



Hybride Lösungen aus internen und externen Security-Anwendungen kennzeichnen den Übergang zu Security as a Service



Interviewrunde: Hosted Security & Security as a Service
Name: Michael Scheffler
Funktion/Bereich: Regional Director Central Europe
Organisation: Websense GmbH
Homepage Orga: <http://www.websense.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 Michael Scheffler, Regional Director Central Europe bei Websense in München dabei folgendermaßen:

„Momentan nutzt hierzulande die große Mehrheit der Unternehmen eine interne IT-Security-Lösung. Das wird sich nach und nach ändern – nicht zuletzt dort, wo als Folge der Finanz- und Wirtschaftskrise die IT-Budgets nach Einsparpotenzialen durchforstet werden. In naher Zukunft bleibt es bei einer Koexistenz von internen und externen Lösungen. Aber auch hybride Modelle, bei denen bestimmte Funktionen intern und andere extern als Service bezogen werden, sind heute schon im Einsatz. Sie sind kennzeichnend für eine Übergangsphase. Auf die nächsten drei bis fünf Jahre betrachtet, werden sich die Security-Services stärker im Markt verbreiten und es ist davon auszugehen, dass sie langfristig die Zahl der internen Lösungen überflügeln. Der Trend geht in diese Richtung. IT-Security ist eine Infrastrukturaufgabe, die in die Hände von Spezialisten gehört.“

Viel Spaß beim Lesen wünscht Ihnen Ihr

NetSkill-Team!



Sehr geehrter Herr Scheffler,

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 Michael Scheffler:**

Es gibt deutliche Unterschiede zwischen diesen Begriffen. Unter dem Label „Hosted Security“ werden Lösungen angeboten, die ursprünglich einmal für den unternehmensinternen Einsatz entstanden sind und im Laufe der Zeit von Hosting-Anbietern im Rahmen eines ASP-Modells in ihr Portfolio übernommen wurden. Aufgrund ihrer Herkunft sind traditionelle Produkte beispielsweise nicht für den Betrieb mit Internet-Protokollen optimiert.

In die Kategorie Security as a Service und Security on Demand – beide Begriffe werden weitgehend synonym verwendet – gehören Lösungen, die eigens für den Hosting-Betrieb entstanden sind. Security as a Service und Security on Demand bedeuten: IT-Security-Funktionen für den Schutz vor Viren, vor Spam und Malware jeder Art sind als Services verfügbar. Ein Spezialist für IT-Security betreibt die von ihm entwickelten Lösungen in seinen Rechenzentren und stellt sie Kunden als Dienstleistung bereit – inklusive der Verschlüsselung des gesamten Datenverkehrs. Die ständig steigende Zahl von Angriffen via Web oder E-Mail-Attachments, aber auch der sorglose Umgang mit unternehmenskritischen Daten erhöhen den Handlungsbedarf. Gerade kleine und mittlere Unternehmen fühlen sich überfordert, wenn sie mit ihren beschränkten Ressourcen eine sichere IT-Infrastruktur aufbauen sollen. Security as a Service bietet hier eine attraktive Alternative.

Websense etwa nutzt für seine Security-Services die eigene ThreatSeeker-Technologie. Sie schützt vor Gefahren aus dem Internet, die mit herkömmlichen Verfahren kaum oder nur mit einem überproportional hohen Aufwand zu vermeiden wären. In seinen Security Labs beobachtet Websense mit der ThreatSeeker-Technologie jede Woche mehrere hundert Millionen Webseiten und sucht nach böartigem Programmcode. Parallel dazu scannen die Hosted Security Services wöchentlich Millionen von E-Mails, um damit verbundene Sicherheitsrisiken frühzeitig erkennen zu können. All diese Ergebnisse fließen in die



Security-Services ein.

Frage 2: Anwendungen & Eignung

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

**Antwort Michael Scheffler:**

Virenschutz, Spamfilter, der Zugang zu sicheren Webseiten und Lösungen für Data Loss Prevention sind heute bereits verfügbar. Aber auch Intrusion Detection und Intrusion Prevention sind Anwendungen, die schon als Services angeboten werden. Dazu kommen weitere Themen wie das Management von Firewalls in heterogenen IT-Umgebungen oder auch das Management der Verschlüsselung von mobilen Datenträgern und Endgeräten. Auch hier erweist sich die zentrale Administration als deutlich effektiver. Bei genauem Hinsehen gibt es keine Security-Funktionen, die nicht in Form einer Dienstleistung angeboten werden könnten.

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 Michael Scheffler:**

Einen wirksamen Schutz allein mit unternehmensinternen Ressourcen aufrechterhalten zu wollen, wird immer schwieriger. Es gibt daher sehr gute Gründe, die Sicherheit des E-Mail-Datenverkehrs an einen darauf spezialisierten Dienstleister auszulagern.

Einer der wichtigsten Punkte sind die Kosten. Da liegen die Vorteile von Security as a Service auf der Hand: Statt selbst mit einem beträchtlichen finanziellen und personellen Aufwand die nötige Security-Infrastruktur aufzubauen und zu betreiben, wenden sich immer mehr Mittelständler, aber auch große Konzerne, an Spezialisten, die Sicherheit als Service anbieten. Wer intern eine Lösung aufbaut, muss die Lizenzkosten für Software, die Implementierung, die Beschaffung neuer Hardware, die Schulung der Administratoren und vieles andere berücksichtigen. Dazu kommen die laufenden Kosten für den Unterhalt und die



Wartung. All dies entfällt beim Bezug von IT-Security als Service. Hier fallen lediglich monatliche Gebühren an. Vergleicht man über einen Zeitraum von drei Jahren alle internen Kosten, angefangen von der Software bis zu den Personalausgaben, mit den Raten für eine externe Lösung, ergeben sich bei Security as a Services im Durchschnitt Einsparungen von rund 40 Prozent.

