Your Key to Cloud Data Protection

Pressemitteilung

Darmstadt, 28. Juni 2017

Nur noch 11 Monate bis zum EU-DSGVO

Mehr als die Hälfte aller Verantwortlichen wollen keine personenbezogenen Daten mehr in der Cloud abspeichern

eperi, ein führender Anbieter von Cloud-Datenschutzlösungen (CDP), hat die Ergebnisse einer Befragung von 250 IT-Sicherheitsprofis auf der Infosecurity 2017 veröffentlicht. Weniger als ein Jahr vor dem Inkrafttreten der EU-Datenschutzgrundverordnung bietet sie einen Einblickdarin, wie Organisationen sich vorbereiten und den Cloud-Gebrauch planen. Die Studie deckt Unsicherheiten beim Thema Cloudsicherheit auf: 53 % der Befragten sagten aus, dass die Datenschutzgrundsätze der EU-DSGVO sie davon abhalten werden, personenbezogene Daten in der Cloud zu speichern. Für die Mehrheit (85 %) lag der Grund dafür in einem Mangel an Vertrauen in den Schutz der personenbezogenen Daten.
Des Weiteren gaben 72 % an, dass sie ihre Datenschutzanforderungen für die Cloud wegen der im Mai 2018 in Kraft tretenden Verordnung neu bewerten müssten. „DSGVO bedeutet, dass die uralte Debatte über die Qualität von Sicherheit in der Cloud wieder aktuell wird“ sagt Ravi Pather, Senior Vice President bei eperi. „Die Geldstrafen, die unter der DSGVO drohen, scheinen der Hauptantrieb dahinter zu sein, das so viele Unternehmen jetzt Compliance herstellen wollen. Denn im schlimmsten Fall kann ein Verstoß das finanzielle Ende der Organisation. Aber bei aller Panik sollten Firmen nicht vergessen, dass sie den Aufwand für DSGVO signifikant reduzieren können, wenn sie ihre Cloud-Daten vor allem mit Verschlüsselung und Tokenisierung schützen und im Besitz der kryptografischen Schlüssel bleiben.“
Eine Verschlüsselung oder Tokenisierung von Daten bedeutet, dass diese von einem Algorithmus unlesbar gemacht. Das macht sie unbrauchbar für jeden unautorisierten Zugriff. Entschlüsselt werden können die Daten nur mit dem kryptografischen Schlüssel. Dieser bleibt idealerweise ausschließlich in der Kontrolle der Organisation, die die Daten besitzt.
Zur Zeit, so Pather, ist dies der Grund, warum so viele Firmen gegenüber Anforderungen der DSGVO nicht erfüllen: 54 % der Befragten gaben zu, dass sie sich auf ihren Cloud- oder Software-as-a-Service- Anbieter (SaaS) verlassen, wenn es um die Verschlüsselung von Daten geht. Etwas mehr als die Hälfte (51 %) denken, dass es akzeptabel ist, wenn Anwendungsanbieter die vollständige oder teilweise Kontrolle über die kryptografischen Schlüssel haben.
„Wenn 54 % auf die Verschlüsselung durch ihren SaaS-Anbieter vertrauen, dann umfasst dies für gewöhnlich nur die gespeicherten Daten. Das stellt aber eigentlich nur eine Untermenge der umfangreichen Grundsätze dar, die den Schutz von personenbezogenen und sensiblen personenbezogenen Daten bei der Übertragung, Speicherung und Benutzung spezifizieren“, erklärt Pather.
„Wenn eine Organisation die volle Kontrolle über ihre eigenen kryptografischen Schlüssel hat, kann sie den Meldeschritt an die Aufsichtsbehörde im Fall von Gefährdung oder Verlust von Daten vermeiden, wenn die Daten unlesbar für die Welt außerhalb der Organisation sind“, führt er weiter aus. „Wenn der Cloud- oder SaaS-Anbieter die Schlüssel verwaltet und einen Sicherheitsvorfall hat,

eperi GmbH
Uhlandstrasse 9 / 64297 Darmstadt / Germany
T +49 6151 9513 0 11
F +49 6151 95130 66
W info@eperi.de / eperi.de
Geschäftsführung: Elmar Eperiesi-Beck

ist es schwer nachzuvollziehen, ob die Daten der Organisation sicher sind und eine Meldung an die Aufsichtsbehörde und Geldstrafen nötig ist.“
Die eperi-Umfrage erscheint kurz nachdem Forrester seinen Cloud Security Solutions Forecast veröffentlicht hat, der zeigt, dass der Cloud Services Markt von $ 114 Milliarden in 2016 auf $ 236 Milliarden in 2020 anwachsen wird. Dieses schnelle Wachstum wird auch den Markt für Cloud-Sicherheitsanwendungen beflügeln, dessen Wachstum Forrester von $ 1 Milliarde in 2016 auf $ 3,5 Milliarden in 2021 schätzt. Der Report merkt auch an, dass Unternehmen das Fehlen von adäquatem Schlüsselmanagement bei den Cloud-Anbietern erkennen, was dieser Funktion eine größere Dringlichkeit bei der Bereitstellung von Zeit und Ressourcen einräumt.

Über eperi
Die eperi GmbH ist ein führender Anbieter von Cloud-Data-Protection-Lösungen (CDP) mit mehreren hundert Kunden. Sie bietet Lösungen für Datensicherheit, Compliance, Datenkontroll-Use-Cases für kundenspezifische Anwendungen und führende SaaS-Anwendungen wie Office 365, Salesforce, ServiceNow und andere.

Unternehmen stehen heute signifikanten rechtlichen und regulatorischen Daten-Compliance- und Datenkontroll-Herausforderungen wie Data Residency, GDPR, PCI/DSS oder HiPPA gegenüber, wenn sie die Cloud und SaaS-Plattformen nutzen wollen. Die eperi-CDP-Lösungen helfen Unternehmen dabei, diese Daten-Compliance- und Datenkontroll-Herausforderungen durch eine Auswahl an kosteneffizienten Datenschutz-Softwarelösungen für die führenden SaaS-Plattformen zu meistern. Die eperi-CDP-Lösungen sind einzigartig, da sie die breiteste und tiefste Unterstützung für Cloud-SaaS, Anwendungen, Datenbanken und Dateien im Markt bieten und mit einem leistungsstarken Template-Konzept ausgestattet sind, das hunderte verschiedene Cloud-SaaS-Anwendungen unterstützt.

Das erlaubt Unternehmen, Cloud-SaaS schneller einzuführen, dabei Datenschutz-, Compliance- und Datenkontrollanforderungen zu erfüllen, die Nutzererfahrung völlig unverändert zu lassen und dabei den Schlüsseldatenschutz und zentrale Datensicherheits-Prinzipien nicht zu kompromittieren. Dadurch haben Unternehmen immer die volle Kontrolle über ihre sensiblen Daten.
Weitere Informationen finden Sie unter www.eperi.de.

Pressekontakt:
Tobias Krebs
tobias.krebs@eperi.de
+49 6151 95 130 11