Bernd Jäger, Reiner Kraft, Annika Selzer, Ulrich Waldmann

Die teilautomatisierte Verifizierung der getrennten Verarbeitung in der Cloud

Automatisiert mess- und auswertbarer Datenschutz in Cloud-Umgebungen kann potenziellen Cloud-Nutzern Datenschutzbedenken nehmen. Doch für jede Messung müssen vorab geeignete Datenquellen gefunden und sinnvoll kombiniert werden, um sich einer automatisierten Verifikation von Datenschutzzielen anzunähern. Dieser Beitrag schlägt ein solches Vorgehen für das Datenschutzziel der getrennten Verarbeitung vor.

Bernd Jäger

ist Sicherheitsarchitekt bei der Colt Technology Services GmbH und zuständig für Plattform-Architekturen und Technologiestrategien.

E-Mail: bernd.jaeger@colt.net

Reiner Kraft

Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie.

E-Mail: reiner.kraft@sit.fraunhofer.de

Annika Selzer

Wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für sichere Informationstechnologie.

E-Mail: annika.selzer@sit.fraunhofer.de

Ulrich Waldmann

Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie.

E-Mail: ulrich.waldmann@sit.fraunhofer.de

1 Datenschutzmessungen in der Cloud[1]

Viele Unternehmen möchten Cloud-Dienste für die Verarbeitung von Mitarbeiter- und Kundendaten nutzen, nehmen aber aufgrund von Datenschutzbedenken davon Abstand. Derartige Barrieren könnten durch Möglichkeiten zur kontinuierlichen und weitgehend automatisierten Messung der Qualität und Wirksamkeit von Datenschutzmaßnahmen eines Cloud-Betreibers abgebaut werden. In diesem Beitrag werden – am Beispiel des Datenschutzziels der getrennten Verarbeitung – Ideen für ein solches vertrauensbildendes Prüfinstrumentarium vorgestellt, das es (nicht nur potentiellen) Kunden eines Cloud-Dienstes ermöglicht, den Grad der Umsetzung von Datenschutzanforderungen nachzuverfolgen und Verletzungen der Anforderungen zeitnah zu erkennen.

2 Getrennte Datenverarbeitung

Das Datenschutzziel der getrennten Verarbeitung ist im Datenschutzrecht verankert. Bei der Umsetzung in der Cloud sind deren technische Besonderheiten zu berücksichtigen.

2.1 Rechtliche Definition

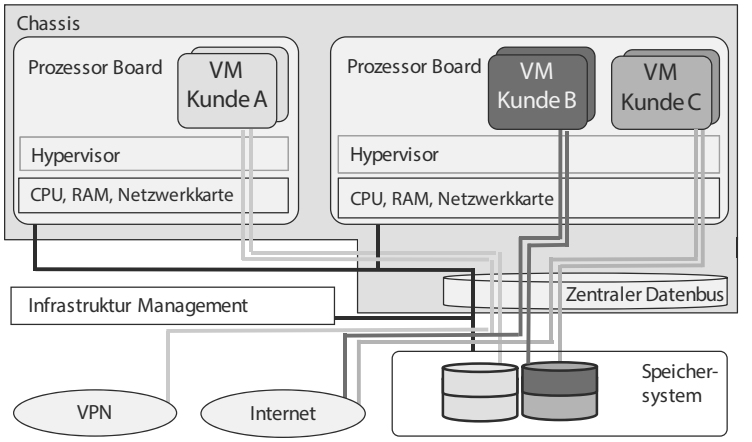
Das Bundesdatenschutzgesetz (BDSG) fordert in § 9 Satz 1 von datenverarbeitenden Stellen technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten. Gemäß Satz 2 Nr. 8 der Anlage zu § 9 Satz 1 BDSG müssen solche Maßnahmen auch gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Ziel der getrennten Verarbeitung ist also die Umsetzung der Zweckbindung durch geeignete und angemessene technische und organisatorische Maßnahmen. Die getrennte Verarbeitung hat auch im Rahmen von Auftragsdatenverarbeitungsverhältnissen eine große Bedeutung: Auftragnehmer, die personenbezogene Daten verschiede-

1 Der Beitrag entstand im Projekt VeriMetrix, gefördert vom BMBF im Programm „IKT 2020 – Forschung für Innovationen", Förderkennzeichen: 16KIS0053K.

ner Auftraggeber verarbeiten, haben sicherzustellen, dass eine „klare und absolute Trennung der [...] innerhalb unterschiedlicher Vertragsverhältnisse erhobenen und verarbeiteten Daten garantiert" werden kann [DKWW13].

