



MESSAGING- UND INTERNET SECURITY IN DER CLOUD – MEHR SICHERHEIT, WENIGER KOSTEN

EIN WHITEPAPER FÜR BUSINESS- UND IT-ENTSCHEIDER

VON SYMANTEC HOSTED SERVICES

EINLEITUNG

Messaging Security, also der Schutz der E-Mail- und Internet-kommunikation vor unberechtigtem Zugriff und gefährlichen Attacken ist in Zeiten wachsender Bedrohung durch Cyberkriminalität ein absolutes Muss für jedes Unternehmen.

Im Jahresbericht 2009 kommt MessageLabs Intelligence¹ zum erschreckenden Ergebnis, dass jede 286. E-Mail mit einem Schadprogramm verseucht ist und eine von 325 E-Mails einen Phishing-Angriff darstellt. Bei 87 % sämtlicher E-Mails handelt es sich um lästige Spam-Mails. Und jeden Tag werden über 2.400 neue Webseiten mit Schadprogrammen entdeckt.

Viele Unternehmen haben das erkannt und klassische Gegenmaßnahmen in Form lokal installierter Security-Software wie Antispam- und Antivirus-Lösungen oder Phishing-Filtern ergriffen.

Das ist gut und schützt auch bis zu einem gewissen Grad, verursacht aber hohe Lizenzkosten und beträchtliche Investitionen in eine leistungsfähige Infrastruktur, was wiederum die Verwaltungs- und Wartungskosten in die Höhe treibt. Denn für die genannten 87 % Spam-Mails müssen Sie teure Mail-Server- und Übertragungskapazitäten bereitstellen, die Sie eigentlich gar nicht brauchen. Nicht zu vergessen, dass sämtliche Malware und verseuchten Daten auf Ihrer Infrastruktur landen, wodurch weitere Sicherheitsrisiken heraufbeschwört werden.

Wäre es da nicht viel sinnvoller und sicherer, unerwünschte Mails abzufangen, bevor sie Ihr Datennetz erreichen? Und wäre es nicht viel effizienter, auf teure Server- und Netzwerk-Überkapazitäten verzichten zu können?

Hier kommen Cloud Computing bzw. Cloud Services ins Spiel. Der ITK-Branchenverband BITKOM definiert Cloud Computing als "eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand²."

Konkreter und Messaging Security-spezifisch gesagt: Ein externer IT-Dienstleister ermöglicht Ihnen über seine Cloud Umgebung den Zugriff auf spamfreie E-Mails und spywarefreie Websites, ohne dass Sie sich um die dazu notwendigen Technologien und Softwarelösungen kümmern müssen.

Auch die Experten von IDC betrachten Hosted Security Services als äußerst sinnvolle Alternative: "Lokal installierte Sicherheitssysteme sind der hochentwickelten Gefahrenlandschaft nicht mehr gewachsen. Die Expertise von IT-Ressourcen ist für den damit verbundenen Verwaltungs- und Überwachungsaufwand nicht effizient eingesetzt. Zudem kann die Entwicklung einer umfassenden Sicherheits-Infrastruktur die Komplexität für viele Unternehmen stark erhöhen. Managed Services werden somit zu einer attraktiven Option."³

Klingt einfach. Aber funktioniert das denn? Ist das auch wirklich sicher? Wie steht es mit der Verfügbarkeit? Und spare ich damit tatsächlich Geld? Dieses Whitepaper über "Messaging Security in der Cloud" gibt Antworten.

¹MessageLabs Intelligence; 2009 Annual Security Report http://de.messagelabs.com/download.get?filename=2009MLIAnnualReport_Final_EN-DE.pdf

²BITKOM-Leitfaden: Cloud Computing – Evolution in der Technik, Revolution im Business

³IDC Whitepaper: Datacenter-Delivered Services: The Service provider Opportunity

CLOUD COMPUTING UND CLOUD SERVICES: VON PRIVATEN, ÖFFENTLICHEN UND GEMISCHTEN CLOUDS

Während Cloud Computing generell das Angebot Internet- und nutzungsbasierter IT-Leistungen beschreibt, sind mit Cloud Services die konkreten IT-Leistungen gemeint, auf die Privat- und Geschäftskunden Zugriff erhalten.

