Sicherheit und Compliance bei der Datenverarbeitung mit Azure

Microsoft

Autoren

Markus Feichtner
Debra Shinder
Dr. Christoph Siegert

Beitragende

Darren Brust
David Burt
Justin Denk
Roger Halbherr
Dr. Marc Holitscher
Shont Miller
Glenn Pittaway
Seth Varty
Stevan Vidich

Inhalt

Einführung

Sicherheit und Compliance sind elementare Bestandteile einer vertrauenswürdigen Cloud, und diese Themen sind somit für alle Organisationen relevant. Microsoft hat dieses Whitepaper erstellt, um Kunden bei Fragen zur datenschutzkonformen Speicherung und Verarbeitung ihrer Daten zu unterstützen.

Transparenz und Kontrolle durch den Kunden sind auch entscheidend, um Vertrauen in die Cloud-Technologie aufzubauen und zu erhalten. Microsoft ist sich bewusst, dass regulierte Branchen zusätzliche Informationen für ihr Risikomanagement und die Einhaltung der entsprechenden Maßnahmen benötigen. Um diesen Prozess zu unterstützen, bietet Microsoft ein umfangreiches, in der Branche führendes Sicherheits- und Compliance-Portfolio.

In die Azure-Plattform sind eine Reihe von Sicherheitsfunktionen integriert, beginnend mit dem Security Development Lifecycle (SDL) über Datenmanagement- und Governance-Tools, Active Directory-Identitäten und -Zugriffskontrollen, Technologien und Werkzeuge für die Netzwerk- und Infrastruktur bis hin zum Schutz vor Bedrohungen, und Verschlüsselung zum Schutz von Daten bei der Übertragung und Speicherung.

Microsoft bietet Kunden die Wahlmöglichkeit, wo sie ihre Daten in der globalen Azure Cloud speichern wollen. Mithilfe unseres innovativen Sicherheits- und Compliance-Frameworks können Kunden aus allen Branchen geschäftskritische Workloads in der Cloud betreiben und von allen Vorteilen unserer Hyperscale Cloud profitieren.

Dieser von Microsoft empfohlene Ansatz kann unseren Kunden dabei helfen, Datenschutzanforderungen oder Unternehmensrichtlinien zu erfüllen:

- Überprüfung der Datenschutzverpflichtungen.
- Von Azure angebotenen Dienste, die Kunden bei der Einhaltung von Compliance-Anforderungen unterstützen.
- Compliance-Nachweise

Das Whitepaper ist in diese drei Abschnitte untergliedert. Der erste betrachtet generelle Richtlinien, der zweite die Technologie. Im letzten Abschnitt werden konkrete Anforderungen erläutert, denen Branchen und Organisationen in Deutschland und Frankreich unterliegen.

I. Überprüfung der Datenschutzverpflichtungen

Der erste Schritt im Prozess ist, die Verpflichtungen sowie zu schützende Datentypen und Speicherorte zu kennen und zu identifizieren. Es sollte eine Analyse durchgeführt werden, damit die gesetzlichen und vertraglichen Anforderungen an die Cloud-Workloads bestimmt werden können. Der Geschäftssitz der Firma des Kunden, der Speicherort der Daten und Branchenregulierung können diese beeinflussen.

Bestandteile dieser Analyse sind die Klassifizierung der Daten, Überlegungen zu Speicherorten und die gemeinsame Verantwortung zum Schutz der Daten.

Die Datenklassifizierung von Microsoft Azure

In jeder Organisation existieren verschiedene Arten von Daten mit unterschiedlichem Schutzbedarf. Dieses Whitepaper beschäftigt sich hauptsächlich mit **Kundendaten** („Customer Data"), die Microsoft wie folgt definiert:

Sämtliche Daten, inklusive Text-, Audio-, Video- oder Bilddateien und Software, die ein Kunde Microsoft zur Verfügung stellt oder die im Rahmen der Nutzung eines Microsoft-Online-Dienstes (in diesem Fall Azure) im Kundenauftrag zur Verfügung gestellt werden. Beispiele für Kundendaten sind unter anderem Inhalte, die der Kunde in Azure Storage oder Azure SQL Database hochlädt, sowie Anwendungen und weitere Inhalte in virtuellen Maschinen, die der Kunde hochlädt, um sie in Azure Virtual Machines auszuführen. Microsoft unterscheidet nicht nach Art der Kundendaten, sondern es werden alle Inhalte als Kundendaten klassifiziert, die dem gleichen, hohen Schutzniveau unterliegen.

- **Personenbezogene Daten:** Hierbei handelt es sich um Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Mit anderen Worten: Personenbezogene Daten sind alle Daten, die mit einer bestimmten Person in Verbindung gebracht werden. Personenbezogene Daten, die von unseren Kunden durch die Nutzung des Dienstes zur Verfügung gestellt werden, wie die Namen und Kontaktdaten der Kunden, zählen auch zu den Kundendaten. Personenbezogene Daten könnten aber auch bestimmte Daten enthalten, die keine Kundendaten sind, wie zum Beispiel die Benutzer-ID, die unser Dienst jedem Nutzer zuweist. Solche personenbezogenen Daten gelten als Pseudonym, weil sie allein für sich genommen nicht den Einzelnen identifizieren können.

Dieses Whitepaper befasst sich mit dem Umgang von Kundendaten (einschließlich personenbezogener Daten), da sie die relevanteste Kategorie für Nutzer sind. Microsoft klassifiziert und implementiert auch Richtlinien für den Schutz weiterer Datenkategorien:

- **Administratordaten:** Es handelt sich dabei um Informationen über Administratoren, die bei der Anmeldung, dem Kauf oder der Verwaltung von Microsoft-Diensten angegeben werden, wie Namen, Telefonnummern und E-Mail-Adressen. Dazu zählen auch aggregierte Nutzungsinformationen und Daten, die mit dem Administratorkonto verbunden sind, wie die von Ihnen gewählten Kontrollmechanismen. Microsoft nutzt Administratordaten, um Dienste bereitzustellen, Transaktionen abzuschließen, Serviceprozesse für das Konto auszuführen und Missbrauch zu erkennen und zu verhindern.

- **Objektmetadaten:** Es handelt sich dabei um Informationen, die von Ihnen oder in Ihrem Namen zur Identifizierung oder Konfiguration von Online-Serviceressourcen wie Software, Systemen oder Containern bereitgestellt werden, aber nicht deren Inhalte oder Nutzeridentitäten umfassen. Beispiele dafür sind die Namen und technischen Einstellungen von Azure Storage Accounts, Virtual Machines, SQL Databases und deren Tabellen, Spaltenüberschriften und Formularen. Kunden sollten keine personenbezogenen Daten oder andere sensible Informationen in Objektmetadaten einfügen, da Objektmetadaten über globale Microsoft-Systeme verteilt werden können, um Operationen und Fehlerbehebungen zu erleichtern.

- **Zahlungsdaten:** Hierbei handelt es sich um die Daten, die Kunden bei einem Onlinekauf bei Microsoft angeben. Unter diese Klassifizierung fallen zum Beispiel Kreditkartennummern inklusive Sicherheitscodes, Namen und Rechnungsadressen sowie andere Finanzdaten. Microsoft verwendet Zahlungsdaten, um Transaktionen zu verarbeiten sowie um Betrugsversuche zu erkennen und zu verhindern.

- **Support- und Consultingdaten:** Gemeint sind alle Daten, einschließlich aller Text-, Audio-, Video- und Bilddateien oder Software, die Microsoft von oder im Namen des Kunden zur Verfügung gestellt werden (oder Daten, für die der Kunde Microsoft ermächtigt, sie aus einem Online-Dienst abzurufen), indem Sie mit Microsoft einen Vertrag über professionelle Dienstleistungen oder Support abschließen. Dazu können Informationen gehören, die per Telefon, Chat, E-Mail oder Onlineformular erfasst werden, zum Beispiel eine Problembeschreibung, Dateien, die an Microsoft übermittelt werden, um Supportprobleme zu lösen, automatisierte Problemlösungsprozesse oder Informationen, die Microsoft durch vom Kunden autorisierte Remote-Zugriffe auf Kundensysteme erhält. Nicht enthalten sind Administratordaten oder Zahlungsdaten.

Datenspeicherung

Der Speicherort der Daten ist ein wichtiger Aspekt bei der Auswahl von Cloud-Diensten. Microsoft Azure bietet Dienste in mehr als 50 Regionen an, die aus mehr als 100 Rechenzentren rund um den Globus bereitgestellt werden. Um den passenden Speicherort für Ihre Cloud-Workloads auszuwählen, sollten folgende Sachverhalte in Erwägung gezogen werden:

- Technische Kriterien
- Regulatorische Vorgaben

Technische Kriterien

Eine hohe Latenz der Netzwerkverbindungen beeinträchtigt Echtzeitanwendungen. Als Latenz wird die zeitliche Verzögerung zwischen der Anfrage eines Kunden und der Antwort durch den Cloud Service Provider bezeichnet. Aufgrund der beispiellosen globalen Präsenz und der führenden Netzwerktechnologie bieten die Microsoft Azure-Dienste eine geringe Latenz für die Kundenanbindung.

Je nach Standort Ihrer Nutzer oder Ihrer Kundenbasis sollte die passende Region für die Cloud-Anwendung ausgewählt werden. Falls mit den Cloud-Workloads eine globale Nutzerbasis angesprochen beziehungsweise unterstützt werden soll, bietet Azure mehrere Dienste an, die den weltweiten Einsatz der Lösung erleichtern, die Latenz verringern und die Anwendungsperformance steigern. Dazu zählen:

- Azure Content Delivery Network (Azure CDN) ist eine skalierbare und schnelle Content-Distributionsplattform für statische und dynamische Inhalte. Azure CDN liefert eine bessere Geschwindigkeit und sorgt für eine höhere Kundenzufriedenheit, da die Latenz verringert wird.
- Azure Cosmos DB unterstützt globale Anwendungen. Der Dienst vereinfacht die Replikation in die Regionen, in denen die Daten benötigt werden.

Regulatorische Vorgaben

Dank der harmonisierten EU- Datenschutz-Grundverordnung (DSGVO/GDPR) und der Politik des digitalen Binnenmarktes, die den freien Datenfluss in der Europäischen Union ermöglicht, sind Kunden aus der Europäischen Union nicht darauf beschränkt, Daten ausschließlich im Herkunftsland zu verarbeiten. Beginnend mit der Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates und gefolgt von der DSGVO, formen die europäischen Institutionen den Schutz der Grundrechte und Freiheiten der Einzelpersonen im Hinblick auf die Verarbeitung und die Gewährleistung des freien Flusses personenbezogener Daten zwischen den Mitgliedstaaten.

Die Europäische Kommission gestaltet aktiv den digitalen Binnenmarkt und beeinflusst die nationale und internationale Regulierung, um den freien Datenfluss auf diesem Markt zu ermöglichen, und dies bietet den Kunden die Wahl, wo sie die Daten einsetzen wollen, um ein hohes Schutzniveau für personenbezogene Daten zu erreichen.

Zusätzlich zu den regulatorischen Vorgaben können sich Datenlokalisierungsanforderungen (Data Residency) aus internen Richtlinien oder vertraglichen Anforderungen unserer Kunden ergeben. Die Kunden können in diesem Fall die für sie passende Azure-Region wählen und die Speicherung von Kundendaten auf diese Region beschränken.

