Sealed-Cloud-Technologie

Technisches Sicherheitskonzept schützt vor internem Datenmissbrauch

Die IT-Giganten Facebook, Yahoo, Microsoft und Google ließen sich für die Weitergabe von Daten Millionenbeträge bezahlen. Meldungen wie diese beunruhigen in letzter Zeit Entscheidungsträger in Unternehmen. Sie fragen sich nun verstärkt, wie sicher die Daten sind, die sie Cloud-Anbietern anvertrauen, oder ob sie überhaupt auf Cloud-basierte Dienste umstellen sollen.

Und wundern sich, ob die Informationstechnologie noch nicht so weit ist, eine technische Lösung anzubieten, die den Unsicherheitsfaktor Mensch aus den Sicherheitskonzepten ausschließt? Tatsächlich existiert bereits eine Lösung. Es ist die Basistechnologie Sealed Cloud. Diese fußt auf einem technischen Sicherheitskonzept.

Selbst wenn Unternehmensdaten in den Rechenzentren von Cloud-Anbietern verschlüsselt werden, so ist dies nur eine Scheinsicherheit. Denn Mitarbeiter in Rechenzentren besitzen meist den Schlüssel zu den Daten, um notwendige Wartungsarbeiten vornehmen zu können. Daher ist vor IT-Mitarbeitern wenig geheim zu halten: Sie können auf die unverschlüsselten Daten zugreifen. Manche Cloud-Anbieter sind sich dieser Sicherheitsrisiken bewusst, sie versuchen sie durch organisatorische Maßnahmen einzudämmen, wie z. B. das „Vier-Augen-Prinzip".

„Rein organisatorische Maßnahmen in Rechenzentren reichen für die Sicherheit der Daten nicht aus", erklärt der Sicherheitsexperte Dr. Hubert Jäger. Der Geschäftsführer des Münchner Unternehmens Uniscon GmbH setzt deshalb „mit der Basistechnologie Sealed Cloud auch auf technische Maßnahmen." Zu diesen zählen Verschlüsselung, Schutzmechanismen im Speichermanagement und Datenlöschfunktionen. Jäger: „Das System sichert die Daten nicht nur bei der Speicherung und beim Transfer, sondern auch in aktiven Sessions." So könnten auch IT-Administratoren nicht an die Daten. Die Sealed-Cloud-Technologie funktioniert nach dem Grundprinzip: „Was ich nicht weiß, kann ich nicht ausplaudern." Und das funktioniert so: Der Anwender meldet sich in seiner Cloud-Umgebung an, das System generiert einen nutzerindividuellen Schlüssel aus den Login-Informationen. Damit werden die Anwenderdaten gefunden, entschlüsselt und zum Bearbeiten in den Hauptspeicher geladen. Beendet der Anwender die Session, werden die Daten verschlüsselt gespeichert und das System zerstört anschließend den individuellen Schlüssel. In der Datenbank existiert für jeden Nutzer ein eigener Datensatz, der jeweils nach AES256 verschlüsselt ist. Die Schlüssel sind im System aber nicht vorhanden.

Damit die Daten bearbeitet werden können, sind sie während einer aktiven Session im Hauptspeicher unverschlüsselt und damit angreifbar. In einer ungeschützten Cloud-Umgebung könnte ein Systemadministrator die Daten während einer aktiven Session kopieren. In der versiegelten Cloud-Umgebung, dagegen, befinden sich alle Applikationsserver - also die Server mit den unverschlüsselten Daten - in elektromechanisch versiegelten Schränken (Rack-Systemen), die durch eine spezielle Versiegelungssoftware gesteuert werden. Die Server beinhalten nur flüchtige Speicher, deren Informationen verloren gehen, wenn der Strom abgeschaltet wird. Bevor ein Administrator Zugang zu den Anwendungsservern erhält, werden diese komplett gelöscht. Außerdem wird ein zusätzlich gehärtetes Betriebssystem verwendet. Durch „Härten" erhöht man, so Jäger, „die Sicherheit eines Systems, indem man nur die Software einsetzt, die für den Betrieb des Systems notwendig ist".

Auf der Basis der versiegelten Cloudtechnologie arbeitet bereits die Anwendung Idgard produktiv. Diese, für Unternehmen sehr wichtige Anwendung, ist ein Kommunikationsdienst, mit dem Unternehmen Daten abhörsicher austauschen können und ihre Projekte in einem vertraulichen Online-Workspace planen und umsetzen. Für Unternehmen, die vertrauliche Daten mit externen Dienstleistern oder mit Kunden austauschen müssen, kann der Dienst den UPS-Kurier, der Daten physisch über USB-Sticks oder Daten-CDs überbringt, sicher kostengünstig ersetzen. Zudem gehört ein abhörsicherer Chat zu den Funktionen und auch von mobilen Geräten kann abhörsicher auf die Daten zugegriffen werden.

Claudia Seidl, freie Journalistin, München.

www.uniscon.de