



## Sicherheitsanwendungen im Rechenzentrum “besuchen” - Hosted Security braucht Vertrauen



**Interviewrunde:** „Hosted Security & Security as a Service“  
**Name:** Holger Schmitz  
**Funktion/Bereich:** Vorstand /Geschäftsführer  
**Organisation:** ComNet GmbH  
**Homepage Orga:** <http://www.comnet.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 Holger Schmitz, Geschäftsführer der ComNet GmbH dabei folgendermaßen:

„Wir glauben, dass Security as a Service die Zukunft gehört. Sobald sich das SaaS-Modell im Allgemeinen durchgesetzt hat, werden auch die Security-Anwendungen vermehrt ins Rechenzentrum wandern. Zu groß ist der Vorteil, das technische Wettrennen den Experten zu überlassen und sich mit diesem Thema nicht mehr befassen zu müssen.“

**Viel Spaß beim Lesen wünscht Ihnen Ihr**

**NetSkill-Team!**



Sehr geehrter Herr Schmitz,

**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 Holger Schmitz:**

Für den Kunden sind diese Begriffe nahezu synonym. Es steckt jedoch jeweils ein anderes Betriebs- bzw. Berechnungsmodell dahinter:

Hosted Security heißt erst einmal nur, dass das Unternehmen die Sicherheitssysteme nicht im eigenen Haus, sondern im Rechenzentrum des Outsourcing-Partners installiert hat. Security as a Service heißt, dass im Rechenzentrum nicht für jeden Kunden eine eigene dezidierte Anwendung läuft, sondern ein mandantenfähiges System. Security on Demand bezieht sich auf ein nutzungsbezogenes Bezahlmodell. Ein System wird nicht gemietet, geleast oder gekauft, sondern es wird nach Nutzung abgerechnet: z. B. nach Anzahl der gescannten E-Mails.

**Frage 2: Anwendungen & Eignung**

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

**Antwort Holger Schmitz:**

Alle Security-Anwendungen, die die Infrastruktur vor Bedrohungen von Außen schützen: Virens Scanner, Spamfilter oder Firewalls. Nicht As-a-Service-fähig ist der Schutz vor internen Gefahren durch kriminelle Mitarbeiter oder verseuchte Datenträger. Dort müssen interne Mechanismen – Zugangskontrolle, Transaktionsprotokolle etc. - greifen, die kaum von Außen bereitgestellt werden können.

**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 Holger Schmitz:**

Zunächst ein|mal ist keine Sprunginvestition für die Anschaffung von Software notwendig. Auch die Kosten für Updates und die ständige Gefahrenanpassungen entfallen. Demgegenüber stehen die As-a-Service-Kosten, die sich vielleicht sogar die Waage halten. Der Haupteinsparungsfaktor sind die Betreuungskosten. Es muss sich im Unternehmen einfach niemand mehr um das Thema kümmern und kann seine Arbeitszeit anderen Dingen widmen. Gerade für mittelständische Unternehmen, die nur eine kleine oder gar keine IT-Abteilung haben, ist das eine ungeheure Entlastung.

**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 Holger Schmitz:**

Interessanterweise gibt es, wenn wir unser Angebot vortragen, kaum Einwände gegen Security as a Service. Alle finden das Angebot absolut überzeugend. Allerdings kommen dafür überraschend wenige Vertragsabschlüsse zustande. Wir sehen dafür zwei Gründe: Das Thema Security wird dramatisch unterschätzt. Viele Unternehmen haben gar keine professionellen Sicherheitssysteme und wollen dafür auch kein Geld ausgeben. Wer bereits Systeme installiert hat, nutzt diese Investitionen erst einmal weiter, bis sie abgeschrieben sind.

**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 Holger Schmitz:**

Unseren Kunden ist es sehr wichtig, einen persönlichen Ansprechpartner zu haben und das Rechenzentrum, in dem ihre Sicherheit „residiert“, prinzipiell besuchen zu können. Dies schafft das Vertrauen, das man benötigt, um die IT-Sicherheit aus der Hand zu geben. Gefragt werden wir auch immer wieder nach Referenzen. Wenn die Kunden dann hören, dass selbst Banken ihre sensiblen Systeme von aixGate, so heißt die ComNet-Security-Lösung, schützen lassen, dann verlagern sie in der Regel früher oder später ihre Sicherheitssysteme ins ComNet-Rechenzentrum.

ComNet bietet drei Modelle an: die aixGate E-Mail-Firewall, die vor Spam und Viren schützt, die aixGate Internet-Firewall, die darüber hinaus das gesamte Unternehmensnetzwerk vor Schädlingen und Eindringlingen schützt und aixGate Connect, das Verbindungen zwischen verschiedenen Unternehmensstandorten, etwa Handelsfilialen, sicher abschirmt.

**Frage 6: Zukunft und Ausblick**

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

**Antwort Holger Schmitz:**

Wir glauben, dass Security as a Service die Zukunft gehört. Sobald sich das SaaS-Modell im Allgemeinen durchgesetzt hat, werden auch die Security-Anwendungen vermehrt ins Rechenzentrum wandern.

Zu groß ist der Vorteil, das technische Wettrennen den Experten zu überlassen und sich mit diesem Thema nicht mehr befassen zu müssen.

**Vielen Dank für das Interview!**