



## Hype und Realität unterscheiden: Auch SaaS-Anbieter unterliegen wechselnden wirtschaftlichen Bedingungen



**Titel des Interviews:** Hosted Security & Security as a Service  
**Name:** Paul Wood  
**Funktion/Bereich:** MessageLabs Intelligence Senior Analyst  
**Organisation:** MessageLabs  
**Homepage Orga:** [www.messagelabs.com](http://www.messagelabs.com)

**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 Paul Wood, Senior Analyst bei MessageLabs dabei folgendermaßen:

„Es ist zu erwarten, dass SaaS in den nächsten Jahren zu einem weitgreifenden Computing-Modell wird. Gerade in der aktuellen wirtschaftlichen Lage wird SaaS als eine skalierbare kosteneffiziente Option gesehen, die es Unternehmen ermöglicht, die Investitionen in die IT dem Wachstum des Unternehmens anzupassen.“

**Viel Spaß beim Lesen wünscht Ihnen Ihr**

**NetSkill-Team!**



Sehr geehrter Herr Wood,

**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 Paul Wood:**

Hosted Security bedeutet, dass der Anbieter dieses Services die für die Nutzung dieses Services nötige Infrastruktur über das Internet („in the cloud“) hostet. Für die Unternehmen hat dies den Vorteil, dass sich die IT-Komplexität reduziert sowie das IT-Risiko und die Betriebskosten gesenkt werden. Bei den so genannten Managed Services wird die Dienstleistung an sich vom Anbieter verwaltet, aber direkt beim Kunden on-premise gehostet. Security-as-a-Service (SaaS) gehört zum Bereich Software-as-a-Service während Cloud Computing einen wesentlich umfassenderen Bereich beschreibt und ein breiteres Spektrum an Produkten und Services abdeckt als der Begriff SaaS. SaaS nutzt cloud-basierte Umgebungen zur Bereitstellung der Services, die von den Kunden auf Basis von „Bestellungen“ genutzt werden. Security-as-a-Service umfasst die Bereitstellung von Sicherheitslösungen, die nach SaaS-Art bereitgestellt und genutzt werden. On-Demand Computing bedeutet, dass Ressourcen dem Kunden je nach Bedarf zur Verfügung gestellt werden. Diese IT auf Abruf kann einerseits innerhalb einer Organisation gehostet oder von einem Dienstleister beschafft werden. Security-on-Demand bezeichnet den Einsatz von Sicherheitslösungen nach dem On-Demand-Modell.

**Frage 2: Anwendungen & Eignung**

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

**Antwort Paul Wood:**

Eine cloud-basierte Security-as-a-Service-Lösung kann etliche Clients über etliche ISPs in diversen Zeitzonen überwachen und im Vergleich zu herkömmlichen Gateway- oder Desktop-basierten Sicherheitsapplikationen effizienter auf neue Bedrohungen reagieren. Für Service-Modelle sind am besten die Applikationen geeignet, die für jede Unternehmensgröße und Nutzeran-



zahl skaliert werden kann und dabei allen Nutzern dieselbe Dienstleistung anbietet.

### 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 Paul Wood:

Reduzierte IT-Budgets und schwindender In-House Support sind zwei Gründe, warum Unternehmen nach Möglichkeiten schauen, mit weniger mehr zu erreichen. SaaS ist eine skalierbare Lösung, die kleinen und mittelständischen Unternehmen dieselbe Technologie bietet wie Fortune-500-Unternehmen. Gleichzeitig werden Investitionsausgaben reduziert und Abschreibungskosten für Hardware und andere Anlagegüter durch vorhersehbare Subscription-Modelle ersetzt. Die flexible Skalierbarkeit macht SaaS zu einer praktischen Alternative zu On-Premise-Lösungen und ermöglicht es, die anfallenden Lizenzkosten zu kontrollieren und den Anforderungen des Unternehmens anzupassen.

### 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 Paul Wood:

Nicht alle Cloud-basierten Lösungen werden auf dieselbe Art und Weise eingerichtet, und die häufigsten Bedenken gegenüber Cloud-basierten Ansätzen betreffen die Bereiche Sicherheit, Integrität und Verfügbarkeit. Ein oft genannter Kritikpunkt zu Cloud Computing ist, dass Unternehmen von einem einzigen Service Provider abhängig sind und nur Zugang zu den vom Provider gebotenen Services und Applikationen haben. Das mag bei manchen SaaS-basierten Applikationen auch der Fall sein, allerdings nicht bei SaaS-basierten Diensten für E-Mail- oder Web-Sicherheit, die abgesehen von der Erstinstallation keine Intervention des Endnutzers verlangen. SaaS-basierte Sicherheitslösungen ermöglichen einfaches Ein- oder Abschalten beziehungsweise einen problemlosen Anbieterwechsel, ohne die Service-Verfügbarkeit für End-



nutzer zu beeinflussen. Die Erfolgsbasis eines solchen Services ist Vertrauen. Die Services von MessageLabs schützen bereits eine Vielzahl an großen internationalen Unternehmen wie Banken, Regierungen und weitere Organisationen des öffentlichen Bereiches weltweit.

