PRESSEMITTEILUNG

Datenaustausch zwischen Europa und den USA ist nicht mehr sicher

Trumps Kündigungen beim Privacy and Civil Liberties Oversight Board haben drastische Folgen für die Datensicherheit zahlreicher europäischer Unternehmen

Organisationen, deren Daten auf amerikanischen Servern verarbeitet oder gespeichert werden, sollten schnellstmöglich neue Datenschutzkonzepte einführen. Mit modernen Encryption-Lösungen beispielsweise lassen sich diese Daten schnell und effektiv verschlüsseln und vor unbefugtem Zugriff, wie etwa durch amerikanische Behörden, schützen.

Im Zuge seiner radikalen Einspar-Projekte hat US-Präsident Donald Trump Ende Januar den Vorsitzenden sowie zwei Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB) entlassen. Das Europäische Zentrum für Digitale Rechte (NOYB) sieht hierin nicht nur negative Konsequenzen für die Funktionsfähigkeit und Wirkungsweise des PCLOB selbst, sondern befürchtet auch eine Reduzierung des Sicherheitslevels für den Datenaustauschs zwischen europäischen und amerikanischen Unternehmen. Warum? Weil das PCLOB für die Überwachung des sogenannten EU-US-Data Privacy Frameworks zuständig ist. Dieses Abkommen soll gewährleisten, dass beim Datenaustausch zwischen Europa und den USA ein angemessenes Datenschutzniveau eingehalten wird.

Infolge der Entlassungen ist die Kontrollfähigkeit des EU-US-Data Privacy Frameworks jedoch nicht mehr garantiert. Da in den USA Geheimdienste und staatliche Stellen weitreichendere Befugnisse haben als das in Europa der Fall ist, besteht die Gefahr, dass US-Behörden auf europäische Unternehmensdaten zugreifen können. Europäische Unternehmen sollten deshalb besser gestern als heute die geeigneten Schutzmaßnahmen ergreifen, um sich selbst und ihre Daten zu schützen.

Staatliche Zugriffsmöglichkeiten der Amerikaner untergraben DSGVO-Vorgaben

In Amerika herrscht grundsätzlich ein konträres Verständnis im Umgang mit Daten im Vergleich zu Europa. Nicht zuletzt deshalb hat der amerikanische Staat zahlreiche Möglichkeiten, auf die Daten ausländischer Unternehmen zuzugreifen. Das ist vor allem für deutsche Unternehmen problematisch, die ihre Unternehmensdaten in US-amerikanischen Rechenzentren speichern. Denn unabhängig von

der derzeitigen Situation in den USA gilt für die Daten europäischer Unternehmen seit 2018 die Datenschutzgrundverordnung (DSGVO). Diese soll dafür sorgen, dass sensiblen Daten, etwa personenbezogene Informationen oder Bankdaten, ein besonderer Schutz zukommt. Vor diesem Hintergrund ist der aktuelle Zustand des PCLOB besorgniserregend, denn so laufen diese Unternehmen Gefahr, bei der Datensicherheit nicht einmal das ohnehin schon schwache Niveau des EU-US-Data Privacy Frameworks gewährleisten zu können – geschweige denn das der DSGVO.

Hinzukommt, dass derzeit eine Kampagne der US-Regierung gegen europäische Datenschutzgesetze wie den DMA (Digital Markets Act) und den DSA (Digital Services Act) stattfindet. Es wird seitens der Trump-Administration unterstellt, dass diese Regularien gegenüber US-Unternehmen diskriminierend seien. Die EU dagegen will mit diesen Gesetzen sicherstellen, dass die Daten europäischer Bürger und Unternehmen vor übergriffigen Zugriffen geschützt bleiben – und Big-Tech-Konzerne klare Grenzen gesetzt bekommen. So wie es sich darstellt, wird aktuell ein politisch motivierter Kampf zur Datenhoheit gekämpft, in dem die europäischen Unternehmen mittendrin stecken.

Vor allem Unternehmen, die mit sensiblen Daten arbeiten, beispielsweise aus der Finanzbranche, dem Gesundheitswesen oder öffentliche Verwaltungen, sind aufgefordert zu handeln, für den Fall, dass sie ihre Daten derzeit mit amerikanischen Unternehmen austauschen oder in einem US-Rechenzentrum speichern.

Datenverschlüsselung ist das Gebot der Stunde

Aber es gibt Möglichkeiten sich proaktiv zu schützen. Moderne Verschlüsselungslösungen gewährleisten Sicherheit und DSGVO-Konformität, ohne die Funktionalität von Cloud-Diensten einzuschränken. sEcure von eperi beispielsweise verschlüsselt Daten bereits, bevor diese die Unternehmensumgebung verlassen und so bleibt die volle Kontrolle beim Unternehmen und die Daten sind vor unbefugten Zugriff geschützt – auch durch amerikanischen Behörden oder Geheimdienste.

Vorteile einer modernen Verschlüsselungsplattform (eperi sEcure)

- **Funktionalität bleibt erhalten:** Wichtige Microsoft-365-Dienste wie Suche, Sortierung und Kollaboration bleiben trotz Verschlüsselung nutzbar. Dies wird durch die patentierte Cloud-Adapter-Technologie von eperi sEcure ermöglicht, die Daten in einer Weise schützt, die eine

volle Nutzung aller Office-Funktionen gewährleistet. Dadurch können Unternehmen ihre gewohnten Arbeitsabläufe beibehalten und gleichzeitig höchste Sicherheit gewährleisten.

- **Komplette Kontrolle über Schlüssel und Daten:** Alle Verschlüsselungsprozesse und Schlüssel liegen ausschließlich beim Dateneigentümer (Key Sovereignty).
- **Maximale Datensouveränität:** Unternehmen behalten die vollständige Kontrolle über ihre Daten, ohne dass Dritte, wie beispielsweise Tech-Konzerne, Zugriff darauf haben. Das bedeutet, dass kein externer Zugriff auf kritische Unternehmensinformationen möglich ist.
- **Umfassender Schutz für diverse Cloud-Anbieter:** eperi sEcure kann nahezu universell als Sicherheitsschicht für Multi-Cloud-Landschaften eingesetzt werden und bietet daher Schutz für eine Vielzahl an internationalen Cloud- und Dienstanbietern.

Europäische Cloud-Souveränität ist dringend von Nöten

Es wird immer deutlicher, dass europäische Unternehmen ihre Daten eigenverantwortlich schützen müssen. Besser sie fangen heute als morgen damit an. Denn seit dem Amtsantritt der neuen US-Regierung ist nur eines sicher – und zwar, dass auf kaum noch etwas Verlass ist, was in der Vergangenheit verbindlich vereinbart wurde.

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