Fachartikel

Neue Wege in der IT-Sicherheitszertifizierung von Cloud-Infrastrukturen

von Jürgen Großmann, Dorian Knoblauch, Fraunhofer FOKUS

Cloud Computing hat sich bei der flexiblen Bereitstellung von IT-Ressourcen inzwischen als das Mittel der Wahl etabliert. Die Cloud bietet eine Reihe von Vorteilen wie Flexibilität, Skalierbarkeit, Kosteneffizienz und Wartungsreduktion, die sich mit eigenen, internen Lösungen nur schwer realisieren lassen. Zugleich bedeutet Cloud Computing aber auch einen Paradigmenwechsel bezüglich der Kontrolle und Governance wichtiger Nutzungsaspekte wie beispielsweise der Informationssicherheit und dem Datenschutz, sodass gerade in diesen Bereichen Transparenz durch Zertifizierung und Auditierung stark an Bedeutung gewinnt. In diesem Artikel stellen wir mit dem Multi-Party-Recognition-Framework (MPRF) und dem Continuous Auditing based Security Certification Scheme (CACS) die beiden Hauptinnovationen des EU-SEC Projekts [1] vor, die zentrale Aufgaben der Sicherheits- und Datenschutzzertifizierung für die Cloud mit innovativen Ideen neu aufstellen.

Motivation

Da beim klassischen Cloud Computing zentrale IT-Infrastruktur nicht mehr durch die eigene IT-Abteilung umgesetzt wird, müssen kritische Aspekte wie IT-Sicherheit und Datenschutz durch normierte Prozesse und transparente Prüfverfahren nachgewiesen werden können. In den letzten Jahren haben sich eine Reihe von Zertifizierungs- und Auditierungsschemata etabliert, die es erlauben, IT-Sicherheit und Datenschutz in der Cloud durch unabhängige und vertrauenswürdige Dritte prüfen und belegen zu lassen. Hierzu zählen Anforderungskataloge wie ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 sowie die CSA Cloud Control Matrix. Hinzu kommen eine Reihe nationaler Regulierungen und Standards wie beispielsweise BSI C5 in Deutschland und SecNumCloud in Frankreich sowie Regulierungen auf europäischer Ebene wie beispielsweise die EU-DSGVO sowie das in der Entstehung befindliche ENISA Cloud Certification Schemes Metaframework [3]. Die notwendigen Auditierungs- und Zertifizierungsprozesse werden durch Prüfnormen wie ISO/IEC 27000 und ISAE 3000 definiert, die festlegen, welche Qualifikation von den Auditoren zu erwarten ist, welche Prüftiefe und Frequenz für Prüfungen vorgesehen werden müssen, wie Prüfergebnisse veröffentlicht werden usw. Für die Cloud Service Provider (CSPs) und Anwender besteht die Herausforderung nun darin, aus der Vielzahl der am Markt befindlichen Zertifizierungs- und Compliance-Programme diejenigen auszuwählen, die dafür geeignet sind, die eigenen Anforderungen bzw. die Anforderungen der potenziellen Kunden zu repräsentieren. Häufig sind CSP damit konfrontiert, dass sie nicht nur einem Zertifizierungsschema entsprechen müssen, sondern aufgrund ihres Engagements in verschiedenen Ländern und mit Kunden aus verschiedenen Anwendungsdomänen, eine Vielzahl unterschiedlicher Schemata bedienen müssen. Große CSPs wie Google, Microsoft, Amazon und Alibaba können es sich leisten, Zertifizierungen weltweit auszurollen und Zertifizierungskosten für die Durchführung und Pflege von Zertifizierungen entlang verschiedener Zertifizierungsschemata bereitzustellen. Für kleinere CSP stellt die Vielzahl am Markt befindlicher Zertifizierungsangebote und die damit einhergehende Notwendigkeit, diesen zu

entsprechen, ein ernstzunehmendes Investitionsrisiko und ein Hindernis für einen umfassenden Marktzugang dar.

