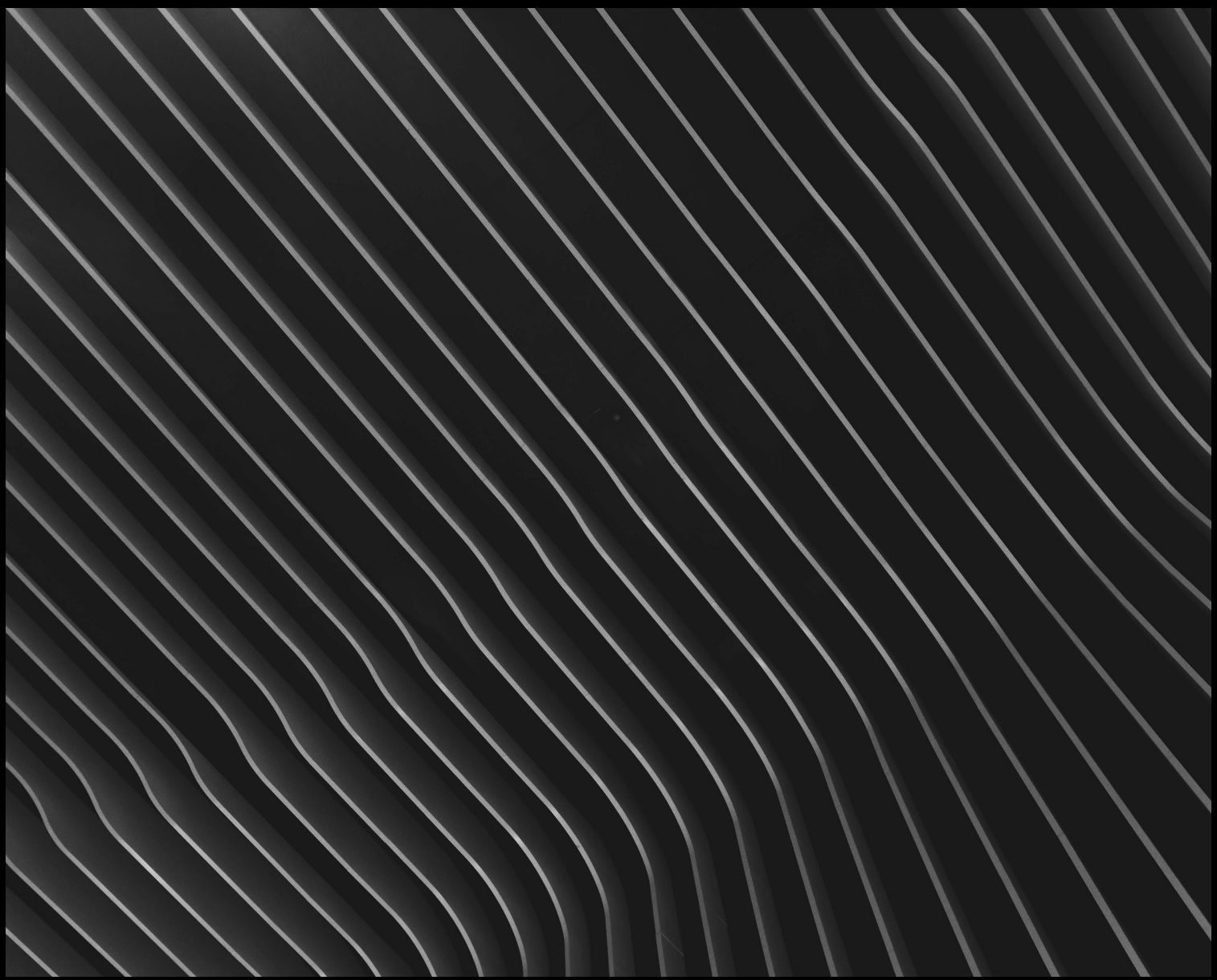
Cloud-Reallabor
Sichere Verarbeitung in der Cloud.