#### 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 Paul Wood:

Es ist zunächst einmal wichtig, den Unterschied zwischen Cloud-basierten Lösungen und herkömmlichen Angeboten zu verstehen. Manche Unternehmen neigen dazu, den Hype um ihre Produkte mit den neuesten Schlagwörtern zu verstärken – es ist daher wichtig, zwischen Hype und Realität zu unterscheiden. Das aktuelle Wirtschaftsklima macht SaaS-Lösungen kurzfristig zu attraktiven Möglichkeiten, um Kosten zu reduzieren, aber man darf nicht vergessen, dass eben solche Service-Anbieter denselben wirtschaftlichen Bedingungen unterliegen. Deshalb sollte man bei der Auswahl eines Service-Anbieters sehr gründlich vorgehen.

MessageLabs bietet eine Vielzahl an hosted E-Mail Security Services:

**a) MessageLabs E-Mail Anti-Virus Service:** Der Managed Service für die Viren-Abwehr ist weltweit die einzige Lösung, die Unternehmen über eine Leistungsvereinbarung eine Erkennungsrate von 100 Prozent aller bekannten und unbekanntem E-Mail-Viren garantiert. Außerdem müssen Anwender weder neue Hard- und Software anschaffen noch aufwändige und teure Installations- und Vorbereitungsmaßnahmen treffen oder laufend Upgrades und Wartungsarbeiten erledigen.

**b) MessageLabs E-Mail Anti-Spam Filter:** MessageLabs bietet Spam-Abwehr für E-Mails als Rund-um-Sorglos-Paket, das auf einer festen Leistungsvereinbarung beruht: Unternehmen können sicher sein, dass 99 Prozent aller Spam-Nachrichten abgefangen werden, ohne dass darunter der reibungslose Versand und Empfang der rechtmäßigen E-Mails leidet. Der Managed Service befreit Anwender zudem von dem enormen Aufwand, für diese Zwecke eigene Hardware und Software kaufen und installieren sowie laufend warten und auf dem neuesten Stand halten zu müssen. Unternehmen können das via Internet bereitgestellte Angebot binnen weniger Minuten aktivieren und den Dienst einfach



so konfigurieren, dass die internen Prozessstandards und Sicherheitsrichtlinien durchgehend gewahrt bleiben.

**c) MessageLabs E-Mail Image Control Service:** Der E-Mail-Image-Control-Service von MessageLabs setzt modernste ICA-Verfahren (Image Composition Analysis) der Bildanalyse ein, um zu verhindern, dass pornografische Inhalte und andere unangemessene Grafikdateien ins Netzwerk gelangen. Ganz gleich, ob solche Bilder in E-Mails eingebettet oder als Anhang mitgeschickt werden – die Technologien spüren sie zuverlässig auf und stoppen die Übermittlung.

**d) MessageLabs E-Mail Content Control Service:** Im Rahmen des Managed Service für die Content-Kontrolle überprüft MessageLabs die Inhalte und Anhänge im E-Mail-Verkehr mit modernen Filter- und Scan-Technologien. Auf diese Weise verhindert MessageLabs, dass beispielsweise ein Mitarbeiter per Mail irgendwelche vertraulichen, schädlichen, beleidigenden oder unangebrachten Informationen verbreitet.

**e) MessageLabs Policy Based Encryption Service:** Mit der Policy Based Encryption von MessageLabs schützen Anwender alle vertraulichen, via E-Mail mit Kunden und anderen Geschäftskontakten ausgetauschten Daten effektiv vor dem Zugriff durch Unbefugte. Automatisch, sofort und sicher – so verschlüsselt dieser Managed Service selbsttätig alle Nachrichten, in denen sich Informationen enthalten könnten, die keinesfalls in fremde Hände fallen sollten.

#### Frage 6: Zukunft und Ausblick

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



#### Antwort Paul Wood:

Es ist zu erwarten, dass SaaS in den nächsten Jahren zu einem weitgreifenden Computing-Modell wird. Gerade in der aktuellen wirtschaftlichen Lage wird SaaS als eine skalierbare kosteneffiziente Option gesehen, die es Unternehmen ermöglicht, die Investitionen in die IT dem Wachstum des Unternehmens anzupassen.

**Vielen Dank für das Interview!**