Herausforderungen

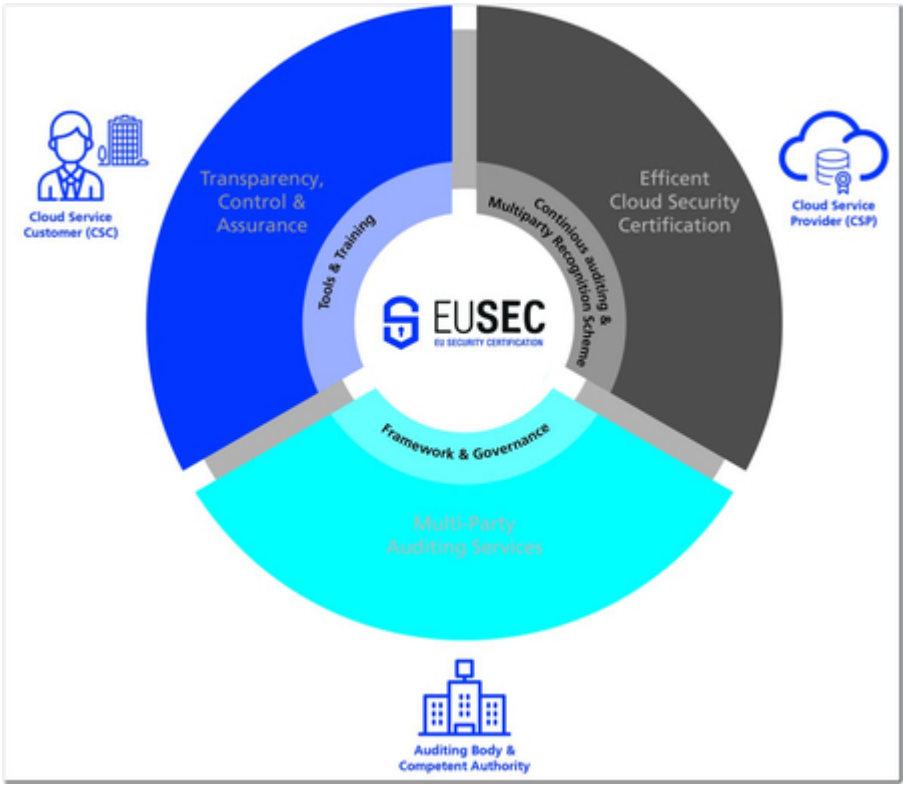


Abbildung 1: EU-SEC Stakeholder, Anforderungen und Ergebnisse

Das H2020-Projekt „European Security Certification Framework“ (EU-SEC) zielt darauf ab, ein europäisches Rahmenwerk für Zertifizierungs- und Auditierungsverfahren zu schaffen, mit dem sich IT-Sicherheit und Datenschutz in Cloud-Infrastrukturen auf Basis existierender internationaler Zertifizierungen sowie nationaler Richtlinien und Regelwerke nachhaltig belegen und flexibel an die Bedürfnisse der Nutzer anpassen lässt. In diesem Artikel stellen wir mit dem Multi-Party-Recognition-Framework (MPRF) und dem Continuous Auditing based Security Certification Scheme (CACS) die beiden Hauptinnovationen des EU-SEC Projekts vor. Das MPRF unterstützt die gegenseitige Anerkennung verschiedener nationaler, internationaler und branchenspezifischer Clo,0ud-Sicherheitszertifizierungen und unterstützt damit einen effizienten Zertifizierungsprozess auf Basis bereits bestehender Zertifikate und seiner Artefakte. CACS hingegen erlaubt die Prüfung von Sicherheitseigenschaften mit einer Häufigkeit, die mit bisherigen Point-in-time-Zertifizierungen nicht zu erreichen sind und ist somit insbesondere für Dienste mit hohen Sicherheitsanforderungen und strengen regulatorischen Auflagen relevant. Beide Innovationen werden durch eine Governance-Struktur ergänzt, mit dem Ziel, durch die Definition von Prinzipien, Regeln und Prozessen für die Einführung, Verbreitung und Pflege des MPRF und des CACS Nutzervertrauen in geschaffene Infrastruktur zu schaffen. Abbildung 1 zeigt die Ergebnisse des EU-SEC Projekts im Kontext der wichtigsten Stakeholder einer Cloud-Sicherheitszertifizierung bestehend aus Cloud Service Customers (CSCs) mit ihren Anforderungen nach Sicherheit und Datenschutz sowie der zur Kontrolle notwendigen Transparenz und Absicherung, den CSPs mit dem Bedarf nach effizienter Cloud Security Zertifizierung sowie den Auditoren, die auf Basis des EU-SEC Frameworks eine effiziente Cloud Security Zertifizierung anbieten können.

Um den Anforderungen der EU-SEC Stakeholder umfassend zu genügen, realisieren wir im EU-SEC Projekt eine flexible und funktionale Architektur, die Werkzeuge und Hilfsmittel für Cloud Security Governance, Risikomanagement und Compliance Management bereitstellt. Sowohl das MPRF wie auch das CACS wurden und werden durch Pilotanwendungen, die von Partnern des öffentlichen und privaten Sektors durchgeführt werden, validiert, um die Effektivität, Effizienz und Marktreife belegen zu können und eine nachhaltige kommerzielle Nutzung über den Rahmen des EU-SEC Projekts hinaus vorzubereiten.

