sofortige Quarantäne veranlassen und diese als „bösartig" definieren. Die Avira Cloud-Sicherheit führt diesen Prozess innerhalb weniger Sekunden aus (bei einer infizierten Datei wird der Anwender natürlich alarmiert).

Andererseits wird die Avira Cloud-Sicherheit eine neue Datei, die als malwarefrei eingestuft wird, als „sicher" kennzeichnen. Diese Information wird allen weiteren Cloud-Nutzern zur Verfügung gestellt, die dann nicht mehr das gleiche Verfahren durchlaufen müssen.



So funktioniert's

1. Die Avira Anwendung entdeckt eine verdächtige Datei auf dem PC.
2. Der digitale Fingerabdruck der Datei wird ermittelt und zur Analyse an Aviras Cloud-Sicherheit gesandt.
3. Der Fingerabdruck wird mit zuvor von der Cloud-Sicherheit geprüften Dateien verglichen, was zu zwei Ergebnissen führen kann:

   A Der Fingerabdruck gehört zu einer bereits von der Cloud-Sicherheit geprüften Datei – und wird sofort entweder als sauber oder als Malware eingestuft.

   B Der Fingerabdruck ist neu für die Cloud-Sicherheit. Diese lädt die gesamte Datei hoch, analysiert sie gründlich und stuft sie entweder als sauber oder als Malware ein.

4. Die Cloud-Sicherheit meldet der Avira Anwendung auf dem PC den Status (sauber oder Malware) des Fingerabdrucks.
5. Sollte die Datei als Malware eingestuft werden, entfernt die Avira Anwendung die Gefahr.

Weitere Informationen zur APC finden Sie im Internet: *http://www.avira.com/de/avira-protection-cloud*

2. Die Vorteile der Avira Cloud-Sicherheit

2.1 Schwarmintelligenz

Einer der Hauptvorteile der Avira Cloud-Sicherheit-Plattform ist deren Zugriff auf das weltweite Avira Netzwerk mit über 100 Millionen Anwendern, um neue Viren zu erkennen. Täglich wird von den Nutzern auf unzählige Dateien zugegriffen – beim Surfen, Scannen, Shoppen, Browsen, Streamen, Herunterladen und Chatten. Daraus resultiert eine gigantische Anzahl an Dateien, die alle untersucht werden müssen. Gleichzeitig bietet dies eine optimale Gelegenheit, um die Fähigkeiten von Avira zur Malware-Detektion immens zu erweitern.

Avira Cloud-Sicherheit nutzt diese Möglichkeit, indem das Scanpotenzial von Millionen unabhängiger Rechner auf einer einzigen zentralen Plattform zur Malwaredefinition vereint wird. Sie fungiert dabei als Verteilungsknoten und stellt den Cloud-Sicherheit-Anwendern weltweit in Echtzeit neue Virenerkennungsmuster zur Verfügung.

Oder einfacher gesagt: Ab jetzt muss ein Rechner nicht mehr alleine neue Malware aufspüren und identifizierten. Die Avira Cloud-Sicherheit versetzt jeden angeschlossenen PC weltweit in die Lage, die globale Internetsicherheit zu erhöhen, indem er unbekannte Dateien zur Analyse übermittelt.

2.2 Echtzeit-Updates

Der zweite Vorteil der Avira Cloud-Sicherheit besteht darin, dass sie – im Gegensatz zu planmäßig aktualisierten Virenschutzsystemen – über ein Echtzeit-System zur Aktualisierung verfügt.

Bei einem traditionellen Antivirus-System muss der PC-Anwender ein manuelles Virenupdate ausführen, um vor neu entstandenen Bedrohungen geschützt zu sein. Zwischen diesen Updates ist die Virendefinition auf diesem PC nicht zu 100 Prozent aktuell. Damit ist der PC angreifbar, bis das nächste Update erfolgt.

