



Security as a Service: Abhängig von Grösse und Agilität der Kunden werden Hardware-, Software- und Servicelösungen koexistieren



Interviewrunde: „Hosted Security & Security as a Service“
Name: Mark Stäheli
Funktion/Bereich: Leiter Business Unit AVANTEC NET (Security-as-a-Service)
Organisation: AVANTEC AG
Homepage Orga: www.avantec.ch/net

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 Marc Stäheli, Leiter Business Unit AVANTEC NET bei der AVANTEC AG dabei folgendermaßen:

„Bei den bestehenden Security Services in den Bereichen E-Mail, Web, Vulnerability Management, IAM und SIEM ist davon auszugehen, dass die Marktanteile ansteigen und insbesondere stärker wachsen als HW/SW-Lösungen. Kaufen werden vor allem kleinere und mittlere Unternehmen, welche zu wenig IT-Ressourcen haben. Aber auch der Mittelstand mit genügend grosser IT wird sich ein Wechsel zu Services auf Grund von Kostenvorteilen überlegen. Insbesondere ist auch davon auszugehen, dass emotionale Hürden mit der Zeit abgebaut werden.“

Viel Spaß beim Lesen wünscht Ihnen Ihr

NetSkill-Team!



Sehr geehrter Herr Stäheli,

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:**

Wichtig ist es zu verstehen, dass beim SaaS-Modell bzw. On-Demand Lösungen Dienste auf Basis von mandantenfähigen Lösungen angeboten werden. Im Gegensatz zu Managed Services, wo für jeden Kunden ein eigenes System betrieben wird, sind dabei die Skalierungseffekte viel grösser. SaaS ist günstiger als Managed Service. Zudem erlaubt das SaaS-Modell, Kunden ihre Einstellungen per Webkonsole selbstständig vorzunehmen und zu kontrollieren.

Die Begriffe werden aber häufig nicht auf verschiedene Weise verwendet, was zu Verwirrungen führen kann.

Frage 2: Anwendungen & Eignung

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

Antwort:

Klassische und bereits reife Dienste findet man bei der E-Mail Content Security, also das Scannen von E-Mails nach Spam und Viren. Ebenfalls bewährt haben sich Vulnerability Management Lösungen, welche als Service die externe Infrastruktur scannen. Auch der firmeneigene Webverkehr kann über einen SaaS-Provider umgeleitet werden, um Inhalte auf böartigen Code zu prüfen und URL-Filter einzusetzen. Wegen der entstehenden Verzögerung sind Web-Security Lösungen noch nicht so stark verbreitet wie E-Mail Security Lösungen. Bei letzteren zeichnen sich immer mehr Zusatzdienste ab, wie beispielsweise das Verschlüsseln oder Archivieren des E-Mail-Verkehrs.

Weniger gut eignen sich Dienste, welche latenzempfindlich sind oder welche Zugriff auf firmeninterne Ressourcen brauchen. Firewall, IDS und IPS Dienste sind daher nicht geeignet. Möglich aber, dass Netzwerkprovider und ISP solche Services in Zukunft mitanbieten.



Erste Lösungen sind zudem in den Bereichen IAM (Identity und Access Management) und SIEM (Security Information & Event Management) zu beobachten. Bis zur Marktreife dürften aber noch einige Jahre vergehen.

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

Die Kostenvorteile ergeben sich aus dem Wegfall von Investitions- und Betriebskosten und dem weitaus tieferen Aufwand für den Systemunterhalt. Der Kunde zahlt lediglich eine monatliche Servicegebühr. Exakte Kostenvergleiche sind schwierig, weil gerade die Systemunterhaltskosten nicht transparent sind. Wie viele Stunden stecken Systemadministratoren in Schulung, Training, Trouble-Shooting, Updates, Testing, Backup, Disaster Recovery etc.? Meist wird diese Komponente sehr stark unterschätzt. Studien gehen davon aus, dass sich IT-Mitarbeiter bis zu 80% um den Betrieb von bestehenden Lösungen kümmern müssen. Selbstverständlich gibt es hier unter den Systemen grosse Unterschiede was den Aufwand für den Systemunterhalt betrifft.

Häufig sieht man bei Preisvergleichen zwischen HW/SW-Lösungen und Services, dass die SaaS-Variante nur unwesentlich günstiger ist. Unter dem Aspekt des fehlenden Systemunterhalts schneidet SaaS dann aber wirtschaftlich deutlich besser ab.

Zu bedenken gilt es jedoch mit realistischen Systemlaufzeiten zu rechnen und den Vergleich über 3-5 Jahre zu erstellen.

Weitere Kostenvorteile für SaaS ergeben sich aus der flexiblen Skalierbarkeit und der raschen Implementierung.

**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**

Kontrollverlust und Abhängigkeit von einem externen Anbieter sind in der Regel die Bedenken. Zum Kontrollverlust gibt es zu bedenken, dass der Kunde gerade bei SaaS-Lösungen per Web viele Einstellungen selbst vornehmen und den Service überwachen kann.

Was die Abhängigkeit und allfällige Sicherheitsbedenken betrifft, gilt es zu beachten, dass viele Security SaaS Provider über professionelle Betriebsabläufe und hochsichere IT-Infrastrukturen verfügen.

Viel häufiger ist die Zurückhaltung aber auch emotional begründet, weil man diese Aufgaben einfach nicht ausser Haus geben will.

Klare Kostenvorteile können hier den Widerstand brechen. Zudem bleibt zu erwähnen, dass sehr viele Grossunternehmen solche Dienste einsetzen.

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**

Wichtig ist: man kauft nicht nur ein Produkt, sondern in erster Linie ein Service. Erfahrung in der Erbringung von Services ist sehr wichtig, wie auch die zugehörigen SLA.

Bei Preise muss darauf geachtet werden, dass saubere Vergleiche durchgeführt werden. Pay-per-Use wird nicht von allen gleichermassen ausgelegt.

Lange Vertragslaufzeiten ergeben Rabatte verhindern dadurch aber auch einen frühzeitigen Providerwechsel.

Auch die SLA sollten bei schwerwiegenden Verstössen dem Kunden die Möglichkeit lassen den Service ausservertraglich aufzukündigen.

Bei ausländischen Service-Providern lohnt sich zudem ein lokaler Partner, der Support bietet inkl. lokale Veträge und Eskalationsmöglichkeit gegenüber dem Leistungserbringer.



Frage 6: Zukunft und Ausblick

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



Antwort

Bei den bestehenden Security Services in den Bereichen E-Mail, Web, Vulnerability Management, IAM und SIEM ist davon auszugehen, dass die Marktanteile ansteigen und insbesondere stärker wachsen als HW/SW-Lösungen. Kaufen werden vor allem kleinere und mittlere Unternehmen, welche zu wenig IT-Ressourcen haben. Aber auch der Mittelstand mit genügend grosser IT wird sich ein Wechsel zu Services auf Grund von Kostenvorteilen überlegen. Insbesondere ist auch davon auszugehen, dass emotionale Hürden mit der Zeit abgebaut werden.

Es wird sich eine Koexistenz einstellen von HW-, SW- und Servicelösungen je nach Grösse und Agilität der Kunden.

Vielen Dank für das Interview!