Multi Party Recognition

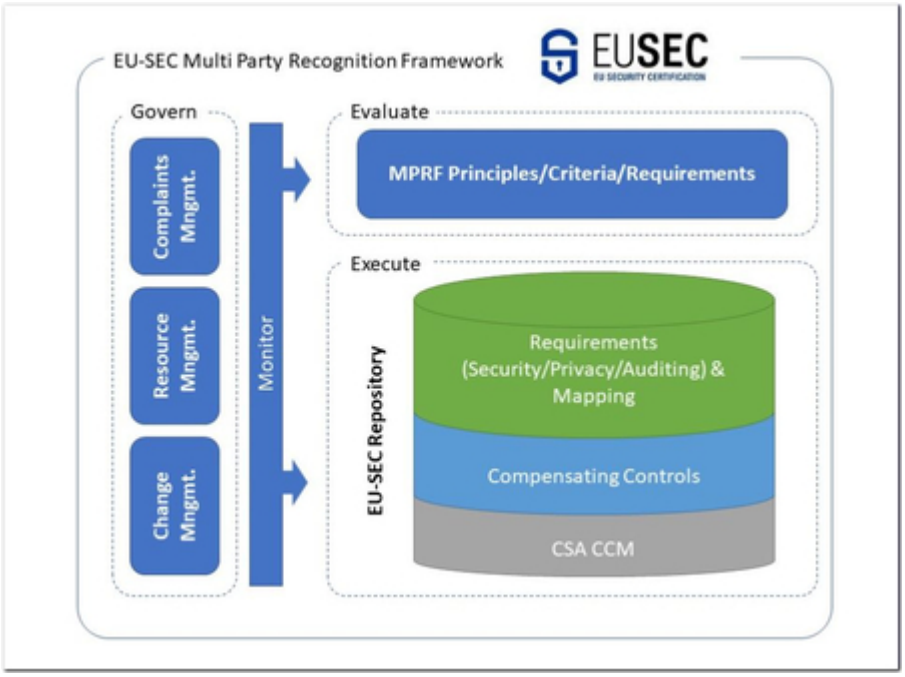


Abbildung 2: Multi Party Recognition Framework

Die Idee des EU-SEC MPRFs besteht darin, die grundlegenden Aufwände und Belastungen für einen CSP dadurch zu minimieren, dass der Aufwand für den Erhalt einer neuen Cloud-Sicherheitszertifizierung durch einen Rückgriff auf die Ergebnisse bereits existierender Cloud-Sicherheitszertifizierungen verringert wird. Ausgehend davon, dass zwischen vielen Zertifizierungsschemata große Ähnlichkeiten hinsichtlich der Sicherheitsanforderungen wie auch der Auditierungsanforderungen bestehen, haben wir diese Ähnlichkeiten systematisch erfasst und formalisiert, sodass diese sinnvoll im Rahmen eines Zertifizierungsprozesses genutzt werden können. Es geht also beim EU-SEC MPRF nicht darum, ein weiteres neues Zertifizierungssystem für die Cloud zu schaffen, sondern vielmehr darum, die Aufwände und Kosten für das Erlangen eines neuen Zertifikats durch die systematische Nutzung bestehender Zertifikate und der im Rahmen der Zertifizierung erstellten Artefakte deutlich zu senken.

Grundsätzlich lässt sich zwischen dem MPRF-Lebenszyklus und der Anwendung des MPRFs im Rahmen einer konkreten Zertifizierung unterscheiden. Der MPRF-Lebenszyklus beschreibt die Genese und die Pflege des MPRFs mit seinem zentralen Werkzeug, dem sog. EU-SEC Repository. Das EU-SEC Repository enthält alle notwendigen Formalisierungen, um Sicherheits-, Datenschutz- und Auditierungsanforderungen verschiedener Zertifizierungsschemata aufeinander abbilden zu können. Die Anwendung des MPRFs im Rahmen eines konkreten Audits oder einer konkreten Zertifizierung hingegen ist ein normaler Auditierungs- bzw. Zertifizierungsprozess, indem das EU-SEC Repository mit all seinen Anforderungen und Abbildungen verwendet wird, um die notwendigen Nachweise im Rahmen eines Audits oder einer Zertifizierung möglichst effizient zu erlangen.

