Meraki

Sicherheit + Cloud = Cisco Meraki

Cisco Meraki ist Branchenführer für Cloud managed IT. Mit nur einer zentralen Management-Platform, dem Meraki Dashboard, lassen sich Meraki Wireless Access Points (MR), Switches (MS), Security Devices (MX), Mobile Device Management (MDM) und Überwachungskameras (MV) überblicken und mit wenigen Klicks konfigurieren, installieren, steuern und managen. Dies erleichtert und verbessert das IT-Tagesgeschäft um ein Vielfaches. Für Cisco Meraki ist bei der Cloud aber vor allem auch eines wichtig: Sicherheit.

8 WICHTIGE FRAGEN & ANTWORTEN ZUR SICHERHEIT DER MERAKI CLOUD:

1. Kann ich über die Verwendung der Cloud benutzerspezifische Daten einsehen?

NEIN! Netzwerkverwaltungsdaten werden von den Benutzerdaten getrennt. Verwaltungsdaten werden von den Meraki-Geräten über eine sichere Internetverbindung und TLS Verschlüsselung zur Meraki-Cloud übertragen. Die Benutzerdaten werden nicht zur Cloud, sondern direkt zum Ziel im LAN oder über das WAN übertragen. Sensible Daten (z. B. Kennwörter) werden immer nur verschlüsselt gespeichert.

2. Was geschieht, wenn die Verbindung des Netzwerks mit dem Meraki Cloud Controller unterbrochen wird?

Meraki's Betriebszeit liegt bei **99.99%** nach dem Service-Level-Agreement (SLA). Im unwahrscheinlichen Fall eines WAN-Ausfalls läuft das LAN weiter und:

- Benutzer können auf das lokale Netzwerk (Drucker, Dateifreigaben usw.) zugreifen.
- Netzwerkrichtlinien (Firewall-Regeln, QoS usw.) werden weiterhin angewandt.
- Wireless-Benutzer können Roaming zwischen Access-Points nutzen.
- Lokale Konfigurations-Tools stehen zur Verfügung (z. B. Geräte-IP-Konfiguration).

3. Wo befinden sich die Rechenzentren von Meraki

Die Rechenzentren von Meraki stehen auf **europäischem Boden** in München, Frankfurt und Dublin mit Zertifizierung nach der Prüfnorm SAS 70 Typ II.

4. Ist die Cloud PCI konform?

JA! Die Meraki Cloud ist zertifiziert für **PCI DSS Level 1**.

5. Ist die Meraki Cloud legal?

JA! Die Meraki Cloud erfüllt folgende rechtliche Rahmenbedingungen:

- EU Directive 95/46/EC
- Deutsches Bundesdatenschutzgesetz
- EU Gesetz: Artikel 29, Working Party Opinion of July 1, 2012

6. Gehe ich durch die Nutzung der Cloud oder das Einrichten von Gäste-WLAN ein Risiko ein?

Mit Security Funktionen, wie z.B. Traffic Shaping/Firewall Rules lassen sich unerwünschte Seiten ganz schnell blockieren. Sodurch haben Sie **Kontrolle über Ihr Netzwerk** und wissen wie und wofür es genutzt wird. Bei Angriffen oder unzulässiger Nutzung Dritter werden Sie alarmiert, sodass Sie sowohl reaktiv als auch proaktiv reagieren können. Service Anbieter mit Meraki Services können außerdem Gäste-WiFi für Sie einrichten und dafür die Haftung übernehmen.

7. Haben Dritte Zugang zu meinen Daten durch die Cloud?

NEIN! Administratoren können die Sichtbarkeit von Meraki's Support Team blockieren. Der Dashboard-Zugang kann auf bestimmte IP-Adressen beschränkt werden. Anmeldungen erfolgen durch SAML und Zwei-Faktor Authentifizierung.

8. Ermöglicht mir das Mobile Device Management (MDM) das Ausspionieren von Personen?

NEIN! MDM dient dem Management von mobilen Endgeräten. Nur ein Minimum von Personendaten geht in die Cloud, z.B. MAC Adressen. Alle Daten sind verschlüsselt. Der Zugang zum Dashboard kann außerdem auf eine geringe Anzahl an IT-Administratoren beschränkt werden.

Jetzt für einen Monat alle Produkte **kostenlos testen!**
Mehr Infos unter **https://meraki.cisco.com/de**