Eine klare Datensichtbarkeit kommt von der Cloud

JOKERPRO/GETTY

Multi-Cloud-SaaS-Beschleuniger für Ihre DSGVO-Bereitschaft

Ein glasklarer - und gesamtheitlicher - Blick auf alle von einer Organisation gehaltenen personenbezogenen Daten ist extrem wichtig dafür, Compliance mit der zukünftigen Datenschutz-Grundverordnung sicherzustellen und schwere Strafen zu vermeiden.

Viele Organisationen stehen vor der Herausforderung, dass sie personenbezogene Daten besitzen, die in verschiedenen Cloud-Umgebungen residieren. Sobald die Datenschutz-Grundverordnung (DSGVO) im Mai 2018 in Kraft tritt, müssen Organisationen dazu in der Lage sein, Anforderungen zu erfüllen, Governance von personenbezogenen Daten unter Beweis zu stellen und nachzuweisen, dass sie personenbezogene Daten geschützt und sicher verwahren.

Organisationen müssen in der Lage sein, personenbezogene Daten zu erfassen, sodass sie wissen, welche Daten wo residieren und wie sie verarbeitet werden. Zugriffsrechte auf diese Daten müssen mit Prüfprotokollen ausgestattet werden, um Compliance zu belegen. Als bestes Verfahren für Datenschutz durch Technik sollten Daten verschlüsselt und, falls notwendig, maskiert werden, um die Wiederidentifizierung von Datensubjekten zu verhindern. Im Falle einer Datenschutzverletzung muss diese innerhalb von 72 Stunden gemeldet werden.

Eine transparente Datenkontrolle ist extrem wichtig, um DSGVO-Anforderungen zu erfüllen und dafür, Datenverarbeitungsaktivitäten die Bestimmungen verletzen zu verhindern. Dies kann zu Strafen von bis zu 20 Millionen Euro oder 4% des Gesamtertrags führen, je nachdem was höher ist.

Datenkontrolle

Eine transparente Datenkontrolle ist extrem wichtig für die Erfüllung der DSGVO-Verpflichtungen und dafür, Datenverarbeitungsaktivitäten die Bestimmungen verletzen zu verhindern. Dies kann zu Strafen von bis zu 20 Millionen Euro oder 4% des Gesamtertrags führen, je nachdem was höher ist.

Organisationen brauchen auf ihrem Weg zur DSGVO-Compliance klare Datensichtbarkeit und einen gesamtheitlichen Blick auf die Sicherung aller personenbezogenen Daten.IBMs Multi-Cloud-Software as a Service (SaaS)-Beschleuniger für DSGVO-Bereitschaft können dabei helfen, diesen Prozess zu beschleunigen.

Unabhängig davon, wo Daten physisch gespeichert werden, bleibt die Organisation bei dem Datenverantwortlichen, der die Letztverantwortung für jedweden Verstoß gegen die DSGVO trägt. Dieser muss deswegen einen kompletten Überblick über alle Daten in der durch dritte Datenverarbeiter betriebenen Cloud besitzen. Der Einsatz von Sicherheitsfähigkeiten zur Verfolgung und Verschlüsselung von Daten ist notwendig - auch wenn ein dritter Cloud-Datenverarbeiter, integrierte Sicherheit anbietet.

Ravi Srinivasan, Vizepräsident für Strategie und Angebotsmanagement bei IBM Security, sagt: „Viele Organisationen betreiben ihr Geschäft in einer Multi-Cloud-Umgebung und sind als Datenverantwortliche Risiken ausgesetzt. Sie schulden den Stakeholdern und den Regulierungsbehörden Rechenschaft, und wenn sie weiterhin ein digitaler Betrieb bleiben wollen, sollten sie Sicherheit und Datenschutz in einer Multi-Cloud-Umgebung im Blick behalten."

Drei Schritte zur Bereitschaft

Der von IBM Security empfohlene Ansatz umfasst drei Komponenten auf dem Weg zur DSGVO-Bereitschaft.

„Es gibt drei Elemente für die DSGVO-Bereitschaft in einer Multi-Cloud-Umgebung - das Auffinden von Daten und den assoziierten Risiken, das Sichern von Datenzugriffen, die verwendet werden und Risiken ausgesetzt sind, und die Fähigkeit, auf einen Vorfall, wie einen Alarm oder eine Verletzung reagieren zu können", sagt Srinivasan.

IBM Security kann Organisationen, die eine hybride oder Multi-Cloud-Umgebung nutzen, bei solchen Herausforderungen durch seine Multi-Cloud-SaaS-Beschleuniger-Angebote helfen, die zur DSGVO-Bereitschaft beitragen. Sie können vor Ort, in der IBM Cloud und in anderen Cloud-Umgebungen, wie Amazon Web Services, Microsoft Azure, Google Cloud und Oracle Cloud, eingesetzt werden.

Da Unternehmen immer häufiger Umgebungen mit mehreren Clouds nutzen, ist die Fähigkeit, personenbezogene Daten und die assoziierten Risiken, unabhängig davon, wo diese angesiedelt sind, zu identifizieren, sehr wichtig, und IBM hilft Organisationen bei dieser Herausforderung.

IBM Guardium deckt die personenbezogenen Daten in Clouds von Dritten auf und besitzt eine vollständige Palette von Fähigkeiten, von Entdeckung und Klassifizierung bis hin zu Verwundbarkeitsbewertung, sowie die Überwachung und Alarmierung der auf die DSGVO ausgerichteten Meldeabläufe.

