Vertrauen

Sicherheit, Zuverlässigkeit und Datenschutz bei den Cloud-Services von Cisco Meraki

Überblick

- SLA mit 99,99 % Zuverlässigkeit
- Zwei-Faktor-Authentifizierung
- Redundante Hochverfügbarkeitsarchitektur
- Datenzentren mit Zertifizierung nach der Prüfnorm SAS 70 Typ II

Cisco Meraki betreibt den größten Cloud-basierten Netzwerkservice in der Branche. Der Cloud-Service von Meraki bildet die Grundlage für mehr als 18.000 Netzwerke auf der ganzen Welt. Zudem verfügt Meraki über die größte Erfahrung im Cloud Computing und bietet seine Dienste durchgehend seit fünf Jahren an. Tausende von IT-Profis in Unternehmen, Krankenhäusern, Banken und im Einzelhandel vertrauen auf die Cloud-basierte Netzwerkplattform von Meraki.

In diesem Dokument sind alle relevanten Informationen zur Sicherheit, zum Datenschutz und zur Zuverlässigkeit im Zusammenhang mit den Cloud-gehosteten Services von Meraki zusammengefasst. Hier finden Sie Informationen zu folgenden Themen:

- Datenzentren, Sicherheitsprozesse und Zertifizierungen
- Schutz Ihrer Daten
- Best Practices zur Verbesserung der Sicherheit Ihres Netzwerks
- Fortsetzung der Meraki-Netzwerkservices, wenn keine Verbindung mit der Cloud besteht
- Informationen, Tools und Best Practices zur PCI-Compliance
- Service Level Agreement von Meraki mit 99,99 % Verfügbarkeit

Aufbau der Meraki-Datenzentren

Der Cloud-Service von Meraki stützt sich auf Tier-1-Datenzentren, die nach SAS 70 Typ II zertifiziert sind. Diese Datenzentren bieten physische Sicherheit und Cyber-Sicherheit nach dem neuesten Stand der Technik sowie äußerste Zuverlässigkeit. Alle Meraki-Services werden über mehrere unabhängige Datenzentren repliziert, sodass bei einem Ausfall eines Datenzentrums ein schneller Failover der kundenbezogenen Services möglich ist.

Überwachung der Verfügbarkeit

- Service Level Agreement mit 99,99 % Verfügbarkeit (weniger als eine Stunde Ausfallzeit pro Jahr)
- Automatisierte Fehlererkennung rund um die Uhr – alle Server werden im Abstand von fünf Minuten von mehreren Standorten aus überprüft
- Schnelle Eskalationsverfahren über mehrere Einsatzteams
- Unabhängiges Ausfallwarnsystem mit dreifacher Redundanz

Redundanz

- Fünf geografisch verteilte Datenzentren
- Replikation aller Kundendaten (Netzwerkkonfiguration und Nutzungsdaten) über drei unabhängige Datenzentren
- Echtzeitreplikation von Daten zwischen Datenzentren (innerhalb von 60 Sekunden)
- Nächtliche Archivierungssicherungen

Disaster Recovery

- Schneller Failover zu Hotspare bei Hardwareausfall oder Naturkatastrophe
- Out-of-Band-Architektur gewährleistet Endbenutzer-Netzwerkfunktionalität, selbst wenn die Verbindung mit den Cloud-Services von Meraki unterbrochen ist
- Wöchentliche Optimierung der Failover-Verfahren

Cloud-Services-Sicherheit

- Automatisierte Angriffserkennung rund um die Uhr
- Schutz durch IP-Adressen- und Port-basierte Firewalls
- Einschränkung des Fernzugriffs anhand der IP-Adresse und Verifizierung durch öffentlichen Schlüssel (RSA)
- Kein Systemzugriff durch Kennworteingabe
- Automatische Benachrichtigung der Administratoren von Konfigurationsänderungen

Out-of-Band-Architektur

- Nur die Netzwerkkonfiguration und Nutzungsstatistiken werden in der Cloud gespeichert
- Endbenutzerdaten durchlaufen nicht das Datenzentrum
- Verschlüsselte Speicherung aller sensiblen Daten (z. B. Kennwörter)

Physische Sicherheit

- Kontrolle des Zutritts durch hochsichere Schlüsselkartensysteme und biometrische Lesegeräte
- Videoüberwachung aller Eingänge, Ausgänge und Schränke
- Überwachung des gesamten Verkehrs an der Einfahrt der Datenzentren durch Sicherheitspersonal rund um die Uhr, um sicherzustellen, dass die Zugangsprozesse eingehalten werden