In der Avira Cloud-Sicherheit hingegen werden permanent detaillierte Informationen über viele Millionen Dateien aktualisiert und bereitgestellt – jede Sekunde, 24 Stunden am Tag, sieben Tage in der Woche. Dies bedeutet, dass jeder Nutzer sofort einen On-Demand-Zugriff auf die aktuellsten Virendefinitionen erhält, oft nur wenige Sekunden nach deren Entdeckung.

2.3 Erkennungsschutz

Wie bereits erwähnt, nutzen Malware-Autoren nicht nur herkömmliche PCs. Sie sind clever genug, sich direkt in ein lokales Antivirus-Programm einzuhacken und die Erkennungsprozesse zu analysieren. Das Antivirusprogramm dient den Hackern dann als eine Art von Labor, um neue Viren zu entwickeln oder ihre Malware anzupassen, damit diese unerkannt bleibt.

Da Avira diese Prozesse in der Cloud ausführt, sind sie für die Hacker unsichtbar. Sie können nicht darauf zugreifen. Avira bezeichnet diesen Vorteil als „Erkennungsschutz“. Da die Avira Cloud-Sicherheit kein lokales Programm ist, können Hacker nicht die gesamte Antivirus-Plattform analysieren. Daher sind sie nicht in der Lage, die verschiedenen Module und Algorithmen, die entsprechende Erkennungsaufgaben ausführen, zu untersuchen. Software, die man nicht sehen kann, ist viel schwieriger zu hacken. Darüber hinaus muss ein Hacker nach der Entwicklung eines Virus dessen Code testen, indem er zahlreiche Varianten hochlädt. Ohne ein lokales Produkt, das als Testplattform dient, können die Hacker diesen kritischen Schritt nicht ausführen.

