



Software as a Service: Zertifizierungen und Zusicherungen im SLA reichen für die Sicherheit wirklich sensibler Informationen nicht aus



Interviewrunde: Hosted Security & Security as a Service
Name: Oliver Gajek
Funktion/Bereich: Vorstand
Organisation: Brainloop AG
Homepage Orga: www.brainloop.de

Liebe Leserinnen und liebe Leser,

In dieser Interviewrunde stellen Experten Ihre verschiedenen Sichtweisen auf das Thema „Hosted Security & Security as a Service“ dar und sprechen dabei über Vorteile, Optionen und Zukunft solcher Modelle. Die Zukunft von Hosted Security sieht Oliver Gajek, Vorstand der Brainloop AG dabei folgendermaßen:

„Ich glaube tatsächlich an die nächste große Architekturrevolution in der Informationstechnologie, bzw. die Rückkehr zur Mainframe-Ära, nur dass der Mainframe jetzt in der „Wolke“ steht. Dies wird für sämtliche Anbieter von Infrastruktur- und Anwendungssoftware weitreichende Konsequenzen haben. Wie alle Megatrends wird auch dieser wahrscheinlich kurzfristig überschätzt und langfristig unterschätzt. Das heißt, dass wir zunächst ein Überangebot an halbfertigen Ideen sehen werden, die mit großem Elan auf den Markt geworfen werden – die nächsten 18 Monate wird es auch hier zu einer Marktberreinigung kommen. Gleichzeitig wird aber die allgemeine wirtschaftliche Entwicklung dafür sorgen, dass die wirklich tragfähigen Innovationen sich überdurchschnittlich schnell etablieren werden. Ob und wann die etablierten Branchenriesen sowohl technisch als auch insbesondere im Businessmodell reagieren, werden wir sicher erst ab 2011 beobachten können.“

Viel Spaß beim Lesen wünscht Ihnen Ihr

NetSkill-Team!



Sehr geehrter Herr Gajek,

Frage 1: Terminologie & Begriffsklärung

Zunächst wollen wir kurz Klarheit über die verschiedenen Begriffe schaffen: Hosted Security, Security as a Service, Security on demand - Was steckt dahinter, gibt es Unterschiede?

**Antwort Oliver Gajek:**

Die ganze Technologie und auch die Spieler im Markt sind noch neu und jeder sucht nach Begriffen, die noch gestaltet werden können. Das ist normal und wird sich irgendwann einspielen. Für uns ist SaaS das führende Konzept und auch der führende Begriff. Wir sehen hier eine grundlegende Architekturrevolution für Infrastruktur- und Anwendungssoftware, vergleichbar mit der vorausgegangen Entwicklung vom Mainframe zum Client-Server zum Web. SaaS ist ein [Geschäftsmodell](#) mit der Philosophie, Software als [Dienstleistung](#) basierend auf [Internettechnologien](#) bereitzustellen, zu betreuen und zu betreiben.

Frage 2: Anwendungen & Eignung

Welche Security-Anwendungen können bereits über diese Methoden bezogen werden? Welche eignen sich möglicherweise nicht?

**Antwort Oliver Gajek:**

Hier gibt es zwei Blickwinkel: Einen inkrementellen, in dem wir uns fragen, welche Services, die wir heute noch nicht haben, zusätzlich als Service bezogen werden können. Spam-Filter, E-Mail Security, Extranet-Lösungen sind hier relevant. Und eine radikale Sicht, in der Schritt für Schritt bereits bestehende Lösungen durch „in the cloud“ Optionen ersetzt werden und am Ende die IT-Architektur weitgehend oder komplett durch Services bedient werden. Letztendlich kehren wir hier wieder zurück zu den Anfängen der Datenverarbeitung mit „dummen“ Terminals am Arbeitsplatz und einem allmächtigen Server, der jetzt eben nicht mehr als Mainframe im eigenen Rechenzentrum, sondern irgendwo in der Wolke steht. In dieser Sicht werden im Prinzip alle Security-Anwendungen und Infrastrukturkomponenten als Services bezogen.

