

Managed Security: Viren, Spam und Phishing abfangen bevor sie das Unternehmen erreichen



Interviewrunde: „Hosted Security & Security as a Service“
Name: Robert Rothe
Funktion/Bereich: Gründer und Geschäftsführer
Organisation: eleven GmbH
Homepage Orga: www.eleven.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 Robert Rothe, Gründer und Geschäftsführer der eleven GmbH dabei folgendermaßen:

„Aufgrund der zahlreichen Vorteile – Risikominimierung, Kosteneffizienz und lückenloser Schutz vor immer komplexeren Gefahren – gehört Managed Services im Bereich der E-Mail-Sicherheit die Zukunft, denn vor dem Hintergrund fortgesetzten Spam-Wachstums sind Modelle gefragt, die Zukunftssicherheit garantieren und auch vor immer neuen Spam-Spitzen nicht in die Knie gehen und gleichzeitig Kosten und Aufwand sparen. Ein zweiter wesentlicher Aspekt sind die immer komplexer werdenden Anforderungen an die E-Mail-Sicherheit. In Zukunft wird das Thema Compliance-konforme E-Mail-Archivierung erheblich an Bedeutung gewinnen. Diese unterschiedlichsten Anforderungen inhouse zu bewältigen, erfordert ein Maß an Ressourcen, aber auch Expertise, das sich viele Unternehmen zukünftig weder leisten wollen noch können. Integrierte Managed E-Mail Security Services bieten die Antwort auf diese Anforderungen.“

Viel Spaß beim Lesen wünscht Ihnen Ihr

NetSkill-Team!



Sehr geehrter Herr Rothe,

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 Robert Rothe:**

Die Grenzen sind fließend, was dazu führt, dass die Begriffe oft synonym eingesetzt werden. Wichtiger als die Unterschiede ist jedoch die Gemeinsamkeit all dieser Konzepte, denn die Grundidee ist jeweils die gleiche: IT-Sicherheitsdienstleistungen werden einem externen Dienstleister übertragen, der diese außerhalb des Unternehmensnetzwerks umsetzt. Unterschiede gibt es lediglich in der Art und Weise und im Umfang dieser Auslagerung. Manche Unternehmen wollen nur einzelne Komponenten auslagern, andere ihre gesamte E-Mail-Infrastruktur. Entscheidend ist aber, das Konzept, IT-Sicherheit einem Spezialisten zu überlassen, wie man ja auch viele andere Bereiche Spezialisten überlässt. Angesichts der immer komplexer werdenden Bedrohungen der IT-Sicherheit gewinnt dieser Ansatz bei Unternehmen jeder Größe zunehmend an Bedeutung.

Frage 2: Anwendungen & Eignung

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

Antwort Robert Rothe:

Vor allem im Bereich der E-Mail-Sicherheit gibt es wenig, was sich nicht als Managed Service auslagern lässt. Ob Anti-Spam, Anti-Virus oder E-Mail-Firewall: Alles lässt sich problemlos an einen spezialisierten Dienstleister auslagern. Dabei gewinnen vor allem integrierte E-Mail-Sicherheitsmaßnahmen an Zuspruch: Statt sich gegen einzelne Gefahren, wie Spam, Viren oder Denial-of-Service-Attacken zu schützen, gelten die Schutzmaßnahmen der gesamten E-Mail-Infrastruktur und der Sicherstellung legitimer E-Mail-Kommunikation zu jedem Zeitpunkt. Hier bieten ausgelagerte Managed Services echte Vorteile, ermöglichen sie Unternehmen doch einen Rundum-Schutz



ohne massive Eingriffe in die eigene IT-Landschaft und ohne jeglichen Wartungsaufwand – betreut von Experten, die sich darauf spezialisiert haben.

Die Vorteile einer Auslagerung sind vielfältiger Natur. Der wichtigste: Viele Gefahren können gar keinen Schaden, mehr anrichten, da sie bereits abgefangen werden, bevor sie das Unternehmen erreichen können. Dies gilt insbesondere für die E-Mail-Sicherheit, also für Viren, Phishing-E-Mails oder auch Spam, der heute mehr als 95 Prozent des täglichen E-Mail-Aufkommens ausmacht. Auch Denial-of-Service-Attacken, wie beispielsweise Mailbombings, können auf diese Weise abgewehrt werden.

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 Robert Rothe:

Im Bereich der E-Mail-Sicherheit bestehen erhebliche Kostenvorteile. Im Durchschnitt kann mehr als 95 Prozent des täglichen E-Mail-Aufkommens als Spam ausgefiltert werden, bevor es das Unternehmen überhaupt erreicht. Der Administrationsaufwand entfällt vollständig, die für den E-Mail-Empfang eingesetzten Hardwareressourcen und damit auch die Energie- und Betriebskosten können drastisch, nicht selten sogar um das Zehnfache, gesenkt werden. Und vor allem: Sie bleiben auch in Zukunft stabil, da nur noch das legitime E-Mail-Aufkommen das Unternehmen erreicht. Die Zeiten, in denen die Hardwareressourcen von Unternehmen immer wieder dem steigenden Spam-Volumen angepasst werden mussten, sind mit Managed Services vorbei. Ausgelagerte E-Mail-Sicherheit paart Kosteneffizienz mit Zukunftssicherheit.