Nicht immer ist die getrennte Verarbeitung durch eine physische Trennung – z. B. in Form eigener Hardware je Auftraggeber – nötig: Soweit die verarbeiteten personenbezogenen Daten keinem besonders hohen Schutzbedarf unterliegen und soweit die datenverarbeitende Stelle die Datentrennung z. B. durch softwareseitigen Ausschluss/Mandantentrennung, logische Trennung innerhalb eines Verarbeitungszusammenhangs, Trennung über Zugriffsregeln oder durch Dateiseparierung bei Datenbanken sicherstellen kann, ist dies angemessen im Sinne des § 9 Satz 2 BDSG, vgl. [DKWW13, Muen10].

Abb. 1 | Datentrennung in modernen Cloud-Infrastrukturen



2.2 Technische Definition

Beim Cloud-Computing werden verschiedene Dienst- und Nutzungsmodelle unterschieden. Das jeweilige Modell und seine technische Umsetzung beeinflussen auch den Grad der Datentrennung. So teilen sich in einem typischen Software-as-a-Service-Szenario (SaaS) alle Benutzer eine Anwendung samt darunter liegender Virtualisierungsschicht und eingesetzter Hardware.[2] Die Trennung erfolgt auf logischer Ebene, die konkrete hard- und softwaremäßige Umsetzung bleibt den Kunden meist verborgen. Bei Infrastructure-as-a-Service (IaaS) gibt es hingegen oft die – je nach Schutzbedarf der betroffenen Daten umso wichtigere – Möglichkeit, einzelne Elemente der Infrastruktur gegen Aufpreis dediziert und exklusiv für einen Kunden (Mandanten) bereitzustellen. Unabhängig von der Implementierung müssen bei Cloud-Diensten Übergriffe von einem Kundensystem auf ein anderes ausgeschlossen sein, ebenso unautorisierte Zugriffe auf die Managementebene der virtuellen Infrastruktur, da ansonsten die Mandantentrennung ausgehebelt oder umgangen werden könnte.

Die zur getrennten Verarbeitung nötigen Absicherungen betreffen alle beteiligten Komponenten, also sowohl die Verarbeitung der Daten in den Virtuellen Maschinen (VMs) als auch deren Übertragung und Speicherung auf virtuellen Speichereinheiten, in Speichernetzen oder auf speziellen Backup-Medien. Abb. 1 zeigt eine typische Cloud-Infrastruktur mit den Ebenen der Datenverarbeitung, Datenübertragung und Datenspeicherung. Beispiele für die gemeinsame Nutzung von Ressourcen durch Cloud-Kunden sind angedeutet.

Üblicherweise setzt ein Cloud-Dienstanbieter heute eine sogenannte konvergente Infrastruktur ein, bei der aus Gründen der ökonomischen Skalierung und der Vereinfachung des Managements die Ressourcen in einem gemeinsamen Chassis mit zentralem Datenbus und zentraler Netzwerkschnittstelle konzentriert sind.

Im Beispiel hat Kunde A im Rahmen eines IaaS-Vertrags ein eigenes Prozessor-Board gemietet. Die physische CPU, der physische Speicher und die entsprechenden virtuellen Adapter einschließlich Hypervisor werden deshalb ausschließlich von den VMs dieses Kunden genutzt. Zusätzlich kann der Kunde bestimmte VMs logisch über ein eigenes VLAN von den anderen VMs trennen, etwa um über ein VPN getrennt vom Internet Daten mit dem internen Firmennetz auszutauschen. Sämtliche Netz- und Speicher-Daten seiner VMs werden allerdings über einen physischen Datenbus übertragen, der mit anderen Kunden geteilt wird (im Bild angedeutet rechts über dem Speicher). Anschließend werden die Datenströme wieder auf verschiedene Netz- und Speicher-Schnittstellen verteilt. Kunde A hat auch eine eigene Speichereinheit gemietet. Seine persistent gespeicherten Daten sind daher zu einem gewissen Grade auch physisch von Daten anderer Kunden getrennt. Das Risiko eines Kollateralschadens, z. B. bei der Beschlagnahme von Speichereinheiten, ist daher deutlich reduziert.