Grundsätzlich durchlaufen alle technischen Inhalte des EU-SEC Repositories (d.h. die Sicherheitsanforderungen sowie die Abbildungsvorschriften, mit denen Anforderungen aus verschiedenen Zertifizie-rungsschemata miteinander in Beziehung gesetzt werden) den MPRF Lebenszyklus. Während der Evaluationsphase (Evaluate) wird ermittelt, ob sich ein Zertifizierungsschema für die Integration in das MPRF Framework eignet. Zu diesem Zweck haben wir im EU-SEC Projekt eine Reihe von Prinzipien, Eignungskriterien und Anforderungen für diese Form der Integration definiert. Zu den Prinzipien zählen Wiederholbarkeit, Äquivalenz, Relevanz und Vertrauenswürdigkeit der durch ein Schema realisierten Zertifizierungen. Zu den Eignungskriterien zählen die Vergleichbarkeit der Anforderungen, die Vergleichbarkeit der Auditierungsmechanismen, die Eignung und Übertragbarkeit der Nachweise, die Auditorenqualifizierung sowie das Governance-Modell. Für alle Kriterien wurden wiederum prüfbare Anforderungen definiert, mit denen sich ein konkretes Schema hinsichtlich der Kriterien evaluieren lässt. In der Ausführungsphase (Execution) werden alle relevanten Anforderungen in das EU-SEC Repository integriert. Zu diesem Zweck haben wir im Rahmen des EU-SEC Projekts eine Abbildungsmethode entwickelt, mit der sich die Anforderungen eines Zertifizierungsschemas mit den Anforderungen aus anderen Schemata in Beziehung setzen lässt. Die Governance Phase (Govern) ist dafür zuständig, die im EU-SEC Repository verwalteten Anforderungen zu warten und zu aktualisieren. Dies ist notwendig, um

das EU-SEC Repository auch nachhaltig aktuell zu halten, auf Änderungen einzelner Zertifizierungsschemata eingehen zu können und den Rücklauf beispielweise zur Validität der im EU-SEC Repository vorgenommenen Abbildungsvorschriften aus der Zertifizierungspraxis zu gewährleisten. Letzteres ist auch deshalb wichtig, da sowohl die Interpretation der Anforderungen wie auch ihre Überprüfung einen hohen subjektiven Anteil aufweisen.