Dabei lassen sich drei grundsätzliche Cloud Services Modelle unterscheiden:

- **Public Cloud Services:** Public Cloud Services werden von IT-Dienstleistern für die breite Öffentlichkeit angeboten. Der Zugriff darauf ist auf keine spezifischen Nutzergruppen beschränkt. Die Möglichkeiten der Services werden vom Anbieter definiert und können meist nicht individuell angepasst werden.
- **Private Cloud Services:** Private Cloud Services werden exklusiv für ein Unternehmen zusammen- und bereitgestellt. Nur Sie als Kunde erhalten darauf Zugriff. Und Sie als Kunde bestimmen, welche Services Sie in welcher Form und mit welchem Leistungsumfang nutzen möchten.
- **Hybrid Cloud Services:** Hybrid Cloud Services vereinen das Beste aus beiden Welten. Hier können standardisierte und individuell angepasste Services kombiniert werden, um eine homogene Gesamtlösung für Ihr Unternehmen zu erreichen.

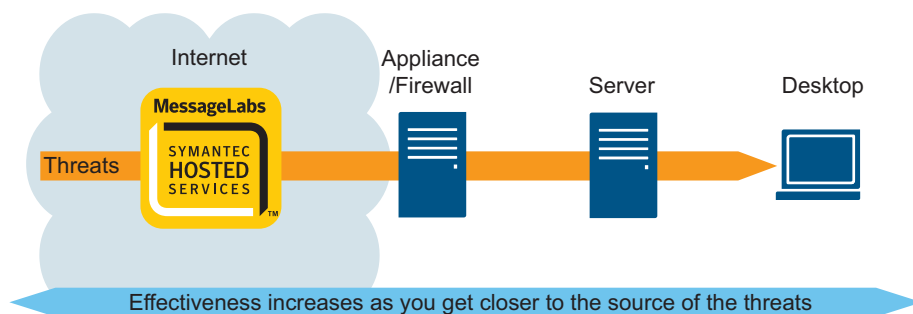
Bei allen Unterschieden lassen sich zwischen den verschiedenen Cloud Service Modellen einige Gemeinsamkeiten feststellen:

- **Nutzung on Demand:** Sämtliche Services können bei Bedarf genutzt werden. Damit müssen Sie keine eigenen Softwarelizenzen kaufen, installieren und warten.
- **Flexible Skalierbarkeit:** Sie möchten mehr Anwendern den Zugriff ermöglichen oder neue Services integrieren? Kein Problem. Eine Erweiterung ist zumindest bei Private und Hybrid Cloud Services jederzeit möglich.
- **Mandantenfähigkeit:** Die Cloud Infrastruktur wird hocheffizient genutzt und optimal ausgelastet, da die Services für eine Vielzahl an Kunden („Mandanten“) auf der gleichen Plattform angeboten werden. Damit werden die Kosten pro Anwender erheblich reduziert, was sich wiederum positiv auf die veranschlagten Servicekosten auswirkt.
- **Einfache Bedienung per Self-Service:** Alle Services können von den Anwendern per Web-Browser genutzt und individuell angepasst werden. Dies entlastet die IT-Abteilung von zeit- und kostenintensiven Softwareanpassungen und Testläufen sowie Installations- und Wartungsaufgaben.
- **Pay per Use / Pay as you go:** Sie bezahlen nur für die tatsächliche Nutzung der Services, ohne Lizenzgebühren für lokale Software, ohne ein veraltetes prozessorbasiertes Abrechnungssystem oder hohe regelmäßige Fixkosten.

INFRASTRUCTURE AS A SERVICE ODER SOFTWARE AS A SERVICE?