Bei den Kunden B und C ist der Trennungsgrad geringer: Beide nutzen Standard-Cloud-Angebote, bei denen VMs vom Betreiber je nach Last auf beliebigen Hardware-Einheiten realisiert werden. CPU, Arbeitsspeicher, Netz und persistente Speichereinheiten werden somit physisch geteilt und ausschließlich logisch getrennt.[3] Üblicherweise werden die Daten der verschiedenen Kunden für die Übertragung ins VPN oder Internet logisch mittels VLAN-Gruppen separiert über den zentralen Datenbus geführt und dann mit Hilfe eines Switches in die verschiedenen physischen Verbindungen weitergeleitet. Virtuelle Bus-Adapter auf Hypervisor-Ebene sorgen für die getrennte Speicherung von Daten.

Über die gezeigten Beispiele hinaus gibt es eine Vielzahl an Varianten zur Datentrennung. Tab. 1 zeigt und bewertet Abstufungen des Trennungsgrades durch unterschiedliche Isolation der Ressourcen. Möglich – wenngleich nicht immer sinnvoll – sind fast alle Kombinationen der verschiedenen Trennungsgrade von Verarbeitung, Netz und Speicher. Eine durchgehende physische Trennung der Daten ist aufwändig oder wäre sehr kostspielig. Falls der Cloud-Betreiber es anbietet, können sich Kunden ein Set der Trennung selbst zusammenstellen. In jedem Fall müssten für eine Verifikation der Datentrennung geeignete Sollwerte definiert werden.

Unabhängig von der Art der Ressourcentrennung erfordert die Umsetzung der getrennten Verarbeitung auch Zugangs- und Zugriffsschutzmaßnahmen (siehe dazu [JKSW16]).

2 Theoretisch könnte der Dienst auch exklusiv für einzelne Kunden aufgebaut werden. Dies würde man dann aber als „Application Hosting" oder „Private Cloud" bezeichnen.

3 Beispielsweise mittels VLANs, Speicher-LUNs (Logical Unit Numbers) oder VSANs (Virtual Storage Area Network).

Tab. 1 | Beispiele für Grade der Datentrennung in Cloud-Ressourcen

Datenverarbeitung	
Sehr hoch	Physisch getrennte Server
Hoch	Hardware-Trennung: eigenes Prozessor-Board, gemeinsames Chassis (siehe Abb. 1, Kunde A)
Mittel	Logische Trennung: getrennte VMs, gleicher physischer Host/ Hypervisor, gemeinsamer Speicher und CPU (siehe Abb. 1, Kunden B, C)
Niedrig	Gleiche VM: mandantenfähige Anwendung
Datenübertragung	
Sehr hoch	Physisch getrenntes Netz (eigene Kabel, Switches, Ports etc.)
Hoch	Gleiches physisches oder logisches Netz mit starker Verschlüsselung, z. B. mittels TLS oder IPSec-Tunnel
Mittel	Gleiches physisches Netz mit logischer Trennung: z. B. separate VLANs (vgl. Abb. 1, zentraler Datenbus)
Datenspeicherung	
Sehr hoch	Physisch getrenntes Speichersystem
Hoch	Hardware Trennung: eigene physische Festplatte (siehe Abb. 1, Kunde A)
Mittel	Logische Trennung: z. B. eigenes LUN (siehe Abb. 1, Kunden B, C)
Niedrig	Gemeinsames LUN (getrennte Dateibereiche)

2.3 Stand der Technik

Im Fokus vieler Untersuchungen sind mögliche Schwachstellen von VMs, Gefährdungen und Gegenmaßnahmen zum Schutz der Vertraulichkeit von Daten unterschiedlicher Mandanten auf derselben physischen Infrastruktur. Zu den Gefährdungen gehören vor allem Cross-VM-Angriffe über Seitenkanäle der gemeinsam genutzten Komponenten CPU, Netzanbindung, Daten-Cache und persistenter Speicher.

