



Continuous Cloud Assurance

Cloudditor



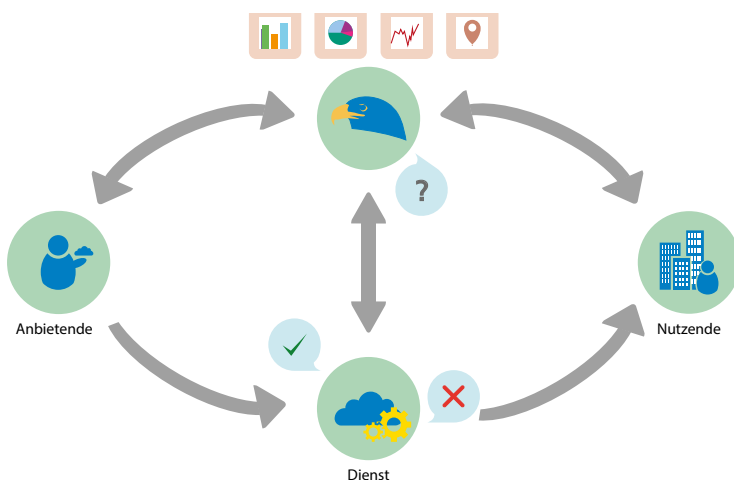
Die Nutzung einer Cloud spart Anwendenden Zeit und Geld. Einfach und schnell können mit modernen Cloud-Diensten selbst komplexe Anwendungen umgesetzt werden – ein Weg, den viele innovative Unternehmen wählen, um wettbewerbsfähig und erfolgreich zu bleiben.

Doch der Einsatz der Cloud erhöht gleichzeitig die Komplexität: Die Kontrolle über abstrakte Cloud-Ressourcen ist anspruchsvoll und vielschichtig, insbesondere kleine und mittelständische Unternehmen setzen deswegen häufig auf Compliance-Tools, um die Herausforderungen der Cloud zu meistern.

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 Cloudditor an, ein Assurance-Werkzeug, das Ihren Produkten und Anwendungen automatisiert kritische Fragen stellt und die Antworten darauf genau auswertet. Es führt automatisierte Prüfungen Ihrer Cloud-Dienste durch und speichert und virtualisiert die Ergebnisse, um sie beispielsweise für Zertifizierungsaudits aufzubereiten.

Maßgeschneiderte Tests für Cloud-Dienste

Der Cloudditor überprüft Anforderungen an Dienste und Anwendungen, insbesondere in der Cloud: Maßgeschneiderte Tests werden kontinuierlich durchgeführt. Dadurch werden präzise Aussagen mit hoher Genauigkeit ermöglicht. Die Ergebnisse stehen unmittelbar nach Abschluss der Tests zur Verfügung, was eine schnelle Reaktion auf detektierte Abweichungen ermöglicht. Somit bietet der Cloudditor einen Mehrwert sowohl für Anbietende als auch Nutzende von Cloud-Diensten.



Kontakt

Christian Banse

Head of »Service & Application Security«

cloudditor@aisec.fraunhofer.de

Fraunhofer AISEC

Lichtenbergstr. 11 | 85748 Garching b. München

www.aisec.fraunhofer.de



Sie bieten 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

Sie nutzen 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

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 200 hochqualifizierte Mitarbeitende entwickeln maßgeschneiderte Sicherheitskonzepte 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 das Fraunhofer AISEC in seinen modernen Testlabs die Möglichkeit zur Evaluation der Sicherheit von vernetzten und eingebetteten Systemen, von Hard- und Software-Produkten sowie von Web-basierten Diensten und Cloud-Angeboten.