Diese generellen Vorteile von Cloud Computing bzw. Cloud Services gegenüber lokalen Software-Installationen sprechen schon für sich. Aber wie lassen sich diese auf den Bereich Messaging Security übertragen? Ein konkretes, grobkörniges Szenario könnte das dann so aussehen:

Ein externer IT-Dienstleister stellt sämtliche Securitylösungen wie AntiVirus- und AntiSpam-Lösungen, Antispyware, E-Mail-Verschlüsselung und Web-Contentfilter in seiner Cloud Umgebung bereit. Sie als Unternehmen stellen sich Ihr Lösungsportfolio nach Ihren individuellen Anforderungen modular zusammen. Der gesamte E-Mail-Verkehr und Internetzugriff wird über die Cloud Umgebung im Rechenzentrum des Dienstleisters auf Internetebene kontrolliert, also noch bevor Spam und Malware Ihre Infrastruktur infizieren kann. Nur absolut sichere E-Mails und Websites mit geprüftem Content erreichen Ihr Netzwerk hinter der Firewall. Sie bezahlen nur für die konkrete Nutzung. Und Sie können bei wachsenden Anforderungen wie etwa bei Firmenzukäufen Ihre „Messaging Security Cloud“ problemlos erweitern.



Dabei lassen sich zwei grundlegende Bereitstellungsmodelle unterscheiden, wie Sie in den Genuss Ihrer Messaging Security Cloud kommen:

Infrastructure as a Service (IaaS): Bei IaaS stellt der IT-Dienstleister Ihnen die komplette Hardware- und Security-Software-Umgebung zur Verfügung, die Sie für Ihre Anforderungen benötigen.

Software as a Service (SaaS): Bei SaaS bietet Ihnen der Hosted Service Provider auf seiner Infrastruktur dedizierte Security-Softwarelösungen, die Sie browserbasiert über das Internet nutzen können.

Welche Bereitstellungsform für Ihr Unternehmen in Frage kommt, hängt natürlich von Ihren individuellen Anforderungen ab. In beiden Fällen liegen die Vorteile gegenüber der Nutzung gekaufter Softwarelizenzen mit eigenen Server-Ressourcen auf der Hand:

- **Reduzierter Investitionsbedarf:** Sie sparen sich hohe Investitionen in Lizenzen für Security- und Messaging-Software sowie Server- und Netzwerk-Kapazitäten, die Sie eigentlich gar nicht brauchen und nur durch überflüssige Spam-Mails auslasten können.
- **Kalkulierbare Kosten:** Sie bezahlen nur für die tatsächliche Nutzung der Infrastruktur bzw. der Security-Software und müssen keine unabsehbaren Folgekosten befürchten.
- **Reduzierte Gesamtkosten (TCO):** Da mehrere Unternehmen die virtualisierte Infrastruktur des Hosted Service Providers nutzen, entstehen Skaleneffekte, die sich in günstigen Gesamtkosten niederschlagen. Sie zahlen schlicht und einfach nur für die Ressourcen, die Sie tatsächlich nutzen. Teure Überkapazitäten sind damit passé.
- **Maximale Entlastung:** Der Hosted Service Provider übernimmt die komplette Administration und Wartung Ihrer Cloud Services. Ihre eigene IT-Abteilung wird entlastet und kann die freien Kapazitäten z.B. für strategische IT-Projekte einsetzen. Darüber hinaus müssen sich Ihre Mitarbeiter nicht in neue Security Lösungen einarbeiten und profitieren von der umfangreichen Expertise des Cloud Service Anbieters.

- **Transparente Service Level:** Die Einhaltung der SLAs werden durch den IT-Dienstleister dokumentiert und garantiert. Auch eine Anpassung der Service Level bei neuen Anforderungen wie steigenden Nutzerzahlen ist problemlos möglich.
- **Flexible Erweiterbarkeit:** Dank der virtualisierten Ressourcen ist eine Erweiterung der benötigten Kapazitäten kein Problem. Wachsen Sie, wächst Ihre Messaging Security Cloud einfach mit.
- **Aktuelle Technologien:** Investieren Sie immer in die neuesten am Markt erhältlichen Technologien? Sicher nicht. Der Zeit- und Kostenaufwand wäre einfach zu hoch. In der Cloud können dagegen z.B. neue Software-Versionen sofort bereitgestellt werden, ohne dass Sie sich darum kümmern müssen. Langwierige Evaluierungen, Implementierungen und Testläufe fallen damit flach. Sie nutzen einfach jederzeit die besten Technologien.