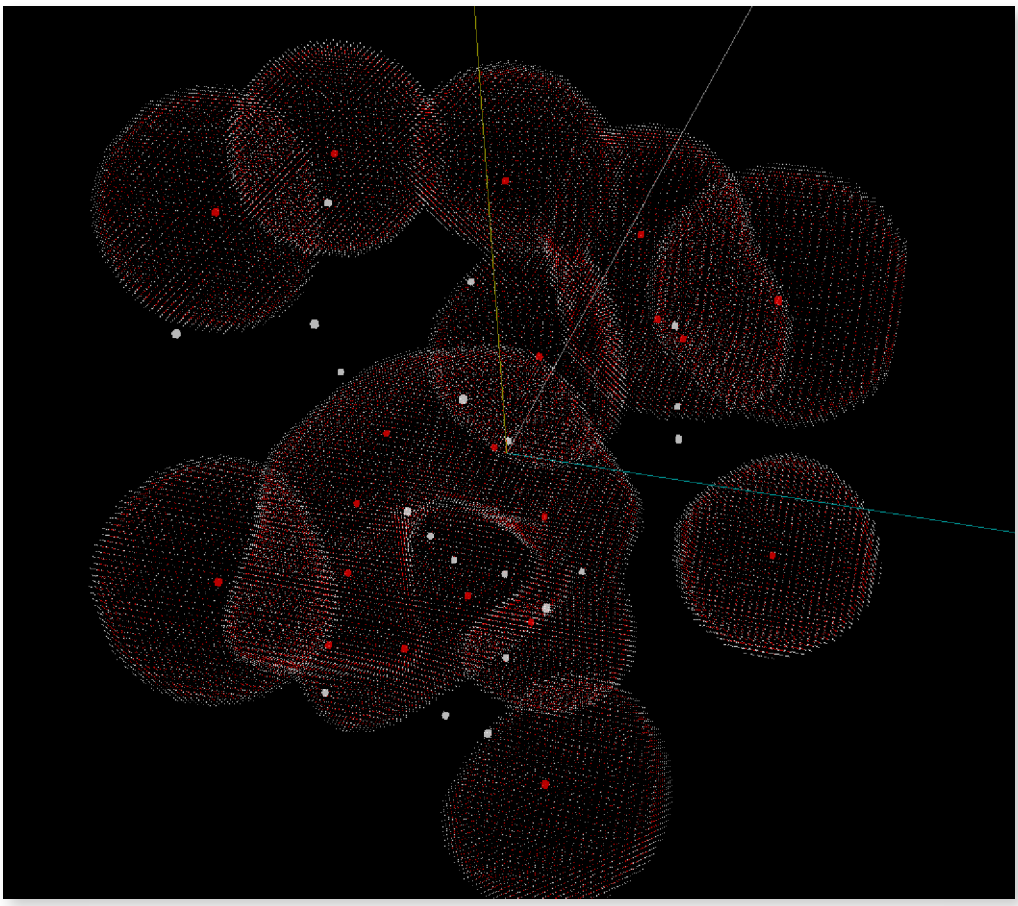
2.4 Geringer Ressourcenverbrauch

Der vierte Vorteil der Avira Cloud-Sicherheit besteht im extrem geringen Ressourcenverbrauch. Da die preisgekrönte Erkennungstechnologie von Avira in der Cloud läuft, profitieren die Nutzer von einem Produkt, das deutlich weniger lokale Ressourcen beansprucht. Darüber hinaus verursacht das Cloud-basierte Scannen viel weniger Netzwerktraffic, da im ersten Schritt nur ein kleiner digitaler Fingerabdruck hochgeladen wird. Somit kann die Avira Cloud-Sicherheit mit nur 12 Kilobyte Traffic über 1.000 Anfragen zur Virenprüfung ausführen.

Gleichzeitig haben die Entwickler von Avira die Latenzzeiten verkürzt, indem die Avira Cloud-Sicherheit mit Hochleistungs-Caches ausgerüstet wurde. Diese werden in Abhängigkeit der Anfragen erweitert. Das Ergebnis: Sie erhalten eine schlankere Virenschutz-Plattform, die im Vergleich zu traditionellen, lokalen Plattformen deutlich weniger PC- und Netzwerkressourcen benötigt. Dies ist insbesondere wichtig, da kein PC für Privatanwender über genügend Ressourcen verfügt, um die erweiterten, generischen Erkennungsverfahren der Avira Cloud-Sicherheit auszuführen. Die Plattform verfügt über künstliche Intelligenz und bietet einige der weltweit innovativsten Module zur Dateianalyse.

Ein Beispiel: Avira besitzt automatische Prozesse zur Malware-Erkennung, die innovative Algorithmen einsetzen. Diese interpretieren neu entdeckte Dateien und klassifizieren diese, ohne dass ein Mensch eingreifen muss. Die künstliche Intelligenz basiert auf konvexer Optimierung. Dies ist eine Methode, mit der konvexe Funktionen und Mengen minimiert werden. Anhand bestimmter Merkmale werden generelle Eigenschaften unbekannter Dateitypen definiert. Diese Eigenschaften werden dann genutzt, um die Dateien als „gut“ oder „böse“ zu klassifizieren. Die Entscheidung beruht jeweils auf Tausenden von Eingangsmerkmalen.

Oder einfacher gesagt: Die bewährten Scanverfahren der Avira Cloud-Sicherheit sind so umfassend, dass sie viel zu aufwendig und komplex sind, um auf einem handelsüblichen PC ausgeführt zu werden.



Avira Cloud-Sicherheit verfügt über ein selbstlernendes System, das die neuesten Erkenntnisse des maschinellen Lernens beinhaltet. Zur Malware-Erkennung kommen optimierte mathematische Modelle zum Einsatz. Innerhalb weniger Minuten kann die selbstlernende Plattform Aufgaben ausführen, für die Wissenschafter viele Jahre benötigen würden.