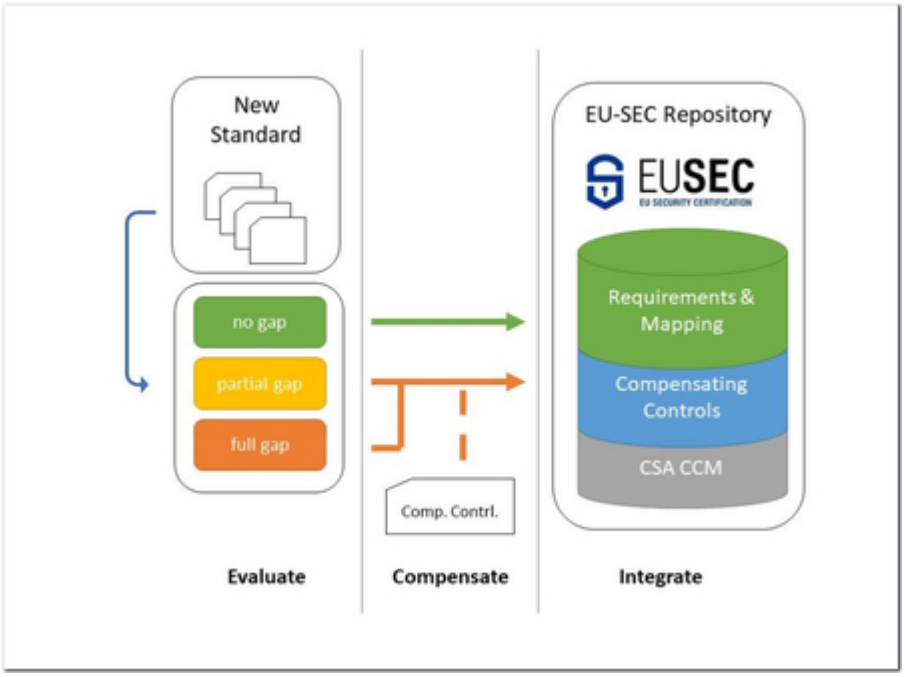


Abbildung 3: Gap-Analyse zur Integration neuer Standards und Schemata

Das EU-SEC Repository verwaltet die relevanten Sicherheits-, Datenschutz- und Auditierungsanforderungen der durch EU-SEC unterstützten Zertifizierungsschemata auf technischer Ebene. Während Datenschutzaspekte maßgeblich durch den EU-SEC Code of Conduct [5] adressiert werden, beinhaltet das EU-SEC Repository die konkrete Abbildung aller relevanten Sicherheitsanforderungen der unterstützten Zertifizierungsschemata auf die CSA CSM. Die CSA CSM fungiert in diesem Zusammenhang als eine Art Middleware, um die Sicherheitsanforderungen aus verschiedenen Standards bewerten und miteinander in Beziehung setzen zu können. Im Rahmen des EU-SEC Projekts ist eine initiale Version des EU-SEC Repositorys entstanden, das Anforderungen u.a. aus der ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, BSI C5, ANSSI SecNumCloud und aus nationalen Regulierungen der Slowakei und Slowenien enthält.

Für jede Sicherheitsanforderung wurde ermittelt, ob sich diese vollständig durch eine oder mehrere CSA CSM Controls darstellen lässt (Mapping Status: no gap), ob es eine Darstellungslücke gibt (Mapping Status: partial gap) oder ob eine Anforderung nicht durch die CSA CCM dargestellt werden kann (Mapping Status: full gap). Für alle Anforderungen mit Mapping Status full gap oder partial gap wurden sogenannte kompensierende Controls in das EU-SEC Repository integriert, sodass sich schlussendlich die Sicherheitsanforderungen aus allen integrierten Standards als Kombination von CCM Controls und kompensierenden Controls darstellen lassen. Die Abbildung der Auditierungsanforderungen erwies sich als problematischer, sodass sich derzeit ISO/IEC 27000 basierte und ISAE 3000 basierte Zertifizierungen nur sehr eingeschränkt aufeinander abbilden lassen.

Das MPRF und das EU-SEC Repository wurde im Rahmen von vier Fallstudien pilotiert und evaluiert, indem wir das MPRF und das EU-SEC Repository durch reale Auditoren im Rahmen einer simulierten Zertifizierung nach den Standards ISO/IEC 27017, ISO/IEC 27018 und BSI C5 angewandt haben. Die Pilotierung beinhaltet dabei all die Tätigkeiten, die auch eine echte Zertifizierung bzw. Auditierung durchlaufen hätte. Alle Fallstudien konnten erfolgreich abgeschlossen werden [5] und die Ergebnisse zeigen, dass das MPRF einen Reifegrad erreicht hat, mit dem sich Zertifizierung und Audits in einem industriellen Umfeld effizient unterstützen lassen.