Cloud-Betreiber können als Gegenmaßnahme das unberechtigte Ausspähen von VM-Standorten erschweren, beispielsweise durch die zufällige Verteilung interner IP-Adressen oder die gezielte Gruppierung der VMs bestimmter vertrauenswürdiger Kunden auf einer gemeinsamen Hardware [XiXi13].

Der Lösungsansatz des Systems HomeAlone [ZJOR11] nutzt die Seitenkanalanalyse für einen Sicherheitszweck: Ein Tool untersucht den Cache-Seitenkanal auf Aktivitäten, die der exklusiven Nutzung der Hardware durch einen Kunden widersprechen. Dafür müssen allerdings die Aktivitäten der rechtmäßigen VMs koordiniert für eine bestimmte Zeit ausgesetzt werden. Zudem bleiben andere mögliche Seitenkanäle unbeachtet.

Die NoHype-Architektur [SKLR11] verzichtet auf gemeinsam genutzte Hypervisor-Schnittstellen, indem sich jede VM weitgehend selbst verwaltet und dedizierte Hardware-Ressourcen nutzt, was allerdings tiefgreifende Änderungen an der Cloud-Infrastruktur erfordert und zudem eine Migration von VMs erschwert.

Andere Arbeiten zielen darauf ab, mögliche Verstöße gegen die getrennte Verarbeitung im laufenden Betrieb zu erkennen, beispielsweise durch automatisierte Suche nach Schwachstellen und Konfigurationsfehlern auf Hypervisor-Ebene [TBK+15]. Demgemäß analysiert das VMware-basierte Monitoring-System Cloud Radar die Konfigurationsänderungen in einer Cloud-Infrastruktur und vergleicht sie mit den Vorgaben zur VM-Isolation [BlVG14]. Dazu werden allerdings weitgehende Hypervisor-Zugriffrechte benötigt, die vom Cloud-Betreiber gewährt werden müssen.

3 Automatische Überprüfung

Der Überblick zum Stand der Technik zeigt, dass es eine Reihe an Vorschlägen dafür gibt, wie Defizite in der Konfiguration und im Betrieb einer Cloud-Infrastruktur sowie direkte Verletzungen des Datenschutzziels der getrennten Verarbeitung automatisiert geprüft und erkannt werden können. Im Projekt VeriMetrix, in dessen Rahmen dieser Beitrag entstand, wird versucht, diese Ansätze aufzugreifen, zu ergänzen und zu systematisieren. Dazu gehört auch, die Grenzen der automatisierten Messbarkeit der Datenschutzeigenschaften eines Cloud-Dienstes aufzuzeigen und Möglichkeiten zur Behebung der daraus folgenden Informationslücke aufzuzeigen.[4]

3.1 Getrennte Verarbeitung

Für die Kontrolle der Einhaltung einer Hardware-Trennung im Bereich der Datenverarbeitung im engeren Sinne gibt es vergleichsweise einfach anzuwendende Mittel. So können Kunden, die aufgrund des hohen Schutzbedarfs ihrer Daten ein eigenes, festes Prozessor-Board für die Verarbeitung ihrer Daten wünschen, mit Hilfe frei verfügbarer Programme zur Abfrage der CPU-Informationen testen, ob ihre Daten tatsächlich auf dem eigenen Host (Prozessor-Board samt Hypervisor) verarbeitet werden oder nicht. Diese Programme liefern umfangreiche Angaben zum Prozessor, beispielsweise Typ, Hersteller, Taktfrequenz und Größe des Caches, die zusammengenommen als Fingerprint der virtuellen CPU betrachtet werden können, der einer gegebenen VM präsentiert wird.

Zwei Beispiele mit Rohdaten für solche CPU-Fingerprints und deren Unterschiede sind in Abb. 2 dargestellt.