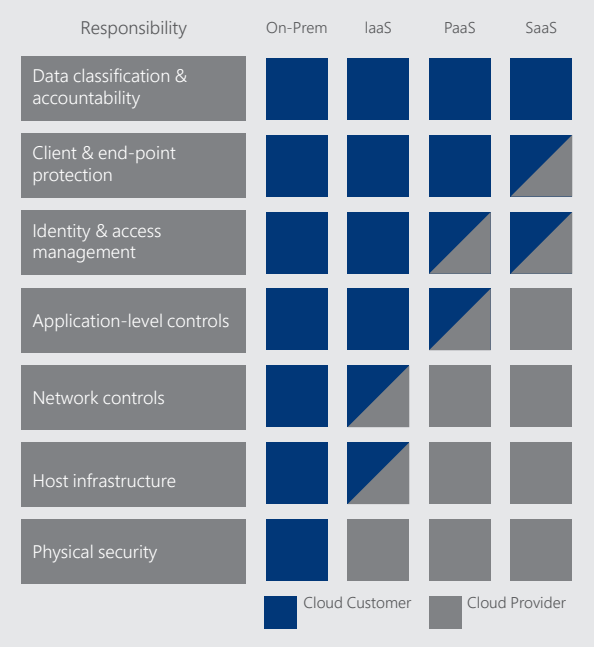
Außerdem gibt es zusätzliche Anforderungen an von staatlichen Stellen klassifizierte geschützte Daten. Microsoft Azure kann diese Anforderungen in mehreren Märkten erfüllen.

Geteilte Verantwortung

Die geteilte Verantwortung in der Public Cloud ergibt sich mit dem Hosten von Ressourcen in der Infrastruktur eines Public Cloud Service Providers. Die Verantwortung für Sicherheit hängt von dem von Ihnen verwendeten Cloud-Servicemodell ab (IaaS/PaaS/SaaS). Bei IaaS ist der Cloud-Dienstleister für die Sicherheit zentraler Infrastruktur verantwortlich, die die Speicherung, Netzwerke und Computing umfasst (zumindest auf der zugrunde liegenden Infrastrukturebene – der physischen Ebene).

Wenn Sie von IaaS zu PaaS und dann auf SaaS wechseln, werden Sie feststellen, dass Sie für weniger Aspekte verantwortlich sind und der Cloud-Dienstleister für weitere Bereiche verantwortlich ist.

Die Grafik zeigt, wie geteilte Verantwortung bei den verschiedenen Cloud-Servicemodellen funktioniert.



Weiterführende Informationen finden Sie im Whitepaper zum Thema „Shared Responsibility".

Microsoft Azure bietet mehrere Schutzmechanismen, Kontrollwerkzeuge und Best Practices, die die Sicherheit Ihrer Anwendungen insgesamt erhöhen.

II. Von Azure angebotene Dienste, die Kunden bei der Einhaltung von Compliance-Anforderungen unterstützen

Sicherheit und Compliance
Einer der wichtigsten Aspekte der Cloud-Sicherheit ist die Entwicklung gesetzeskonformer und sicherer Anwendungen und Workloads. Microsoft Azure bietet eine Reihe von Schutzmaßnahmen und Best Practices, die die Sicherheit der Kundenanwendungen insgesamt verbessern und Kunden dabei unterstützen, regulatorische Vorgaben und interne Richtlinien zu erfüllen. Azure bietet eine breite Palette von Schutzmaßnahmen, Sicherheitskontrollen und Best-Practice-Dokumentationen an, die in den nachfolgenden Abschnitten beschrieben werden.

Konkrete Empfehlungen zum Thema Sicherheit für Azure-Lösungen sind im Dokument Security Best Practices for Azure Solutions beschrieben.

Azure Secure Score

Die Azure Secure Score-Funktion im Azure Security Center ist ein Sicherheitsanalysewerkzeug, das einen Einblick in den aktuellen Stand der Unternehmenssicherheit gibt und bei der Bewertung der Systemsicherheit hilft. Der Secure Score berücksichtigt die Priorität und die Auswirkungen von einzelnen Empfehlungen und weist auf der Grundlage dieser Informationen einen numerischen Wert zu, der Ihnen zeigt, wie das Handeln auf diese Empfehlung hin Ihre Sicherheit im Hinblick auf Cloud-Lösungen verbessern kann.

Wenn eine empfohlene Maßnahme umgesetzt ist, werden auch die Empfehlungspunkte und die Gesamtpunktzahl aktualisiert. Der Secure Score ist eine Zusammenfassung aller Empfehlungspunkte.

Die wichtigsten Ziele des Secure Score:

- Visualisierung der Sicherheitslage
- Schnelle Klassifizierung und Vorschläge mit sinnvollen Maßnahmen, damit die Sicherheitslage verbessert wird
- Kontinuierliche Messung der Sicherheit von Workloads

Dienste und Werkzeuge für Datenmanagement und Data Governance

Datenmanagement und Data Governance sind der Schlüssel zu einem erfolgreichen Geschäftsbetrieb in der heutigen datengestützten Welt. Die Datenflut bringt für alle Organisationen eine Verantwortung mit sich, damit wertvolle Chancen ergriffen und schützenswerte Daten gesichert werden.

Microsoft stellt Tools zur Verfügung (in Übereinstimmung mit der ISO/IEC 38505), die Kunden bei der Bewertung, Steuerung und Überwachung der Verarbeitung und Nutzung von Daten innerhalb ihrer Organisationen unterstützen. Durch den Einsatz dieser Tools können Unternehmen umfassende Transparenz hinsichtlich der Daten erhalten, die in der Plattform gespeichert werden, und diese Daten effektiver verwalten.

Microsoft empfiehlt den folgenden vierstufigen Prozess, um Daten in der Public Cloud zu identifizieren, zu verwalten, zu schützen und zu dokumentieren:

1. **Identifizieren: Ermitteln Sie, welche verschieden Datentypen existieren und wo sie sich befinden.**
   Um die Datenklassifizierung unserer Kunden zu unterstützen, bietet Microsoft den Azure Information Protection (AIP) service. Azure Information Protection ist eine cloudbasierte Lösung, die einer Organisation hilft, ihre Dokumente und E-Mails zu

klassifizieren, zu kennzeichnen und zu schützen. Dieser Schutz kann automatisch von Administratoren umgesetzt werden, die Regeln und Bedingungen definieren, manuell von Benutzern oder durch eine Kombination aus den beiden Varianten, sodass den Benutzern Empfehlungen gegeben werden.

Die Klassifizierung ist immer erkennbar, unabhängig davon, wo die Daten gespeichert werden oder mit wem sie geteilt werden. Die Labels enthalten visuelle Markierungen wie Kopf- und Fußzeilen oder Wasserzeichen. Metadaten werden im Klartext zu Dateien und E-Mail-Headern hinzugefügt. Der Klartext sorgt dafür, dass andere Dienste, wie etwa Data Loss Prevention-Lösungen, die Klassifizierung erkennen und entsprechende Maßnahmen ergreifen können.

2. **Verwalten: Bestimmen Sie, wie personenbezogene Daten verwendet und abgerufen werden.**
   Der Schutz von Daten wird über Azure Rights Management (Azure RMS) realisiert. Das ist die Technologie, die von AIP verwendet wird und die in andere Microsoft-Cloud-Dienste und Anwendungen wie Office 365 und Azure Active Directory integriert ist. Diese Schutztechnologie verwendet Verschlüsselungs-, Identitäts- und Berechtigungsrichtlinien, um Daten über mehrere Geräte hinweg zu schützen. Der Schutz, der durch Azure RMS angewendet wird, bleibt unabhängig vom Speicherort in den Dokumenten und E-Mails erhalten – innerhalb oder außerhalb Ihres Unternehmens sowie Ihrer Netzwerke, Dateiserver und Anwendungen.

   Mit AIP und RMS behalten Kunden die Kontrolle über ihre Daten, auch wenn diese mit anderen Personen geteilt werden. AIP und RMS sind weltweit verfügbare Dienste, integriert in die Azure-Plattform. Sie können Azure RMS auch mit Ihren eigenen Business-Anwendungen und Informationsschutzlösungen von anderen Softwareherstellern nutzen, und zwar unabhängig davon, ob diese Anwendungen und Lösungen On-Premises oder in der Cloud eingesetzt werden.

3. **Schützen: Etablieren Sie Sicherheitskontrollen, um Schwachstellen und Verletzungen der Datensicherheit zu verhindern, zu erkennen und darauf zu reagieren.**
   Kunden sollen im Rahmen einer effizienten Datenmanagement-Strategie geeignete technische und operative Maßnahmen wählen, um ihre Daten in der Cloud zu schützen. Microsoft bietet Hilfestellungen an, damit Kunden die Anforderungen an regulierte Datenarten erfüllen können. Diese Dokumente sind zum Download auf der Service Trust Platform (STP) verfügbar. Die STP ist eine Erweiterung des Microsoft Trust Center und bietet:

   - Zugriff auf Audit-Berichte über Microsoft-Cloud-Dienste an einer zentralen Stelle,
   - Zugriff auf Compliance-Leitfäden, um zu verstehen, wie Sie Funktionen aus den Microsoft-Cloud-Diensten einsetzen können, um die Einhaltung verschiedener Compliance-Anforderungen zu ermöglichen,
   - Zugriff auf Trust-Dokumente, um Ihnen das Verständnis zu erleichtern, wie Microsoft-Cloud-Dienste helfen, Ihre Daten zu schützen.

   Kunden, die aktive oder Test-Abonnements mit Azure-Konten haben, können direkt auf das STP zugreifen. Neukunden und Interessenten, die die Microsoft-Online-Dienste evaluieren möchten, können auf die STP zugreifen, indem sie sich für eine Testlizenz anmelden.

Überblick über Anleitungen und zentrale Whitepaper-Themen:

Vertical	Region	Angebot	Verfügbar	Ermöglicht den Einsatz in
Öffentliche Verwaltung	Deutschland	Microsoft Azure wird ein C5-Assessment für seine neuen deutschen Rechenzentren durchführen, um Kunden in regulierten Branchen bei der Bereitstellung von gesetzeskonformen Workloads in der Cloud zu unterstützen. Die C5-Attestierung wird den Betrieb von unklassifizierten Cloud-Workloads der öffentlichen Verwaltung in Deutschland vereinfachen.	Microsoft Trust Center	Azure Cloud-Rechenzentren in Deutschland
Öffentliche Verwaltung	Vereinigtes Königreich	Der Crown Commercial Service hat die Microsoft Cloud Services-Klassifizierung für Government Cloud v6 erneuert. Behörden und Partner der Regierung des Vereinigten Königreichs können die zertifizierten Services nutzen, um nationale Regierungsdaten, die als „offiziell" klassifiziert sind, in ausgewählten Rechenzentren von Microsoft Azure zu speichern.	Microsoft Trust Center	Azure Cloud-Rechenzentren im Vereinigten Königreich
Automobil-industrie	Europa	Microsoft hat eine TISAX-Zertifizierung für ausgewählte Azure-Rechenzentren erhalten. Einige sind auch für streng vertrauliche Daten zertifiziert.	ENX Portal	ausgewählten Azure Public Cloud-Umgebungen
Finanzwirtschaft und Versicherungen	Ausgewählte Märkte	Microsoft bietet Whitepaper zum Thema Regulierung in der Finanz- und Versicherungswirtschaft.	Microsoft Trust Center	allen Azure Public Cloud-Umgebungen
Handel	Global	Microsoft führt jährlich ein PCI-DSS Assessment mit einem Qualified Security Assessor durch.	Microsoft Trust Center	Zahlungskartendaten können in der Azure-Plattform gespeichert und verarbeitet werden.
Gesundheits-wesen	Global	Microsoft Azure hat eine Zertifizierung für HITRUST CSF erhalten, die die Bereitstellung von HITRUST-Lösungen in der Cloud ermöglicht. Außerdem hat Microsoft für Azure die Zertifizierung als Hébergeur de données de santé (HDS) erhalten, die das Verarbeiten und Speichern von Gesundheitsdaten in Rechenzentren in Frankreich erlaubt.	Microsoft Trust Center	ausgewählten Azure Public Cloud-Umgebungen
Öffentliche Verwaltung	Australien	Microsoft ist als erster Public Cloud Provider für die Speicherung von Daten in Australien zertifiziert worden, die als „protected" klassifiziert sind.	Microsoft Trust Center	Azure Cloud-Rechenzentren in Australien

Eine detaillierte Übersicht der Zertifizierungen und Compliance-Angebote von Microsoft finden Sie im Trust Center.