GovTech Campus Deutschland

Cloud-Reallabor: YEAR **ONE**

Erfahrungen nach einem Jahr Projektarbeit



„Die digitale Infrastruktur in Deutschland darf nicht von Wahlen in anderen Ländern oder anderen Ereignissen beeinflusst werden.“

Harald Joos
Projektleiter Cloud-Reallabor

Liebe Leserinnen und Leser,

trotz größerer Fortschritte steht die deutsche Verwaltung beim Thema „Cloud“ noch relativ am Anfang. Mehrere Cloud-Broker-Ausschreibungen wurden in diesem Jahr erfolgreich durchgeführt und auch die gemeinsame Ausschreibung der Sozialversicherungsträger wird voraussichtlich noch in diesem Jahr abgeschlossen. Bedarfsträger können damit Cloud-Dienste von deutschen und europäischen Anbietern und den US-Hyperscalern einfacher beziehen. Auch im Jahr 2024 ist der Cloud-Markt erneut stark gewachsen. Das bietet deutschen und europäischen Anbietern die Chance, größere Marktanteile zu gewinnen und lässt gleichzeitig ausreichend Raum für eine Koexistenz mit US-amerikanischen Angeboten.

Nachdem der Bezug von Cloud-Diensten vereinfacht wurde, rückt die praktische Umsetzung noch stärker in den Vordergrund. Wirtschaft und Verwaltung müssen ihre Kräfte bündeln, noch enger zusammenarbeiten, um gemeinsam zukunftsfähige Strukturen zu schaffen und die Herausforderungen von morgen zu meistern. Zeit zu verlieren ist keine Option – in der Verwaltung werden rund ein Drittel der Beschäftigten bis zum Ende dieses Jahrzehnts altersbedingt ausscheiden, bei gleichzeitig steigenden Anforderungen und Erwartungen.

Mit unserem Projekt „Cloud-Reallabor - Sichere Verarbeitung in der Cloud“ tragen wir mit dazu bei, die Potenziale der Cloud zu erschließen. Durch die enge Zusammenarbeit von öffentlichen und privaten Partnern sowie die Einbindung zentraler Stakeholder wie dem BSI und BfDI konnten Vorbehalte abgebaut und mehrere PoCs erfolgreich umgesetzt werden. Die Ergebnisse zeigen, dass Cloud-Dienste fallbezogen auch für die öffentliche Verwaltung sicher und flexibel nutzbar sind. Auch die Möglichkeit zwischen Cloud-Providern zu wechseln konnte nachgewiesen werden – allerdings besteht weiterhin der Bedarf nach mehr standardisierten Verfahren für den sicheren Ein- und Ausstieg in eine Cloud.

Ein unerwarteter Schwerpunkt im Projekt war der hohe Aufklärungsbedarf rund um das C5-Testat. Wir greifen das in unserem Projekt auf und werden den richtigen Umgang mit den Testaten ab sofort stärker in den Mittelpunkt stellen.

Abschließend möchte ich allen Beteiligten für ihre Unterstützung danken. Das Projekt läuft weiter und es bleibt noch viel zu tun.

Harald Joos
Projektleiter Cloud-Reallabor

Über dieses Dokument

Dieser Kurzbericht ist exklusiv für das erste Projekttreffen am 5. November 2024 auf dem GovTech Campus in Berlin erstellt worden und fasst die wichtigsten Ergebnisse nach einem Jahr Projektlaufzeit zusammen. Es werden Fortschritte in Sicherheitsfragen und Ergebnisse der Proof of Concepts (PoCs) zur flexiblen Cloud-Nutzung für den öffentlichen Sektor aufgezeigt. Ein Schwerpunkt liegt auf der Wechselfähigkeit zwischen Cloud-Lösungen und dem Bedarf an standardisierten Prozessen für einen sicheren Ein- und Ausstieg in die Cloud.

Für das Jahr 2025 plant das Projektteam den Fokus weiter auf die Entwicklung einer standardisierten Wechselstrategie zu legen, Maßnahmen zur weiteren Absicherung der Cloud-Nutzung zu vertiefen und neue PoCs aufzusetzen. Dank der engagierten Mitarbeit aller Beteiligten ist das Cloud-Reallabor gut aufgestellt, um weiter an praxistauglichen Lösungen für den öffentlichen Sektor zu arbeiten.

Warum ein Cloud-Reallabor?

Cloud ist kein „Allheilmittel". Die digitale Transformation macht Cloud-Dienste heute allerdings nahezu unverzichtbar. Sie bieten fallbezogene Lösungen für zentrale Herausforderungen der Digitalisierung: Skalierbarkeit, Kosteneffizienz, Innovation und Agilität. Der Fachkräftemangel im IT-Bereich verstärkt den Bedarf zusätzlich. Unternehmen und öffentliche Verwaltungen müssen mit knappen Personalressourcen nicht nur ihre Kernprozesse sicherstellen, sondern auch immer komplexere regulatorische Anforderungen erfüllen - eine Tatsache, die in starkem Umfang die öffentliche Verwaltung betrifft. Die eigene Fertigungstiefe muss laufend weiter überprüft werden, um den ständig steigenden Anforderungen erfolgreich zu begegnen.