Die Unterschiede weisen darauf hin, dass die beiden Prozessor-Boards verschiedene CPUs nutzen und dass damit die Daten auf Hardware-Ebene getrennt sind. Abweichungen in aufeinanderfolgenden Messungen auf einer Kunden-VM sind ein Beleg für einen zwischenzeitlichen Wechsel des zugrundeliegenden Hosts. Identische Messungen in VMs, die eigentlich getrennt sein sollten, weisen darauf hin, dass sich diese VMs auf demselben Host befinden, die gesetzte Anforderung also nicht erfüllt wird.

3.2 Getrennte Übertragung

Auch für die Prüfung, ob eine virtualisiert oder hardwaremäßig beabsichtigte Netztrennung wie geplant funktioniert, kann ein Sensor auf einer kundenspezifischen VM dienen. So ermöglicht ein passiv die Kenndaten von IP-Verbindungen aufzeichnender Sniffer[5] es, IP-Adressen benachbarter Kundennetze zu erkennen, die eigentlich über logische Maßnahmen abgetrennt sein sollten. Ein solcher Netz-Sensor könnte aus technischer Sicht auch aktive Verfahren wie *Spoofing* oder *Packet Injection* zur Bestimmung der Netzumgebung und somit auch des Trennungsgrades anwenden. Da aber auch Angreifer solche Methoden nutzen, würde dies vom Cloud-Betreiber nur in Ausnahmefällen toleriert und wäre das Risiko groß, dass die entsprechende VM von automatisierten Netzüberwachungssystemen als infiziert oder bösartig klassifiziert und deren IP-Adresse gesperrt würde.

4 Die automatisierte Messung von Datenschutzeigenschaften zur Erfüllung des Transparenzgrundsatzes kann im Spannungsfeld zu den Grundsätzen Datensparsamkeit und Datenvermeidbarkeit stehen. Um diesem Spannungsfeld zu begegnen, muss sichergestellt werden, dass die automatisierte Messung wiederum datenschutzkonform erfolgt.

5 Z. B. mithilfe des freien Tools *p0f* (http://lcamtuf.coredump.cx/p0f3).

Abb. 2 | Rohdaten für unterschiedliche CPU-Fingerprints

Prozessor Board 1

```
[verimetrix@centos-de ~]$ cpuinfo
Vendor ID: GenuineIntel
Hardware Raw:
...
Hz Advertised Raw: (2200000000, 0)
Hz Actual Raw: (2200000000, 0)
Arch: X86_64
Bits: 64
Count: 2
Raw Arch String: x86_64
L2 Cache Size: 20480 KB
Stepping: 7
Model: 45
Flags: aes, aperfmperf, apic, arat, arch_perfmon, avx,
bts, clflush, cmov, constant_tsc, cx16, cx8, de, dtherm,
dts, epb, fpu, fxsr, hypervisor, ida, lahf_lm, lm, mca,
mce, mmx, msr, mtrr, nonstop_tsc, nopl, nx, pae, pat,
pcid, pclmulqdq, pebs, pge, pln, pni, popcnt, pse, pse36,
pts, rdtscp, sep, ss, sse, sse2, sse4_1, sse4_2, ssse3,
syscall, tsc, tsc_reliable, vme, x2apic, xsave, xtopology

[verimetrix@centos-de ~]$ uuid
2c093ee0-b55a-11e5-b37f-005056051777
```

Prozessor Board 2

```
[verimetrix@centos-fr-a ~]$ cpuinfo
Vendor ID: GenuineIntel
Hardware Raw:
...
Hz Advertised Raw: (2200000000, 0)
Hz Actual Raw: (2200000000, 0)
Arch: X86_64
Bits: 64
Count: 2
Raw Arch String: x86_64
L2 Cache Size: 20480 KB
Stepping: 1
Model: 37
Flags: aes, aperfmperf, apic, arat, arch_perfmon, bts, clflush,
cmov, constant_tsc, cx16, cx8, de, dtherm, dts, epb, fpu, fxsr,
hypervisor, lahf_lm, lm, mca, mce, mmx, msr, mtrr,
nonstop_tsc, nopl, nx, pae, pat, pclmulqdq, pebs, pge, pln,
pni, popcnt, pse, pse36, pts, rdtscp, sep, ss, sse, sse2, sse4_1,
sse4_2, ssse3, syscall, tsc, tsc_reliable, vme, x2apic,
xtopology

[verimetrix@centos-fr-a ~]$ uuid
5f01375c-b55b-11e5-ac5d-005056030c97
```