MESSAGELABS: DER PIONIER FÜR MESSAGING SECURITY HOSTED SERVICES

Es gibt noch in vielen Unternehmen Vorbehalte gegen Cloud Computing und Hosted Services. Meist kreisen die Bedenken um die Verfügbarkeit und Sicherheit der Services.

So mahnt beispielsweise der Hightech Verband BITKOM⁴: „Eine stärkere Akzeptanz von Cloud Computing setzt voraus, dass die Anbieter dessen Vorzüge in Referenzprojekten dem Markt beweisen. ... Das betrifft in erster Linie die rechtliche Situation, die Sicherheit und den Datenschutz, aber auch die Integrationsfähigkeit mit den vorhandenen IT-Systemen sowie Fragen von Verfügbarkeit, Performanz und der ganzheitlichen reibungsfreien Unterstützung der Geschäftsprozesse.“

Kurz gesagt: Unternehmen auf dem Weg in die Cloud sollten nicht nur auf ein umfangreiches Service-Portfolio des Hosted Service Providers achten, sondern vor allem auch auf nachgewiesene Kompetenz und Erfahrung in anspruchsvollen Projekten.

MessageLabs ist ein Tochterunternehmen des amerikanischen Software-Herstellers Symantec und die weltweite Nummer Eins bei Hosted Security Lösungen für Unternehmen. Gemeinsam mit Symantec liegt MessageLabs mit über 50% mehr Umsatz als der nächste Wettbewerber klar vor der Konkurrenz.⁵ Während Gartner das Unternehmen im aktuellen Magic Quadrant 2010 als „Leader“ bei Secure E-Mail Gateways listet⁶, nimmt MessageLabs auch bei Forrester Wave™ in punkto E-Mail-Filterung die Spitzenposition ein⁷.

Weltweit setzen rund 22.000 Kunden von kleinen Firmen bis zum Fortune 500-Unternehmen mit insgesamt über 9 Millionen Anwendern in 102 Ländern auf die MessageLabs Hosted Services von Symantec. Warum? Nun, die Erfolge im Kampf gegen Spyware, Viren und Spam sprechen eine deutliche Sprache:

- Täglich werden in den 14 weltweit verteilten, hochverfügbaren Rechenzentren rund 25 Milliarden E-Mails und 1 Milliarde Webzugriffe geprüft, von denen nicht ein Mal 15 Prozent als „erwünscht“ zu den Kunden weitergeleitet werden.
- Pro Tag werden 200 neue Viren durch die MessageLabs Kern technologie Skeptic™ erkannt, die von Securitylösungen anderer Anbieter übersehen werden.
- Das Risiko der Virusinfektion eines Unternehmens mit 3.000 Mitarbeitern liegt mit herkömmlichen Securitylösungen bei rund 70 Prozent, mit den Symantec Hosted Services nachweislich bei unter einem Prozent.
- MessageLabs gewährleistet in den Service Level Agreements eine nahezu hundertprozentige Erkennungsquote von unbekannter Malware.
- Unternehmen können sich rund um den Globus auf 24/7 Support in 7 Sprachen verlassen.
- 95 Prozent aller Kunden sind mit der Bearbeitung der Support-Tickets zufrieden.

Beeindruckende Zahlen, aber was bedeutet das für Ihr Unternehmen. Und welche Hosted Services stehen Ihnen konkret in der Cloud zur Verfügung?

⁴BITKOM-Leitfaden: Cloud Computing – Evolution in der Technik, Revolution im Business

⁵IDC: Worldwide Network Security 2009-2013 Forecast and 2008 Vendor Shares, Januar 2009

⁶Gartner Research: Magic Quadrant for Secure E-Mail Gateways, April 2010

⁷Forrester Wave™: Email Filtering, Q2 2009

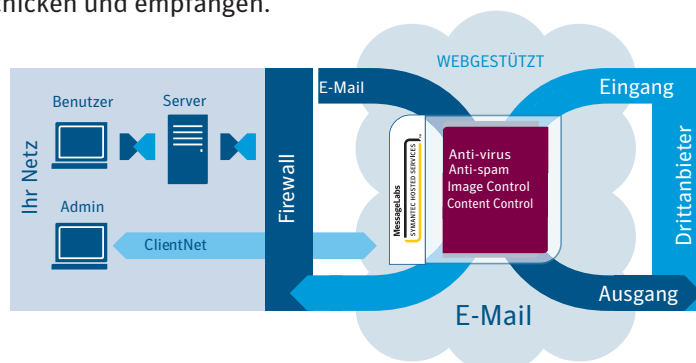
SYMANTEC HOSTED SERVICES: LÜCKENLOSE MESSAGING SECURITY IN DER CLOUD

MessageLabs bietet Unternehmen jeder Größe mit den Symantec Hosted Services ein umfangreiches Portfolio zum Schutz der E-Mail- und Instant Messaging-Kommunikation sowie für sicheren Webzugang.