Technische Lösungen sind vorhanden, die Herausforderung liegt darin, verstärkt die am Markt verfügbaren Lösungen zu nutzen und weniger Eigenentwicklungen zu verfolgen. Cloud-Dienste bieten ein hohes Maß an Informationssicherheit, sind schnell und flexibel skalierbar und ermöglichen einen schnelleren Einsatz innovativer Technologien, insbesondere der Künstlichen Intelligenz. So kann die Cloud als Katalysator wirken, zumal immer mehr Lösungen nur noch aus der Cloud und nicht mehr für den Betrieb „on premises" im eigenen Rechenzentrum verfügbar sind.

Der Mangel an IT-Fachkräften führt zugleich zu steigenden Betriebskosten und erschwert den effizienten internen Betrieb und die Wartung eigener IT-Systeme. Prognosen gehen davon aus, dass die öffentlichen Verwaltungen bis 2030 bis zu 30 Prozent ihres Personals verlieren könnten, was den Druck auf das IT-Personal laufend weiter erhöht. Cloud-Dienste können zur Entlastung beitragen, denn sie ermöglichen die Auslagerung von IT-Infrastruktur und -Management und erlauben es Unternehmen und öffentlichen Einrichtungen, sich stärker auf ihre Kernaufgaben zu konzentrieren, ohne durch den IT-Betrieb zu viele Ressourcen zu binden.

Und gleichzeitig nehmen geopolitische und wirtschaftliche Abhängigkeiten immer weiter zu. Die Bedeutung eines Angebots, in dem deutsche und europäische Anbieter fester Bestandteil sind, reduziert Abhängigkeiten und schafft Optionen, so dass wir auch in Zukunft handlungs- und steuerungsfähig sind und unsere Resilienz erhöhen können. Wir müssen alle Lösungen nutzen können, aber nicht nutzen müssen. Wir als Kunden müssen uns so aufstellen, dass die Möglichkeit, flexibel

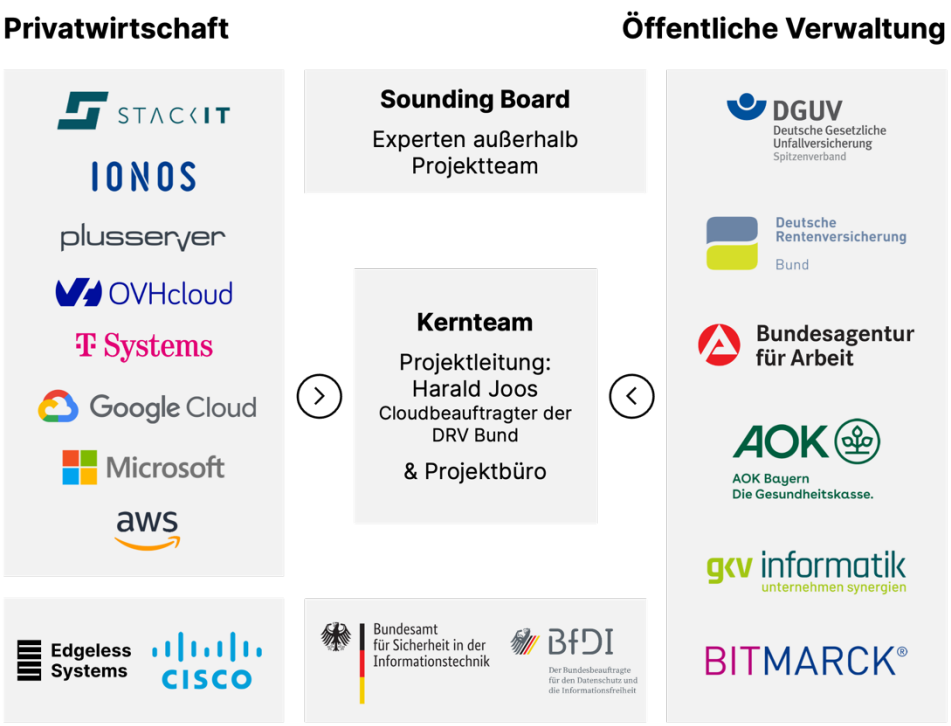
zwischen verschiedenen Cloud-Anbietern zu wechseln, besteht. Damit können wir uns flexibel an veränderte Rahmenbedingungen anpassen.