4. **Dokumentieren: Sorgen Sie für die Vorhaltung der erforderlichen Unterlagen, die Beantwortung von Datenschutzanfragen sowie Benachrichtigungen bei Sicherheitsvorfällen mit Diebstahl beziehungsweise Offenlegung von Daten.** Das Azure Portal bietet Verantwortlichen in den Firmen ein einfaches, leistungsfähiges Instrument, um die Datenschutzanfragen, die für die Einhaltung der EU-Datenschutz-Grundverordnung (DSGVO) von zentraler Bedeutung sind, schnell zu erfüllen. Kunden können nach relevanten Daten mit dienstspezifischen Data-Discovery-Werkzeugen suchen, auf die per API oder über das Azure-Portal zugegriffen werden kann. Das macht es für Kunden leicht, die für diese Anfragen relevanten Daten zu löschen oder zu pflegen. Details sind in den Referenzdokumentationen der jeweiligen Dienste beschrieben, die Hilfestellung für anwendbare CRUD-Verfahren (Create, Read, Update, Delete: Erstellen, Lesen, Aktualisieren, Löschen) geben.

Speicherorte der Daten

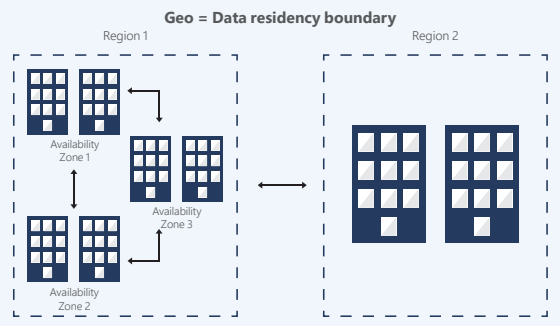
Jede Azure-Region (außer Brasilien) bildet mit einer anderen Region ein „Pair", zusammen bilden sie ein „Regional Pair" oder eine „Geo". Eine Geo kann aus einem oder mehreren Ländern bestehen (Details sind hier beschrieben). Für Azure werden die geplanten Plattform-Updates so koordiniert, dass nur eine Region der Geo zu einem Zeitpunkt aktualisiert wird. Darüber hinaus wird im Falle eines Ausfalls, der mehrere Regionen betrifft, mindestens eine Region pro Geo für die Wiederherstellung priorisiert. Dies verbessert die Resilienz und Verfügbarkeit.

Die meisten Azure-Dienste werden direkt in den regionalen Rechenzentren bereitgestellt. Sie erlauben dem Kunden, die Region auszuwählen, in der der Dienst genutzt werden soll, und geben ihm damit die Kontrolle darüber, wo seine Kundendaten gespeichert werden. Azure Virtual Machines, Azure Storage und Azure SQL Database sind Beispiele für Dienste, die in den regionalen Rechenzentren bereitgestellt werden. Die vollständige Liste kann auf der Website Verfügbare Produkte nach Region eingesehen werden. Für diese Dienste nimmt der Kunde eine Vorauswahl vor, in welcher Region der jeweilige Dienst bereitgestellt werden soll. Der Service kann Kundendaten in andere Regionen innerhalb der Geo replizieren, um die Resilienz des Dienstes zu stärken. Microsoft wird jedoch keine Kundendaten außerhalb dieser Geo replizieren oder übertragen.

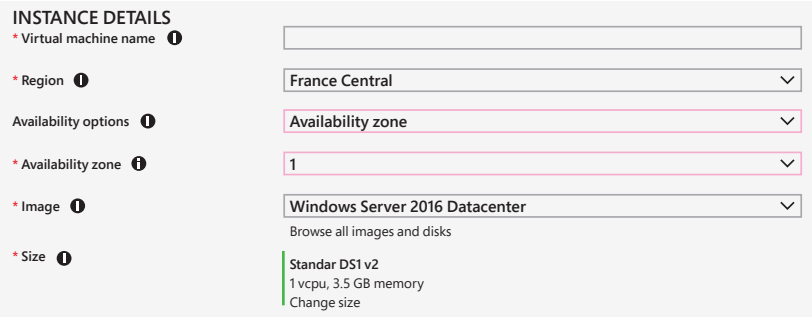
Kunden und ihre Endanwender können jederzeit auf die Daten von jedem Ort aus zugreifen, sie transferieren und kopieren. Das Microsoft Trust Center beschreibt, wo Kundendaten gespeichert werden, und dokumentiert die Ausnahmen auf der Website „Azure Datacenter Map". Beispielhaft erklärt: Wenn ein Kunde den Dienst Azure SQL Database oder Storage in der Region Germany West Central bereitstellt, können die Daten durch den jeweiligen Dienst zu Sicherungszwecken nach Germany North repliziert werden, sie verbleiben aber innerhalb Deutschlands.

Da einige Azure-Dienste (nicht-regionale Dienste) auf einer globalen Architektur basieren, bieten diese nicht die Möglichkeit, die Region auszuwählen, in der der Dienst bereitgestellt werden soll. Falls dies anderweitig nicht spezifiziert ist, können diese Dienste Daten in allen Microsoft-Rechenzentren speichern. Beispiele für solche Dienste sind Azure Active Directory, Azure Content Delivery Networks oder Dienste, die wie Traffic Manager globale Routing-Funktionen bereitstellen und nicht selbst Kundendaten verarbeiten oder speichern.

Informationen über die nicht-regionalen Dienste sind auf der Website „Azure datacenter map website" dokumentiert, und eine Liste der nicht-regionalen Dienste kann auf der Website „Services by Region" eingesehen werden.



Für regionale Dienste kann der Speicherort im Azure-Portal oder über ein ARM-Skript (Azure Resource Manager) festgelegt werden. Wie oben beschrieben, werden die Kundendaten in Ruhe (at Rest) nur in der Geo für diese Region gespeichert.



Die meisten Azure-Dienste werden regional bereitgestellt und ermöglichen dem Kunden, die Region für die Bereitstellung seines Dienstes selbst festzulegen, sodass er die Kontrolle über den Speicherort seiner Daten behält.

Verwendung von Azure-Richtlinien zur Steuerung des Datenspeicherorts

Microsoft bietet den Service Azure Policy an, damit Kunden ein Steuerungs- und Regelungssystem (Governance) für ihre Cloud-Infrastruktur und -Daten implementieren können. Dieser Service ermöglicht unter anderem die Festlegung der Bereitstellung von Diensten, der Monitoring-Anforderungen für Ressourcen oder der Regionen, in denen Ressourcen bereitgestellt werden können. Sobald die entsprechenden Richtlinien etabliert sind, werden nicht nur neue Ressourcen auf Konformität mit der Richtlinie überprüft, sondern es werden alle Ressourcen regelmäßig gescannt, um die Einhaltung der Richtlinien sicherzustellen.

Richtlinien setzen sich aus Regeln zusammen, die beschreiben, wann eine Richtlinie durchgesetzt werden soll und welche Handlung auszuführen ist, wenn die Bedingungen erfüllt sind. Neben der Möglichkeit, eigene Regeln einzurichten und zu verwenden, bietet Azure Policy mehrere vordefinierte Richtlinien, die standardmäßig verfügbar sind. Unter anderem existiert eine Richtlinie für erlaubte Standorte (Allowed Locations), die dazu verwendet werden kann, die Speicherorte zu beschränken, die die Nutzer bei der Bereitstellung neuer Ressourcen auswählen können. Weitere Informationen über Azure Policy finden Sie auf der Website Übersicht über Azure Policy.

Trennung von Instanzen

Die Azure-Plattform nutzt eine virtualisierte Umgebung, in der Cloud-Workloads verschiedener Kunden isoliert auf den gleichen physischen Servern laufen, um die Daten der Kunden in der Multi-Tenant-Umgebung abzusichern. Benutzerinstanzen arbeiten als eigenständige virtuelle Maschinen, die keinen Zugriff auf einen physischen Host-Server haben, und diese Isolation wird durch die Verwendung von physikalischen Prozessor-Privilegien durchgesetzt.

Hypervisors sind so klein wie möglich konzipiert und werden strengen Sicherheitsüberprüfungen unterzogen, um zu verhindern, dass ein Cloud-Workload andere Cloud-Workloads erkennen kann. Für jeden Workload wird ein virtuelles Speichersystem verwendet, das nur die Dateien enthält, die mit seinen eigenen Daten verbunden werden können. Darüber hinaus hat der Hypervisor die volle Kontrolle, um Workloads zu starten, zu stoppen und zu unterbrechen. Er steuert auch die physischen Netzwerkkarten, sodass alle Netzwerkpakete auf Grundlage der Workload-Identität und der Instanz gefiltert werden können. Die physikalischen Speichermedien-Inhalte werden dem Inhaber der Instanz und der verknüpften virtuellen Maschine zugeordnet.

Außerdem können Kunden die Netzwerkverbindung zwischen Servern und Internet steuern und separate virtuelle Netzwerke für verschiedene Zwecke einrichten. Diese können unterschiedliche Anwendungsfälle trennen, zum Beispiel das Produktivsystem sowie Testing- und Entwicklungsumgebungen. Der Infrastruktur-Controller des Hosting-Dienstleisters stellt gemeinsam mit den Hypervisors sicher, dass nur die Cloud-Anwendungen in den gleichen virtuellen Netzwerken einer Instanz ihren gegenseitigen Traffic sehen oder eine gemeinsame Verbindung zum Internet nutzen können.

Weitere Informationen sind im Dokument Isolation in der Azure Public Cloud zu finden.

Identitätsverwaltung

Azure Active Directory (Azure AD) ist der mehrinstanzenfähige, cloudbasierte Dienst für Verzeichnis- und Identitätsverwaltung von Microsoft. Um mehr darüber zu erfahren, wo die Identitätsdaten von Kunden gespeichert werden, nutzen Sie bitte das Wo befinden sich Ihre Daten?-Werkzeug aus dem Microsoft Trust Center.