Notfallvorsorge

- Brandschutz in den Datenzentren durch hochmoderne Sprinkleranlagen mit Sperrvorrichtungen, die das Einleiten von Löschwasser bei Fehlauslösungen verhindern
- Notstromversorgung über Dieselgeneratoren bei Ausfall der Netzstromversorgung
- USV-Systeme zur Kompensation von Spannungseinbrüchen und Spannungsspitzen sowie zum koordinierten Herunterfahren bei vollständigem Stromausfall
- Versorgung jedes Datenzentrums durch mindestens zwei Top-Tier-Unternehmen
- Seismische Isolierung der Doppelböden, Schränke und Trägersysteme durch Aussteifung
- Bei Ausfall eines Datenzentrums Failover der Services zu einem Datenzentrum an einem anderen Standort

Steuerung der Umgebungsbedingungen

- Regelung der Temperatur und Luftfeuchtigkeit durch überdimensionierte Klimaanlagen
- Luftumwälzung durch eigens vorgesehene Fußbodensysteme

Regelmäßige Penetrationstests

- Tägliche Penetrationstests in allen Meraki-Datenzentren durch unabhängige Dritte

Zertifizierung der Datenzentren

- Zertifizierung aller Meraki-Datenzentren nach SAS 70 Typ II

Out-of-Band-Steuerungsebene

Die Out-of-Band-Steuerungsebene von Meraki trennt die Netzwerkverwaltungsdaten von den Benutzerdaten. Die Verwaltungsdaten (z. B. Konfiguration, Statistiken und Überwachungsdaten) werden von den Meraki-Geräten (Wireless Access Points und Router) über eine sichere Internetverbindung zur Meraki-Cloud übertragen. Die Benutzerdaten (Webbrowsing, interne Anwendungen usw.) werden nicht zur Cloud, sondern direkt zum Ziel im LAN oder über das WAN übertragen.

Eine Out-of-Band-Steuerungsebene bietet folgende Vorteile:

Skalierbarkeit

- Unbegrenzter Durchsatz: keine zentralisierten Controller als Engstellen
- Anbindung neuer Geräte und Standorte ohne MPLS-Tunnel

Zuverlässigkeit

- Hohe Verfügbarkeit durch redundante Cloud-Services
- Aufrechterhaltung der Netzwerkfunktionen, selbst wenn die Verwaltungsdaten nicht übertragen werden können

Sicherheit

- Keine Übertragung von Benutzerdaten durch die Meraki-Datenzentren
- Vollständig HIPAA-/PCI-konform

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

Aufgrund der Out-of-Band-Architektur von Meraki sind die meisten Endbenutzer nicht betroffen, wenn die Wireless Access Points und Router nicht mit den Meraki-Cloud-Services kommunizieren können (z. B. wegen eines vorübergehenden WAN-Problems):

- Die Benutzer können weiterhin auf das lokale Netzwerk (Drucker, Dateifreigaben usw.) zugreifen.
- Wenn eine WAN-Verbindung besteht, können die Benutzer auf das Internet zugreifen.
- Die Netzwerkrichtlinien (Firewall-Regeln, QoS usw.) sind weiterhin in Kraft.
- Die Benutzer können sich über 802.1X/RADIUS authentifizieren.
- Per WLAN verbundene Benutzer können zwischen den Access Points wechseln.
- Die Benutzer können DHCP-Leases anfordern und erneuern.
- Eingerichtete VPN-Tunnel sind weiterhin funktionsfähig.
- Lokale Konfigurationsprogramme (z. B. für die IP-Adresse von Geräten) können verwendet werden.

Während die Meraki-Cloud nicht erreichbar ist, stehen die Verwaltungs- und Überwachungsfunktionen sowie die gehosteten Services vorübergehend nicht zur Verfügung:

- Die Konfigurations- und Diagnosetools sind nicht verfügbar.
- Die Nutzungsstatistiken werden bis zur Wiederherstellung der Verbindung mit der Cloud lokal gespeichert und dann zur Cloud übertragen.
- Splashseiten und damit in Verbindung stehende Funktionen sind nicht verfügbar.

Sicherheitstools und Best Practices für Administratoren

Meraki bietet neben der sicheren Out-of-Band-Architektur und den hochsicheren Datenzentren eine Reihe von Tools, mit denen Administratoren die Sicherheit ihrer Netzwerkimplementierungen maximieren können. Diese Tools bieten optimale Schutz-, Analyse- und Steuerungsmöglichkeiten für Ihr Meraki-Netzwerk. Auf dieser Seite finden Sie Informationen, wie Sie die Sicherheit Ihrer Konten bei meraki.com schnell und einfach erhöhen können. Zudem werden unsere empfohlenen Best Practices zu Kontensteuerung und Auditing beschrieben. Weitere Informationen finden Sie im Handbuch zum Meraki Cloud Controller.

