

Die neue geographische Positionsbestimmung im StoneGate Management Center zeigt den Ursprung von Netzwerkattacken an. Damit bietet Stonesoft Firmen und Organisationen noch besseren Schutz für ihre Netzwerküberwachung: Dank der neuen StoneGate-Funktion "Geolocation" können Netzwerkadministratoren den geographischen Ursprung von Netzwerkattacken und verdächtigem Datenverkehr ermitteln.

Die Geolocation-Funktion ruft dazu automatisch den geographischen Ursprung schädlicher Datenpakete aus der GeoIP-Datenbank ab, die im StoneGate Management Center integriert ist und bei Updates des zentralen Management-Centers aktualisiert wird. Zudem kann der Administrator die geographische Position von privaten Netzwerken und Adressbereichen angeben.

Die Einschätzung von anormalem oder merkwürdigem Datenverkehr kann in Verbindung mit der Geolocation-Funktion signifikant erleichtert werden. Der Verkehr in einem Netzwerk folgt in der Regel einem bestimmten Schema. Kommen dabei fragwürdige Datenpakete zudem aus einer fragwürdigen Region, lassen sie sich entsprechend einstufen und behandeln. Dadurch wird dem Administrator die Unterscheidung zwischen tatsächlichen Ereignissen (true positive) und Fehlalarmen (false positive) enorm erleichtert.

Die Universität Paderborn setzt das StoneGate IPS mit dem StoneGate Management Center inklusive Geolocation bereits für den Schutz ihrer Netzwerkumgebung ein: Für uns ist die StoneGate-Funktion Geolocation äußerst nützlich, wenn es darum geht, den Ursprung von verdächtigem Datenverkehr zu ermitteln. Auf Basis dieser Informationen können wir rasch entscheiden, ob eine verdächtige Verbindung auf die Blacklist gesetzt werden soll. Zudem lassen sich fälschlicherweise auf die Blacklist gesetzte Verbindungen oder unberechtigter Datenverkehr ganz einfach erkennen. Dadurch können wir schneller reagieren, die Sicherheit unseres Netzwerks erhöhen und Zeit sowie Kosten sparen", fasst Barbara Bajer, Leiterin der Netz- und Systemadministration an der Universität Paderborn, zusammen.