Continuous Auditing Based Certification

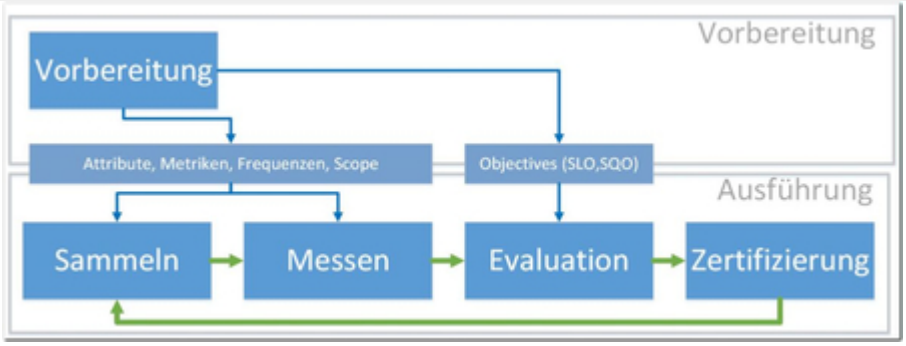


Abbildung 4: Phasen in der Referenzarchitektur

Moderne IT-Landschaften unterliegen einem ständigen Wandel. Insbesondere für kritische Anwendung ist ein solcher Wandel notwendig wie auch technisch und organisatorisch eine große Herausforderung. Neue Sicherheitsrisiken und eine sich kontinuierlich verändernde IT-Infrastruktur erfordern, dass technische und organisatorische Sicherheitsmaßnahmen immer wieder neu ausgerichtet und angepasst werden müssen. Doch wie spiegeln sich solche Anpassungsmaßnahmen in der Sicherheitszertifizierung wieder? In traditionellen Sicherheitszertifizierungen werden Sicherheitsmaßnahmen in der Regel alle zwei Jahre auditiert. Dies ist, berücksichtigt man eine sich stetig ändernde IT-Landschaft, gerade bei sicherheitskritischen Anwendungen zu wenig. Wenn zwischen den Audits Änderungen an der Sicherheitsimplementierung vorgenommen werden, dann werden diese Änderungen bis zur nächsten Prüfung nicht durch einen unabhängigen Auditor bewertet. Dies resultiert in der Unsicherheit für den Kunden, ob die durch das Zertifikat bestätigten Standards über die gesamte Gültigkeitsdauer des Zertifikats eingehalten werden. Je nach Schutzbedarf und branchenspezifischen Regularien stellt dies für bestimmte Kunden eine Hürde zur Migration in die Cloud dar. Daher hat das EU-SEC Projekt das Continuous Auditing based Certification Scheme (CACS) entwickelt. Die Grundidee dieses Ansatzes ist es, jede Sicherheitsmaßname mit einer adäquaten, dem Risiko angepassten Prüffrequenz zu versehen. Die Wirksamkeit jeder Sicherheitsmaßname wird dann gemäß der Prüffrequenz überprüft und die entsprechenden Prüfergebnisse werden veröffentlicht. Ziel ist es, durch Continuous Auditing die Frequenz aller angewendeten Security Controls auf ein Niveau anzuheben, welches möglichst in Echtzeit die Konformität einer Cloud-Infrastruktur gegenüber den Sicherheitsanforderungen wiedergibt. Um die Frequenz anzuheben und dabei gleichzeitig kosteneffizient zu sein, muss ein Großteil der Überprüfungen automatisiert ablaufen. Continuous Auditing Based Certification (CAC) ist, im Gegensatz zum traditionellen dokumentenbasierten Auditing, ein kontinuierlicher datenbasierter Prozess. Dies ermöglicht ein teilautomatisiertes Auditing.

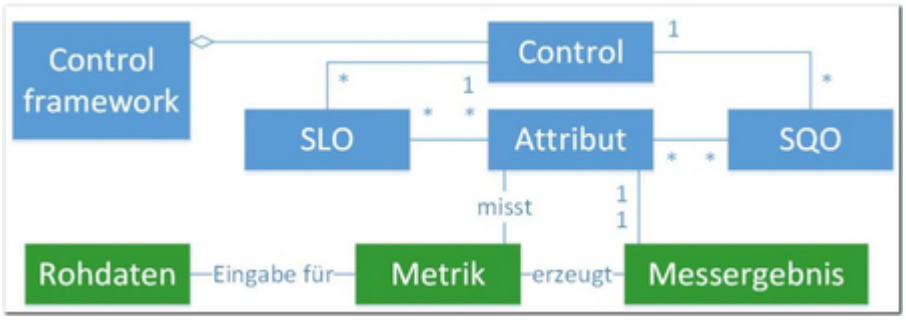
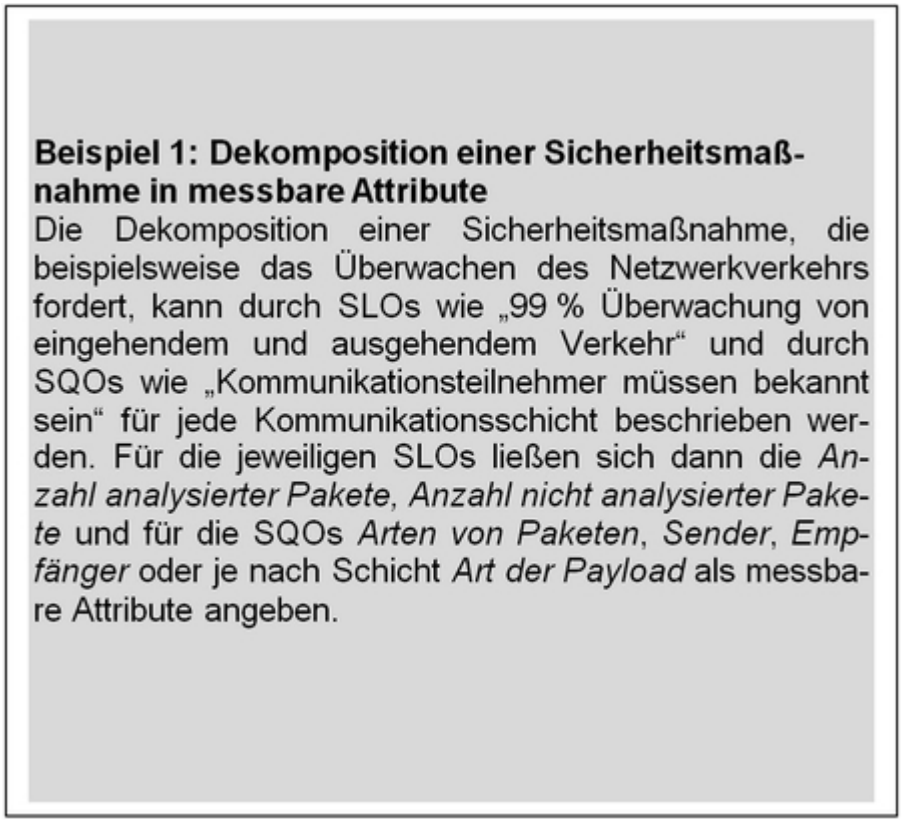