Als Messdaten werden in diesem Fall ausschließlich IP-Adressen und andere Metadaten der Pakete ausgewertet. Inhaltsdaten, die bei einer festgestellten Verletzung der Datentrennung unter Umständen sensible, datenschutzrechtlich relevante Angaben enthalten können, werden hingegen weder benötigt noch protokolliert.

3.3 Getrennte Speicherung

Während Sensoren für Verarbeitung und Übertragung auf kundenspezifischen VMs unmittelbar Aufschluss über die Qualität der Datentrennung geben und zur Erkennung von Verletzungen beitragen können, ist dies im Bereich des persistenten Speichers auf dieser Ebene nicht möglich. Sofern der Cloud-Betreiber lesenden Zugriff auf eine geeignete Schnittstelle gewährt, können hingegen auf der Ebene des VM-Managements umfangreiche Implementierungsdetails abgerufen werden, die über die Parameter zur Speicherkonfiguration auch eine Sicht auf die Art und die Stärke der Maßnahmen zur logischen Trennung der Kundendaten auf einem gemeinsam genutzten Massenspeicher bieten.

Zusätzlich lassen sich an dieser Schnittstelle weitere Informationen gewinnen. So lassen sich über die festgelegten Administratorrollen und Berechtigungsprofile indirekt Rückschlüsse auf den Umgang mit sensiblen Daten ziehen, zeigen die Parameter zur Netz-Konfiguration doch, wie gut Kommunikationsflüsse logisch getrennt werden und erlaubt die Auswertung des VM-Aktivitätsprotokolls zudem Bewertungen zum Zugriffsschutz.

3.4 Grenzen für automatisierte Messungen

Ob und in welchem Umfang ein Messverfahren genutzt werden kann, hängt von seiner Art und der Zustimmung des Cloud-Betreibers ab. Am unproblematischsten sind in dieser Hinsicht Messungen innerhalb eines Kundensegments, etwa auf einer kundenspezifischen VM. Allerdings ist der Umfang der Informationen begrenzt, der sich hier gewinnen lässt. Dies gilt insbesondere für Indikatoren zur Umsetzung der Datentrennung im Bereich des persistenten Speichers.

Umfassendere Einsichten bieten Messungen (z. B. mit speziellen Mess-VMs) auf den Ebenen des Hypervisors oder der Cloud-Infrastruktur, die allerdings das Einverständnis des Betreibers erfordern. Besonders sensibel sind in dieser Hinsicht Erhebungen zu dessen Infrastruktur und Prozessen. Zwar könnte auch hier zumindest teilweise automatisiert ermittelt werden, ob Rahmenbedingungen für eine effektive Mandantentrennung eingehalten werden, etwa dedizierte Management-Systeme eingerichtet sind oder Zugriffe ordnungsgemäß protokolliert werden. Der Betrieb von Sensoren in diesem sensiblen Bereich wäre aber schwierig. Die Messung organisatorischer und infrastruktureller Maßnahmen (z. B. das Vorliegen eines datenschutzkonformen Auftragsdatenverarbeitungsvertrags) wird wegen fehlender Standards – etwa zu Struktur und Inhalt solcher Verträge – und Online-Zugängen zu den zu erhebenden Informationen bis auf weiteres die manuelle Prüfung durch einen Auditor erfordern.

