Avira Protection Cloud – Sandboxing und Machine Learning der LANCOM R&S®Unified Firewalls

Malware und Viren gehören zu den größten Bedrohungen für die Netzwerksicherheit. Für deren effektive Abwehr können Virensignaturen genutzt werden. Diese Signaturen sind vergleichbar mit einer eindeutigen, digitalen Unterschrift, welche für die Identifizierung von Schadsoftware und -dateien gescannt wird. Da immer neue Viren in den Umlauf gebracht oder weiterentwickelt werden, müssen auch die Signaturen fortlaufend angepasst werden. Um den Schutz vor Malware und Viren auch vor einer täglichen Aktualisierung der Signaturen auf dem Gerät aufrechtzuerhalten, arbeitet LANCOM mit Avira zusammen und setzt die Avira Protection Cloud ein. In diesem Infopaper erfahren Sie mehr über den Ablauf zur Identifzierung schädlicher Dateien mit der Avira Protection Cloud.

Schutz vor noch nicht bekannten Bedrohungen

Um vor Cyber-Angriffen auf bisher unbekannte Schwachstellen („Zero-Day-Exploits“) zu schützen, werden in den LANCOM R&S®Unified Firewalls Maschinelles Lernen und Sandboxing verwendet. Diese Testumgebung befindet sich in einer geschützten in Deutschland gehosteten Cloud, die mit Hilfe von maschinellem Lernen der dritten Generation zuverlässig analysiert, scannt, testet und bei Bedarf Dateien blockiert.

Das Betriebssystem der LANCOM R&S®Unified Firewalls arbeitet dafür seit LCOS FX 10.2 mit dem erweiterten Schutz der Avira Protection Cloud (APC) zusammen, bei der pro-aktiv verdächtige Dateien angefragt werden. Die kontinuierlich wachsende Datenbank der Avira Protection Cloud wird täglich mit tausenden neuen Virusstämmen gespeist und fortlaufend aktualisiert. Durch die heuristische Erkennung und direkte Abwehr potentieller Gefahren bietet sie umfassenden Schutz vor Bedrohungen.

Arbeitsweise der Avira Protection Cloud

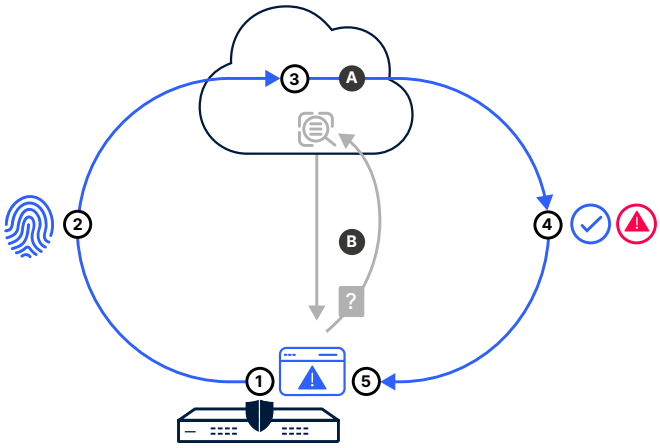

Abbildung 1:
Prozess zur Identifizierung schädlicher Dateien in der Avira Protection Cloud

1. Neue, unbekannte Dateien werden zunächst basierend auf den tagesaktuellen Signaturen bekannter Viren der lokalen Avira Engine gescannt und geprüft. Die Datei kann nach der lokalen Prüfung entweder als unverdächtig, auf Grund ihrer Signatur als infiziert oder als „verdächtig und unbekannt“ eingestuft werden.
2. Wird die Datei als „verdächtig und unbekannt“ eingestuft, wird eine Art Fingerabdruck der Datei extrahiert. Dies geschieht durch die Bildung eines Hash-Wertes zur Komprimierung und Anonymisierung der Informationen.
3. Der Fingerabdruck wird an die Avira Protection Cloud übermittelt und dort mit allen in der Cloud bekannten Fingerabdrücken verglichen. Somit wird die zeitliche Lücke zwischen täglichen Signatur-Updates und neuen Viren geschlossen. Die Prüfung kann wieder drei mögliche Ergebnisse hervorbringen:
   a) Der Fingerabdruck gehört zu einer bekannten, ungefährlichen Datei oder zu einer bekannten Malware, die bereits von der Avira Protection Cloud analysiert wurden.
   b) Der Fingerabdruck ist weiterhin neu für die Avira Protection Cloud. Daraufhin wird die vollständige Datei in die Cloud hochgeladen und da in einer Sandbox in Echtzeit analysiert und als neue Datei „erlernt“.
4. Die Avira Protection Cloud greift für die Bewertung des Fingerabdrucks als gefährlich oder ungefährlich auf die bereits vorliegende Einstufung zurück oder klassifiziert die Datei aus Basis von Machine Learning-Algorithmen neu ein.
5. Der Status des Fingerabdrucks (gefährlich oder ungefährlich) wird an die LANCOM R&S®Unified Firewall zurückgemeldet, die das weitere Vorgehen verwaltet.

Über Avira

Seit über drei Jahrzehnten ist das deutsche Unternehmen Avira (seit 2020 Teil von NortonLifeLock) führend in der Entwicklung von Anti-Malware-Technologien für Unternehmen jeder Größenordnung als auch für Privatanwender. Die Technologien werden in den Sicherheitslösungen vieler weltweit führender Unternehmen für Netzwerksicherheit eingebettet.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Germany
info@lancom.de
www.lancom-systems.de