Abbildung 5: UML Diagramm der Operationalisierung

Entscheidend hierfür ist es, eine Architektur zu schaffen, welche die automatisierte als auch die händische Überprüfung gleichermaßen erlaubt, da zum gegenwärtigen Zeitpunkt sowie in naher Zukunft ein voll automatisiertes Ermitteln der Konformität nicht möglich ist. Zu diesem Zweck wurde im EU-SEC Projekt eine Referenzarchitektur entwickelt, mit der Zertifizierung kontinuierlich durchgeführt werden kann. Grundsätzlich lässt sich der CAC Prozess in eine Vorbereitungs- und eine Ausführungsphase unterteilen (siehe Abbildung 4). Erstere beinhaltet die Operationalisierung der Security Controls in messbare Attribute, die dann automatisiert gemessen werden können und so erst CAC ermöglichen. Die Vorbereitungsphase beginnt mit der Definition des Umfanges (Scope) der zu zertifizierenden Sicherheitsmaßnahmen. Anschließend folgt die Identifikation der Sicherheitsziele. Wir unterscheiden hier in sog. Service Level Objective (SLOs) und Service Qualitative Objective (SQOs). Jede Sicherheitsmaßnahme lässt sich durch ein oder mehrere SQOs oder SLOs beschreiben und für jedes SLO und SQO werden angemessene Prüffrequenzen definiert. Anschließend wird jedes SLO und SQO durch eine Menge messbarer Attribute beschrieben, die durch ihre Bestimmung entscheiden, ob das Sicherheitsziel erfüllt ist oder nicht. Attribute werden mit einem geeigneten Messverfahren ermittelt, wobei der Begriff Messung hier etwas breiter gefasst ist. So kann das Bewerten eines

Dokuments genauso eine Messung sein wie das Bestimmen einer konkreten Kennziffer. Abbildung 5 zeigt das Modell für die vollständige Dekomposition der Sicherheitsmaßnahmen bis hin zu den automatisiert messbaren Attributen. Grundlage für die Messungen sind immer die Rohdaten (Logs, Konfigurationen, Dokumente usw.). Sie werden im Messprozess bewertet und liefern ein Messergebnis, das einen Wert für das jeweilige Attribut darstellt. Das Beispiel 1 zeigt, wie sich die Forderung nach Überwachung des Netzwerkverkehrs in messbare Attribute darstellt.



Beispiel 1: Dekomposition einer Sicherheitsmaßnahme in messbare Attribute

Die Dekomposition einer Sicherheitsmaßnahme, die beispielsweise das Überwachen des Netzwerkverkehrs fordert, kann durch SLOs wie „99 % Überwachung von eingehendem und ausgehendem Verkehr“ und durch SQOs wie „Kommunikationsteilnehmer müssen bekannt sein“ für jede Kommunikationsschicht beschrieben werden. Für die jeweiligen SLOs ließen sich dann die *Anzahl analysierter Pakete*, *Anzahl nicht analysierter Pakete* und für die SQOs *Arten von Paketen*, *Sender*, *Empfänger* oder je nach Schicht *Art der Payload* als messbare Attribute angeben.

