Handelsblatt Beilage reflex - de — Print

Medientyp:	Supplement	Gedruckte Auflage:	144.274
Veröffentlichungsdatum:	22.09.2015	Verkaufte Auflage:	122.939
Seite:	9	Verbreitete Auflage:	128.976
		Reichweite:	470.000

BIG DATA UND CLOUD SECURITY

Mit Sicherheit in die Zukunft

Die fortschreitende Digitalisierung der Geschäftswelt erfordert von Unternehmen mehr Effizienz, Agilität und Flexibilität. In innovativen Technologien schlummert viel Potenzial, sie schaffen aber auch neue Sicherheitsbaustellen. Werden diese nicht behoben, sind die vielfältigen Vorteile schnell verpufft.

Von Mark Krüger

Verbrechen verhindern, bevor sie entstehen? Vorab wissen, wo die nächste Straftat begangen wird? Was nach Science-Fiction klingt, ist bereits Realität und nennt sich „Predictive Policing". Dafür bedarf es keines Blickes in die Kristallkugel, es reicht die logische Verbindung vieler Daten aus unterschiedlichen Quellen und deren schnelle Auswertung. Auch die Wirtschaft hat längst das Potenzial von Big Data erkannt, aber auch den hohen Implementierungsaufwand. Einen Ausweg bietet hier die Symbiose zwischen Big Data und Cloud – vor allem was die Datenbereitstellung und -speicherung anbelangt. Doch wie ist es um die Sicherheit der Daten bestellt? Eine Frage, die beim Cloud Computing grundsätzlich nicht an Aktualität verloren hat. Nicht zu vergessen, dass auch diese Technologie besondere Anforderungen an die Netzwerkinfrastruktur stellt.

Neue Lösungen, mehr Vertrauen

Obwohl die Vorteile der „Wolke" auf der Hand liegen, kommt die Implementierung einer Cloud-Infrastruktur in vielen Unternehmen nur schleppend voran. Größter Hemmschuh: Sicherheitsbedenken. Anbieter von Cloud-Services haben inzwischen erkannt, dass die Gewährleistung von Informationssicherheit, die Garantie des Datenschutzes und die Umsetzung von Compliance-Anforderungen wichtige Faktoren sind, um Bedenken auf Seiten der Nutzer aus dem Weg zu räumen. Grundsätzlich stehen für den Skeptiker drei Fragen im Raum: Wie sicher ist die Datenübertragung? Wie sicher sind meine Daten auf den Servern? Und wer hat Zugriff?

Es sind innovative Lösungen, die darauf Antworten bieten und – nach Schlagzeilen zu Datenklau, Cyber Warfare und NSA – zunehmend Vertrauen schaffen. Beispiel gefällig?

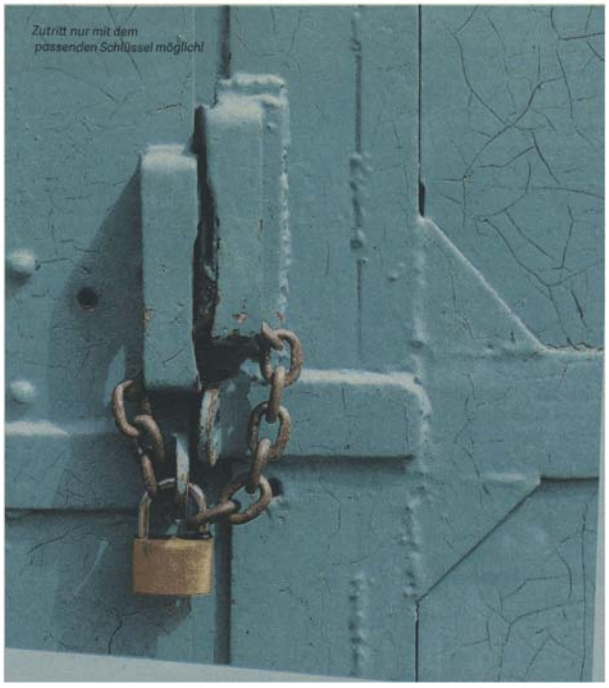
Daten im sicheren Käfig

Die sogenannte Sealed Cloud verhindert jeglichen unbefugten Zugriff – auch den vom Betreiber des Cloud-Dienstes und seinen Mitarbeitern. Möglich macht dies eine verschlüsselte Speicherung der Daten mittels eines temporären Schlüssels pro Nutzer – und nicht wie bislang durch einen serverweit gültigen Schlüssel. Jeder einzelne Anwenderserver befindet sich zudem in einem Käfig, den ein Administrator nur mit einem „remote" übermittelten Token öffnen kann. Während der Wartung des Servers befinden sich dort keine Anwendungsdaten. Sie werden zuvor auf andere, sichere Server verschoben. Daten- und Arbeitsspeicher sind somit sowohl technisch als auch organisatorisch gesichert, sprich, „versiegelt".

Sicherheitsstrategie anpassen

In Bezug auf den Megatrend Big Data spielt noch ein weiterer Aspekt in puncto Sicherheit eine Rolle: der Datenschutz. So muss die Auswertung der Daten anonymisiert erfolgen und einer Überprüfung durch Datenschutzbeauftragte von Bund und Ländern standhalten. Zudem sollten Unternehmen bereits in der Planung von Big-Data-Projekten Zugriffsrechte und Sicherheitsregeln festlegen. Wo kryptographische Verfahren für Vertraulichkeit und Integrität sorgen, stoßen diese bei großen Mengen an Daten schnell an ihre Grenzen. Laut Fraunhofer-Allianz Big Data können spezielle Algorithmen Abhilfe schaffen, welche effiziente Verschlüsselung gewähren und hierarchische Hash-Verfahren realisieren.

Ob Cloud Computing oder Big Data – derartige Projekte gehen zwangsläufig mit einer größeren Abhängigkeit von der Netzwerkinfrastruktur einher. Verfügbarkeit und Netzwerksicherheit sollten daher regelmäßig auf den Prüfstand gestellt werden. Stresstests zeigen zum Beispiel auf, wo im Falle einer hohen Belastung der Flaschenhals sitzt und wie es um die Sicherheit des Netzwerkes in puncto Vertraulichkeit, Integrität und Authentizität bestellt ist. Fazit: Die Chancen neuer Technologien wie Cloud und Big Data sind vielversprechend. Wer dabei nicht vergisst, Sicherheitskonzepte unter die Lupe zu nehmen und anzupassen, kann diese auch für sich nutzen. •


Zutritt nur mit dem passenden Schlüssel möglich!