Your Key to Cloud Data Protection

Pressemitteilung

Pfungstadt, 7. Januar 2019

Daten-Diebstahl im Bundestag: Wäre er zu verhindern gewesen?

Welche Sicherheitsmaßnahmen für den Schutz von sensiblen Daten sinnvoll sind

Korrespondenz von Bundeskanzlerin Angela Merkel, die Handynummer von Jan Böhmermann oder private Urlaubsbilder von ZDF-Journalisten - diese und ähnliche sensiblen Daten sind im Dezember über einen Twitter-Account frei zugänglich veröffentlicht worden. Die Daten enthielten sowohl ältere als auch aktuelle Informationen sowie persönliche Daten wie Namen, Handynummern, E-Mail-Adressen, Kreditkartendaten oder Chatverläufe. Betroffen sind alle Parteien im Bundestag außer der AfD, Journalisten von ARD und ZDF, Entertainer, Musiker und Schauspieler. Wie die Daten gestohlen werden konnten, ermitteln derzeit das Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesverfassungsschutz, das Bundeskriminalamt und der Bundesnachrichtendienst. „Niemand kann verhindern, dass Daten gestohlen werden, aber man kann durch entsprechende Sicherheitsmaßnahmen verhindern, dass Angreifer etwas mit den gestohlenen Informationen anfangen können“, sagt Elmar Eperiesi-Beck, Geschäftsführer der eperi GmbH.

Wie könnten solche Sicherheitsmaßnahmen aussehen? „Für den Fall, dass die Daten von Servern gestohlen und veröffentlicht werden, hilft eine Verschlüsselungslösung bei der nicht einmal die IT-Administratoren Zugriff auf unverschlüsselte Daten haben“, so Elmar Eperiesi-Beck. Auch wenn die Daten über eine Cloud-Anwendung wie Salesforce oder Office 365 gestohlen würden, wäre eine zusätzliche Verschlüsselung der einzige Schutz. „Verschlüsselung zählt zu den effektivsten Möglichkeiten, wertvolle Daten zu schützen. In Kombination mit einer Pseudonymisierung eignet sie sich bestens dazu, persönlich identifizierbare Daten in sinnlosen Text zu verwandeln, so dass keine Rückschlüsse mehr auf die betroffene Person gemacht werden können. Das gilt gleichermaßen für Daten in Use, in Transit und at Rest.“ Nur diejenigen, die Zugriff auf die kryptografischen Schlüssel haben, können die verschlüsselten Daten lesen.

Wenn es um den Schutz von Cloud-Daten geht, ist die Verschlüsselung also der beste Weg, um kritische Daten vor unbefugtem Zugriff durch Dritte, Kriminelle oder Administratoren in externen Rechenzentren zu schützen. „Die gesamte E-Mail-Kommunikation, Termine und andere sensible Daten, die auf Cloud-Plattform gespeichert und verarbeitet werden, sollten in jedem Fall durch Verschlüsselung und Pseudonymisierung vor dem Zugriff von Angreifern geschützt werden“, rat Elmar Eperiesi-Beck. Ganz nebenbei lassen sich so auch die strengen Anforderungen der Europäischen Datenschutzgrundverordnung und anderen Gesetzen umsetzen.

eperi GmbH
Gutenbergstraße 4-6 / 64319 Pfungstadt / Germany
T +49 6157 98 950 00
F +49 6157 98 950 29
W info@eperi.com / eperi.com
Geschäftsführung: Elmar Eperiesi-Beck

Über eperi
Die eperi GmbH ist ein führender Anbieter von Cloud Data Protection-Lösungen mit 15 Jahren Erfahrung auf dem Gebiet der Datenverschlüsselung für Web- und SaaS-Anwendungen wie Salesforce und Office 365. Mehrere hundert Kunden vertrauen bereits auf eperi. Die eperi Lösungen tragen dazu bei, dass interne und externe Datenschutz- und Compliance-Anforderungen an zentraler Stelle durchgesetzt werden und Kunden als Cloud-Nutzer die alleinige Kontrolle über alle Datenschutz-Prozesse behalten.
www.eperi.com

Hinweis an die Redaktionen:
Elmar Eperiesi-Beck steht für Interviewanfragen telefonisch zur Verfügung. Bei Interesse melden Sie sich bitte unter 06157-98950 15.

Pressekontakt
Michaela Ohlsen
michaela.ohlsen@eperi.com
+49 6157 98950 15