Hier finden Sie weitere Informationen:

- Microsoft Trust Center
- Microsoft Trust Center: Wo befinden sich Ihre Daten?
- Speicherung von Identitätsdaten für europäische Kunden in Azure Active Directory
- Azure Active Directory Data Security Considerations Whitepaper (Englisch)

Azure Encryption

Verschlüsselung ist eine grundlegende Komponente, um die Vertraulichkeit von Cloud-Workloads zu gewährleisten. Microsoft Azure umfasst mehrere Angebote, um den Schutz von Kundendaten zu steuern und zu kontrollieren, einschließlich Mitteln zur Verschlüsselung von:

- gespeicherten Daten (Data at Rest)
- Daten während der Übertragung (Data in Transit)
- Daten während der Verarbeitung (Data during Processing) – Confidential Computing

Microsoft verwendet mehrere Verschlüsselungsmethoden, Protokolle und Algorithmen in seinen Produkten und Diensten, um einen möglichst sicheren Weg für Daten zu bieten, die sich durch die Azure-Infrastruktur bewegen, und um die Vertraulichkeit von Daten zu schützen, die innerhalb der Infrastruktur gespeichert werden. Microsoft verwendet einige der stärksten, sichersten Verschlüsselungsprotokolle in der Branche, um einen Schutz gegen unbefugten Zugriff auf Ihre Daten zu bieten. Weitere Informationen sind auf der Website Übersicht über die Azure-Verschlüsselung zu finden.

Das richtige Schlüsselmanagement ist ein wesentliches Element der Best Practices zum Thema Verschlüsselung, und mit Azure Key Vault trägt Microsoft dazu bei, dass Schlüssel ordnungsgemäß gesichert sind. Bei der Verwendung von Azure Key Vault und Bring Your Own Key (BYOK) besitzen die Kunden die volle Kontrolle über das Schlüsselmanagement. Beide Konzepte werden weiter unten noch genauer vorgestellt.

Verschlüsselung von gespeicherten Daten (Data at Rest)

Microsoft Azure bietet mehrere Methoden, damit Kunden ihre Speicherinstanzen effektiv schützen können. Empfohlen ist die Nutzung von rollenbasierter Zugriffskontrolle (Role-Based Access Control, kurz RBAC) und Azure Active Directory, um den Zugriff auf die Daten zu steuern.

Erfahren Sie mehr über RBAC und die Zugriffsverwaltung für Cloud-Ressourcen im Dokument Was ist die rollenbasierte Zugriffkontrolle?

Mit der Funktion Storage Service Encryption werden die Kundendaten „at Rest" automatisch beim Schreibvorgang im Azure Storage verschlüsselt. Mit dieser Funktion verschlüsselt die Azure-Speicherplattform die Daten automatisch, bevor sie auf Azure Managed Disks, Azure Blob, Queue oder in Table Storage oder Azure Files geschrieben werden, und entschlüsselt die Daten vor dem Abruf. Der Umgang mit der Verschlüsselung, die Verschlüsselung von gespeicherten Daten, die Entschlüsselung und das Schlüsselmanagement in Storage Service Encryption, erfolgt für den Nutzer transparent. Alle Daten, die auf die Azure-Speicherplattform geschrieben werden, werden durch das 256-Bit-AES-Verfahren, eine der stärksten verfügbaren Blockchiffren, verschlüsselt. Kunden können je nach Bedarf kryptographische Schlüssel konfigurieren, die entweder von Microsoft oder durch sie selbst verwaltet werden.

Erfahren Sie mehr über Storage Service Encryption im Dokument Azure Storage Service Encryption für Data at Rest.

Kunden können mithilfe von Azure Disk Encryption Betriebssystem- und Speicherlaufwerke so konfigurieren, dass diese verschlüsselt von den virtuellen Maschinen von Azure verwendet werden können. Microsoft Azure bietet mehrere Optionen zur Verschlüsselung von Betriebssystem- und Speicherlaufwerken für Windows Server- und Linux-Instanzen. Azure Disk Encryption verschlüsselt Ihre virtuellen Maschinenspeicher unter Windows und Linux als Infrastructure as a Service (IaaS), indem sie die BitLocker-Funktion von Windows und die DM-Crypt-Funktion von Linux nutzt, um die Laufwerkverschlüsselung für die Betriebssystem- und Datenmedien bereitzustellen. Bitlocker verschlüsselt auch Shielded VMs in Windows Server 2016, um sicherzustellen, dass Administratoren der Azure-Infrastruktur nicht auf die Informationen innerhalb der virtuellen Maschine zugreifen können. Die Shielded VMs-Lösung beinhaltet die neue Host Guardian Service-Funktion, die für die Integrität der Virtualisierungsumgebung (Host-Attestation) und das Management der Schlüsselfreigabe verwendet wird.

Weitere Informationen über die Verschlüsselung von Windows- und Linux VM-Laufwerken finden Sie im Dokument Azure Disk Encryption for IaaS VMs.

Zudem stehen weitere Verschlüsselungstechnologien für verschiedene Speichertypen zur Verfügung:

- Transparent Data Encryption (TDE) verschlüsselt Data at Rest, wenn sie in einer Azure SQL Database und Azure SQL Data Warehouse gespeichert sind.
- Die Funktion Always Encrpyted ermöglicht es, Daten innerhalb von Client-Anwendungen zu verschlüsseln, bevor sie in Azure SQL Database gespeichert werden.
- Azure Cosmos DB wird standardmäßig mit einem sicheren Schlüsselverwaltungssystem, verschlüsselten Netzwerken und kryptographischen APIs verschlüsselt. Die Schlüssel werden von Microsoft verwaltet und nach Microsoft-internen Richtlinien variiert.
- Azure Data Lake Storage (ADLS) implementiert eine transparente Verschlüsselung von Data at Rest, vergleichbar mit den Funktionalitäten, die Azure SQL Database zur Verfügung stellt. Azure Data Lake Storage ist standardmäßig aktiviert und verwaltet die Schlüssel standardmäßig für Sie, aber es gibt eine Option für Kunden, die Schlüssel selbst zu verwalten.

Um einen delegierten Zugriff auf die Datenobjekte in Azure Storage zu gewähren, können Sie Shared Access Signaturen (SASs) verwenden. Eine SAS gibt Ihnen modulare Kontrolle über die Art des Zugriffs, den Sie Clients gewähren, zum Beispiel spezifische Berechtigungen und zugelassene IP-Bereiche. Erfahren Sie mehr über SAS im Dokument Nutzung von Shared Access Signaturen (SAS).

Azure Storage Analytics kann zudem die Authentifizierungsmethode nachverfolgen, die jemand beim Zugriff auf den Storage benutzt. Die Protokollierung der Storage Analytics sind standardmäßig für neue Speicherkonten aktiviert. Die Protokollierung kann ebenfalls aktiviert werden, und Sie können sowohl die Protokollierung als auch die Protokollierung im Azure-Portal konfigurieren.

Erfahren Sie im Dokument Storage Analytics mehr darüber, wie Sie dieses Tool aktivieren und verwenden können.

Verschlüsselung von Daten während der Übertragung (Data in Transit)

Microsoft stellt die notwendigen Technologien bereit, damit Azure-Kunden ihre sensiblen Daten bei der Übertragung in die Microsoft-Rechenzentren verschlüsseln können. Microsoft verwendet dafür Transport Layer Security (TLS), die eine Kombination aus asymmetrischer (TLS Handshake) und symmetrischer (Shared Secret) Kryptographie bietet, um Kommunikationsvorgänge zu verschlüsseln, während diese über das Netzwerk transportiert werden. Um unser Anliegen, unseren Kunden die beste Verschlüsselung zur Verfügung zu stellen, zu verwirklichen, wird Microsoft die Unterstützung für die weniger sicheren Transport Layer Security (TLS)-Versionen 1.0 und 1.1 zugunsten der TLS-Version 1.2 einstellen.

Microsoft verwendet auch das Internet Protocol Security (IPsec), ein Industriestandardpaket von Protokollen, um Authentifizierung, Integrität und Vertraulichkeit von Daten auf IP-Paketebene zu gewährleisten, während die Daten über das Netzwerk übertragen werden.

Durch die Investitionen von Microsoft in Forschung und Entwicklung konnte ein Durchbruch bei der Verschlüsselung von Daten während der Übertragung erzielt werden. Jeder Azure-Server enthält Azure Smart NICs, die auf der Field Programmable Gate Array-Technologie (FPGA) basieren. Diese FPGAs sind programmierbare Hardware-Module, die die Verarbeitung von Daten deutlich beschleunigen, einschließlich der Verschlüsselung von Data in Transit. Dies ermöglicht eine hohe Leistung für alle Cloud-Workloads bei geringer Latenz. Microsoft veröffentlicht das Hardware-Design unter einer Open-Source-Lizenz, sodass die Nutzer-Community und Kunden von dieser Innovation profitieren können.

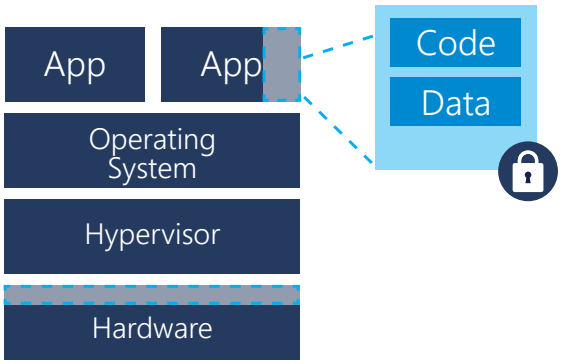
Erfahren Sie mehr über die Hardware-Innovation von Microsoft für die Cloud.

Verschlüsselung von Daten während der Verarbeitung (Data during Processing) – Confidential Computing

Azure Confidential Computing ist ein neues Angebot, das eine zusätzliche Sicherheitsebene für Kundendaten darstellt, während diese auf der Plattform verwendet werden. Es schützt Daten während der Laufzeit und schafft so eine vertrauenswürdige Umgebung für hohe Sicherheitsanforderungen. Confidential Computing bietet Schutzfunktionen für Daten in einer vertrauenswürdigen Ausführungsumgebung (Trusted Execution Environment, kurz TEE), wenn sie sich „im Klartext" (also in einem unverschlüsselten Zustand) befinden, der für eine effiziente Verarbeitung erforderlich ist. Ein Beispiel dazu ist in der Abbildung unten zu sehen.

Confidential Computing bringt TEEs wie Intel SGX und Virtualization Based Security (VBS – früher bekannt als Virtual Secure Mode) in die Cloud. TEEs helfen sicherzustellen, dass niemand von außerhalb Daten und deren Verarbeitung in der TEE einsehen kann, auch nicht mit einem Debugger. Dies unterstützt auch die Kontrolle, dass nur autorisierter Code auf Daten zugreifen darf. Falls der Code geändert oder manipuliert wird, wird die Bearbeitung verweigert und die Umgebung wird deaktiviert. Die TEE erzwingt diese Schutzmaßnahmen während der Verarbeitung der Daten gegen Einsicht und Modifizierung, einschließlich Zugriffen von Microsoft-Mitarbeitern.

Die folgende Abbildung zeigt, wie die TEE Daten und Code während der Verarbeitung schützt.



