Fraunhofer
AISEC

FRAUNHOFER-INSTITUT FÜR
ANGEWANDTE UND INTEGRIERTE SICHERHEIT

ÜBER UNS

Das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC ist eine der international führenden Einrichtungen für angewandte Forschung im Bereich IT-Sicherheit. Mehr als 150 hochqualifizierte Mitarbeiterinnen und Mitarbeiter arbeiten an maßgeschneiderten Sicherheitskonzepten und Lösungen für Wirtschaftsunternehmen und den öffentlichen Sektor, mit dem Ziel, die Wettbewerbsfähigkeit von Kunden und Partnern zu verbessern. Dazu zählen Lösungen für eine höhere Datensicherheit sowie für einen wirksamen Schutz vor Cyberkriminalität wie Wirtschaftsspionage und Sabotageangriffe.
Das Kompetenzspektrum erstreckt sich von Embedded und Hardware Security, über Automotive und Mobile Security bis hin zu Sicherheitslösungen für Industrie und Automation. Zudem bietet Fraunhofer AISEC in seinen modernen Testlaboren die Möglichkeit zur Evaluation der Sicherheit von vernetzten und eingebetteten Systemen, von Hard- und Software-Produkten sowie von Web-basierten Diensten und Cloud-Angeboten.

Christian Banse
Head of Department
Service & Application Security

Fraunhofer AISEC
Lichtenbergstr. 11 | 85748 Garching b. München
clouditor@aisec.fraunhofer.de
www.aisec.fraunhofer.de

CLOUDITOR

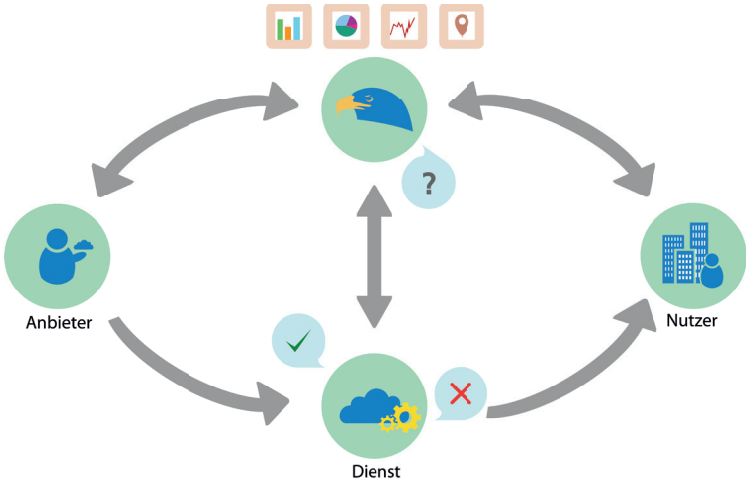
CONTINUOUS CLOUD ASSURANCE

Clouditor

Continuous Cloud Assurance

Die Cloud spart Anwendern Zeit und Geld. Einfach und schnell können mit heutigen Cloud-Diensten selbst komplexe Anwendungen realisiert werden - ein Weg, den viele innovative Unternehmen wählen, um so konkurrenzfähig und erfolgreich zu sein. Die erhoffte Ersparnis und Agilität birgt jedoch Herausforderungen. Die Kontrolle abstrakter Cloud-Ressourcen ist anspruchsvoll und vielschichtig. Oft lassen sich wichtige Fragen wie etwa *Ist meine Anwendung in der Cloud gegen Angriffe geschützt?* oder *Verhält sich ein Dienst wie per SLA zugesichert?* nicht eindeutig beantworten. Hier setzt der Clouditor an, ein Assurance-Werkzeug, das Ihre Cloud-Dienste automatisiert prüft und die Ergebnisse speichert und virtualisiert, um sie z. B. auf den nächsten Zertifizierungsaudit vorzubereiten.

Der Clouditor überprüft Anforderungen an Dienste und Anwendungen, insbesondere in der Cloud: Maßgeschneiderte Tests, die kontinuierlich ausgeführt werden, erlauben hohe Genauigkeit und präzise Aussagen. Die Ergebnisse sind unmittelbar nach Ausführung der Tests verfügbar, was eine prompte Reaktion auf entdeckte Abweichungen erlaubt. Somit bietet der Clouditor sowohl Anbietern als auch Nutzern von Cloud-Diensten einen Mehrwert.



Bieten Sie selbst Cloud-Dienste an?

Mit dem Clouditor können Sie kontinuierlich prüfen und nachweisen, dass Ihre Cloud-Dienste zugesagte Sicherheits- oder Compliance-Anforderungen, z.B. aus einem SLA, erfüllen. Dies schafft Sicherheit, Vertrauen sowie Transparenz, erhöht die Kundenbindung und minimiert Ihr Geschäftsrisiko. Der Clouditor lässt sich nahtlos in bestehende Geschäftsprozesse integrieren: Änderungen der existierenden Infrastruktur sind nicht notwendig.

Der Clouditor überprüft beispielsweise typische Anforderungen aus Sicherheitsrichtlinien, wie:

- Korrekte Konfiguration von Firewalls und Security Groups
- Sichere Verbindung, insbesondere korrekte TLS-Konfiguration
- Keine Verwendung von Software mit bekannten Schwachstellen
- Sicheres User- und Rollenmanagement in der Cloud
- Einhaltung der zugesicherten Verfügbarkeit eines Dienstes
- Geographische Lage eines Dienstes

Nutzen Sie Cloud-Dienste in Ihrem Unternehmen?

Mit dem Clouditor können Sie kontinuierlich überprüfen, ob die in Ihrem Unternehmen genutzten Cloud-Dienste Sicherheits- oder Compliance-Anforderungen erfüllen. Unabhängig vom verwendeten Servicemodell - SaaS, PaaS oder IaaS - schafft der Clouditor Transparenz und hilft auf diese Weise Geschäftsrisiken frühzeitig zu erkennen. Die Informationen des Clouditors ergänzen ISMS-Werkzeuge um anwendungsspezifische Sicherheitsinformationen.

So können Sie unter anderem die Erfüllung folgender Anforderungen mit dem Clouditor nachweisen:

- Einhaltung der Ihnen zugesicherten Verfügbarkeit eines Dienstes
- Geographische Lage eines Dienstes
- Erwartete Verhaltensweise eines Dienstes
- Verwendung einer Verbindungsverschlüsselung, z.B. TLS
- Keine Verwendung von Software mit bekannten Schwachstellen, z.B. in Web-Anwendungen und Linux-Systemen