Neben der Technik bedarf es einer engen Zusammenarbeit aller Akteure innerhalb eines geschützten Rahmens. Hier setzt das Cloud-Reallabor an: Es bietet eine Plattform für die vernetzte Zusammenarbeit, auf der Wirtschaft und Verwaltung Lösungen entwickeln und umsetzen können - praxisnah, zielgerichtet, gemeinsam.

Ein Jahr Projekt - eine Momentaufnahme

Zu Projektbeginn stellten wir uns einige Fragen: Gelingt es uns, alle relevanten Akteure organisationsübergreifend an einen Tisch zu bringen, Barrieren aufzubrechen und gemeinsam etwas zu bewegen, ohne dass wir uns gegenseitig ausbremsen und langsamer werden? Ist es möglich auf die Gründung neuer Ausschüsse, Gremien zu verzichten? Wie schaffen wir es schneller voranzukommen? Und können wir den Einsatz von Cloud-Lösungen voranbringen, indem wir Berührungsängste abbauen und gemeinsam voran gehen?

Im Cloud-Reallabor arbeiten führende Cloud-Anbieter aus Deutschland, Europa und den USA mit Organisationen aus allen vier Zweigen der Sozialversicherung sowie dem BSI und BfDI zusammen. Gemeinsam entwickeln wir Blaupausen für eine sichere Verarbeitung in der Cloud. Das Projekt ist auf dem GovTech Campus in Berlin angesiedelt, sodass ein legitimierter Rahmen für einen transparenten und offenen Austausch geboten wird: Der Campus ist unser neutraler Ort für Innovation und Zusammenarbeit.



Projektmitglieder aus öffentlicher Verwaltung und Privatwirtschaft

Viele Ideen und Vorschläge waren neu und bewegten sich auf unbekanntem Terrain. Gleichzeitig wuchs das Interesse der Campusgemeinschaft, sich am Projekt zu beteiligen und gerne hätten wir mehr Mitglieder mit in unser Projekt aufgenommen. Wir mussten allerdings auch immer unsere Ressourcen im Blick behalten, konnten daher nicht zu stark in die Breite gehen, und mussten zunächst eine stabile Basis für die weitere Arbeit schaffen.

In 2024 wurden folgende Handlungsschwerpunkte verfolgt: (1) Projektkommunikation nach außen, (2) Vernetzung der Projektmitglieder, (3) Wechselfähigkeit zwischen Anbietern und (4) Erhöhung der Informationssicherheit.

(1) Projektkommunikation nach außen

Cloud-Lösungen sind bereits im Einsatz und ihre Nutzung nimmt stetig zu. Dennoch bestehen nach wie vor Unsicherheiten: Können bzw. *dürfen* diese Lösungen genutzt werden oder nicht? Ein Schwerpunkt des Projekts ist es, nicht nur über Risiken zu sprechen, sondern auch die Chancen herauszuarbeiten und zu zeigen, wo Cloud-Lösungen bereits erfolgreich eingesetzt werden. Dabei bleibt klar: Eine perfekte Lösung gibt es weder im eigenen Rechenzentrum noch in der Cloud - eine Eignung hängt immer vom konkreten Anwendungsfall ab.

FAQ-Dokument sowie weitere Veröffentlichungen sind über die offizielle Projektwebsite www.reallabor.cloud abrufbar.

Im Frühjahr hat das Projekt ein erstes FAQ-Dokument für Entscheider veröffentlicht, in dem die wichtigsten Fragen zu Chancen und Risiken der „Cloud“ beantwortet werden. Als Zielgruppe wurde hier bewusst die Leitungs- bzw. Entscheidungsebene adressiert. Warum? Die Frage zur Nutzung der Cloud wird nicht innerhalb der IT beantwortet, entscheidend ist ob und wie die Geschäftsziele damit schneller und besser erreicht werden können. Das FAQ-Dokument soll zur Versachlichung der Diskussion beitragen und eine Grundlage bieten, um über Chancen und Risiken zu diskutieren, um danach eine fundierte Entscheidung treffen zu können. So können Entscheider die strategische Bedeutung der Cloud für ihr Unternehmen faktenbasiert bewerten und einordnen.