Weitere Informationen zu Azure-Verschlüsselungstechnologien und -optionen:

- Azure Encryption im Überblick
- Azure Data Encryption-at-Rest
- Best Practices für Azure Data Security und Encryption
- Azure Cosmos DB Encryption
- Storage Service Encryption mit durch Kunden verwalteten Schlüsseln in Azure Key Vault
- Leitfaden für Azure Storage Security
- Azure Confidential Computing

Azure Key Vault mit BYOK (Bring Your Own Key)

Der oben bereits erwähnte Azure Key Vault ist ein Cloud-Service, der eine zentrale Speicherung und Verwaltung von kryptographischen Schlüsseln und anderen geheimen Informationen ermöglicht, die in den Cloud-Anwendungen von Kunden genutzt werden können. Mit diesem Azure-Dienst können Sie Ihre kryptographischen Schlüssel, Zertifikate und Anwendungspasswörter sichern und dafür sorgen, dass geheime Informationen nicht versehentlich offengelegt werden.

Azure Key Vault verwendet spezielle Hardware-Sicherheitsmodule (HSMs) für maximalen Schutz und ist so konzipiert, dass unsere Kunden die Kontrolle über ihre Schlüssel und Daten behalten. Sie können die Verwendung Ihrer gespeicherten Schlüssel auf unterschiedliche Weise überwachen und -prüfen, einschließlich mit Hilfe des Azure Loggings und des Imports dieser Protokolle in Azure HDInsight. Kunden können diese Informationen auch in ihr vorhandenes Sicherheitsinformations- und Eventmanagement

(SIEM) einbinden. Dies unterstützt unsere Kunden bei der Durchführung zusätzlicher Analysetätigkeiten, wie zum Beispiel der Erkennung von Bedrohungen (Threat Detection).

Mit Azure Key Vault können Sie geheime Informationen auf mehrere Vaults aufteilen. Dies trägt dazu bei, die Wahrscheinlichkeit einer unbeabsichtigten Offenlegung von Sicherheitsinformationen aufgrund zentralisierter Speicherung von Anwendungsgeheimnissen zu verringern. Azure Key Vault kann Anfragen und Erneuerungen von Transport Layer Security (TLS)-Zertifikaten verarbeiten. Es bietet auch Funktionen, die ein robustes Lifecycle-Management für die Zertifikate ermöglichen.

Beachten Sie, dass Azure Key Vault entwickelt wurde, um Anwendungsschlüssel und geheime Informationen zu unterstützen. Der Dienst ist jedoch nicht als Ablageort für Benutzerpasswörter gedacht. Der Zugang zu einem Key Vault wird über zwei separate Schnittstellen gesteuert: Die Managementebene und die Datenebene. Die Zugriffskontrollen der beiden Ebenen funktionieren unabhängig voneinander. Kunden sollten spezielle Rollendefinitionen in dem Azure Active Directory verwenden, um einen rollenbasierten Zugriff zu steuern. Mit diesem Ansatz kann eine effektive Aufgabenteilung umgesetzt werden.

Azure Key Vault bietet auch eine Bring Your Own Key (BYOK)-Funktion. An einer Offline-Workstation, die mit einem Thales HSM ausgestattet ist, können Kunden die Schlüssel On-Premises generieren und die Schlüssel dann sicher an die Azure HSMs in der Cloud übermitteln. Die Thales-Software, die für die Schlüsseleingabe verwendet wird, stellt sicher, dass die Schlüssel an diese Umgebung gebunden sind und nicht aus den HSMs extrahiert werden können. Kunden, die zusätzliche Funktionen wie Enterprise-Key-Management-Prozesse oder Hybrid-Cloud-Setups benötigen, können den CipherTrust Cloud Key Manager von Thales nutzen.

Erfahren Sie mehr darüber, wie Sie mit Azure Key Vault geheime Informationen, Zertifikate und Schlüssel schützen können:

- Integration von Azure Key Vault-Protokollen in HDInsights
- Bring Your Own Key – Azure Key Vault

Lösungen für Telemetriedaten

Telemetrie bezeichnet die automatisierte Sammlung von Daten und kann verschiedene Formen annehmen. Bei Cloud-Services, in denen Kundendaten gespeichert und verarbeitet werden, bestehen Telemetriedaten aus Anwendungs- und Serverprotokollen. Diese liefern die Informationen, die von den Kunden benötigt werden, um moderne Anwendungen und Plattformen zu betreiben. Sie erlauben Kunden die Fehlersuche in ihren Cloud-Anwendungen und liefern zugleich Microsoft die benötigten Informationen, um die Platform zu betreiben, Fehler zu beheben und die Systeme zu verbessern.

Microsoft nutzt Telemetriedaten für klar definierte Nutzungsszenarien, die den DSGVO-Vorgaben und den Best Practices entsprechen, wie sie in der ISO/IEC 19944 beschrieben sind. Die Funktionstüchtigkeit des Dienstes ist ein wichtiger Aspekt der Telemetrie-Analyse. Microsoft erfasst schematisierte Telemetriedaten, um Diagnosen für die Plattform durchzuführen und die Ursachensuche von Vorfällen voranzutreiben. Die Dienste machen sich diese Daten zunutze, um Selbstoptimierungs- oder -reparaturprozesse auszulösen, und dies reduziert die Anzahl von notwendigen manuellen Eingriffen. Wenn beispielsweise die Auslastung für eine bestimmte Komponente zunimmt, weist die Plattform mehr Ressourcen zu, um der Nachfrage gerecht zu werden.

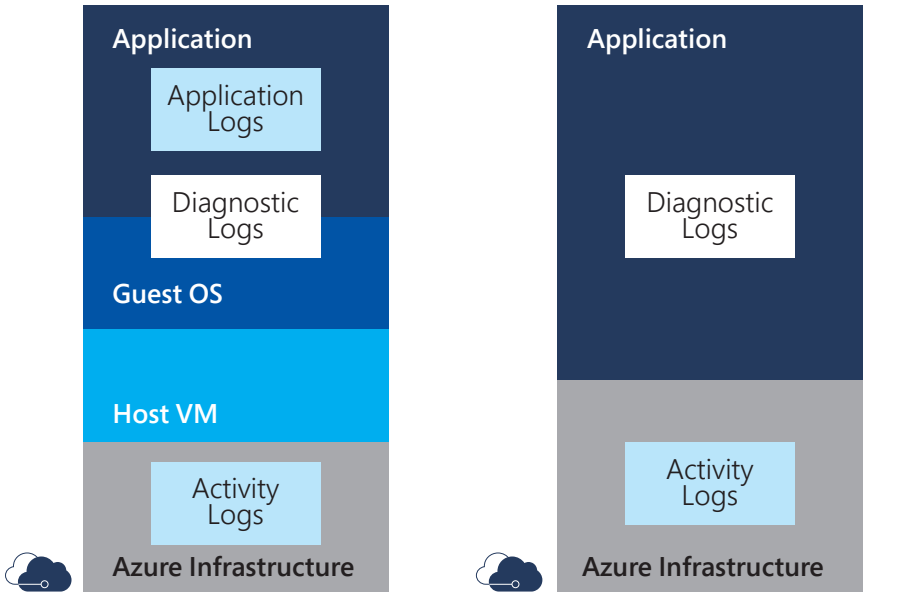
Microsoft hat die anonymisierte Telemetrie in die Azure DevOps-Tools integriert und bietet den Servicemitarbeitern auf diese Weise wertvolle Informationen, um Fehler im Code zu reduzieren. Darüber hinaus werden Telemetriedaten zu Abrechnungszwecken verwendet und an zentrale Fakturierungssysteme übermittelt.

Kunden können die Tools von Microsoft Azure nutzen, um die Funktionstüchtigkeit ihrer Cloud-Workloads zu verwalten. Telemetriedaten werden zum Beispiel von folgenden Diensten erfasst:

- **Azure Monitor:** Dieser Service bietet eine ganzheitliche Sicht auf Ihre Anwendungen sowie auf Infrastruktur und Netzwerk – mit umfassenden Analysewerkzeugen, Dashboards und Visualisierungsübersichten. Azure Monitor bietet einen zentralen Anlaufpunkt, der Kunden dabei hilft, Beeinträchtigungen des Netzwerks, hohe CPU-Auslastungen, Speicherlecks im Code und andere Probleme zu identifizieren, bevor sie ihre Workloads beeinflussen.

- **Application Insights:** Application Insights ist ein erweiterbarer Application Performance Management (APM)-Service für Webentwickler, verfügbar auf mehreren Plattformen. Kunden können ihn nutzen, um Web-Anwendungen während der Laufzeit zu überwachen. Der Dienst erkennt automatisch Leistungsanomalien und umfasst leistungsstarke Analysewerkzeuge, die helfen, Probleme zu diagnostizieren und die tatsächliche App-Nutzung durch die Anwender zu verstehen. Application Insights ist entwickelt worden, um Ihnen dabei zu helfen, die Leistung und Benutzerfreundlichkeit kontinuierlich zu verbessern, indem Telemetriedaten aus Ihren Web-Anwendungen an das Azure-Portal gesendet werden. Der Dienst funktioniert für Apps auf einer Vielzahl von Plattformen, einschließlich .NET, Node.js und J2EE, die entweder im eigenen Rechenzentrum oder in der Cloud gehostet werden. Die Collectors sind so konzipiert, dass sie eine schematisierte Ausgabe von Daten liefern, die Übermittlung personenbezogener Daten so weit wie möglich verhindern und Daten sicher übermitteln. Vom Nutzer muss eine Aufbewahrungsrichtlinie für die Daten festgelegt werden. Kunden können diese Daten auch nutzen, um hochverfügbare Workloads zu erstellen, die einen Vorfall anhand der Telemetrie-Informationen erkennen und automatisierte vordefinierte Maßnahmen durchführen können, um die Auswirkungen abzumildern.

Die folgende Abbildung veranschaulicht die Bereiche, die durch die Protokollierungslösungen abgedeckt werden.



Transparenz und Kontrolle für Kunden
Azure bietet Transparenz und Steuerungsfunktionen für einige der gängigsten Telemetrie-Szenarien unter der Verwendung von Windows Server und mit virtuellen Maschinen unter Linux.

Windows Server VM auf Azure: Telemetrie
Windows Server Images auf Azure sind ähnlich zu den Standard Windows Server Images aufgebaut. Administratoren der Kunden können die Telemetrie-Konfiguration von bestehenden Images (On-Premises) auf die Cloud-Instanzen adaptieren.

Kunden können die Diagnosedaten, die sie mit Microsoft teilen, selbst steuern und hierfür einfach zu bedienende Management-Tools verwenden, die von Microsoft zur Verfügung gestellt werden. Zum Beispiel können Windows Security Baselines verwendet werden, um Windows 10 und Windows Server effizient nach Best-Practice-Empfehlungen zu konfigurieren.

Weitere Informationen dazu finden sich im Dokument Windows security baselines.

Einige Kunden könnten die Verbindungen ihrer Windows-Systeme zu den Microsoft Services minimieren wollen. Sie können hierzu die Funktion „Windows Restricted Traffic Limited Baseline" nutzen, um derartige Verbindungen des Windows Servers zu Microsoft einzuschränken.

Die Windows Restricted Traffic Limited Baseline (ZIP-Datei) kann hier heruntergeladen werden: https://go.microsoft.com/fwlink/?linkid=828887.

Erfahren Sie hier mehr über die Verwendung der Windows Restricted Traffic Limited Baseline-Funktionalität.

