Meraki

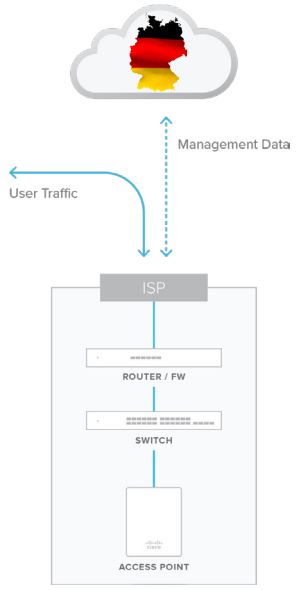
Die Cisco Meraki Cloud

Sicherheit und Datenschutz im Fokus

Überblick

Sicherheit, Datenschutz und Vertrauen wird bei Cisco Meraki großgeschrieben. Die Lösung von Meraki baut daher auf einer Out-of-Band Management Architektur auf. Damit fließen keinerlei Nutzerdaten je durch unsere Datacenter oder werden dort gespeichert. Die einzigen spezifischen Daten, die sich in den Meraki Datacenter befinden, sind die MAC-Adresse und der Name des Gerätes (z.B. Stefans iPhone), welches sich mit dem Cisco Meraki Netzwerk verbindet. Darüber hinaus fließen ausschließlich Management-Daten in die Meraki Datacenter - dies beinhaltet primär IP- und Netzwerkkonfigurationen. Die Lösung ist darüber hinaus in der Lage offenzulegen, welcher User welche Daten generieren. Diese Funktion lässt sich vom Kunden jedoch mit wenigen Klicks vollständig ein- oder ausschalten.

Alle Informationen zum Thema Sicherheit und Datenschutz:
meraki.cisco.com/trust



DATENSCHUTZ

Wird beim Anlegen der Organisation im Meraki Dashboard die Region EU-Geo-Cloud ausgewählt, sendet Meraki die eingangs genannten Management-Daten unter anderem in Datacentern in Deutschland - **Frankfurt** und **München**. Sie unterliegen damit auch den Vorgaben zur Verarbeitung personenbezogener Daten nach EU-Recht sowie den Vorgaben zur Auftragsdatenverarbeitung gemäß dem deutschen Bundesdatenschutzgesetz (BDSG).

Vertraglich festgehalten wird dies zwischen Cisco Meraki und dem Kunden in dem online abrufbaren Data Processing Addendum (DPA). Dieses kann auch direkt digital signiert werden:

Englisch (rechtskräftig) | Deutsch (zum Verständnis)

Die europäischen Vorgaben zum Datenschutz halten darüber hinaus fest, welche Sicherheitsmaßnahmen von Cisco Meraki ergriffen werden müssen. Diese sind damit ebenfalls Bestandteil des DPA und können unter diesem Link eingesehen werden.

Das DPA enthaelt zudem EU-Standardvertragsklauseln (Attachment 1 des DPA), an welche die Meraki LLC international (auch in den USA) gebunden ist. Diese regeln, wie Daten außerhalb der EU zu behandeln sind. Dies ist etwa bei einem Supportfall, der außerhalb der EU betreut wird, von Relevanz. Das Attachment 1 stellt damit sicher, dass Ihren Daten international der gleiche Schutz gleichkommt wie innerhalb der EU.

Cisco Meraki ist neu auch unter dem EU-US-Datenschutzschild, welches den Schutz personenbezogener Daten, die aus einem Mitgliedsstaat der Europäischen Union in die USA übertragen werden, regelt. Details hierzu finden Sie unter www.privacyshield.gov, wenn Sie nach „Cisco Systems“ suchen.

DATENSICHERHEIT

Cisco Meraki legt höchsten Wert auf die Auswahl unserer Datacenter. Insbesondere die Sicherheitsstandards und die eingehaltenen Normen sind von größter Wichtigkeit. So verlangen unsere oben genannten Sicherheitsmaßnahmen unter anderem, dass:

> *“(...) datacenters are certified by industry-recognized standards including ISO 9001:2008, ISO 27001, PCI DSS, SSAE16, and ISAE 3402 (SAS70) including Type II. (...)“*

Alle kritischen Elemente wie etwa SSID- und Admin-Passwörter (Zwei-Faktor-Authentifizierung) oder PSK-Informationen werden gesondert verschlüsselt gespeichert.