E-MAIL SECURITY

In den MessageLabs Rechenzentren wurde im Februar 2010 eine E-Mail-Spamrate von enormen 89,4% gemessen. Von rund 300 E-Mails enthielt mindestens eine einen gefährlichen Virus. D.h. dass 9 von 10 ankommenden E-Mails und selbstverständlich sämtliche Viren herausgefiltert werden sollten, bevor Sie Ihre Infrastruktur erreichen.

- AntiSpam:** Der AntiSpam-Filter bietet effektiven Schutz durch mehrschichtige Abwehr-Technologien. So garantieren wir Ihnen über Service Level Agreements, dass 99 Prozent des Spams draußen bleiben (tatsächlich filtern wir sogar 99,99999% heraus!). Und wir sichern Ihnen maximal 0,0003% fälschlich aussortierter E-Mail zu, was wir in der Praxis mit 0,000006% weit übertreffen. Ganz gleich, ob Sie Exchange Server, GroupWise oder Lotus Notes-Domino einsetzen: Der AntiSpam-Filter von MessageLabs harmoniert reibungslos mit jedem SMTP-fähigen Messaging-System. Im Zusammenspiel mit unserem MessageLabs AntiVirus können Sie die Sicherheit Ihrer E-Mail-Kommunikation noch einmal deutlich erhöhen.
- AntiVirus:** Die signaturbasierter Anti-Virus-Lösung mit unserer Kerntechnologie Skeptic™ schützt Ihr Unternehmen zuverlässig vor bekannten und unbekanntem Schadprogrammen. Als einziger Dienst auf dem Markt sichert Ihnen unser mehrschichtiger Abwehr-Service über SLAs einen umfassenden Schutz vor Viren zu – sowohl für ältere als auch für neue Computerschädlinge. Darüber hinaus garantieren wir Ihnen maximal 0,001% fälschlich aussortierte E-Mails, was uns mit echten 0,000004% problemlos gelingt. So bleiben Ihnen die Folgekosten eines Virenbefalls erspart. Sie sind vor Ausfallzeiten Ihrer IT-Systeme ebenso zuverlässig geschützt wie vor Produktivitätseinbußen und Imageverlusten.
- Image Control:** Unser Hosted Service für die Bilddatei-Kontrolle im E-Mail-Verkehr durchleuchtet mit Verfahren der ICA-Bildanalyse (Image Composition Analysis) jede zu übermittelnde Nachricht und deren Anhänge. So gelingt es uns, alle unangemessenen Grafikdateien wie etwa pornografische Inhalte zuverlässig aufzuspüren und aufzuhalten, bevor sie Schaden anrichten können.
- Content Control:** Zur Überprüfung gefährlicher Web-Inhalte werden die Inhalte und Anhänge aller E-Mails, die Ihre Mitarbeiter versenden oder erhalten, mit Scanning-Technologien durchleuchtet. Dabei haben Sie es über Ihren System-Administrator stets selbst in der Hand, wie umfassend die Prüfung ausfällt und wie scharf der Filter eingestellt ist.
- E-Mail-Continuity:** Mit unserer E-Mail-Continuity-Lösung bewahren wir Sie zuverlässig vor Störungen Ihrer Geschäftsaktivitäten und vor Datenverlusten, wenn es zum Ausfall Ihres E-Mail-Systems kommen sollte. Sie können auf ein Notfallsystem bauen, das immer dann einspringt, wenn Ihr eigentlicher E-Mail-Server nicht verfügbar ist oder wegen Wartungsarbeiten vorübergehend abgeschaltet werden muss. So können Ihre Mitarbeiter auch in dieser Zeit unterbrechungsfrei E-Mails verschicken und empfangen.