(2) Vernetzung der Projektmitglieder

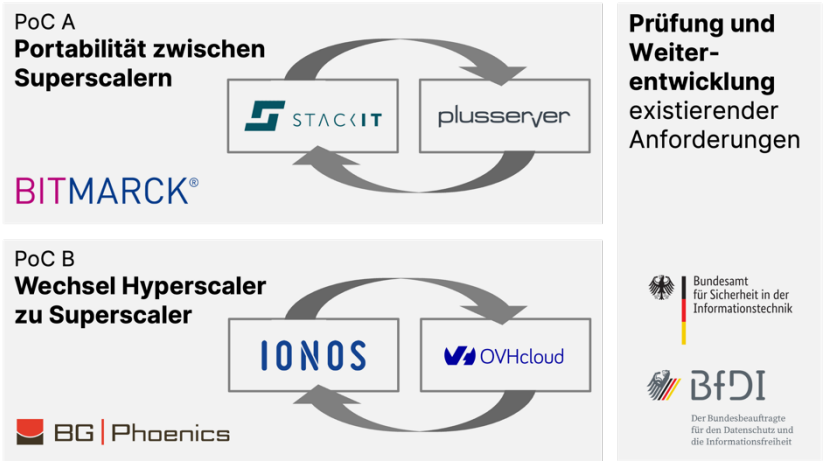
Ein weiteres Ziel war die Etablierung von PoCs für nationale, europäische und US-amerikanische Angebote in Zusammenarbeit mit öffentlich-rechtlichen Organisationen und insbesondere unter Beteiligung des BSI. Dadurch sollte Wissen ausgetauscht werden, um näher an den Fragestellungen der Praxis zu sein und diese direkt in die Weiterentwicklung betroffener Standards oder auch in die Weiterentwicklung des C5-Kriterienkatalogs einfließen zu lassen. Erste Erfolge konnten bereits erreicht werden, zudem laufen ausgewählte PoCs weiter. Ein Fokus bei den PoCs lag dabei auch auf der Nutzung von KI-Lösungen in Verbindung mit Cloud und Confidential Computing Lösungen.

(3) Wechselfähigkeit zwischen Anbietern

Im Rahmen des Projekts sollte der Nachweis erbracht werden, dass ein Wechsel zwischen Cloud-Anbietern technisch möglich ist und dadurch die Risiken eines zu starken Vendor-Lock-Ins reduziert werden können. Auch wollten wir herausfinden, wo die Hürden liegen und wie ein Wechsel zukünftig einfacher gestaltet werden kann. Der Fokus lag dabei zunächst auf deutschen und europäischen Anbietern, da das Projekt auch die Stärkung des europäischen Marktes im Fokus hat und deutsche, europäische Lösungen fester Bestandteil eines Multi-Cloud-Angebots und auch ein Aspekt in der Multi-Cloud-Strategie bei den Nutzern sein müssen. Hinzu kommt, dass die deutschen und europäischen Anbieter die Ergebnisse und Anforderungen des Projektes leichter und schneller aufgreifen können. Bei den multinationalen über Europa hinaus agierenden US-Hyperscalern sind die

direkten Einflussmöglichkeiten aufgrund der Rahmenbedingungen naturgemäß geringer als bei den deutschen und europäischen Anbietern.

Die Tests und Ergebnisse zeigten, dass ein Wechsel prinzipiell möglich ist, und lieferten wichtige Erkenntnisse in Bezug auf Flexibilität und Interoperabilität. Gleichzeitig wurde deutlich, dass ein reibungsloser Wechsel eine sorgfältige Planung im Vorfeld erfordert - insbesondere in Bezug auf einheitliche Sicherheitsstandards, Datenportabilität & Systemkompatibilität. Im Projekt haben wir diesen Aspekt unterschätzt. Die Vorab-Planung bietet hohes Potenzial für die Zukunft.



Zwei PoCs zur Weiterentwicklung der Standards

(4) Erhöhung der Informationssicherheit

Der C5-Kriterienkatalog ist ein zentraler Baustein für die Beurteilung eines Cloud-Dienstes. Von besonderer Bedeutung ist dabei u.a. die Verschlüsselung in allen Nutzungsphasen: Verschlüsselung der Daten bei der Speicherung („in rest“), bei der Übertragung („in transport“) und bei der Verarbeitung („in use“). Ein Schwerpunkt in einem unserer PoCs lag daher auf der Erprobung von Lösungen zur Verschlüsselung während der Verarbeitung, auch bekannt als „Confidential Computing“. Zugleich haben wir auch in anderen PoCs erkannt, dass es nicht ausreicht, nur zu wissen, „wie man wieder aus der Cloud herauskommt“, sondern dass es auch einer sorgfältigen Vorbereitung bedarf, „bevor man in die erste Cloud geht“. Dabei haben wir die Bedeutung und den richtigen Umgang mit dem C5-Kriterienkatalog und dem zugehörigen Testat als Nachweis für die Erfüllung der Kriterien als wichtiges Hilfsmittel zunächst unterschätzt.

