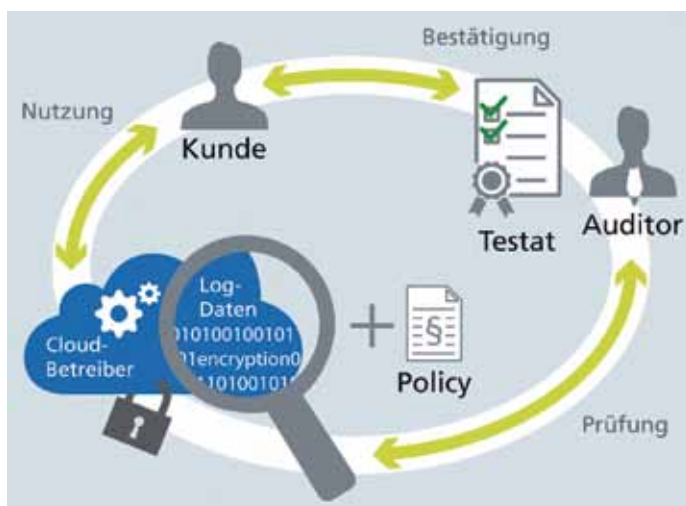




CLOUDCYCLE

CLOUDCYCLE COMPLIANT UND SICHER IN DIE CLOUD

Cloud Computing bietet Flexibilität und Kostenersparnis sowohl für Anbieter als auch Nutzer. Doch Unsicherheiten bei Datenschutz und IT-Sicherheit sowie die Befürchtung, von einem Cloud-Anbieter abhängig zu werden, lassen gerade mittelständische Unternehmen und Behörden vor dem Schritt in die Cloud zögern. CloudCycle schafft eine standardisierte Basis, mit der Cloud-Anbieter ihre Dienste bei garantierter Sicherheit und Compliance kosteneffizient und skalierbar für den öffentlichen Sektor und den Mittelstand bereitstellen können. Zudem können die Cloud-Anwender jederzeit automatisiert prüfen lassen, ob Datenschutzvorgaben eingehalten werden.



*Fraunhofer-Institut für Sichere
Informationstechnologie*

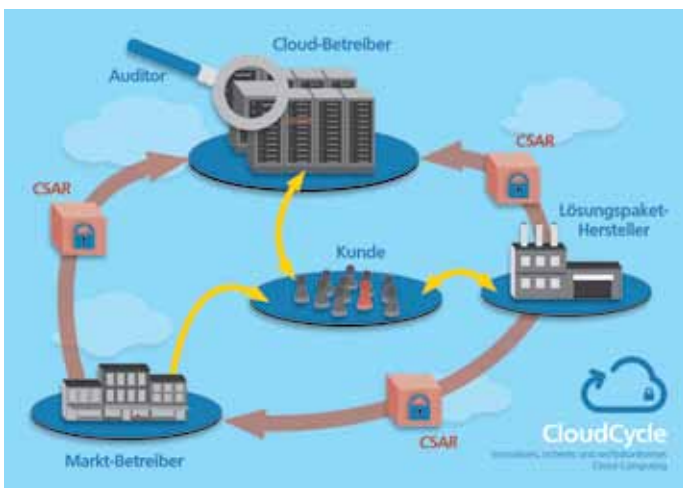
*Kontakt:
Oliver KÜch
Rheinstraße 75
64295 Darmstadt*

*Telefon 06151 869-213
Fax 06151 869-224
oliver.kuech@sit.fraunhofer.de
www.sit.fraunhofer.de*

Cloud-Dienste eröffnen kleineren und mittleren Unternehmen sowie Behörden und Bildungseinrichtungen einzigartige Möglichkeiten für flexible und vernetzte Zusammenarbeit. Anpassungsfähigkeit und Kostenersparnis, die zentralen Vorteile von Cloud Computing, erhöhen die Nachfrage nach cloudbasierten Dienstleistungen gerade in der öffentlichen Verwaltung und im Mittelstand. Gleichzeitig schrecken gerade diese potenziellen Anwender davor zurück, angesichts der hohen Anforderungen an Sicherheit und Compliance Dienste und Daten in die Cloud abzugeben. Auch die Sorge, bei der Nutzung von Cloud-Diensten die Kontrolle über die Verarbeitung datenschutzrechtlich sensibler und vertraulicher Daten zu verlieren und sich in die Abhängigkeit von einem bestimmten Anbieter (»Vendor Lock-In«) zu geben, zählen zu den wesentlichen Hindernissen. In dem vom BMWi im Rahmen von Trusted Cloud geförderten Projekt CloudCycle hat Fraunhofer SIT zusammen mit den Konsortialpartnern regio IT, der Universität Stuttgart, IBM und der kommunalen Informationsverarbeitung Baden-Franken Lösungen für standardisierte Cloud-Dienste entwickelt, sodass öffentliche Verwaltungen und der Mittelstand von den Vorteilen des Cloud Computing profitieren können, ohne Abstriche bei Sicherheit, Compliance oder Kontrolle machen zu müssen.

