

## Echtes SaaS oder „nur“ eine Hosted-Lösung? - SaaS heißt Verzicht auf jegliche Hard- oder Software auf Kundenseite



**Interviewrunde:** „Hosted Security & Security as a Service“  
**Name:** Daniel Wolf  
**Funktion/Bereich:** Territory Manager Deutschland, Österreich, Schweiz  
**Organisation:** Zscaler Europe  
**Homepage Orga:** [www.zscaler.com](http://www.zscaler.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 Daniel Wolf, Territory Manager Deutschland, Österreich, Schweiz bei Zscaler Europe bei dabei folgendermaßen:

„Eine eigene Infrastruktur für die IT-Sicherheit zu betreiben, wird für die meisten Unternehmen hinsichtlich Kosten, Zeit und Know-how immer aufwändiger. Das SaaS-Modell bietet die Möglichkeit, zu kalkulierbaren Kosten ein hohes und vertraglich geregelter Sicherheitslevel zu erhalten. SaaS-Modelle werden sich aber nur dort durchsetzen, wo tatsächlich Skaleneffekte zum Tragen kommen und damit die Kosten deutlich sinken. Unternehmen werden sich mehr mit organisatorischer Sicherheit, der Definition entsprechender Richtlinien oder Interpretation von Reports beschäftigen. Alle Security-Anwendungen, die nicht zu den Kernkompetenzen eines Unternehmens zählen, stehen zur Disposition für ein Outtasking. Der Druck auf die IT-Budgets in wirtschaftlich schwierigen Zeiten und die zunehmende Mobilität der Mitarbeiter wird SaaS erheblichen Zuspruch bringen.“

**Viel Spaß beim Lesen wünscht Ihnen Ihr**

**NetSkill-Team!**



Sehr geehrter Herr Wolf,

#### 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 Daniel Wolf:

Hosting ist in der Regel 1:1. Dabei betreibt der Dienstleister Anwendungen und Hardware, deren Management übernimmt entweder der Kunde selbst oder der Hoster. SaaS oder auch Security on demand funktioniert hingegen 1:n – eine multimandatenfähige Infrastruktur wird von vielen Kunden genutzt. Der Kunde erwirbt weder Hard- noch Software, sondern abonniert einen Dienst nach Bedarf. SaaS erzielt in hohem Maße Skaleneffekte, die in Form von günstigeren Preisen an Kunden weitergegeben werden. Ein Großteil der SaaS-Angebote am Markt sind bei genauerer Betrachtung jedoch „nur“ Hosted-Lösungen. Richtiges SaaS verzichtet auf jegliche Hard- oder Software auf Kundenseite, ist hoch skalierbar, zwingend mandatenfähig und lässt sich in der Regel nicht mit herkömmlichen Enterprise Systemen realisieren.

#### Frage 2: Anwendungen & Eignung

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

#### Antwort Daniel Wolf:



Hosted-Lösungen können prinzipiell alle Security-Anwendungen realisieren, die serverseitig sind. Bei SaaS hat sich E-Mail-Sicherheit mit AV-Filter, Anti-Spam und Verschlüsselung bereits sehr gut etabliert.

Für Web Security gab es bislang keine echte SaaS-Lösung. Zscaler ist der erste Anbieter in diesem Bereich, der von Grund auf eine Infrastruktur für SaaS entwickelt hat. Wir setzen sowohl klassische Erkennungsmethoden wie URL-Filter, Anti-Virus und Anti-Spyware ein, als auch Verfahren, die aktive Inhalte erkennen und damit vor komplexen Bedrohungen, z.B. durch Web 2.0-Anwendungen und P2P-Verbindungen, schützen.

**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 Daniel Wolf:**

Die Kostenvorteile bei SaaS entstehen durch Skaleneffekte, da sowohl die Infrastruktur als auch das Know-how der Security-Experten von vielen Kunden genutzt wird. Über ein einzelnes Zscaler Gateway können wir zum Beispiel den Webverkehr von tausenden Kunden laufen lassen. Dadurch ist der Zscaler-Dienst um etwa 30 bis 40 Prozent günstiger als eine selbstbetriebene Inhouse-Lösung. Bei Hosted kommt es dagegen kaum zu Skaleneffekten.

**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 Daniel Wolf:**

Die Bedenken sind oft psychologischer Natur: Was geschieht mit meinen Daten? Wie werden diese gesichert und wer hat wie und wann Zugriff darauf? Deshalb ist organisatorische und technische Aufklärung notwendig. So garantieren insbesondere die Verträge dem Kunden Datenschutz und Vertraulichkeit. Eine der weitverbreitetsten SaaS-Anwendungen sind ausgerechnet CRM-Systeme, bei denen Unternehmen ihre gesamten Kundendaten in die Hand eines externen Anbieters geben. Auf der anderen Seite kann ein guter SaaS-Anbieter eine wesentlich höhere Sicherheit gewährleisten, da er über das entsprechende Know-how und die Ressourcen verfügt. Es wäre enorm aufwändig, dies als Unternehmen selbst vorzuhalten. Zudem ist 100-prozentiger Datenschutz auch bei inhouse betriebenen Lösungen nicht immer gewährleistet, z.B. wenn Mitarbeiter irgendwann mal das Unternehmen verlassen.

**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 Daniel Wolf:**

Neben dem Funktionsumfang sollte man vor allem auf die Service Level Agreements (SLA) achten. Eine wichtige kaufmännische Betrachtung sind zudem die Total Cost of Ownership (TCO). Sollte das Unternehmen international agieren, gilt es zudem zu prüfen, ob der Service weltweit in gleicher Qualität verfügbar ist. Eine administrative Multimandantenfähigkeit ist ein weiteres Kriterium vor allem für Konzerne. Der Kunde muss prüfen, ob er mit dem jeweiligen SaaS-Anbieter seine Unternehmensrichtlinien und andere regulatorische Vorgaben umsetzen kann. Trotz eines 1:n-Ansatzes muss SaaS also ausreichend Flexibilität für das jeweilige Unternehmen bieten.

Zscaler sichert den Webzugriff unabhängig von Ort, Zeit und Endgerät und ermöglicht es Unternehmen, ihre Sicherheitsrichtlinien weltweit umzusetzen. Der gesamte Webtraffic wird trotz vielfältiger Filter in Echtzeit analysiert. Dabei sind jedoch je nach Bedarf unterschiedliche Sicherheitsmodule möglich. Die Preise berechnen sich nach Nutzerzahl und Security-Module (z.B. URL-Filter).

**Frage 6: Zukunft und Ausblick**

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

**Antwort Daniel Wolf:**

Eine eigene Infrastruktur für die IT-Sicherheit zu betreiben, wird für die meisten Unternehmen hinsichtlich Kosten, Zeit und Know-how immer aufwändiger. Das SaaS-Modell bietet die Möglichkeit, zu kalkulierbaren Kosten ein hohes und vertraglich geregelter Sicherheitslevel zu erhalten. SaaS-Modelle werden sich aber nur dort durchsetzen, wo tatsächlich Skaleneffekte zum Tragen kommen und damit die Kosten deutlich sinken. Unternehmen werden sich mehr mit organisatorischer Sicherheit, der Definition entsprechender Richtlinien oder Interpretation von Reports beschäftigen. Alle Security-Anwendungen, die nicht zu den Kernkompetenzen eines Unternehmens zählen, stehen zur



Disposition für ein Outtasking. Der Druck auf die IT-Budgets in wirtschaftlich schwierigen Zeiten und die zunehmende Mobilität der Mitarbeiter wird SaaS erheblichen Zuspruch bringen.

**Vielen Dank für das Interview!**