Das C5-Testat steht am Anfang

Wer sich mit dem Einsatz von Cloud-Lösungen beschäftigt, stößt früher oder später auf den C5-Kriterienkatalog. Der „Cloud Computing Compliance Criteria Catalogue“ (C5) des BSI hat sich in Deutschland zu einem zentralen Werkzeug für die Beurteilung der Sicherheit von Cloud-Diensten entwickelt. Der Katalog definiert für jeden einzelnen Service die Anforderungen an die Informationssicherheit in der Cloud, weiter wird das C5-Testat als Nachweis in vielen Ausschreibungen als Mindestanforderung an die Anbieter bzw. deren Services gestellt.

In zahlreichen Cloud-Broker-Ausschreibungen wird ein C5-Testat als unabdingbare Voraussetzung gefordert. Dies betrifft alle Anbieter bzw. deren Services und gilt somit gleichermaßen für deutsche, europäische und US-amerikanische Cloud-Provider. Die Basiskriterien des C5-Kriterienkatalogs spiegeln aus Sicht des BSI das Niveau an Informationssicherheit wider, das ein Cloud-Dienst mindestens bieten muss, wenn Cloud-Kunden mit diesem Informationen mit normalem Schutzbedarf verarbeiten. Darüber hinaus bilden die Basiskriterien den Mindestumfang einer Prüfung (Testierung) nach diesem Kriterienkatalog ab. Für Cloud-Kunden, deren Informationen einen höheren Schutzbedarf

haben, können die Zusatzkriterien des C5-Kriterienkatalogs einen Ausgangs- bzw. Ansatzpunkt für die Bewertung des Cloud-Dienstes darstellen. Damit wird er zu einem wesentlichen Bestandteil bei der Auswahl und Nutzung von Cloud-Angeboten im öffentlichen Sektor. Auch im privaten Sektor werden der C5-Kriterienkatalog und das C5-Testat als Orientierungshilfe genutzt.

Häufiger wird das C5-Testat fälschlicherweise noch als „Zertifizierung" verstanden, und der Unterschied zwischen einem Zertifikat und einem Testat ist nicht allen bewusst. Ein Testat bestätigt, wie ein Anbieter definierte Anforderungen umgesetzt hat (Testat Typ 1 - zum zu prüfenden Zeitpunkt; Testat Typ 2 - Wirksamkeit während des zu prüfenden Zeitraums). Ein Zertifikat hingegen bescheinigt, dass ein bestimmter/definierter Standard erfüllt wird. Darüber hinaus besteht häufig die Erwartung, dass mit dem C5-Testat bereits viele Sicherheitsfragen geklärt sind und der Kunde sich weniger darum kümmern muss. Das Testat ersetzt jedoch nicht die Notwendigkeit einer individuellen Sicherheitsbetrachtung, da es die Verantwortung für den sicheren Einsatz und die Integration des Services in die eigene IT-Landschaft nicht abnimmt, sondern bei der Bewertung der Sicherheitseigenschaften des Services unterstützt, die mit dem Testat nachgewiesen werden. Ein umfassendes Sicherheitskonzept bleibt daher auch mit einem Testat unerlässlich.

In der konkreten Projektarbeit hat sich gezeigt, dass es zunächst gar nicht so einfach ist, diese Testate zu erhalten, da sie auch streng vertrauliche Interna der Anbieter beinhalten. Sie stehen deshalb oft unter einem Non Disclosure Agreement (NDA) und sind daher nicht ohne Weiteres zugänglich.

