Immer wieder werde ich gefragt was bei einem Sicherheitsprogramm „Heuristische Analyse" bedeutet.

Ich habe anschließend eine relativ einfach Beschreibung bei *Kaspersky* gefunden.

Als die Anzahl der Viren einige Hundert überschritten hat, haben unsere Spezialisten eine Möglichkeit zum Auffinden schädlicher Programme entwickelt, die das Antiviren-Programm noch nicht erkennt, da sie in den Antiviren-Datenbanken noch nicht enthalten sind.

Die Lösung hierfür ist die so genannte heuristische Analyse, die den Code von ausführbaren Dateien analysiert, um darin verschiedene Arten schädlicher Programme zu entdecken, die mithilfe der Antiviren-Datenbanken nicht gefunden werden können.

Die heuristische Analyse dient also der Suche nach unbekannten Viren. Bei der Überprüfung eines Programms emuliert die Analyse seine Ausführung und protokolliert alle „verdächtigen" Aktionen, wie z. B. Öffnen oder Schreiben in eine Datei, das Abfangen von Interrupt Vektoren usw. Anhand dieses Protokolls fällt die Entscheidung, ob das Programm mit einem Virus befallen ist.

So können mithilfe der heuristischen Code-Analyse bis zu 92% der neuen Viren entdeckt werden.
Diese Methode ist sehr effizient und führt nur äußerst selten zu Fehlalarmen. Die Dateien, in denen die heuristische Analyse den Verdacht auf einen Virus festgestellt hat, sind *möglicherweise infiziert* oder *verdächtig*.