**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 Robert Rothe:**

Die größte Angst vieler Unternehmen ist, einen so sensiblen Bereich wie die IT-Sicherheit in fremde Hände zu geben. Das gilt ganz besonders für die E-Mail-Kommunikation, das geschäftliche Kommunikationsmedium Nummer 1. Unternehmen versenden vertrauliche und hochsensible Informationen, per E-Mail, z. B. Angebote, Rechnungen oder Aufträge, und das nicht selten unverschlüsselt. Ihre wichtigste Frage: Sind sensible Daten, z. B. die Inhalte wichtiger Geschäfts-E-Mails, sicher, wenn ich sie außer Haus gebe?

Hier sind vor allem drei Aspekte entscheidend: 1. Wird durch die eingesetzte Lösung der Zugriff und damit der Missbrauch auf die Inhalte der E-Mail ermöglicht? Hier haben beispielsweise inhaltsbasierte Technologien, welche die E-Mail auf bestimmte Wörter oder Phrasen hin durchsuchen, das Nachsehen. 2. Betreibt der Dienstleister seine Infrastruktur in einem Land mit strengster Datenschutzgesetzgebung, idealerweise Deutschland? 3. Hat der Dienstleister ein Interesse am Sammeln und Nutzen von Daten, weil er beispielsweise sein Geld mit entsprechenden Angeboten, z. B. zielgruppenspezifischem Marketing, verdient? Wer diese drei Punkte beachtet, kann seine E-Mail-Sicherheit guten Gewissens auslagern.

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 Robert Rothe:**

Im Bereich E-Mail-Sicherheit sind neben den bereits genannten vor allem drei Punkte von Bedeutung: Sie müssen 1. zuverlässig vor Spam und anderer Malware schützen (Erkennungsrate über 99 Prozent), 2. Fehlkategorisierungen legitimer E-Mails verhindern (False-Positive-Rate unter 0,00001 Prozent) und 3. sicherstellen, dass die geschäftsrelevante E-Mail-Kommunikati-



on auch bei höchster Belastung – z. B. durch Denial-of-Service-Attacken oder Spam-Wellen – aufrechterhalten bleibt.

eleven bietet Unternehmen jeder Größe integrierte E-Mail-Sicherheitslösungen, die zuverlässig vor Spam, Viren, Phishing sowie anderer Malware schützen und die genannten Anforderungen mühelos erfüllen. Zudem erfordern sie keinerlei Wartung und Pflege. Die unerreichte Leistungsfähigkeit der eleven Lösungen – bis zu 5.000 E-Mails pro Sekunde pro Server – stellt zudem sicher, dass sich auch einem weiteren Spam-Wachstum gewachsen sein werden. eleven bietet Managed Services ebenso wie Inhouse-Software-Lösungen. Wir passen uns den spezifischen Anforderungen des Unternehmens an und finden gemeinsam die passende Lösung.

Frage 6: Zukunft und Ausblick

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



Antwort Robert Rothe:

Aufgrund der zahlreichen Vorteile – Risikominimierung, Kosteneffizienz und lückenloser Schutz vor immer komplexeren Gefahren – gehört Managed Services im Bereich der E-Mail-Sicherheit die Zukunft, denn vor dem Hintergrund fortgesetzten Spam-Wachstums sind Modelle gefragt, die Zukunftssicherheit garantieren und auch vor immer neuen Spam-Spitzen nicht in die Knie gehen und gleichzeitig Kosten und Aufwand sparen.

Ein zweiter wesentlicher Aspekt sind die immer komplexer werdenden Anforderungen an die E-Mail-Sicherheit. Ging es zunächst nur um die Abwehr von Viren, kam später der Schutz vor Spam, Phishing und anderer Malware hinzu. Heute steht der Schutz vor Überlastung und die Aufrechterhaltung legitimer E-Mail-Kommunikation zu jedem Zeitpunkt im Mittelpunkt. In Zukunft wird das Thema Compliance-konforme E-Mail-Archivierung erheblich an Bedeutung gewinnen. Diese unterschiedlichsten Anforderungen inhouse zu bewältigen, erfordert ein Maß an Ressourcen, aber auch Expertise, das sich viele Unternehmen zukünftig weder leisten wollen noch können. Integrierte Managed E-Mail Security Services bieten die Antwort auf diese Anforderungen.

Vielen Dank für das Interview!