Nach Erhalt des C5-Testats liegt es in der Verantwortung des Kunden, jedes einzelne Kriterium und dessen Umsetzung für sich zu bewerten - allein die Basiskriterien umfassen aktuell 121 Punkte. Anhand dieser Kriterien kann der Kunde auch feststellen, welche Sicherheitsaspekte vom Cloud-Anbieter abgedeckt werden und für welche er selbst oder mitverantwortlich ist („Shared Responsibility"). Ein gründliches Verständnis der Verantwortlichkeiten und eine klare Abstimmung und enge Zusammenarbeit mit dem Anbieter sind unerlässlich, um eine sichere und bedarfsgerechte Cloud-Nutzung zu gewährleisten. Weitere wichtige Punkte sind unter anderem die Auswahl der Rechenzentren und deren Standorte für die Datenspeicherung, der erforderliche Verschlüsselungsgrad entsprechend des Schutzbedarfs der Daten (da der Cloud-Anbieter die Dateninhalte des Kunden nicht kennt), Netzanbindung, Backup-Strategie und notwendige Verfügbarkeit von Wiederherstellungskopien. Diese detaillierte Prüfung ist notwendig, da das Testat allein keine Auskunft darüber gibt, ob die spezifischen Sicherheitsmaßnahmen die individuellen Anforderungen des Kunden erfüllen - das kann nur der Kunde selbst. Dies bedeutet, dass die Prüfung von jedem Kunden für jeden Cloud-Anbieter bzw. Cloud-Dienst separat durchgeführt werden muss. Die Anforderungen der Kunden sind häufig identisch, doch es gibt bisher keine Empfehlungen, die speziell auf den Public Sector zugeschnitten sind. Diese Lücke wollen wir im nächsten Jahr im Cloud-Reallabor schließen.

Wir machen unser Projektwissen zugänglich!

Im Laufe des Projekts haben wir viele Erfahrungen und Erkenntnisse gesammelt - sowohl durch die PoC-Arbeiten als auch durch den intensiven Austausch mit Branchenvertretern, Experten unseres Sounding Boards und den vielen Mitgliedern des GovTech Campus, mit denen wir in einem laufenden Austausch stehen. Dieses Wissen wollen wir weiter sammeln und in angemessener Form zugänglich machen und so der Community zurückgeben. Auch hier müssen wir andere Wege gehen, statische Dokumente verlieren zu schnell an Aktualität. Statt dem ursprünglich angedachten Whitepaper oder weiteren Positionspapieren wollen wir sukzessive eine Wissensplattform aufbauen, um unsere Perspektiven zur sicheren Cloud-Nutzung, Blaupausen und Referenzmodelle für die öffentliche Verwaltung und kontinuierlich wachsende Inhalte aus der Community anzubieten.

Ausblick 2025: Es bleibt viel zu tun!

Nach dem Start in diesem Jahr und den gemachten Erfahrungen sind einige Handlungsschwerpunkte der nächsten Zeit bereits klar: Wir wollen (1) Wissen pragmatisch vermitteln, (2) Blaupausen entwickeln, (3) Ergebnisse nutzbar machen, um zur sicheren Cloud-Nutzung für die öffentliche Verwaltung beizutragen, sowie (4) die laufenden PoCs abschließen und neue PoCs starten.

(1) Wissen pragmatisch vermitteln

Ein erster direkter Einstieg ist den Umgang mit dem C5-Testat zu vermitteln. Das BSI hat zugesagt, eine erste Informationsveranstaltung zum korrekten Umgang mit dem C5-Testat für alle Projektmitglieder anzubieten. Eine entsprechende Einladung wird vom Projektteam zeitnah versandt. Auf Basis der Ergebnisse der Veranstaltung wird geprüft, ob und in welcher Form dieses Angebot weitergeführt oder ergänzt werden sollte, um einen optimalen Nutzen für alle Beteiligten zu gewährleisten.

(2) Blaupausen entwickeln

Begonnen haben wir mit dem „Wechsel-PoC“. Vor dem Wechsel ist allerdings ein sauberer Einstieg in eine Cloud und deren Services unentbehrlich. Diese Chance haben wir jetzt einmalig, da wir noch am Beginn der Cloud-Nutzung stehen. Aufbauend auf den Ergebnissen der C5-Testate wird das Projekt den strukturierten Einstieg in und die Nutzung von Cloud-Lösungen gezielt aus Sicht des öffentlichen Sektors untersuchen. Ein geordneter Weg in die Cloud ist notwendig, um sicherzustellen, dass Daten und Anwendungen nicht nur sicher in die Cloud integriert, sondern auch jederzeit kontrolliert und geordnet wieder herausgenommen werden können.