**Frage 3: Konkrete Vorteile von Hosted Security**

Ein Vorteil von Sicherheitslösungen als Service sollen Kostenvorteile sein. Woraus entstehen diese? Wie konkret können sie festgestellt werden? Hätten Sie ein Praxisbeispiel?

**Antwort Oliver Gajek:**

Ein großer Kostenvorteil von Hosted Services ist, dass der Einkauf von Technologie skaliert, also kleine Firmen oder einzelne Abteilungen von größeren Unternehmen mit best-in-class Produkten ausgestattet werden können, wo das zuvor aufgrund von budgetären oder technischen Engpässen nicht möglich war. So kann, abhängig von den ganz spezifischen Anforderungen, die bestmögliche Technologie an den entsprechenden Arbeitsplatz gebracht werden, ohne Kompromisse bei Preis oder Funktionalität. Brainloop Secure Dataroom als führende Lösung für Document Compliance Management wird heute von kleinen Management Consulting Firmen oder Investmentboutiquen genauso eingesetzt wie von großen Konzernen, die mehrere tausend Mitarbeiter mit dem bestmöglichen Dokumentenschutz absichern wollen.

Frage 4: Vorbehalte und die Fakten dahinter

Was sind übliche Bedenken und Vorbehalte von IT-Entscheidern gegenüber Hosted Security bzw. Security als Service? Was können Sie diesen antworten?

**Antwort Oliver Gajek:**

Das Management vertraulicher Daten und Prozesse durch den externen Dienstleister wird selbstverständlich kritisch beurteilt. Hier muss der externe Lieferant genaue Rechenschaft ablegen über die konkrete Sicherheitstechnologie, die dafür sorgt, dass die Informationen des Kunden nicht eingesehen werden können. Diese Architektur sollte dann auch der intensiven Prüfung durch einen vom Kunden ausgewählten Experten Stand halten, der dann auch die Vorteile gegenüber den „Bordmitteln“ dokumentieren kann.

**Frage 5: Anbietersauswahl und Angebote**

Worauf sollten Entscheider bei der Auswahl eines Providers achten? Was können Sie und Ihr Unternehmen für Unternehmen und ihre Sicherheit tun? Welche Modelle bieten Sie an?

**Antwort Oliver Gajek:**

Die meisten Anbieter versuchen, mit verschiedenen Zertifizierungen und entsprechenden Zusicherungen im Service Level Agreement das Vertrauen des Auftraggebers zu dokumentieren. Für die wirklich sensiblen Informationen und Prozesse ist das unserer Meinung nach aber nicht ausreichend. Hier sollte zwingend nach Technologie gefragt werden, die den externen Dienstleister konsequent aus dem Datenbestand des Kunden „aussperren“. So bietet Brainloop Secure Dataroom unter dem Schlagwort „Operator Shielding“ die Möglichkeit, dass Dokumente bei der Speicherung auf dem zentralen Server so verschlüsselt werden, dass der Dienstleister die Dokumente des Kunden nie einsehen kann.

Frage 6: Zukunft und Ausblick

Wie sehen Sie die Zukunft für SaaS-Modelle im Security-Markt? Können Sie die nächsten Schritte kurz zusammenfassen?

**Antwort Oliver Gajek:**

Ich glaube tatsächlich an die nächste große Architekturrevolution in der Informationstechnologie, bzw. die Rückkehr zur Mainframe-Ära, nur dass der Mainframe jetzt in der „Wolke“ steht. Dies wird für sämtliche Anbieter von Infrastruktur- und Anwendungssoftware weitreichende Konsequenzen haben. Wie alle Megatrends wird auch dieser wahrscheinlich kurzfristig überschätzt und langfristig unterschätzt. Das heißt, dass wir zunächst ein Überangebot an halbfertigen Ideen sehen werden, die mit großem Elan auf den Markt geworfen werden – die nächsten 18 Monate wird es auch hier zu einer Marktbereinigung kommen. Gleichzeitig wird aber die allgemeine wirtschaftliche Entwicklung dafür sorgen, dass die wirklich tragfähigen Innovationen sich überdurchschnittlich schnell etablieren werden. Ob und wann die etablierten Branchenriesen sowohl technisch als auch insbesondere im Businessmodell reagieren, werden wir sicher erst ab 2011 beobachten können.

Vielen Dank für das Interview!