PRESSEMITTEILUNG

Erste Warnungen in Europa vor US-Clouds

Norwegen und Dänemark warnen vor US-Cloudanbietern. Werden Deutschland und weitere europäische Länder diesem Beispiel folgen? Wann werden Regeln zum Datenschutz verschärft und wie können Unternehmen diese Hürde meistern?

Dass zunehmend mehr Unternehmen und Organisationen viele ihrer sensiblen Daten bei US-basierten Cloud-Anbietern speichern und verarbeiten, ist mangels europäischer Alternativen Fakt. Aktuelle politische Trends in den USA veranlassen jedoch europäische Sicherheitsbehörden zu deutlichen Warnungen, da die Daten auch dort nicht mehr sicher sein könnten. Im schlimmsten Fall könnte die Verarbeitung und Speicherung sensibler Daten in den US-Clouds sogar gemäß der europäischen Sicherheitsgesetzgebung unzulässig werden. Die proaktive Lösung des Problems kann eine funktionserhaltende Verschlüsselung sensibler Daten sein – egal für welche Cloud und egal wo auf der Welt.

Europäische Datenschutzexperten sind besorgt und mit Norwegen und Dänemark schlagen die ersten beiden Länder offiziell Alarm. Die norwegische Datenschutzbehörde hat die klare Empfehlung ausgesprochen, dass Unternehmen eine Strategie vorbereiten sollten, wie sie mit amerikanischen Cloud-Diensten umgehen, falls der Datentransfer in die USA plötzlich nicht mehr zulässig ist. Eine ähnliche offizielle Empfehlung der dänischen Datenschutzbehörde nur einige Tage zuvor betont, dass sich Unternehmen nicht auf den aktuellen Angemessenheitsbeschluss verlassen dürfen, da die rechtliche Lage viel zu unsicher sei.

Dass deutsche Datenschutzbehörden mit einer vergleichbaren Warnung nachziehen, ist wahrscheinlich. Die deutschen Aufsichtsbehörden standen in der Vergangenheit bei vielen Risikoeinschätzungen und Datenschutzinitiativen Seite an Seite mit den europäischen Partnerstaaten. Bereits jetzt lassen Aufsichtsbehörden keinen Zweifel daran, dass deutsche Unternehmen sich nicht auf langfristige Rechtssicherheit beim Einsatz von US-Cloud-Diensten verlassen sollten. Sie haben in der Vergangenheit immer wieder betont, dass der Schutz personenbezogener Daten oberste Priorität hat – auch wenn dies für Unternehmen unbequem in der Umsetzung ist.

Ein gesamteuropäisches Problem

Die jüngsten Warnungen der beiden nordeuropäischen Länder begründen sich auf einem zentralen und für gesamt Europa existenten Risiko: Sollten sich europäische Unternehmen zu stark an US-Cloud-Dienste binden, stehen diese bei einem plötzlichen Wegfall der Rechtsgrundlage vor einer Herausforderung, die sowohl die Sicherheit der Unternehmen, aber auch deren Handlungsfähigkeit elementar stören kann. Das Problem liegt darin, dass für viele US-Clouddienste keine europäischen Alternativen existieren. Beschlüsse oder regulatorische Entscheidungen, die den Transfer sensibler Daten in die USA untersagen, würden die Nutzung vieler Cloud-Dienste, auf die Unternehmen im Tagesgeschäft angewiesen sind, abrupt unterbrechen. Mit einem Verbot der Datenflüsse werden kritische Arbeitsprozesse unterbrochen, was in den meisten Fällen zu Betriebsunterbrechungen und in Folge zu Reputationsschäden führen kann.

Sollten offizielle Regelungen und Handlungsanweisungen in den europäischen Staaten oder aus Brüssel heraus konkretisiert und in einem neuen Regelwerk manifestiert werden, müssen viele Unternehmen sehr kurzfristig handeln – insbesondere dann, wenn geschäftskritische Prozesse ausschließlich mit Cloud-Diensten von US-Unternehmen durchgeführt werden. Die kurzfristigen Konsequenzen derartiger Neuregulierungen sind gravierend. Dazu gehören

- die sofortige Neubewertung bestehender Verträge mit US-Cloud-Anbietern,
- die Risikobewertungen für alle Datenflüsse in die USA,
- das Erstellen und Umsetzen von Plänen für die Gewährleistung der Datensicherheit,
- ein enorm hoher Zeitdruck, da Datenschutzbehörden in solchen Fällen kurze Fristen setzen,
- und die wesentlich strengere Prüfung bei künftigen Cloud-Projekten, ob diese den Datenschutzanforderungen entsprechen.