3. Die Vorteile der Avira Cloud-Sicherheit im Überblick

- Die Schwarmintelligenz erweitert die Erkennungsmöglichkeiten signifikant;
- Mit der Cloud-Speicherung können die Anwender die Scan-Engine von Avira nutzen. Dieser belegt bei proaktiven und reaktiven AV-Tests regelmäßig den ersten Platz;
- Die selbstlernende Technologie von Avira klassifiziert Dateien, ohne auf menschliche Intervention angewiesen zu sein;
- Äußerst geringer Ressourcenverbrauch für lokale Rechner;
- Die Datenbank der Avira Cloud-Sicherheit enthält mehrere Hundert Gigabyte und Terabyte hochgeladener Dateien. Diese Dateien müssen nicht lokal gespeichert werden;
- Die automatisierte Datenbank erfordert keinerlei Vorkenntnisse und ist sehr benutzerfreundlich;
- Die Avira Cloud-Sicherheit wird stetig erweitert und durch die alltäglichen PC-Aktivitäten der Nutzer weiterentwickelt;
- Die dynamische Dateiklassifizierung schützt vor besonders bösartigen Bedrohungen;
- Der erweitere Schutz blockiert sich schnell weiterentwickelnde Malware-Familien;
- Nahtlose Integration bestehender Avira Produktlinien und plattformübergreifender Support, ohne dass die Servicequalität leidet;
- Die Avira Cloud-Sicherheit ist ein geschlossenes Regelsystem. Es werden keine persönlichen Informationen gespeichert.

4. Häufig gestellte Fragen (FAQ)

Welche Daten tauscht mein PC mit der Avira Cloud-Sicherheit aus?

Zuerst wird nur ein kleiner Identifikationsbereich der Datei hochgeladen – der sogenannte „Fingerabdruck". Wenn dieser Fingerabdruck unbekannt ist, fordert Avira Cloud-Sicherheit den Nutzer auf, die gesamte Datei für eine umfassende Analyse hochzuladen. In die Cloud werden nur Informationen zu ausführbaren Dateien hochgeladen (Dateien mit den Endungen .exe oder .dll). Dateiformate wie PDF, Textdateien (.txt und .rtf), Bilder (.jpeg etc.), Word-Dokumente und sonstige private Dateien werden nicht in die Cloud hochgeladen.

Kann jeder auf meine hochgeladenen Daten zugreifen?

Nein. Hochgeladene Daten dienen nur der Malware-Analyse und werden in unserem Cloud-Datencenter gespeichert. Die Weitergabe dieser

Daten an Dritte ist nicht möglich. Das Verfahren ist vollständig automatisiert und an der individuellen Dateiprüfung ist kein Mensch beteiligt. Darüber hinaus wird die Identität des Nutzers beim Hochladen von Fingerabdrücken oder Dateien automatisch entfernt, um die volle Anonymität zu gewährleisten.

Werden die hochgeladenen Daten verschlüsselt?

Ja. Jeder Kommunikationsschritt zwischen dem Anwendersystem und der Avira Cloud-Sicherheit erfolgt immer verschlüsselt. Hierbei wird das Transport-Layer-Security-Verfahren (TLS) genutzt.

5. Über Avira

Avira hat sich zum Ziel gesetzt, dass seine Kunden „frei leben" können – ohne Spyware, Phishing, Viren oder sonstige Bedrohungen aus dem Internet.

Das Unternehmen wurde vor 25 Jahren von Tjark Auerbach unter dem Motto „Ich entwickle Software, die Gutes für meine Freunde und Familie tut" gegründet. Mehr als 100 Millionen Kunden und kleine Unternehmen setzen heutzutage auf die Sicherheitserfahrung von Avira und dessen preisgekrönter Virenschutzsoftware. Damit ist das Unternehmen die weltweite Nummer zwei nach Marktanteil. Avira bietet IT-Sicherheitslösungen für Computer, Smartphones, Server und Netzwerke – in Form von Software und cloudbasierten Diensten.

Neben dem Schutz der Online-Welt setzt sich der Geschäftsführer von Avira auch für die Offline-Welt ein. Die Auerbach Stiftung unterstützt gemeinnützige und soziale Projekte. Die Stiftung möchte mit ihrer Hilfe die Menschen in die Lage versetzen, sich selbst zu helfen.

Avira GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang | Germany
Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de