Markt & Technik

Datum 11.12.2020 | Verbreitete Auflage 31.333
Seite 29-31 | Reichweite 172.573

Mit Continuous Security und Shared Responsibility zum Erfolg

Sicheres Cloud Computing heute

Weil immer mehr Unternehmen auf ein immer größeres Angebot von Cloud-Lösungen zurückgreifen, kommt es in zunehmendem Maße auf geeignete Cybersecurity-Lösungen an. Welche technischen Möglichkeiten gibt es dafür, und welche Zertifizierungsverfahren sind derzeit im Entstehen?

Von Christian Banse, Abteilungsleiter des Bereichs Service und Application Security am Fraunhofer AISEC und Leiter der Geschäftsstelle des Fraunhofer Cluster of Excellence Cognitive Internet Technologies (CCIT)

Das Cloud-Computing-Angebot wächst immer weiter, so dass auch der Bedarf an Sicherheitslösungen zunimmt, die speziell auf die Bedürfnisse von Cloud- und Container-Diensten zugeschnitten sind. Denn traditionelle Sicherheitslösungen sind den Herausforderungen in der Cloud oft nicht gewachsen, weil sie statisch und nicht dynamisch bzw. kontinuierlich arbeiten. So zwingt die Dynamik der Cloud – etwa die automatische Skalierung und flexible Provisionierung von Ressourcen – Unternehmen dazu, stets einen Überblick über die Sicherheit ihrer genutzten oder angebotenen Services zu behalten, um sicher vor Angriffen oder Datenabflüssen zu sein.

Das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC beschäftigt sich schon seit einigen Jahren mit den Konzepten der „Continuous Security", also der kontinuierlichen Sicherheit, und dem Modell der „Shared Responsibility". Als Shared Responsibility versteht man die Aufteilung des Verantwortungsbereichs zwischen Cloud-Provider und Cloud-Nutzer. In mehreren Forschungsprojekten wie NGCert und EU-SEC (https://www.sec-cert.eu) forschte das Institut an Lösungen und Technologien, die die Sicherheit in der Cloud kontinuierlich überprüfen, und veröffentlichte Open-Source Tools wie etwa den „Clouditor" (https://clouditor.io). Mittlerweile haben auch die größeren Public-Cloud-Provider wie AWS und Azure diese Herausforderungen aufgegriffen, und sie bieten Möglichkeiten, Gegenmaßnahmen zu ergreifen – die freilich oft mit zusätzlichen Kosten verbunden sind.

Shared Responsibility

Der Begriff der „Shared Responsibility", also der geteilten Verantwortung für die IT-Sicherheit, hat sich in den letzten Jahren immer weiter etabliert. Während der Begriff zunächst nur im akademischen Umfeld Verwendung fand, ist das Konzept mittlerweile ein fest verankerter Bestandteil der Absicherung von Cloud-Systemen. Weil die Benutzer von Cloud-Diensten Teile ihrer Infrastruktur auslagern, ergibt sich eine neue Aufteilung der Verantwortung für IT-Sicherheit und Datenschutz. In den Anfangszeiten des Cloud Computing waren die Unternehmen oft der Meinung, als Cloud-Nutzer sei man nicht mehr in der Verantwortung für die Sicherheit.

In der Praxis ergibt sich jedoch eine geteilte Verantwortung zwischen den involvierten Parteien. So ist der Cloud-Provider meist in der Pflicht, geeignete Sicherheitsmechanismen wie etwa die Verschlüsselung anzubieten. Die Nutzer sind jedoch weiterhin in der Verantwortung, Daten in ihrem Cloud-System sicher zu verarbeiten und zu speichern. Dies umfasst beispielsweise die Konfiguration und Aktivierung der vom Provider zur Verfügung gestellten Sicherheitsfunktionen.

Darüber hinaus zeigt sich in der Praxis, dass die Trennung zwischen Anbieter und Nutzer oft verschwimmt. So sind viele Provider mehr-

Fortsetzung...

wertiger Software-as-a-Service-Produkte oft selbst Nutzer von Infrastruktur-Diensten. Dies erschwert eine korrekte Umsetzung des Modells. Als Unterstützung finden sich daher auch in immer mehr Zertifizierungen und Sicherheitskatalogen Hinweise zur Umsetzung von Sicherheitsfunktionen in der Cloud (www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html). Speziell der Kriterienkatalog BSI C5 hat in seiner neuesten Version C5:2020 das Problem aufgegriffen und führt separate Controls und Maßnahmen auf, die Nutzer von Cloud-Diensten ergreifen sollten.

Generell befinden sich Zertifizierungen für Cloud Computing derzeit im Wandel. Schon seit mehreren Jahren deutet sich an, dass durch die Schnelllebigkeit des Cloud-Marktes bestehende traditionelle Zertifizierungen wie ISO 27001 an ihre Grenzen stoßen. Während es in früheren IT-Landschaften oft ausreichend war, eine Bestandsaufnahme durch einen Auditor in Jahresabständen durchführen zu lassen, zwingt die bewusste Dynamik von Cloud-Diensten die Provider und Auditoren zu neuen Modellen wie etwa einer kontinuierlichen Überwachung.

Aus diesem Grund hat die ENISA durch den EU Cyber Security Act (EUCA) den Auftrag bekommen, neue Zertifizierungen zu entwickeln und so die Zertifizierungslandschaft in Europa zu harmonisieren. Eine erste Ad-Hoc Working Group, bestehend aus Vertretern von Wirtschaft, Wissenschaft und Verwaltung, beschäftigt sich mit der Zertifizierung im Bereich Cloud-Sicherheit. Obwohl die Arbeiten noch nicht abgeschlossen sind, zeigt sich bereits, dass es in Zukunft drei bereits im EUCA verankerte Assurance-Levels geben wird: Basic, Substantial und High. Während für das Basic Level nur einfache Nachweise zu erbringen sind, ist davon auszugehen, dass das Level Substantial und besonders das Level High Audits oder sogar einen kontinuierlichen Nachweis erfordern.