Die Kostenbetrachtung ist jedoch nur der eine Punkt. Ein externer Dienstleister ist darauf angewiesen, dass seine Sicherheitstechnologien und die Hardware immer auf dem neuesten Stand sind. Hier sind permanente Anpassungen und Änderungen erforderlich. Dazu ist der Service Provider schon aufgrund des hohen Wettbewerbsdrucks gezwungen. Oft sehen Unternehmen, die ihre Sicherheitsaufgaben ausgelagert haben, dann erstmals was es heißt, modernste Sicherheitstechnologien für sich arbeiten zu lassen, ohne dafür selbst große Investitionen tätigen zu müssen.

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 Michael Scheffler:

Der gängigste Einwand lautet: IT-Security ist eine unternehmenskritische Aufgabe und muss deshalb auch intern betrieben werden. Untermauert wird dies mit dem Hinweis, dass die internen Ressourcen dazu vorhanden sind. Dabei wird unterstellt, dass es entsprechend qualifiziertes Personal gibt, das einen wesentlichen Teil seiner Arbeitszeit für Security-Aufgaben reserviert. So werden also beträchtliche Ressourcen gebunden, die ansonsten für den Betrieb und die Weiterentwicklung etwa der umsatzrelevanten Kernsysteme eines Unternehmens genutzt werden könnten. Zudem wird unterstellt, dass die Security-Ziele intern besser oder zumindest ebenso gut erreicht werden können wie dies ein externer Security-Spezialist kann, der sich mit nichts anderem als IT-Sicherheit befasst.

Wichtig sind in diesem Zusammenhang auch die Abläufe, bei denen es um die Erfüllung sicherheitstechnischer Vorgaben geht. Ein Beispiel dafür ist die Zertifizierung nach ISO 27001. Bei einem Anbieter von Security-Services wie WebSense sind die Rechenzentren ISO-27001-zertifiziert. Dieses Qualitätssiegel für



seine Security-Prozesse zu erlangen ist enorm aufwändig und bringt einem Unternehmen, das Security intern betreibt, keinen greifbaren Nutzen. Verfügt jedoch der Dienstleister, von dem Security-Services bezogen werden über das Zertifikat, ist dies ein schwergewichtiger Qualitätsbeweis und ein Argument für die Auslagerung von IT-Security.

Wer dann immer noch nicht überzeugt ist, kann eine hybride Lösung nutzen: Der Dienstleister etwa filtert Spam, aber auch Viren und vor Ort gibt es beim Anwender eine Software für ausgehende E-Mails. Unternehmen haben so die Möglichkeit, fein abgestufte Vorgaben für die Inhalte der ausgehenden Mails zu definieren.

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 Michael Scheffler:

IT-Security umfasst heute weit mehr als nur Virenschutz und Spam-Filter. Die Angriffe werden gewiefter und die Vorgehensweise ändert sich ständig. Dazu trägt auch das enorme Aufkommen an komplexen Bedrohungen bei, mit denen die Netzwerke der Unternehmen jeden Tag bombardiert werden. Phishing, Spam-Mails, Trojaner und Viren sind noch immer gefährlich. Dazu kommen vielfältige neue Formen kombinierter Angriffe aus dem Web-2.0-Baukasten, um Malware in unterschiedlichsten Ausprägungen in die Netzwerke einzuschleusen und vertrauliche Daten zu stehlen.

Zunächst einmal zählen die fachlich-technischen Voraussetzungen in den Bereichen Virenschutz, Spam- und Content-Filter, Verschlüsselung des Datenverkehrs und dem Schutz vor neuartigen Bedrohungen aus dem Web 2.0. Darüber hinaus kommt es bei der Provider-Auswahl auf organisatorische Aspekte an.

Ein wichtiges Auswahlkriterium dabei: Kann der Anbieter von Security-Services das notwendige Maß an Datensicherheit, Datenschutz und Vertraulichkeit gewährleisten? Sind diese Punkte geklärt, werden Details zur Verfügbarkeit und der Bereitstellung von Notfallplänen in Service Level Agreements festgehalten.

Das Lösungs- und Serviceportfolio von Websense in den Bereichen Web-, Messaging- und Data-Security reicht von Angeboten für den unternehmensinternen



Einsatz über hybride Security-Produkte bis zu reinen Service-Modellen.

Frage 6: Zukunft und Ausblick

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

**Antwort Michael Scheffler:**

Momentan nutzt hierzulande die große Mehrheit der Unternehmen eine interne IT-Security-Lösung. Das wird sich nach und nach ändern – nicht zuletzt dort, wo als Folge der Finanz- und Wirtschaftskrise die IT-Budgets nach Einsparpotenzialen durchforstet werden. In naher Zukunft bleibt es bei einer Koexistenz von internen und externen Lösungen. Aber auch hybride Modelle, bei denen bestimmte Funktionen intern und andere extern als Service bezogen werden, sind heute schon im Einsatz. Sie sind kennzeichnend für eine Übergangsphase. Auf die nächsten drei bis fünf Jahre betrachtet, werden sich die Security-Services stärker im Markt verbreiten und es ist davon auszugehen, dass sie langfristig die Zahl der internen Lösungen überflügeln. Der Trend geht in diese Richtung. IT-Security ist eine Infrastrukturaufgabe, die in die Hände von Spezialisten gehört.

Vielen Dank für das Interview!