Die Vorbereitungsphase sollte, analog zu einem klassischem Audit, durch eine dritte Partei entweder unterstützt oder sogar ausgeführt werden. Letzten Endes wird die Qualität und Aussagekraft einer CAC in dieser Phase bestimmt. Die Vorbereitungsphase wird initial einmalig durchgeführt, wobei einzelne Schritte im Zuge einer Anpassung durchaus wiederholt werden können. In der Ausführungsphase wird ermittelt, ob das System konform zu den Sicherheitsanforderungen ist. Diese Phase wird in einem kontinuierlichen Zyklus ausgeführt und stellt somit das Äquivalent zu einem ständig ausgeführten traditionellen Audit dar. Ziel ist es, einen Prozess zu etablieren, der mit einem hohen Automatisierungsgrad durchgeführt werden kann. Die Ausführungsphase beginnt mit dem Sammeln der notwenigen Rohdaten für die Messung. Die eigentliche Messung findet in einem zweiten Schritt statt. In einem dritten Schritt wird geprüft, ob die jeweiligen Sicherheitsziele erfüllt sind. Dies geschieht durch die Auswertung der einzelnen Attribute. Letzten Endes wird anhand des Ergebnisses der Evaluation entweder ein Zertifikat ausgestellt, ausgesetzt oder entzogen.

Die Regeln für die Erteilung eines Zertifikates werden durch das Zertifizierungsschema bestimmt. Das Zertifizierungsschema baut auf standardisiertem Vergleich und Validierung auf. Jeder Cloud-Dienstanbieter hat, je nach Zielgruppe, verschiedene individuelle Sicherheitsanforderungen. Diese können unterschiedlich strikt sein, daher bietet das CACS mehrere Stufen der Zertifizierung an. Jede dieser aufsteigenden Stufen zeichnet sich durch einen jeweils höheren Grad an Zusicherung aus. Der höhere Grad der Zusicherung wird durch eine intensivere Einbindung einer dritten Partei erreicht.

Zusammenfassung und Ausblick

Das EU-SEC Projekt hat mit dem EU-SEC Framework eine Zertifizierungsinfrastruktur geschaffen, die es erlaubt, Sicherheitszertifizierungen für Cloud-Infrastrukturen auf eine neue Stufe zu stellen. Mit dem MPRF und CACS stehen Rahmenwerke zur Verfügung, die sowohl die Frage nach heterogenen Zertifizierungsanforderungen und dem Bedarf der Konformität zu nationalen Regulierungen wie auch die Frage nach Zertifizierungslösungen für besonders kritische Anwendungen effizient

beantworten. Das EU-SEC Projekt konzentriert sich aktuell darauf, das EU-SEC Framework für den kommerziellen Markt vorzubereiten. Zu diesem Zweck werden Informations- und Schulungsveranstaltungen durchgeführt, die jeweils zugeschnitten auf die Bedarfe der EU-SEC Stakeholder Informationen zur Nutzung des Frameworks bereitstellen. Darüber hinaus wird eine Governance Struktur etabliert, die eine längerfristige Verfügbarkeit und den Betrieb des EU-SEC Frameworks gewährleistet. Weiterführende Informationen hierzu finden sich auf der Website des EU-SEC Projekts www.sec-cert.eu). Das EU-SEC Projekt wurde aus Mitteln des HORIZON-Rahmenprogramms der Europäischen Union für Forschung, technologische Entwicklung und Demonstration im Rahmen der Fördervereinbarung Nr. 731845 finanziert.

Literatur & Links

1. EU-SEC Projekt: Forschungsprojekt im HORIZON-Rahmenprogramms der Europäischen Union, https://sec-cert.eu

2. Dr. M.A.C. Dekker, Dimitra Liveri: ENISA Cloud Certification Schemes Metaframework, https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework, 2014

3. CSPCERT: European Trusted Cloud Service Provider Working Group, https://cspcerteurope.blogspot.com/

4. CSA CCM: Cloud Control Matrix, https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview

5. EU-SEC: Privacy Code of Conduct, https://cdn0.scrvt.com/fokus/b46fac6d509ee426/724ab3e73ad4/8Privacy-Code-of-Conduct-Draft.pdf

6. EI-SEC Audit Reports (SI-MPA Audit Report, MF-SR Audit Report, SixSQ Audit Report, Fabasoft Audit Report) auf https://www.sec-cert.eu/eu-sec/project-outcome

---

Jürgen Großmann

ist Teamleiter am Fraunhofer Institut FOKUS und arbeitet als Experte für IT-Sicherheitsprüfungen im Bereich kritischer Anwendungen der Automobilindustrie und im Finanzsektor. Er ist aktuell Koordinator des H2020 Projekts EU-SEC.

E-Mail: juergen.grossmann(at)fokus.fraunhofer.de

Dorian Knoblauch

ist Wissenschaftlicher Mitarbeiter am Fraunhofer Institut FOKUS im Bereich IT-Security und automatisiertes Testen.

E-Mail: dorian.knoblauch(at)fokus.fraunhofer.de

Bildnachweise:

Abb. 1–5: EU-SEC Konsortium, Fraunhofer FOKUS