4 Ergänzende Audits

Die vorstehend beschriebenen automatisierten Verfahren geben insbesondere Hinweise zur Beschaffenheit und Wirksamkeit der IT-bezogenen Maßnahmen und liefern damit wichtige Indikatoren dafür, ob und wie gut das Datenschutzziel der getrennten Verarbeitung in einer Infrastruktur-Cloud erfüllt ist. Gleichwohl bleiben Vor-Ort-Audits für ein umfassendes Bild zur Datenschutz-Konformität eines Cloud-Dienstes erforderlich. Diese beziehen sich insbesondere auf die infrastrukturellen und organisatorischen Gegebenheiten. Zu den überhaupt nicht oder nur unvollständig automatisiert prüfbaren Aspekten gehören beispielsweise die folgenden Punkte, vgl. [DKWW13], [Muen10]:

- Vorhandensein „eigener", kundenspezifischer Hardware bei sehr hohem Schutzbedarf: Die Hardware ist einem einzelnen Kunden zugewiesen und die Zuweisung ist nachvollziehbar.
- Vorhandensein eines ADV-Vertrags mit Regelungen zur getrennten Verarbeitung: Der Vertrag liegt schriftlich vor und enthält Details zur Umsetzung der getrennten Verarbeitung und dem Auftraggeber sind umfangreiche Weisungs- und Kontrollbefugnisse zugeordnet.
- Ordnungsgemäße Umsetzung der Zugriffskontrolle: [JKSW16]: Vorhandensein eines schriftlichen Zugriffsberechtigungskonzepts, Vorhandensein einer datenschutzkonformen Protokollierungsstrategie und Nachweis der Benutzerkennung, sowie das Vorhandensein von Zugriffsschutzmaßnahmen für Datenträger.

Im Fokus der Erhebungen eines Auditors stehen folglich neben der technischen Umsetzung der Datentrennung auch die vertraglichen Regelungen zwischen Cloud-Betreiber und Kunde sowie die internen Regelungen des Cloud-Betreibers.

5 Kombination und Ausblick

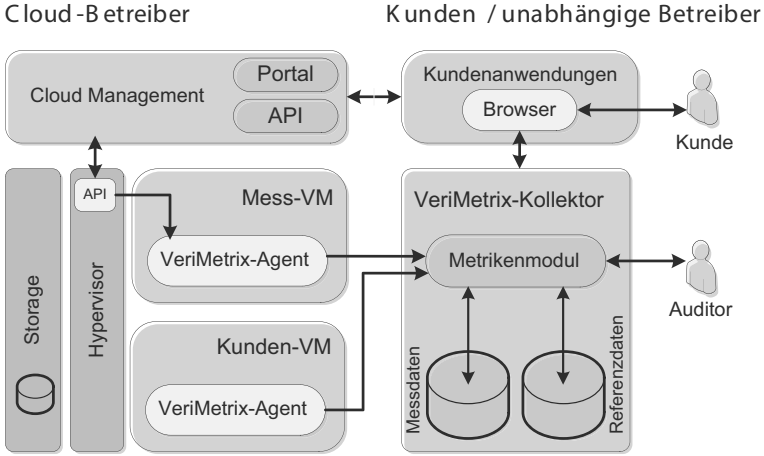
Wie erwähnt entstanden die dargestellten Prüfverfahren im Rahmen des Forschungsprojekts VeriMetrix, das darauf abzielt, Verfahren und Werkzeuge zur umfassenden Kontrolle und Bewertung der Datenschutz-Qualität von Cloud-Angeboten zu entwickeln. Mit einem Demonstrator soll veranschaulicht werden, wie die kontinuierlich und automatisiert erhobenen Messergebnisse und die periodisch vorgenommenen Audit-Ergebnisse in eine

als Metrik angelegte Gesamtbewertung der Maßnahmenqualität zur getrennten Verarbeitung einfließen können. Die in Abb. 3 dargestellte Architektur dieses Werkzeugs sieht neben Sensoren für die automatisierten Messungen eine Schnittstelle zur manuellen Erfassung der Prüfergebnisse des Auditors vor.

Automatisierte Messungen und manuelle Bewertungen werden in einer zentralen Komponente (Kollektor) zusammengefasst und zu Metriken aufbereitet. Ein Kunde kann die Ergebnisse zum Beispiel über einen Browser einsehen, mit dem er auch seine virtuelle Infrastruktur beim Cloud-Betreiber administriert.