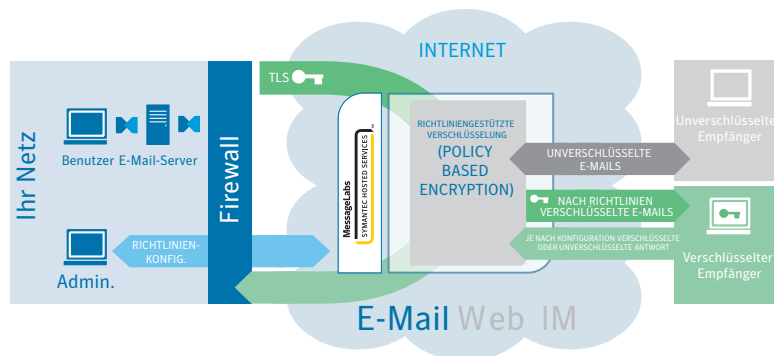


ENCRYPTION

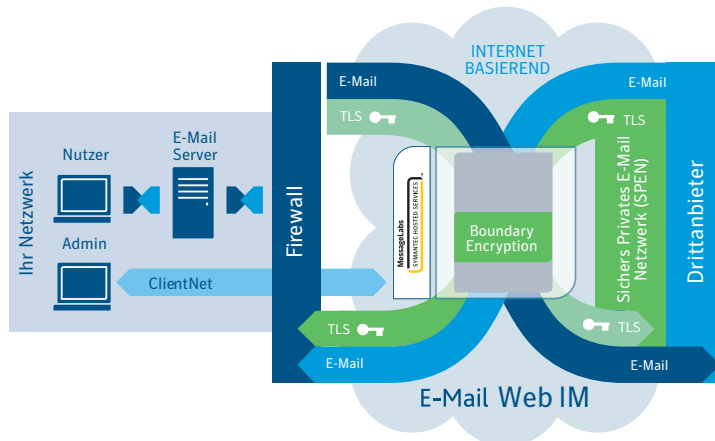
MessageLabs bietet Ihnen für die Sicherheit Ihrer E-Mail-Kommunikation einen Hosted Encryption Service, der die Vorteile einer richtlinien- und regelgesteuerten Verschlüsselung und einer durchgängigen Boundary Encryption in einer Lösung kombiniert.

Damit sind Sie jederzeit auf der sicheren Seite - ganz gleich, ob Sie die komplette E-Mail-Kommunikation zwischen Mitarbeitern und Geschäftspartnern verschlüsseln wollen oder alle E-Mails mit vertraulichen Daten wie Sozialversicherungsnummern, Kennworten oder Kreditkarteninformationen zuverlässig vor fremden Blicken schützen möchten.

- Policy-Based-Encryption:** Mit der regelsteuerten Verschlüsselung können Sie eindeutige Richtlinien vorgeben, nach denen alle ein- und ausgehenden Nachrichten automatisch chiffriert werden. Als Kriterien, die darüber bestimmen, ob und wie die Verschlüsselung einer E-Mail erfolgt, kommen beispielsweise deren Inhalte, Absender und Empfänger oder Dateianhänge in Frage. Damit können Sie nun auch vertrauliche Dokumente, die Sie bisher per Post verschickt haben, wie Lohnzettel, Bewerbungsunterlagen, Rechnungen und Kontoauszüge, auf sichere Weise per E-Mail versenden.



- Boundary Encryption:** Beim Boundary Encryption Service wird die E-Mail-Korrespondenz mit allen Nachrichten und Dateianhängen zwischen Ihrem Unternehmen und allen hierfür ausgewählten Firmen verschlüsselt. Das Resultat ist ein Höchstmaß an Diskretion und Datenschutz.