Verwendung der Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung bildet im Netzwerk einer Organisation eine weitere Sicherheitsebene. Für die Anmeldung bei den Meraki-Cloud-Services muss zusätzlich zum Benutzernamen und zum Kennwort ein an das Telefon des Administrators gesendeter Code eingegeben werden. Bei der Implementierung der Zwei-Faktor-Authentifizierung von Meraki wird die sichere, bequeme und kostengünstige SMS-Technologie verwendet: Sobald ein Administrator seinen Benutzernamen und sein Kennwort eingegeben hat, wird ihm per SMS ein Einmal-Zugangscode gesendet, den er ebenfalls eingeben muss, damit die Authentifizierung abgeschlossen werden kann. Falls ein Hacker das Kennwort eines Administrators errät oder in Erfahrung bringt, kann er dennoch nicht auf das Konto der Organisation zugreifen, da er nicht im Besitz des Telefons des Administrators ist. Meraki bietet die Zwei-Faktor-Authentifizierung für alle Unternehmensbenutzer ohne zusätzliche Kosten an.

Verbesserung der Kennwortrichtlinien

Sie können unternehmensweite Sicherheitsrichtlinien für Ihre Meraki-Konten konfigurieren, um den Zugang zum Meraki-Dashboard besser zu schützen. Unter „Organization -> Configure“ (Organisation -> Konfigurieren) können Sie folgende Einstellungen vornehmen:

- regelmäßige Änderung des Kennworts verlangen (z. B. alle 90 Tage)
- minimale Kennwortlänge und -komplexität festlegen
- Benutzer nach mehrmaligen fehlgeschlagenen Anmeldeversuchen sperren
- Wiederverwendung von Kennwörtern unterbinden
- Anmeldungen auf Basis der IP-Adresse einschränken

Umsetzung des Prinzips der geringsten Rechte mit rollenbasierter Administration

Rollenbasierte Administration bedeutet, dass Sie Administratoren für bestimmte Teilbereiche Ihrer Organisation bestimmen und dabei festlegen, ob diese den Lesezugriff auf Berichte und Tools zur Fehlerbehebung erhalten, den Gastzugang über Meraki Lobby Ambassador verwalten können oder Änderungen an der Konfiguration des Netzwerks vornehmen dürfen. Die rollenbasierte Administration verringert das Risiko versehentlicher oder böswilliger Fehlkonfigurationen und beschränkt Fehler auf isolierte Teile des Netzwerks.

Aktivierung der E-Mail-Benachrichtigung bei Konfigurationsänderungen

Das Meraki-System kann automatisch E-Mail-Benachrichtigungen in natürlicher Sprache („Klartext“) senden, wenn Änderungen an der Netzwerkkonfiguration vorgenommen werden, damit die gesamte IT-Organisation über neue Richtlinien auf dem Laufenden bleibt. Änderungsbenachrichtigungen sind besonders in großen oder verteilten IT-Organisationen von Bedeutung.

Regelmäßige Überprüfung der Konfiguration und Anmeldungen

Meraki protokolliert die Uhrzeit, die IP-Adresse und den ungefähren Standort (Bundesland, Ort) der angemeldeten Administratoren. Außerdem bietet Meraki ein durchsuchbares Änderungsprotokoll, in dem verzeichnet ist, welche Änderungen an der Konfiguration vorgenommen wurden, wer sie durchgeführt hat und in welchem Teil der Organisation sie erfolgt sind. Durch die Überprüfung der Konfigurations- und Anmeldeinformationen erhalten Sie einen besseren Einblick in die Vorgänge in Ihrem Netzwerk.

Verifizierung von SSL-Zertifikaten

Auf die Meraki-Konten kann ausschließlich über https zugegriffen werden. Damit wird sichergestellt, dass die gesamte Kommunikation zwischen dem Browser eines Administrators und den Meraki-Cloud-Services verschlüsselt erfolgt. Wie bei allen sicheren Webservices sollten Sie sich auf keinen Fall anmelden, wenn im Browser Zertifikatwarnungen angezeigt werden, da dies auf einen Man-in-the-Middle-Angriff hindeuten kann.

Zeitüberschreitung

Den Benutzern wird 30 Sekunden vor der Abmeldung eine Meldung angezeigt, dass sie ihre Sitzung verlängern können. Nach Ablauf dieses Intervalls werden die Benutzer aufgefordert, sich erneut anzumelden.