Cloud-Ökosystem

Im Gegensatz zu bestehenden Ansätzen sichert CloudCycle den gesamten Lebenszyklus eines Cloud-Dienstes ab: von der Erstellung über den Betrieb bis hin zur Löschung. Dafür schafft das Projekt ein eigenes Cloud-Ökosystem, das allen am Lebenszyklus eines Cloud-Dienstes Beteiligten (Anwender, Lösungsanbieter, Marktplatzbetreiber, Cloud-Betreiber, Auditor) eine gemeinsame,



standardisierte Basis bietet. CloudCycle standardisiert Formate und Schnittstellen der Cloud-Dienste im Zusammenspiel all dieser Akteure und gewährleistet damit Sicherheit und Rechtskonformität sowie Interoperabilität von Cloud-Diensten über den ganzen Lebenszyklus hinweg. Die Grundlage hierfür bildet TOSCA (Topology and Orchestration Specification for Cloud Applications), ein OASIS-Standard für die formale Beschreibung von Cloud-Diensten. Mit diesem Standard können Lösungshersteller und Cloud-Betreiber ihre Sicherheits- und Compliance-Garantien von Diensten und die damit verbundenen Anforderungen an die Laufzeitumgebung beschreiben.

Fraunhofer SIT hat hierfür einen Katalog aus rechtlichen und technischen Anforderungen zusammengetragen, die sich aus den einschlägigen Datenschutzgesetzen und Sicherheitsempfehlungen ergeben. Auf Grundlage dieses Anforderungskatalogs wurden exemplarische Sicherheits- und Compliance-Richtlinien formal beschrieben. Cloud-Betreiber können diesen Richtlinien schnell, kostengünstig und verbindlich entsprechen. Anwender können zwischen verschiedenen Softwareherstellern und Cloud-Betreibern wählen und bei einem Wechsel die Daten nahtlos und mit garantierter Sicherheit und Compliance weiter verwenden.

Automatisierte Datenschutz-Audits

Wenn öffentliche Einrichtungen oder Unternehmen Cloud-Dienste nutzen, liegt in der Regel eine Auftragsdatenverarbeitung nach §11 Bundesdatenschutzgesetz (BDSG) vor. Damit bleiben Cloud-

Nutzer für die Sicherheit und den Schutz der personenbezogenen Daten in der Cloud verantwortlich. Konsequenterweise besteht die gesetzliche Verpflichtung, den Cloud-Betreiber vor Beginn der Verarbeitung und währenddessen in regelmäßigen Abständen zu überprüfen. Der Anwender selbst kann regelmäßige Vor-Ort-Kontrollen beim Cloud-Betreiber in einer komplexen Cloud-Umgebung praktisch nicht leisten, da Daten und Anwendungen in der Regel über mehrere geographisch getrennte Standorte und auf verschiedene Cloud-Betreiber verteilt sind.

Fraunhofer SIT hat - aufbauend auf der Testatlösung der »AG Rechtsrahmen« des Technologieprogramms Trusted Cloud – ein Lösungskonzept für ein automatisiertes Testat entwickelt, sodass ein unabhängiger und akkreditierter Auditor im Auftrag des Kunden diese Datenschutzkontrollen anhand einheitlicher Prüfkriterien effizient durchführen kann. Der Kunde erhält die Ergebnisse dieser Prüfung in Form eines Testats. Durch die Automatisierung können Kontrollen jederzeit und ohne Notwendigkeit der umfangreichen Vor-Ort-Kontrollen durchgeführt werden. Das ermöglicht eine kontinuierliche Überwachung der Sicherheits- und Compliance-Vorgaben während des gesamten Lebenszyklus eines Cloud-Dienstes. Die Prüfkriterien, wie etwa Datensicherung, Verarbeitungsstandort oder die logische Mandantentrennung, werden in einer Richtlinie formal beschrieben und auf einer vertrauenswürdigen Informationsbasis automatisiert überprüft. Die entwickelte Testatlösung beruht auf manipulationssicheren Log-Dateien. Diese eignen sich sehr gut, da Log-Daten routinemäßig beim Cloud-Betreiber anfallen und den ganzen Lebenszyklus eines Cloud-Dienstes widerspiegeln.

Mehr Informationen unter

www.sit.fraunhofer.de/cloudcycle oder www.cloudcycle.org



Gefördert durch:



aufgrund eines Beschlusses des Deutschen Bundestages