Die Einstellungen zur Verwaltung der Diagnosedaten des Windows Servers können mit vertrauten Management-Tools wie Group Policy, MDM, Windows Provisioning oder der Registry konfiguriert werden. Das Setzen der Levels für die Windows Server-Diagnosedaten durch eine Verwaltungsrichtlinie überschreibt alle Einstellungen, die lokal auf einem Endgerät vorgenommen wurden.

Microsoft bietet auch ein PowerShell-Cmdlet an, mit dem von einem Endgerät bereits an Microsoft gesendete Windows-Diagnosedaten gelöscht werden können. Das Cmdlet kann manuell mit der Eingabeaufforderung aufgerufen oder als automatisiertes Skript für virtuelle Maschinen unter Windows Server 2016/2019 implementiert werden.

Weitere Informationen über die Verwaltung von Windows-Diagnosedaten können hier eingesehen werden:

- WindowsDiagnosticData: Dokumentation
- Download: Powershell WindowsDiagnosticData

Linux VM auf Azure: Telemetrie
Für Kunden, die virtuelle Maschinen unter Linux auf Azure betreiben, stellt Microsoft den Linux-Agenten als Open-Source-Software zur Verfügung (WALinuxagent). Dieser ist auf Github erhältlich. Administratoren erhalten volle Transparenz, welche Daten von Linux an die Azure-Plattform gesendet werden. Diese Informationen können korreliert und für weitere Analysen verwendet werden, um wichtige Systemkennzahlen zu überwachen und datenbasierte Entscheidungen zu treffen. Zusätzlich können Protokollanalysen auf Anwendungsebene implementiert werden.

Bei Microsoft sind nahezu alle Serviceoperationen automatisiert, und menschliches Eingreifen wird stets strikt kontrolliert und abseits von Kundeninhalten abstrahiert.

DevOps-Zugriff und Lockbox

Nur in seltenen Fällen benötigt ein Microsoft-Mitarbeiter Zugriff auf Kundendaten, um einen Supportfall zu bearbeiten. Fast alle von Microsoft durchgeführten Service-Operationen sind voll automatisiert, und menschliches Eingreifen wird strikt kontrolliert und von Kundendaten abstrahiert.

Die Entwicklungsvorgaben für Azure Services verlangen einen schematisierten Aufbau der verwendeten Telemetrie. Der wichtigste Anwendungsfall für Telemetrie ist die Verwendung als Sensor für den automatisierten Betrieb der Cloud. Auf Basis der Telemetrie-Informationen und der verlangten Zielkonfiguration werden automatisierte Wiederherstellungs-Maßnahmen ausgelöst. Dies reduziert das zusätzliche Risiko, das durch manuelles menschliches Eingreifen verursacht werden könnte.

Azure wird alle drei Monate von einem AICPA-akkreditierten Prüfbeauftragten (American Institute of Certified Public Accountants) einer SOC-Prüfung (Service Organization Control) unterzogen, um die Wirksamkeit der Sicherheitskontrollen im Prüfungsbereich des Audits zu überprüfen. Der SOC 2 Typ-II-Prüfbericht ist eine von einem akkreditierten Prüfer veröffentlichte Erklärung, die darlegt, unter welchen Umständen der Zugriff auf Kundendaten möglich ist und auf welche Weise dieser erfolgt. Weitere Informationen finden Sie im jeweils aktuellen Audit-Report mit dem Titel „Azure and Azure Government SOC 2 Type II Report". Das bei weitem häufigste Szenario besteht darin, dass ein Kunde mit dem Azure-Support einen Troubleshooting-Prozess beginnt und den Zugang zu Kundenressourcen autorisiert, die möglicherweise Kundendaten enthalten könnten. Für die Mehrheit der Support-Szenarien ist der Zugriff auf Kundendaten nicht erforderlich.

Der Zugang zu Kundendaten wird durch eine rollenbasierte Zutrittskontrolle eingeschränkt, die ausschließlich für diesen geschäftlichen Zweck notwendige Zugriffe erlaubt. Darüber hinaus greifen Methoden wie Multi-Faktor-Authentifizierung, Minimierung des Dauerzugriffs auf Produktivdaten und weitere Kontrollmechanismen. Zugriffe auf die Plattform von Microsoft-Mitarbeitern (DevOps-Personal) werden über das Access-Tool Just-in-time (JIT) angefordert. Alle Zugriffe auf Kundendaten werden protokolliert, und sowohl Microsoft als auch Dritte führen regelmäßige Audits (einschließlich einer Detailprüfung von ausgewählten Zugriffen) durch, um zu bestätigen, dass jeder Zugriff angemessen ist.

Customer Lockbox für Microsoft Azure

Um Kundendaten möglichst weitreichend abzusichern, hat Microsoft die Customer Lockbox für Azure eingeführt. Bei der Customer Lockbox handelt es sich um einen Service, mit dem Kunden kontrollieren können, wie ein Microsoft-Mitarbeiter Zugriffe auf Kundendaten anfordern kann, die in seltenen Fällen notwendig sein können. Als Teil des Support-Workflows kann ein Microsoft DevOps-Mitarbeiter einen erweiterten Zugriff auf Kundeninhalte benötigen. Die Customer Lockbox überlässt dem Kunden die Entscheidung, die Anfrage zu überprüfen, um sie entweder zu genehmigen oder abzulehnen.

Die Customer Lockbox ist eine Erweiterung des Just-in-time-Workflows und bietet eine vollständige Audit-Protokollierung. Der Kunde kann auf die Customer Lockbox-Protokolldateien über das Azure-Portal zugreifen und diese in seine SIEM-Systeme integrieren.

Erfahren Sie mehr über die Customer Lockbox für Azure.

Wie bereits erwähnt: Für die Mehrheit der Support-Szenarien wird kein Zugang zu Kundendaten benötigt, und der Workflow sollte in der Regel keine Nutzung der Customer Lockbox erforderlich machen.

Implementierung von Richtlinien

Microsoft hat eine Reihe interner Richtlinien und technischer Kontrollmechanismen geschaffen, die den Umgang mit Daten regeln. Die Kontrollen und Richtlinien wurden nach dem International Organization for Standardization ISO 27018-Standard entworfen, der den Schutz personenbezogener Daten in öffentlichen Clouds und bei der Verarbeitung durch Cloud-Dienstleister regelt. Für den Anwendungscode wird zum Beispiel jeder Output, der in die Protokolldateien geschrieben wird, durch den Data Scrubber geschickt, der Kundendaten entfernt, bevor diese an zentrale Systeme weitergeleitet werden. Diese Maßnahmen minimieren das Risiko, dass Kundendaten in Analysesysteme oder operative Systeme kopiert werden.

Lösungen für Hybrid- und On-Premises-Umgebungen

Microsoft bietet verschiedene Lösungen an, um intelligentes Edge Computing zu unterstützen. So können Kunden von Cloud-Diensten profitieren, während sie gleichzeitig ihre Daten in der eigenen Infrastruktur – On-Premise – vorhalten und Anforderungen festlegen können, nach denen Daten die eigene Umgebung des Kunden nicht verlassen darf – auch nicht aufgrund von technischen oder regulatorischen Anforderungen.

Microsoft Azure Stack

Microsoft Azure Stack ist eine Erweiterung von Azure. Es ermöglicht die Agilität und Innovation von Cloud Computing in Ihrer lokalen IT-Umgebung und ermöglicht die einzige hybride Cloud, mit der Sie praktisch überall Hybridanwendungen aufbauen und betreiben können. Unternehmen können moderne Anwendungen über hybride Cloud-Umgebungen hinweg aufbauen und dabei das geforderte Gleichgewicht zwischen Flexibilität einerseits und Kontrolle andererseits realisieren.

Entwickler können Anwendungen mit einer konsistenten Auswahl aus Azure-Diensten und DevOps-Prozessen und -Tools erstellen, um die Anwendungen dann in Zusammenarbeit mit dem operativen Bereich an dem Ort bereitgestellt zu stellen, der die geschäftlichen, technischen und regulatorischen Anforderungen bestmöglich erfüllt. Entwickler können die Entwicklung neuer Cloud-Anwendungen beschleunigen, indem sie auf Anwendungskomponenten aus dem Azure Marketplace aufbauen, darunter Open-Source-Tools und -Technologien.

Azure Stack bietet eine umfassende Palette an Werkzeugen und Automatisierungslösungen, die es unseren Kunden ermöglichen, ihre On-Premises-Workloads auf ähnliche Weise wie ihre Cloud-Workloads zu verwalten. Kunden haben die volle Kontrolle über ihre Daten und können Hybrid-Szenarien einrichten, bei denen klassifizierte On-Premises-Workloads sicher mit Workloads in der Cloud interagieren können. Sicherheitsüberlegungen und Compliance-Vorschriften sind wichtige Treiber für Organisationen, die sich für die Kontrolle ihrer Infrastruktur mit privaten/hybriden Clouds und gleichzeitig, um ihre Anwendungen zu modernisieren, für die Nutzung von IaaS- und PaaS-Technologien entscheiden. Azure Stack wurde für diese Szenarien entwickelt, und Sicherheit und Compliance sind Bereiche, in denen für Azure Stack massive Investitionen getätigt wurden und werden.

Erfahren Sie mehr über Azure Stack, indem Sie das Whitepaper Azure Stack: An Extension of Azure (Englisch) herunterladen.

Mehr über die Sicherheits- und Compliance-Kontrollmechanismen in Azure Stack erfahren Sie zudem im Dokument Azure Stack Infrastructure Security Posture (Englisch).

Data Box Edge and gateway

Microsoft hat Hardware-Geräte und virtuelle Maschinen für den On-Premises-Einsatz angekündigt, die Integrationsfunktionen für hybride Workloads bieten. Azure Data Box Edge ist eine Speicherlösung, die KI (künstliche Intelligenz)-Workloads On-Premises vorverarbeiten kann. Es handelt sich um ein physisches System, das sich vor Ort beim

Kunden befindet und das die sichere Datenübertragung beschleunigt. Nur eine Teilmenge von Informationen muss an die Azure Cloud gesendet werden, was dem Kunden die Kontrolle über den Datenfluss und die Datenhoheit gibt. Das System etabliert eine zentral verwaltete und sichere Verbindung zur Cloud. Das Schlüsselmanagement kann vollständig durch den Kunden erfolgen.

Erfahren Sie mehr über Azure Data Box Edge.

III. Compliance-Nachweise

Die Compliance mit regulatorischen Anforderungen und Richtlinien allein ist nicht ausreichend. Unternehmen müssen auch in der Lage sein, die Compliance nachzuweisen. Microsoft kann Unternehmen bei diesem Nachweis, mithilfe von Compliance-Angeboten und -Diensten wie zum Beispiel dem Compliance Manager und mit den Compliance-Commitments in den Online Services Terms (OST) unterstützen. Zusätzlich helfen Azure Security und Compliance Blueprints bei der Bereitstellung von Lösungen in Szenarien, die hohe Compliance-Anforderungen mit sich bringen.

Mit dem Compliance Manager können Kunden ihre eigenen Compliance-Maßnahmen an zentraler Stelle verwalten.

Compliance-Angebote

Microsoft Azure verfügt über ein branchenführendes Compliance-Portfolio. Dieses hilft unseren Kunden, ihre Compliance-Verpflichtungen zu erfüllen. Die Azure Compliance-Angebote sind in vier Kategorien unterteilt: global einschlägig, für US-Regierungsorganisationen, branchenspezifisch und regional/länderspezifisch. Die Compliance-Angebote basieren auf verschiedenen Arten von Commitments, einschließlich formaler Zertifizierungen, Bestätigungen, Validierungen, Genehmigungen und Assessments unabhängiger Prüfgesellschaften sowie individueller Vertragsanpassungen, Selbsterklärungen und Dokumentationen für Kunden, die von Microsoft erstellt wurden.