Jetzt vorbereiten, anstatt auf den heftigen Einschlag zu warten

Warten ist in der aktuellen Abhängigkeitssituation keine gute Option. Das weitreichende und zu einem Teil berechtigte Vertrauen in die Cloud- und IT-Partner in den USA steht im Moment jedoch zunehmend auf der Kippe und die Wahrscheinlichkeit, dass sich die europäischen Datenschutzorgane zugunsten der Sicherheit der europäischen Wirtschaft aussprechen, ist groß.
Noch haben die Unternehmen gute Chancen, die Weichen zu ihren Gunsten zu stellen. In einem ersten Schritt sorgt eine Dateninventur für das valide Wissen darüber, welche Daten mit welchen Grad

an Sensibilität wo verarbeitet und gespeichert werden. Darüber hinaus gilt es zu prüfen, welche Prozesse unausweichlich mit Anbietern aus den USA durchgeführt werden müssen und welche vielleicht anders organisiert oder mit europäischen Anbietern umgesetzt werden könnten. Danach folgen möglichst rasch die Strategie und konkrete Pläne, wie sich kritische Daten kurzfristig schützen lassen. Dabei steht immer die maximale Datensouveränität im Vordergrund, bei der mit geeigneten Technologien und Diensten sichergestellt ist, dass der Schutz und der Zugriff auf Unternehmensdaten stets unter eigener Kontrolle bleiben.

Verschlüsselung erfüllt Regulatorik und Compliance auch unter besonderen Umständen

Da es in einigen Fällen an Alternativen und Optionen zu den US-basierten Cloud-Anwendungen und -Diensten mangelt und keine kurzfristigen Ausweichmöglichkeiten bestehen, ist die gezielte Verschlüsselung ein probates und vor allem sicheres Mittel, um die Regulatorik und Compliance einzuhalten. Bei einer geeigneten Datenverschlüsselung wird sichergestellt, dass der Klartext ausschließlich im Unternehmen verbleibt – auch wenn die Speicherung und Datenverarbeitung weiterhin bei nicht europäischen Anbietern verbleibt. Wichtig dabei ist, dass die Unternehmensdaten bereits vor dem Upload in die Cloud verschlüsselt werden. Erst damit ist der Zugriff auf die Daten durch Dritte ausgeschlossen.
Eine Datenverschlüsselung, welche die Kriterien einer Regulatorik und der Compliance erfüllt, ist allerdings nur dann hilfreich, wenn mit den Daten in der Cloud und in den Applikationen trotz Verschlüsselung uneingeschränkt gearbeitet werden kann. Daher sorgt ausschließlich eine funktionserhaltende Verschlüsselung für Abhilfe und Sicherheit zugleich.

Unternehmen sollen bei der Wahl einer Cloud-Verschlüsselungslösung auf folgende Merkmale achten:

- Verschlüsselung vor der Cloud: Die Daten verlassen das Unternehmen nur in verschlüsselter Form.
- Schlüsselkontrolle: Nur das Unternehmen besitzt die Schlüssel – kein Cloud-Anbieter, keine Behörde, kein Partner.
- Volle Funktionalität: Trotz Verschlüsselung bleiben Funktionen wie Suche, Sortierung und Kollaboration erhalten.
- Flexibel einsetzbar: Kompatibel mit Microsoft 365, Salesforce und fast jeder weiteren (auch hybriden) Cloud-Umgebung.

Die Warnungen aus Norwegen und Dänemark sind ein deutliches Signal. Es ist davon auszugehen, dass weitere europäische Länder dem Beispiel folgen, oder auch konkrete Verbote und Regeln für das ungeschützte Übertragen sensibler Daten in die USA oder andere Regionen der Welt in Kraft treten werden. Unternehmen, die sich jetzt unabhängig machen und eine echte Datensouveränität etablieren, brauchen keine Unterbrechung der Betriebsabläufe und Prozesse aufgrund strengeren Regeln zu fürchten.

Über die Eperi GmbH:

Wir bei eperi® sind der festen Überzeugung, dass Datenschutz ein grundlegendes Menschenrecht ist. Unser Ziel ist es, dass Menschen und Unternehmen zu jeder Zeit die Kontrolle über ihre Daten behalten. Ohne Kompromisse und mit der besten Technologie. Mit dem Fokus auf die Sicherheit unserer Kunden haben wir eine Lösung geschaffen, die für den Benutzer unsichtbar ist und gleichzeitig die höchsten Sicherheitsstandards erfüllt.
Mit der eperi® Lösung profitieren unsere Kunden von allen Vorteilen der Cloud-Nutzung, wie beispielsweise einer effizienten unternehmensweiten Kollaboration, und bleiben dabei rechtssicher gemäß weltweiten Datenschutzgesetzen. Wir besitzen mehrere internationale Patente für unsere innovative Multi-Cloud-Technologie, die einen konkurrenzlosen Datenschutz für SaaS Anwendungen, individuelle Applikationen und Dateien bietet. Unsere Kunden behalten die alleinige Kontrolle über alle sensiblen Daten, da keine unverschlüsselten Daten in die Cloud gesendet werden.
Wir ermöglichen die Cloud – einfach, sicher, individuell, DSGVO-konform.

Pressekontakt eperi
Eperi GmbH
Sabine Jost
Werner-von-Siemens-Str. 2
64319 Pfungstadt
Tel: +49 (0)6157 95639 16
E-Mail: sabine.jost@eperi.com
Web: www.eperi.com

Pressekontakt Agentur
TC Communications
Thilo Christ
Tel: +49 171 6220610
Alexandra Schmidt
Tel: +49 170 3871064
E-Mail: eperi@tc-communications.de