Pressemitteilung

Nürnberg, 15. Juli 2013

Die Cloud in Zeiten von PRISM, Tempora und Co.

Unternehmen müssen zukünftig bei ihren Dienstleistern ganzheitlicher und sensibler zu denken.

In den letzten Wochen wurde ausgiebig über umfangreiche Datenüberwachungen berichtet. Dabei stand jedoch vorrangig der Privatanwenderbereich im Mittelpunkt der Betrachtungen. Inwiefern auch Unternehmen von den Skandalen betroffen sind, wird nach wie vor vernachlässigt oder nur vereinzelt thematisiert.

Dieter Kempf, Präsident des Hightech-Verbands BITKOM, fasste die aktuelle Stimmung in der Osnabrücker Zeitung treffend zusammen: "Einige Kunden haben neuerdings ein mulmiges Gefühl, wenn es darum geht, Daten in die Cloud zu verlagern". Waren es vor den aktuellen Entwicklungen besonders die Hackerangriffe und der Handel mit Insiderdaten, die Unternehmen Sorge bereiteten, so erreicht die Angreifbarkeit deutscher Firmen nun einen neuen Höhepunkt.

Das BSI und auch BITKOM raten Unternehmen dringend zur Nutzung tief integrierter Verschlüsselungssysteme beim Datentransfer in die Cloud. Dabei stehen den Firmen verschiedene Methoden zur Verfügung. Die Daten können zum Beispiel verschlüsselt übertragen werden. Problematisch ist in diesem Fall, dass die Daten zwar komplett kodiert übertragen, jedoch auf dem Server letztlich unverschlüsselt abgelegt werden. Auch eine serverseitige Verschlüsselung ist nur bedingt sicher, da in diesem Falle auch die Entschlüsselungskeys auf dem Server hinterlegt und somit theoretisch für jeden abrufbar sind. Unternehmen sollten aus diesem Grund auf eine clientseitige Verschlüsselung setzten, bei der die Daten lokal verschlüsselt und anschließend als chiffrierte Datenpakete auf den externen Servern abgelegt werden. Der Dienstleister respektive der „Mitlesende“ kann in diesem Fall mit den Daten nichts anfangen. Diese Art der Verschlüsselung ist jedoch technisch umfangreich, bedarf einer komplexeren Koordinierung und ist entsprechend teuer.

Ein weiterer wichtiger Punkt ist die Standortpolitik der Cloud-Dienstleister, die oftmals ihre Rechenzentren in den USA betreiben. Problematisch ist hierbei die Unterschiedlichkeit der Datenschutzansätze. Während in Deutschland auf den restriktiven Umgang mit personenbezogenen- und allgemeinen Kundendaten gepocht wird, sichert der „Patriot Act“ den US-Behörden einem umfassenden Zugriff auf alle Serverdaten zu. Zu glauben, dass es hierbei nur um Daten zur Terrorabwehr ginge, wäre blauäugig.

Einige Experten empfahlen in diesem Zusammenhang die Nutzung europäischer Cloud-Dienste, da diese einem einheitlicheren und umfangreicheren Datenschutzgesetz folgen würden. Jedoch ist auch diese Empfehlung in Folge des Bekanntwerdens von Tempora hinfällig. Das englische Pendant zum amerikanischen PRISM überwacht ebenfalls in großem Stil den internationalen Datenverkehr. Des Weiteren wurde jetzt erst bekannt, dass im Rahmen dieses Programms jeglicher Datenverkehr abgefangen wird, der über englische Server bzw. Verbindungen läuft.

Edward Snowden und dem "Guardian" zufolge werden diese Verbindungsdaten zudem durch ein "Full Take"-System bis zu 30 Tage gespeichert. Auch alle anderen Inhalte werden in einem sogenannten Pufferspeicher bis zu drei Tage aufbewahrt. "Dieser Zwischenspeicher macht nachträgliche Überwachung möglich, ihm entgeht kein einziges Bit", sagte Snowden zum SPIEGEL. "Wenn Sie ein Datenpaket verschicken und wenn das seinen Weg durch Großbritannien nimmt, werden wir es kriegen."