Erfahren Sie mehr über die umfangreichen Microsoft Azure Compliance-Angebote in dem Whitepaper Overview of Microsoft Azure Compliance (Englisch).

Eine Liste der Compliance-Angebote von Microsoft finden Sie in der Online-Datenbank im Microsoft Trust Center.

Compliance Manager

Der Compliance Manager ermöglicht Kunden die Verwaltung ihrer Compliance-Aktivitäten an einem zentralen Ort. Es handelt sich um eine übergreifende Microsoft-Cloud-Lösung, die Unternehmen dabei unterstützt, die komplexe Compliance-Landschaft zu verstehen und zu verwalten. Organisationen können den Compliance Manager zur kontinuierlichen Durchführung von Risikobewertungen nutzen, und Sie erhalten Empfehlungen, die Ihnen dabei helfen, den Datenschutz zu verbessern und Prozesse durch integrierte Funktionen für die Zusammenarbeit sowie durch Audit-fähige Berichtswerkzeuge zu vereinfachen.

Der Compliance Manager bietet drei Schlüsselfunktionen:

- **Abgleich von Kontrollmechanismen** – DSGVO/GDPR, ISO 27001 und ISO 27018
- **Vereinfachung der Zusammenarbeit** – Compliance-bezogene Aktivitäten delegieren, nachverfolgen und dokumentieren, um eine effizientere Zusammenarbeit zwischen den beteiligten Teams zu ermöglichen
- **Bewertungen und Prüfungen** – Vor-Audits durchführen, um externe Prüfungen vorzubereiten

Um Sie dabei zu unterstützen, die Microsoft Cloud im Rahmen des Shared-Responsibility-Modells zu evaluieren, bietet der Compliance Manager einen Dashboard-Überblick über Bewertungen, der Ihnen klar den Implementierungsfortschritt für die Kontrollmechanismen zeigt, die unter die Verantwortung von Microsoft fallen,

ebenso wie für diejenigen, die unter der Verantwortung Ihres Unternehmens liegen. Die Compliance-Maßnahmen des Compliance Managers sind reine Empfehlungen. Es obliegt dem Kunden, die Wirksamkeit dieser empfohlenen Kontrollmechanismen zu bewerten und zu bestätigen, da sie sich auf das regulatorische Umfeld des Kunden beziehen. Die Umsetzung der Empfehlungen garantiert keinesfalls eine Compliance mit den regulatorischen Anforderungen.

Erfahren Sie mehr über den Einsatz des Compliance Managers, um Datenschutzvorgaben und regulatorische Anforderungen bei der Nutzung von Microsoft-Cloud-Diensten zu erfüllen.

Geschützte Daten

Microsoft Azure bietet Schutzmaßnahmen, die die Anforderungen von vielen lokalen Regulierern rund um den Globus erfüllen können. Zum Beispiel wurde Microsoft in einem IRAP (Information Security Registered Assessors Program)-Assessment geprüft. Diese Zertifizierung bietet Kunden des öffentlichen Sektors in der Regierung Australiens und ihren Partnern die Sicherheit, dass Microsoft über angemessene und effektive Sicherheitskontrollen für die Verarbeitung, Speicherung und Übermittlung sensibler und offizieller Informationen verfügt, die Dissemination Limiting Markings (DLMs) enthalten oder als „protected" klassifiziert sind. Dies umfasst die Mehrheit der Regierungs-, Gesundheits- und Bildungsdaten in Australien.

Erfahren Sie mehr über IRAP-Bewertungen.

Microsoft ist davon überzeugt, dass Privatsphäre ein Grundrecht ist und dass die DSGVO ein wichtiger Schritt nach vorn ist, um die Datenschutzrechte des Einzelnen zu präzisieren und zu stützen.

Datenschutz und die DSGVO / GDPR

Microsoft verpflichtet sich zur Einhaltung der lokalen Datenschutzgesetze und zum Schutz der Privatsphäre seiner Nutzer. Das Compliance-Portfolio von Azure umfasst die Konformität mit Cloud-Datenschutzpraktiken nach den Verfahren ISO/IEC 27018. Zu diesem Engagement gehört auch, dass unsere Produkte und Dienste den Anforderungen, die auf Cloud-Anbieter anwendbar sind, einschließlich der DSGVO, entsprechen.

Microsoft wird alle Gesetze und Vorschriften einhalten, die für die Bereitstellung von Online-Dienste gelten, einschließlich der Gesetze hinsichtlich der Benachrichtigung bei Sicherheitsverletzungen. Microsoft ist jedoch nicht verantwortlich für die Einhaltung von Gesetzen oder Vorschriften, die für die spezifische Branche des Kunden oder den Kunden selbst gelten und die für IT-Dienstleister nicht allgemein anwendbar sind. Microsoft ermittelt nicht, ob Kundendaten Informationen enthalten, die einem bestimmten Gesetz oder einer Verordnung unterliegen.

Microsoft ist davon überzeugt, dass die Privatsphäre ein Grundrecht ist und dass die DSGVO ein wichtiger Schritt nach vorn ist, um die Datenschutzrechte des Einzelnen zu präzisieren und zu stützen. Microsoft ist sich auch bewusst, dass die DSGVO bedeutende Veränderungen bei Organisationen auf der ganzen Welt mit sich gebracht hat, insbesondere im Hinblick auf die Ermittlung, Verwaltung, den Schutz und das Berichten im Zusammenhang mit personenbezogenen Daten, die in einer Organisation erfasst, verarbeitet und gespeichert werden.

Microsoft verpflichtet sich regelmäßig vertraglich zur Erfüllung der DSGVO-Anforderungen – nicht nur in der Europäischen Union, sondern in allen Public-Cloud-Regionen. Microsoft trägt auch aktiv zu den kommenden Datenschutzstandards, wie zum Beispiel ISO/IEC 27522, bei.

Sicherheit

Microsoft unterstützt Kunden beim Thema Sicherheit, unter anderem durch Anwendung des Security Development Lifecycles (SDL), die regelmäßige Durchführung von Penetrationstests von Azure und weitere Methoden, mit denen die Sicherheit in der Cloud-Umgebung verbessert werden soll.

Microsoft Security Development Lifecycle (SDL)

Der Microsoft SDL wurde im Jahr 2004 als integraler Bestandteil des Softwareentwicklungsprozesses bei Microsoft konzipiert und durch verpflichtende interne Richtlinien etabliert. Die Entwicklung, Umsetzung und ständige Verbesserung des SDL stellt eine unserer strategischen Investitionen in die Sicherheit dar.

Der SDL steht für eine Evolution, wie Software konzipiert, entwickelt und getestet wird, und ist inzwischen zu einer klar definierten Methodik gereift. Das Engagement von Microsoft für ein sichereres und vertrauenswürdiges Computing-Ecosystem hat auch zur Erstellung von zahlreichen Leitfäden, Werkzeugen und Schulungsressourcen geführt, die der Öffentlichkeit zugänglich sind.

Erfahren Sie mehr über den Security Development Lifecycle.

Penetrationstests

Microsoft führt kontinuierlich Penetrationstests der Azure-Plattform durch. Um den Penetrationstest zu optimieren, setzt Microsoft auf einen Red-Team-/Blue-Team-Ansatz. Das Red Team konzentriert sich auf den Angriff auf die interne Azure-Infrastruktur, während es Einsatzregeln unterworfen ist. Das Blue Team ist die Abwehrmannschaft, die sich auf reaktive Maßnahmen fokussiert. Seine Mitglieder haben die Aufgabe, Angriffe aufzuspüren und zu verhindern. Zusätzlich zu unserem internen Penetrationstests wird Azure auch jährlichen Penetrationstests durch eine externe, unabhängige Einrichtung unterzogen.

Zusätzlich können Kunden die Penetrationstests selbst oder über eine spezialisierte Firma durchführen lassen. Dazu müssen sie die in den Microsoft Cloud Unified Penetration Testing Rules of Engagement genannten Bedingungen einhalten. Laden Sie die Regeln zur Durchführung von Penetrationstests herunter.

Verpflichtungen, die in den Online Services Terms definiert sind

Wenn Kunden einen Online-Dienst über ein Microsoft Volume Licensing-Programm abonnieren, gelten die Bedingungen zur Servicenutzung, wie sie in dem Volume Licensing Online Services Terms (OST)-Dokumenten und der Programmvereinbarung definiert sind. Da Microsoft regelmäßig neue Dienste hinzufügt, werden die OST monatlich aktualisiert. Es gibt zudem Vertragszusätze, um die Anforderungen in regulierten Branchen, zum Beispiel in der Finanzwirtschaft, abzudecken. Die OST sind in 35 Sprachversionen verfügbar. Ein Archiv ist zugänglich, das ältere Versionen als Referenz enthält.

Erfahren Sie auf der Webseite mit den Lizenzbedingungen mehr über die OST.

Die Online Services Terms decken wichtige Aspekte der Cloud-Nutzung durch unsere Kunden ab, darunter auch:

- **Verpflichtungen zum Datenschutz:** Microsoft hat operative Prozesse implementiert, um die hohen Anforderungen der DSGVO zu erfüllen. Microsoft bietet auch den Abschluss von EU-Standardvertragsklauseln, in den Online Services Terms als Standard Contractual Clauses bezeichnet, die Zusagen bezüglich der Übertragung von personenbezogenen Daten im Geltungsbereich von Microsoft Azure Services enthalten.

- **Technische und organisatorische Maßnahmen:** Microsoft beschreibt und dokumentiert in den Online Services Terms die technischen und organisatorischen Maßnahmen. Diese Maßnahmen sind in der Microsoft Security Policy dargelegt, die als Download im Trust Center zur Verfügung steht. Sie sind konform mit den Anforderungen für Information Security Management Systems (ISMS), wie sie in ISO 27001, ISO 27002 und ISO 27018 definiert sind. Weitere Beschreibungen der technischen und organisatorischen Maßnahmen finden Sie im Microsoft Azure SOC 2 Typ II Assessment-Bericht, der ebenfalls im Trust Center verfügbar ist.
- **Service Level Agreements (SLAs):** Die detaillierten Service-Level-Bedingungen für Microsoft Azure finden Sie auf der Azure-Website.

Blueprints für Sicherheit und Compliance

Microsoft Azure bietet eine Reihe von Sicherheits- und Compliance-Blueprints, die unsere Kunden in stark regulierten Märkten unterstützen, um gesetzeskonforme Cloud-Architekturen zu erstellen. Die Blueprints beinhalten auch Best Practices und Muster für verschiedene Compliance-Kontrollmechanismen, die es unseren Kunden ermöglichen, die neuesten Technologien und die modernste Sicherheit für ihre Workloads zu nutzen.

Diese Blueprints liefern detaillierte Bereitstellungsanleitungen, einschließlich Richtlinien zur Automatisierung, sowie Architekturdiagramme und Dokumentation. Sie liefern auch Bedrohungsmodelle, die den Risikomanagement-Prozess unterstützen und auf potenzielle Risiken hinweisen, wenn Kunden Änderungen vornehmen.