Dabei wird ein an dem Modell der Ampel angelehntes Bewertungsschema angewendet: Befunde aus Messungen zur Einhaltung der Datenschutzziele können als angemessen (grün), als möglicherweise (Verdacht, gelb) oder als gesichert unangemessen (rot) eingestuft, zusätzlich einzelne Audit-Kriterien als nicht relevant gekennzeichnet werden. Mehrere Messquellen sowie die Befunde aus Audits und automatisierten Messungen werden gemäß der Matrix in Tab. 2 miteinander kombiniert. Die Maßnahmen eines Cloud-Betreibers zur getrennten Verarbeitung werden demgemäß nur dann als angemessen eingestuft, wenn alle Teilprüfungen zu diesem Ergebnis kommen.

Abb. 3 | VeriMetrix-Architektur



Tab. 2 | Kombination von Messergebnissen

Befund aus Messung	Befund der Auditorprüfung		
	Angemessen	Nicht relevant	Unangemessen
Angemessen			
Verdacht			
Unangemessen			

Die Benutzungsoberfläche des VeriMetrix-Demonstrators bietet zwei abgestuft granulare Sichten auf die Prüfergebnisse, mit denen unterschiedlichen Zielgruppen und Informationsbedürfnissen entsprochen werden kann.

Abb. 4 | Ergebnisdarstellung in der VeriMetrix-Benutzungsoberfläche

Auf oberster Ebene (siehe Abb. 4) sieht der Benutzer eine Gesamtbewertung des betrachteten Cloud-Betreibers, in die neben der getrennten Verarbeitung weitere Datenschutzziele einfließen. Im Demonstrator sind dies die Konformität des Verarbeitungsstandorts, ein angemessen starker Zugriffsschutz sowie die Zuverlässigkeit der Mechanismen zur Löschung und Sperrung von Daten. Für jedes dieser Ziele wird das Prüfergebnis angezeigt, sodass eventuelle Problembereiche unmittelbar erkannt werden können.

Zu jedem Datenschutzziel kann sich der Benutzer zudem nähere Informationen zu den Messungen in einer Detailansicht anzeigen lassen, mit der Ursachen möglicher Probleme genauer bestimmt werden können. Diese granulare Darstellung richtet sich insbesondere an Datenschutz- und Informationssicherheitsbeauftragte.

Als Auswahlkriterium für die Messverfahren im VeriMetrix-Demonstrator gilt neben der Robustheit gegenüber technischen Änderungen der Hersteller auch eine die verschiedenen Dienstmodelle übergreifende Anwendbarkeit. Zu beachten ist ferner, dass kaum eine Datenquelle eine absolut sichere Zuordenbarkeit bietet. Diesem Umstand muss Rechnung getragen werden, um die Zuverlässigkeit der Gesamtaussagen zu erhöhen.

Literatur

[BlGV14] Bleikertz/Groß/Vogel: Cloud Radar: *Near Real-Time Detection of Security Failures in Dynamic Virtualized Infrastructures*, in: Proc. Computer Security Applications Conference, S. 26-35, 2014.

[DKWW13] Däubler/Klebe/Wedde/Weichert: *Bundesdatenschutzgesetz Kompaktkommentar*, 2013.

[JKSW16] Jäger/Kraft/Selzer/Waldmann: *Die Kontrolle des Umsetzungsgrades des Zugangs- und Zugriffsschutzes*, DuD 2016, S. 239-243.

[Muen10] Münch: *Technisch-organisatorischer Datenschutz*, 2010.

[SKLR11] Szefer/Keller/Lee/Rexford: *Eliminating the hypervisor attack surface for a more secure cloud*, in: Proc. 18th ACM conference on Computer and communications security, S. 401-412, 2011.

[TBK+15] Takeshi/Blanc/Kadabayashi et al.: *Enabling Secure Multitenancy in Cloud Computing: Challenges and approaches*, in: Proc. of the 2nd Baltic Congress on Future Internet Communications, S. 72-79, 2012.

[XiXi13] Xiao/Xiao: *Security and Privacy in Cloud Computing*, in: IEEE Communications Surveys and Tutorials, S. 843-859, 2013.

[ZJOR11] Zhang/Juels/Oprea/Reiter: HomeAlone: *Co-Residency Detection in the Cloud via Side-Channel Analysis*, in: IEEE Symposium on Security and Privacy, S. 313-328, 2011.