PCI-Compliance

Meraki stellt eine umfassende Lösung bereit, um sicherzustellen, dass in einer PCI-konformen WLAN-Umgebung die strengen Standards von Level 1 der PCI-Sicherheitsprüfung (die strikteste Prüfungsstufe) eingehalten werden. Die umfangreichen Sicherheitsfunktionen von Meraki decken alle PCI-Datensicherheitsnormen ab und unterstützen die Kunden dabei, ein sicheres Netzwerk einzurichten und zu betreiben, die Daten der Karteninhaber zu schützen, ein Schwachstellenmanagement-Programm zu unterhalten, effektive Maßnahmen für die Zugriffskontrolle zu implementieren und die Netzwerksicherheit zu überwachen.

Die intelligente Meraki-Sicherheitsinfrastruktur eliminiert die bei einem herkömmlichen WLAN notwendigen komplexen Verwaltungsaufgaben, manuellen Tests und laufenden Wartungsmaßnahmen, die zu Sicherheitslücken führen. Die intuitiven und kostengünstigen Sicherheitsfunktionen von Meraki sind ideal für Netzwerkadministratoren geeignet, während die leistungsfähigen und differenzierten Administrationstools, die Kontoschutzfunktionen, die Überprüfungen und das Änderungsmanagement auf die Leiter der IT-Sicherheit zugeschnitten sind.

Meraki ermöglicht durch die zentrale Verwaltung aus der Cloud die einfache und kostengünstige Implementierung, Überwachung und Sicherstellung einer PCI-konformen WLAN-Umgebung über verteilte Netzwerke jeder Größe.

Service Level Agreement von Meraki

Während der Laufzeit der Lizenz für den Meraki Cloud Controller („Vertrag“) ist die Weboberfläche des Meraki Cloud Controllers in jedem Kalendermonat mindestens 99,9 % der Zeit funktionsfähig und für den Kunden verfügbar („Meraki-SLA“). Falls Meraki das Meraki-SLA nicht erfüllt und der Kunde seinen Verpflichtungen aus diesem Meraki-SLA nachgekommen ist, ist der Kunde zum Erhalt der unten beschriebenen Service-Gutschriften berechtigt. Die Regelungen in diesem Meraki-SLA stellen die einzigen und ausschließlichen Rechtsmittel des Kunden bei Nichterfüllung des Meraki-SLA durch Meraki dar.

Begriffsbestimmungen
Im Zusammenhang mit dem Meraki-SLA gelten die folgenden Begriffsbestimmungen.

Als „Ausfallzeit“ gilt eine Fehlerquote von mehr als fünf Prozent für den Benutzer. Die Ausfallzeit wird auf Basis der serverseitigen Fehlerquote gemessen.

Als „Meraki-Services“ wird der Meraki-Cloud-Controller-Service für jedes Meraki-Produkt bezeichnet.

„Monatliche Betriebszeit in Prozent“ ist die Gesamtzahl der Minuten in einem Kalendermonat minus der Anzahl der Minuten Ausfallzeit in diesem Kalendermonat, dividiert durch die Gesamtzahl der Minuten dieses Kalendermonats.

„Service-Gutschrift“ bedeutet, dass der Kunde nach dem Ende der Servicelaufzeit den Service an einer bestimmten Anzahl von Tagen kostenlos in Anspruch nehmen kann.

Service-Gutschrift muss vom Kunden angefordert werden:
Um eine der oben beschriebenen Service-Gutschriften zu erhalten, muss der Kunde Meraki innerhalb von dreißig Tagen nach dem Entstehen seines Anspruchs auf die Gutschrift benachrichtigen. Kommt der Kunde dieser Verpflichtung nicht nach, verfällt sein Anspruch auf die Service-Gutschrift.

Maximale Service-Gutschrift:
Die maximale Gesamtsumme der Service-Gutschriften, die einem Kunden von Meraki für alle in einem einzigen Kalendermonat auftretenden Ausfallzeiten gutgeschrieben wird, ist auf 15 zusätzliche Service-Tage am Ende der Service-Laufzeit des Kunden beschränkt, alternativ auf den Wert von 15 Service-Tagen in Form einer monetären Gutschrift auf das Konto eines Kunden mit monatlicher Zahlung. Service-Gutschriften können nicht in Geldbeträge umgetauscht oder umgerechnet werden.

Meraki-SLA – Ausschlüsse:
Das Meraki-SLA gilt nicht für Services, die dieses SLA ausdrücklich ausschließen (gemäß der Dokumentation dieser Services), oder bei Leistungsproblemen, die (i) durch „höhere Gewalt“ oder (ii) durch Geräte des Kunden oder von Drittanbietern bzw. von beiden (außerhalb der primären Kontrolle von Meraki) verursacht werden.