Die Azure Security und Compliance Blueprints können im Abschnitt „Compliance" von der Website zur Azure Security Documentation abgerufen werden.

Microsoft hat eine starke öffentliche Haltung zum Schutz von Kundendaten vor unangemessenen Zugriff durch Regierungen eingenommen, und wenn nötig wurde diese Position auch vor Gericht verteidigt. Microsoft wird weiterhin auf neue internationale Abkommen drängen, die die Rechte der Kunden weiter stärken.

Wie Microsoft mit staatlichen Anfragen umgeht

Microsoft hat eine starke öffentliche Haltung bezüglich des Schutzes von Kundendaten vor unangemessenem Zugriff durch Regierungen eingenommen, und wenn nötig wurde diese Position auch vor Gericht verteidigt. Microsoft wird weiterhin auf neue internationale Abkommen drängen, die die Rechte der Kunden weiter stärken.

Wenn Microsoft eine Anfrage seitens der Regierung oder von Strafverfolgungsbehörden nach Kundendaten erhält, versucht Microsoft, die Anfrage der Behörde weiterzuleiten, um die angeforderten Daten vom Kunden direkt zu erhalten. Um diesen Vorgang zu erleichtern, kann Microsoft die regulären Kontaktdaten des Kunden zur Verfügung stellen. Microsoft wird den Kunden unverzüglich über jede Anfrage Dritter informieren und dem Kunden eine Kopie zur Verfügung stellen, soweit dies zulässig ist. Für rechtsgültige Anfragen, bei denen Microsoft nicht in der Lage ist, diese an den Kunden weiterzuleiten, legt Microsoft die Kundendaten nur im Falle einer gesetzlichen Verpflichtung offen und wird immer sichergehen, nur die Kundendaten herauszugeben, die von der jeweiligen Anordnung verlangt werden.

Microsoft hat sich zur Transparenz verpflichtet und stellt auf der Law Enforcement Request Report-Webseite zentral alle Berichte zur Verfügung, die Microsoft regelmäßig bei Anfragen nach Kundendaten durch Strafverfolgungsbehörden veröffentlicht, einschließlich staatlicher Anfragen im Zusammenhang mit der nationalen Sicherheit der Vereinigten Staaten von Amerika.

Die gesammelten Daten, die Microsoft veröffentlicht hat, zeigen deutlich, dass nur ein winziger Prozentsatz der Kunden von Microsoft – ein Bruchteil eines Prozents – jemals einer behördlichen Anforderung im Zusammenhang mit dem Strafrecht oder der nationalen Sicherheit unterworfen war. Für Unternehmenskunden sinkt diese Zahl weiter auf eine Handvoll.

IV. Anwendung des Frameworks für ausgewählte europäische Märkte

Der allgemeine Sicherheits- und Compliance-Framework, das in diesem Whitepaper dargelegt wurde, kann auf verschiedene geografische Märkte konkreter angewendet werden. In den folgenden Abschnitten wird die Anwendbarkeit auf den deutschen und französischen Markt diskutiert.

Frankreich

Microsoft betreibt zwei Azure-Rechenzentrumsregionen in Frankreich, um seinen Kunden eine Plattform zur Bereitstellung ihrer Workloads in unmittelbarer Nähe ihrer Kunden in Frankreich zu bieten.

Datenschutz

Dank der Compliance-Bemühungen von Microsoft in Bezug auf die DSGVO können personenbezogene Daten, wie im französischen Datenschutzgesetz (FDPA und die Erweiterung FDPA2) definiert und von der CNIL (Commission Nationale de l'Informatique et des Libertés) reguliert, in allen Public-Cloud-Rechenzentren von Azure gespeichert werden. Kunden müssen die Compliance des Datenstandortes, je nach Klassifizierung der Daten, im Voraus beurteilen. Der Abschnitt zum Thema geteilter Verantwortung in diesem Whitepaper bietet zusätzliche Hilfestellung für die Ermittlung der geeigneten technischen und organisatorischen Maßnahmen, die für den Schutz personenbezogener Daten erforderlich sind.

Regulierung der Finanzbranche

Microsoft bietet eine Checkliste mit Anleitungen zur Erfüllung der regulatorischen Anforderungen der Finanz- und Versicherungsbranche für die Kunden an, die durch die Autorité des Marchés Financiers (AMF) und die Autorité de Contrôle Prudentiel et de Résolution (ACPR) reguliert sind.

Die Checkliste kann vom Service Trust Portal heruntergeladen werden.

Hébergeur de Données de Santé (Hosting von Gesundheitsdaten)

Microsoft hat am 31. Oktober 2018 als erster Cloud-Anbieter die Zertifizierung als Hébergeur des données de santé für das Azure-Rechenzentrum in Frankreich erhalten. Cloud-Services tragen dazu bei, die französischen IT-Systeme im Gesundheitswesen zu modernisieren und den Service für die Patienten zu verbessern. Organisationen aus den Bereichen Life Science und Gesundheitswesen können zentrale Azure-Dienste nutzen, um Gesundheitsdaten in ihren Cloud-Anwendungen zu verarbeiten.

TISAX (Trusted Information Security Assessment Exchange)

Die europäische Automobilindustrie hat den TISAX-Standard (Trusted Information Security Assessment Exchange) geschaffen, um einen gemeinsamen Bewertungsrahmen für alle Zulieferer zu etablieren. Microsoft hat die TISAX-Zertifizierung für spezifische Microsoft-Rechenzentren auf Level 2 (AL2) durch einen unabhängigen Auditor erhalten. Ein AL2-Assessment ist für Daten mit hohem Schutzbedarf erforderlich, das heißt für Daten, die als vertraulich klassifiziert sind. Der TISAX-Prüfbericht kann von den Mitgliedern über das ENX (European Network Exchange)-Portal abgerufen werden.

Compliance-Mapping für Azure-Regionen in Frankreich

Branche	ISO 27001 Validierung von Sicherheits-kontrollen und ISMS	ISO 27018 Schutz von personenbezogenen Daten	Checkliste für die Finanzbranche	SOC 2 Typ II Unabhängige Bewertung der AICPA SOC-Kontrollmechanismen	TISAX Unterstützung klassifizierter Workloads für die Automobilindustrie
Öffentliche Verwaltung	✓	✓		✓	
Finanzen/ Versicherungen	✓	✓	✓	✓	
Automobil-industrie	✓	✓		✓	✓
Gesundheits-wesen	✓	✓		✓	

Deutschland (neue Regionen)

Microsoft Azure bietet Lösungen, die Kunden dabei unterstützen, ihre Compliance-Anforderungen zu erfüllen. Hier finden Sie Informationen für den deutschen Markt im Vorfeld der Einführung der neuen deutschen Regionen im Jahr 2019, die von den leistungsstarken Sicherheitslösungen und Kontrollmechanismen der globalen Azure Public Cloud profitieren werden.

IT-Sicherheitsgesetz

Alle Microsoft Azure-Rechenzentren auf deutschem Boden werden als kritische Infrastruktur im Sinne des IT-Sicherheitsgesetzes angemeldet. Unabhängige Prüfungen von qualifizierten Auditoren werden verwendet, um die Einhaltung dieser Verordnung für die in Deutschland eingesetzten Microsoft Azure-Dienste anzustreben.

C5-Compliance-Attestierung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat „Cloud Computing Compliance Controls Catalog (C5)" eingeführt, der die Anforderungen für die Cloud-Sicherheit für regulierte Märkte, insbesondere für die öffentliche Verwaltung und die Finanz- und Versicherungsbranche, beschreibt. Microsoft Azure wird ein C5-Assessment für die deutschen Rechenzentren anstreben, das die regulierten Branchen dabei unterstützt, gesetzeskonforme Workloads in der Cloud bereitzustellen. Die C5-Attestierung würde den Einsatz von nicht klassifizierten Workloads durch Kunden aus dem deutschen öffentlichen Sektor in der Cloud vereinfachen.

IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik hat die Vorgehensweise IT-Grundschutz entwickelt. Diese besteht aus einem nach ISO 27001 kompatiblem ISMS (BSI Standards 200-1, 200-2) und einer speziellen Methode zur Risikoanalyse (BSI Standard 200-3).

Microsoft plant, zusammen mit einem Partner ein Arbeitshandbuch zu erstellen, das Microsoft Azure-Kunden hilft, die mit Azure-Diensten die IT-Grundschutz-Methodik im Rahmen ihrer bestehenden oder geplanten ISO 27001-Zertifizierung auf Basis des IT-Grundschutzes implementieren möchten.

Datenschutz

Dank der Bemühungen, die Microsoft in die DSGVO investiert hat, können personenbezogene Daten, wie sie im Bundesdatenschutzgesetz (BDSG-neu) definiert sind, in allen Public-Cloud-Rechenzentren von Azure gespeichert werden. Kunden müssen die Compliance des Datenstandortes, je nach Klassifizierung der Daten, im Voraus beurteilen. Der Abschnitt zum Thema geteilter Verantwortung in diesem Whitepaper bietet zusätzliche Hilfestellung für die Ermittlung der geeigneten technischen und organisatorischen Maßnahmen, die für den Schutz personenbezogener Daten erforderlich sind.

TISAX (Trusted Information Security Assessment Exchange)

Die europäische Automobilindustrie hat den TISAX-Standard (Trusted Information Security Assessment Exchange) geschaffen, um einen gemeinsamen Bewertungsrahmen für alle Zulieferer zu etablieren. Microsoft plant die TISAX-Zertifizierung für Azure Deutschland. Der TISAX-Prüfbericht für europäische Länder kann von den Mitgliedern über das ENX (European Network Exchange)-Portal abgerufen werden.

Compliance-Mapping für Azure-Regionen in Deutschland

Branche	IT Sicherheitsgesetz	BSI C5 Attestierung für BSI C5-Anforderungen	ISO 27001 Validierung von Sicherheits-kontrollen und ISMS	ISO 27018 Schutz von personenbezogenen Daten	Grundschutz-Arbeitshandbuch Unterstützt unsere Kunden bei dem Mapping der bestehenden Sicherheitskontrollen von Azure auf ihre Grundschutz- ISMS	SOC 2 Typ II Unabhängige Bewertung der AICPA SOC-Kontrollmechanismen	TISAX Unterstützung klassifizierter Workloads für die Automobilindustrie
Öffentliche Verwaltung	✓	✓	✓	✓	✓	✓	
Finanzen/ Versicherungen	✓	✓	✓	✓	✓	✓	
Automobil-industrie	✓		✓	✓		✓	✓
Gesundheits wesen	✓	✓	✓	✓	✓	✓	

Fazit

Dieses Whitepaper gibt Einblicke in wichtige Sicherheitsangebote der Azure-Plattform und zeigt Kunden in regulierten Branchen auf, wie sie gesetzeskonforme Workloads in der Azure Public Cloud realisieren können, einschließlich in den neuen Regionen Deutschland, Frankreich und anderen öffentlichen Azure-Regionen.

Microsoft fügt kontinuierlich Funktionen und Dokumentationen hinzu, die es Kunden ermöglichen, ihre Compliance-Anforderungen zu erfüllen, und die Transparenz hinsichtlich der Vorgehensweisen und Prozesse bei Microsoft schaffen. Dieses Whitepaper wird aktualisiert, sobald neue Funktionen verfügbar werden.


Microsoft