WEB-PROTECT & CONTROL

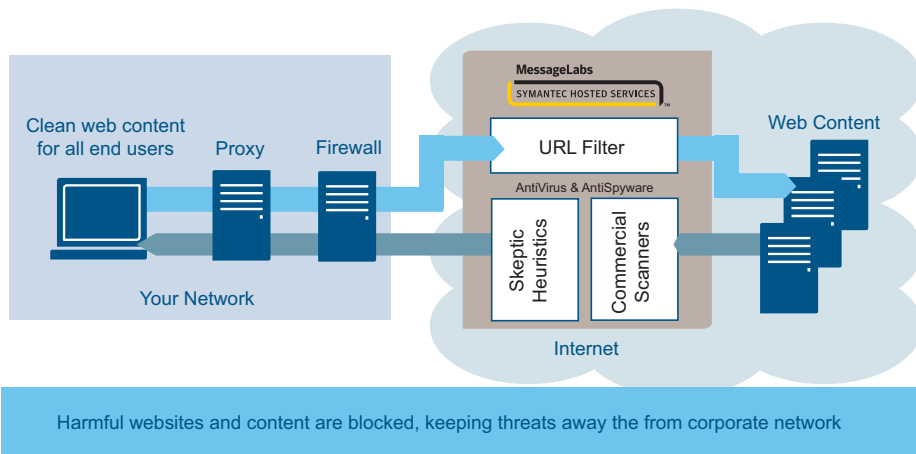
Um Viren und Spyware abzufangen und Ihr Netzwerk einschließlich aller mobilen Anwender vor Malware-Gefahren zu schützen, überprüfen die Hosted Web-Security-Services von Mitarbeitern aufgerufene URLs auf Verdachtsmomente hin und sperren diese bei Gefahr.

- **Web URL-Filtering:** Mit unserem URL-Filter behalten Sie die volle Kontrolle darüber, auf welche Weise Ihre Belegschaft im Internet surft. Gleichzeitig sind Sie in der Lage, den Zugriff auf bestimmte Websites anhand der Internetadressen, der Tageszeit oder der Dateitypen zu unterbinden. So schützen Sie Ihr Unternehmen zuverlässig vor den juristischen und finanziellen Konsequenzen, die Ihnen drohen können, wenn Ihre Mitarbeiter das Internet auf unangemessene Weise nutzen.

Der Web-Filter von MessageLabs bietet Ihnen vielfältige Konfigurationsmöglichkeiten und basiert auf einer ausgeklügelten Datenbank mit einem Verzeichnis verdächtiger und einschlägig bekannter Websites. Auf dieser Grundlage können Sie eigene Richtlinien und Regeln für die Kontrolle der Internetnutzung verankern.

- **Web-Sicherheit:** Die Zahl bisher vertrauenswürdiger Websites, die nun Schadprogramme wie Spyware oder Viren verbreiten, wächst ständig. Diese werden automatisch heruntergeladen und installiert, sobald ein User die entsprechenden Links anklickt.

Der MessageLabs Hosted Service für Viren- und Spyware-Abwehr im Web unterbindet zuverlässig den Download von Spionageprogrammen und garantiert Ihnen über SLAs die Abwehr von 100 Prozent aller via Internet verbreiteten Viren. Dazu nutzen wir mehrere Scanning-Verfahren, die mittels Signaturabgleich arbeiten, sowie unsere Skeptic™-Technologie. Das Resultat: Sie sind vor dem Diebstahl vertraulicher Informationen geschützt. Ihre Mitarbeiter werden von Suchmaschinen nicht ungewollt auf gefährliche Websites weitergeleitet. Und solche Malware-Angriffe können auch die Performance Ihres Unternehmensnetzwerks nicht mehr ausbremsen.