Ein zentrales Element dieses Vorgehens sind sogenannte „Landing Zones“. Dabei handelt es sich um eine sichere, vorkonfigurierte Cloud-Umgebung, die es ermöglicht, Cloud-Ressourcen effizient und sicher zu verwalten. Diese Landing Zone bildet eine Art „Basisschicht“ in der Cloud, auf die mehrere Nutzer, zugreifen können. Sie stellt sicher, dass alle grundlegenden Sicherheits- und Compliance-Anforderungen von Anfang an eingehalten werden und ermöglicht eine standardisierte und skalierbare Nutzung. Das geht allerdings nicht theoretisch. Im Projekt werden wir daher ausgehend von einer Behörde und einem konkreten Anwendungsfall in

Zusammenarbeit mit einem Cloud-Anbieter ein standardisiertes Verfahren entwickeln, das in einem nächsten Schritt auf weitere Cloud-Anbieter ausgeweitet werden kann. Auch für diesen Prozess suchen wir Organisationen und Unternehmen, die sich beteiligen möchten. Im Gegensatz zum letzten Jahr konnten wir diesmal bereits im Vorfeld eine Teilnehmerorganisation der öffentlichen Verwaltung gewinnen und auch das BSI ist wieder mit an Bord!

Und: Die US-amerikanischen Anbieter arbeiten bereits seit mehr als einem Jahrzehnt an Lösungen, die den Kunden die Nutzung ihrer Cloud und deren Services erleichtern. Hier gibt es eine dreistellige Anzahl von Lösungen, die genutzt werden können. Nicht alle diese Lösungen sind zwingend erforderlich, allerdings gibt es bei den deutschen und europäischen Cloud-Anbietern an dieser Stelle einen Nachholbedarf. Die Bereitschaft diese Lösungen zu erstellen ist bei allen Anbietern vorhanden und an den Lösungen wird bereits intensiv gearbeitet. Das Cloud-Reallabor kann bei der Prioritätensetzung unterstützen, damit die Lösungen, die den Kunden am meisten helfen, schneller zur Verfügung stehen.

(3) Ergebnisse nutzbar machen

Die Ergebnisse der PoCs werden weiterhin in geeigneter Form als praxisorientierte „Koch-Rezepte“ veröffentlicht, so dass möglichst viele Organisationen davon profitieren können - schließlich stehen alle vor ähnlichen Aufgaben und ein gemeinsames Vorgehen bringt uns allen einen Mehrwert.

(4) PoCs abschließen und neue starten

Neben den laufenden PoCs gibt es aus der Community zahlreiche Ideen für weitere PoCs, die wir in diesem Jahr nicht umsetzen konnten und perspektivisch aufgreifen wollen. Neben „Hype-Themen“ wie Künstliche Intelligenz sollten wir auch Grundlagenthemen wie verschlüsselte Backups und Desaster Recovery verstärkt in den Fokus nehmen. Die kontinuierliche Verbesserung des Sicherheitsniveaus unserer IT bleibt angesichts des stetig steigenden Digitalisierungsgrades und der sich verschärfenden Bedrohungslage eine der zentralen Herausforderungen und hier besteht nach wie vor Nachholbedarf. Eine Aufgabe, bei der uns Cloud-Lösungen unterstützen können.

Es bleibt viel zu tun, wir machen weiter und bauen weiter auf Eure Unterstützung!

Impressum

Herausgeber
GovTech Campus Deutschland e.V.
Max-Urich-Straße 3
13355 Berlin

Ansprechpartner
Harald Joos
Projektleiter Cloud-Reallabor &
Cloudbeauftragter der DRV Bund

Cloud-Reallabor
Sichere Verarbeitung in der Cloud.

Das Projekt „Cloud-Reallabor: Sichere Verarbeitung in der Cloud“ bringt öffentliche Verwaltung und Privatwirtschaft auf dem GovTech Campus zusammen, um Blaupausen für den sicheren Einsatz von Public- Cloud-Lösungen zu entwickeln. Auf Basis einer Evaluierung verschiedener Public-Cloud-Angebote aus Deutschland, der EU und den USA wird deren Nutzbarkeit für die öffentliche Verwaltung untersucht. Ein besonderer Fokus liegt dabei auf der Konsolidierung einschlägiger Proof of Concepts und deren Übertragbarkeit, um entsprechende Handlungsempfehlungen abzuleiten. Die Ergebnisse des Projekts werden öffentlich zugänglich gemacht, um einen Mehrwert für die gesamte öffentliche Verwaltung und einen sachlichen Beitrag zur Diskussion zu schaffen, für die sichere Nutzung von Public-Cloud-Lösungen.

Stand
Dezember 2024

Genderhinweis
Um die Lesbarkeit zu verbessern, wird in diesem Dokument das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen schließen – wenn nicht anders angegeben – alle Geschlechter ein.

Bildquellen
Titelseite: Adrien Olichon / Pexels.com
Vorwort: msg