Die Wahl des Cloud-Rechenzentrumsstandortes ist demzufolge mehr als eine reine Kosten- und Rechtsfrage. Gerade

Hightech-Unternehmen sollten sich bewusst sein, dass ihre Daten in manchen Ländern dem Zugriff Dritter ausgeliefert sind. Selbst bei umfangreichen Verträgen und Vereinbarungen können sich die Firmen vor staatlich gelenkten Datenzugriffen nur äußerst schwer schützen. Letztlich ist es zu empfehlen das Rechenzentrum in einem bekannten Wirtschaftraum, mit möglichst hoher Rechtssicherheit und umfassendem Datenschutz anzusiedeln. Der britische Datenschutzaktivist Caspar Bowden gibt in diesem Zusammenhang zu bedenken: "Es könnte aber andere geben, die Business-Cloud-Dienste wie Microsoft Azure oder Amazon Web Services anzapfen." Die Cloud-Industrie sei hauptsächlich amerikanisch, "wir sollten die Situation komplett überdenken.“ Auch Verschlüsselung biete keinen Schutz, wenn staatliche Dienste direkten Zugriff auf Rechenzentren haben. „Cloud-Daten sollten möglichst in der Heimat bleiben.“

Die Unternehmen begeben sich durch die rasante Erschließung der Cloud in Abhängigkeiten, die es eigentlich zu vermeiden gilt. Wird man zu eng an einen Dienstleister gebunden, steigt auch das Schadenspotenzial, welches dieser dem eigenen Unternehmen zufügen kann. Nicht nur technische Probleme können somit zu einem Totalstillstand führen, sondern auch die Kontrolle der hinterlegten Daten wird zunehmend schwieriger. Im schlimmsten Fall werden Unternehmen erpressbar oder öffnen der ausländischen Konkurrenz Tür und Tor. Standortunabhängiger Datenzugriff ist wichtig und zukunftsweisend, sollte jedoch gerade dann kritisch hinterfragt werden, wenn man existenzrelevante Daten auf diese Art verlagert.

Der Trend in Richtung Cloud ist im Allgemeinen ein Schritt in die richtige Richtung - aber nicht um jeden Preis und schon gar nicht unter Verlust des Kontrollrechts an den eigenen Daten. Letztlich ist wohl die Kombination aus lokalen Speichermedien für sensible Daten und clientseitiger Verschlüsselung für die Cloudnutzung ein guter Kompromiss. In Zeiten von PRISM, Tempora und Co müssen Unternehmen beginnen umfassender und sensibler zu denken. IT-Sicherheit endet nicht mehr am eigenen Werkstor und nicht immer können Cloud-Dienstleister den notwendigen Datenschutz garantieren. Ein umfassendes Risikomanagement und ausgewogene IT-Infrastrukturen sind für eine zukunftsfähige Einbindung der Cloud unerlässlich. Manche Dinge sind nun einmal nicht für fremde Ohren bestimmt.

Pressekontakt:

Tom Strube
Marketing & PR

Tel.: 0911/9626324-0
E-Mail: Presse@sysfire.de

Über die sysfire GmbH

Das Kerngeschäft der in Nürnberg ansässigen sysfire GmbH umfasst qualitativ hochwertige und anspruchsvolle IT-Dienstleistungen sowie den Betrieb komplexer Infrastrukturen. Der Fokus liegt auf individuellen und optimal auf die Kundenbedürfnisse zugeschnittenen IT-Lösungen. Durch diese Fokussierung konnten in den letzten Jahren Projekte für Unternehmen der verschiedensten Größen und Branchen realisiert werden. Weitere Informationen stehen unter www.sysfire.de, bei Twitter @sysfire, unter facebook.de/sysfire oder über YouTube zur Verfügung.