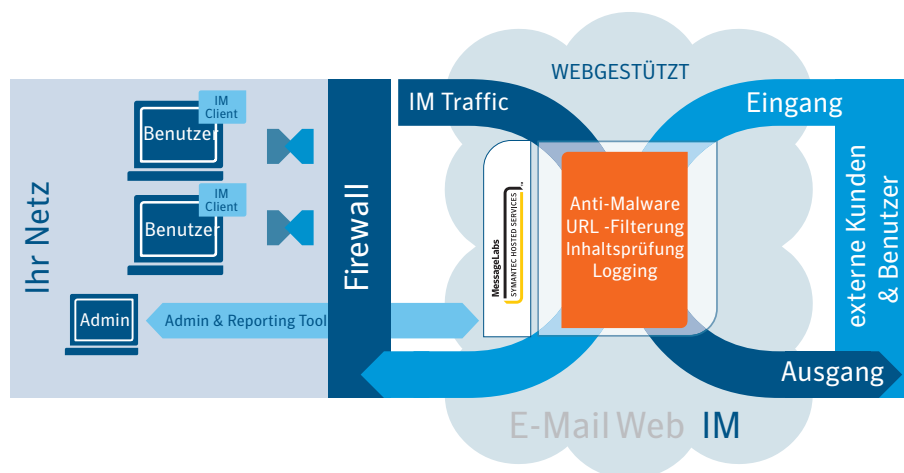


INSTANT MESSAGING

Ob Sie ein nicht-öffentliches Instant Messaging-Netzwerk benötigen oder öffentliche Instant Messaging-Programme wie Yahoo! Mail, AOL AIM oder Microsoft Live Messenger für die interne Kommunikation oder für die Kommunikation mit Kunden und Zulieferern nutzen: MessageLabs IM Services bieten die passende Lösung für Ihre Anforderungen.

- **Instant Messaging Security Service (IMSS):** Der Hosted IMSS-Service von MessageLabs bietet Unternehmen Virenschutz, URL-Filterung, Inhaltskontrolle und Kommunikationsprotokollierung. Mehrere Engines anderer Anbieter plus die MessageLabs Skeptic™-Technologie sorgen für umfassenden Virenschutz. Instant Messages und Anhänge werden nach den vom Unternehmen definierten Regeln gescannt. Sämtliche Nachrichten werden protokolliert und in einer sicheren Infrastruktur gespeichert. Alle Web-Links in den Nachrichten werden mit einer URL-Datenbank abgeglichen und auf bekannte vireninferierte Websites untersucht.
- **Enterprise Instant Messaging (EIM):** Mit dem Hosted Service für das Enterprise Instant Messaging (EIM) kommen Sie in den Genuss eines sicheren, nicht öffentlichen Netzwerks, das Ihre gesamte IM-Kommunikation zuverlässig vor dem Zugriff durch Unbefugte bewahrt.

Dabei setzen wir auf TLS-Technologien (Transport Layer Security) zur Verschlüsselung der IM-Kommunikation zwischen allen berechtigten Anwendern. Durch ein umfassendes Reporting inklusive Zugriff auf Log-Daten und Aktivitäts- und Nutzungsprotokolle sowie durch die zentrale Speicherung der Log-Files haben Sie Ihr Enterprise IM-System jederzeit im Griff. Ihre Mitarbeiter und Geschäftspartner können in Echtzeit kommunizieren, zusammenarbeiten und Informationen austauschen, ohne dass Sie sich Sorgen wegen der Sicherheitsrisiken machen müssten, die in öffentlichen IM-Systemen entstehen.



ALLES IM BLICK DURCH UMFANGREICHES REPORTING

Wie gut die MessageLabs Hosted Services funktionieren, können Sie und Ihre Mitarbeiter in der Praxis erfahren, wenn Sie spamfrei kommunizieren und ohne Angst vor Viren und anderer Malware im Internet unterwegs sein können.

Damit Sie jederzeit den Überblick über Ihre Hosted Services in der Cloud und deren Ergebnisse haben, bieten wir Ihnen umfangreiche Reportingfunktionen im ClientNet Web-Portal. Darin können Sie sich den Status sämtlicher E-Mail-, Web-, und IM-Services in grafischer Form, als Tabelle und als PDF ausgeben lassen.

www.messagelabs.de
info@messagelabs.com
Gebührenfreies Telefon, Deutschland (D,A, CH) 0800 6647453

>EUROPE

>HEADQUARTERS

1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733
Support: +44 (0) 1452 627 766

>LONDON

3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

>NETHERLANDS

WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801
Support +44 (0) 1452 627 766

>BELGIUM/LUXEMBOURG

Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

>DACH

Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94302 120
Support :+44 (0)870 850 3014

>AMERICAS

>UNITED STATES

512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

>CANADA

170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

>ASIA PACIFIC

>HONG KONG

Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

>AUSTRALIA

Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

>SINGAPORE

6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

>JAPAN

Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130



Confidence in a connected world.