„Organisationen möchten Daten in ihrem alltäglichen Geschäft weiter nutzen. IBM Guardium kann dabei helfen, Daten zu verfolgen und zu verschlüsseln, sodass sie in laufenden Geschäftsvorgängen in Multi-Cloud-Umgebungen verwendet werden könne, während gleichzeitig Schritte in Richtung DSGVO-Bereitschaft unternommen werden“, sagt Srinivasan.

Erfassung von Datenzugriffen

Als Datenverantwortlicher kann die Organisation unter Beweis stellen, dass sie die Kontrolle über die von ihr gehaltenen Daten besitzt, und dass keine Drittpartei mit schlechten Absichten auf diese Daten zugreifen kann.

Indem sie den Datenzugriff auf die Geschäftsbereiche, die sie besitzen und verwenden, erfassen, können Entscheider ihre Prozesse ändern, wo dies nötig ist, um die DSGVO zu erfüllen.

Als Datenverant-wortlicher kann die Organisation unter Beweis stellen, dass sie die Kontrolle über die von ihr gehaltenen Daten besitzt, und dass keine Drittpartei mit schlechten Absichten auf diese Daten zugreifen kann.

IBM Guardium findet und klassifiziert personenbezogene Daten in Clouds von Drittanbietern und verfolgt und verschlüsselt sie, um die Transparenz zu maximieren.

VEGE/ADOBE

IBMs Agile 3-Lösungen helfen dabei, die mit Geschäftsbereichen assoziierten Risiken zu erfassen, sodass gezielte Zugriffsrichtlinien eingesetzt werden können. Informationen können weiterhin gesammelt und genutzt werden, aber einige Elemente können maskiert werden. Zum Beispiel können persönliche Einstellungen innerhalb einer E-Mail maskiert werden, sodass die gesammelten Daten weiterhin durch die Firma genutzt werden können.

„Geschäftsbereiche können Prozesse ändern, um auf dem Weg zur DSGVO-Bereitschaft zu helfen. Indem ein gesamtheitlicher Blick auf die Daten angeboten wird, wird der Fokus auf diese Daten gerichtet, sodass die Firma handeln und Geschäftspraktiken ändern kann. Falls nötig können sie den Zugriff komplett unterbinden, um die Identity Governance-Anforderungen in der DSGVO zu erfüllen“, sagt Srinivasan.

Mit nur 72 Stunden, um das Ausmaß einer Datenschutzverletzung zu bestimmen und die Regulierungsbehörde und die Betroffenen zu informieren, ist es wichtig zu wissen, welche Daten sich wo befinden, um eine schnelle Reaktion zu ermöglichen. Wenn Sie Daten generell verschlüsseln, kann es sein, dass Sie das Datensubjekt nicht informieren müssen, wenn die Regulierungsbehörde dies als unnötig erachtet. IBM Resilient unterstützt eine beschleunigte Reaktion auf Vorfälle, während ein Unternehmen den durch die DSGVO vorgeschriebenen Zeitrahmen einhält und die richtigen Personen informiert, sodass gehandelt und der Vorfall schnell angegangen werden kann.

Analyse und Sicherheit

IBMs Analysewerkzeuge ergänzen ihre Sicherheitswerkzeuge, um beim Erreichen von DSGVO-Bereitschaft zu helfen.

Die Fähigkeit, Daten, die sich in der Cloud befinden, zu erfassen, verbessert die Katalogisierung, sodass die Organisation genau weiß, welche Daten sich wo befinden.

„Ein Information Governance-Katalog bietet einen Einblick in Daten, die in Multi-Cloud-Umgebungen residieren, und wird eine wichtige Quelle für Fakten, was sehr wichtig für die DSGVO-Bereitschaft ist“, sagt Richard Hogg, Globaler Sprecher für DSGVO- und Governanceangebote bei IBM Cloud.

IBM InfoSphere Optim Data Privacy bietet einen Werkzeugkasten, mit dem Organisationen notwendige Maßnahmen im Zusammenhang mit der DSGVO-Bereitschaft im Hinblick auf strukturierte Daten vornehmen können, wie etwa die Maskierung von personenbezogenen Daten, sodass Datensubjekte nicht identifizierbar sind.

„Organisationen möchten genaue, vertrauenswürdige Informationen besitzen, sodass sie auf einer soliden Grundlage eine persönlichere und vertrauensvollere Beziehung zu jedem Kunden aufbauen können“, sagt Hogg.

Wenn Sie mehr darüber erfahren möchten, wie Multi-Cloud-SaaS-Beschleuniger für die DSGVO-Bereitschaft Ihrer Organisation helfen können, besuchen Sie unsere Website oder kontaktieren Sie Ihren IBM-Vertreter.

Erfahren Sie hier mehr über den Weg zur DSGVO-Bereitschaft bei IBM selbst und über unsere DSGVO-Fähigkeiten und Angebote zur Unterstützung auf Ihrem Weg zur Compliance.

IBMs Analysewerkzeuge ergänzen ihre Sicherheitswerkzeuge, um beim Erreichen von DSGVO-Bereitschaft zu helfen. Die Fähigkeit, Daten, die sich in der Cloud befinden, zu erfassen, verbessert die Katalogisierung, sodass die Organisation genau weiß, welche Daten sich wo befinden.