Um dies zu realisieren, bedarf es meist eines Sets von Werkzeugen, die idealerweise die Nachweise in Form von technischen Evidenzen automatisch (und regelmäßig) erbringen. Hierbei gibt es zahlreiche Möglichkeiten der technischen Umsetzung, auf die im nächsten Abschnitt genauer eingegangen wird.

Ein derzeit aber noch ungelöstes Problem ist die automatische Prüfung organisatorischer Maßnahmen. Bestehende Werkzeuge konzentrieren sich oft auf die Einhaltung technischer Maßnahmen wie etwa Verschlüsselung oder Zugangskontrolle. Aber auch das Vorhandensein bestimmter Prozesse oder Dokumente ist sicherheitskritisch, etwa um rechtzeitig auf Sicherheitsvorfälle reagieren zu können. Im Rahmen des von der EU geförderten Projektes „MEDINA" forscht das Fraunhofer AISEC daher ab November 2020 mit anderen Partnern an Lösungen, um einerseits automatisch Evidenzen für die Effektivität der organisatorischen Maßnahmen zu sammeln und andererseits allgemein technische Evidenzen sicher und vertrauenswürdig im Kontext einer kontinuierlichen Zertifizierung zu verarbeiten und auszuwerten.

Technische Umsetzung von kontinuierlicher Sicherheit

Unabhängig davon, ob langfristig eine Zertifizierung angestrebt wird oder nicht, ist es für Cloud-Nutzer und besonders für Betreiber von Diensten dennoch ein Muss, sich mit dem Aspekt der kontinuierlichen Sicherheit zu beschäftigen und sie bestenfalls schon jetzt umzusetzen. Die Wissenschaft unterscheidet diesbezüglich mehrere Ansätze. Detektive Ansätze verfolgen das Ziel, Beweise zu sammeln, um zu garantieren, dass Sicherheitsanforderungen zum aktuellen Zeitpunkt eingehalten werden oder in der Vergangenheit wurden. Hierzu wird beispielsweise auf Informationen aus Log-Dateien zurückgegriffen oder direkt mittels APIs der aktuelle Zustand und die Konfiguration der Cloud-Umgebung angefragt. Neben diversen kommerziellen Tools haben sich auch Open-Source Tools wie „Clouditor" (https://github.com/clouditor/clouditor) zum Ziel gesetzt, die Konfigurations-Checks zu automatisieren und somit regelmäßig zu überprüfen, ob Anforderungen erfüllt werden. Aber auch die großen Cloud-Provider wie Azure und AWS bieten mittlerweile – teils kostenpflichtige – Lösungen an, um den Zustand der vom Kunden genutzten Cloud-Ressourcen zu überwachen.

Fortsetzung...

Darüber hinaus oder oft komplementär dazu genutzt verfolgen präventive Ansätze die Idee, Cloud-Ressourcen nur so zu nutzen oder zu konfigurieren, dass Anforderungen an die Sicherheit der Ressource von Anfang an eingehalten werden. Microsoft Azure bietet beispielsweise mittels „Azure Policy" die Möglichkeit, Einschränkungen für die Erstellung von Cloud-Ressourcen (etwa nur in einer bestimmten Region) festzulegen. Auch Policy-Enforcement-Systeme oder Service-Meshes wie „Istio" (https://istio.io) können helfen, Sicherheitsanforderungen wie etwa einen eingeschränkten Zugriff auf Daten präventiv einzuhalten. Weil diese Systeme ebenfalls Teil der Cloud sind und von einem begrenzten Personenkreis administriert werden, ist eine Kombination der beiden Ansätze sinnvoll.

Ausblick und GAIA-X

Die konkreten Auswirkungen des EU Cyber Security Act auf Unternehmen lassen sich derzeit nur schwer ableiten, besonders weil die Ad-Hoc Working Group zunächst einen ersten Draft der konkreten Zertifizierung vorlegen muss. Es ist zu erwarten, dass Unternehmen, die ihre IT-Produkte und -Dienstleistungen einer Zertifizierung unterziehen, einen Vertrauensvorschuss genießen – vor allem weil noch nicht absehbar ist, ob die Zertifizierung ähnlich wie die EU-DSGVO zu einer Pflicht gemacht wird, wenn IT-Dienste innerhalb der EU erbracht werden. Dies haben auch die Arbeitsgruppen rund um die europäische Cloud GAIA-X erkannt. Experten des Fraunhofer AISEC und anderer Partner diskutieren dort in der Arbeitsgruppe „Zertifizierung", wie Konzepte der kontinuierlichen Sicherheit innerhalb von GAIA-X genutzt werden können, um auch Cloud-Dienste zu implementieren, die sehr hohen Ansprüchen genügen müssen. Erste Ergebnisse der Spezifikationsphase werden im ersten Quartal 2021 erwartet. Daher gilt für Cloud-Nutzer und -Anbieter: Bereits jetzt handeln und schrittweise Methoden der kontinuierlichen Sicherheit in den Cloud-Systemen nutzen! (ak)

Christian Banse, Fraunhofer AISEC bzw. CCIT

Der Bedarf an Sicherheitslösungen, die speziell auf die Bedürfnisse von Cloud- und Container-Diensten zugeschnitten sind, nimmt zu.